REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2025/302 AL COMISIEI

din 23 octombrie 2024

de stabilire a standardelor tehnice de punere în aplicare pentru aplicarea Regulamentului (UE) 2022/2554 al Parlamentului European și al Consiliului în ceea ce privește formularele, modelele și procedurile standard pentru raportarea de către entitățile financiare a unui incident major legat de TIC și notificarea de către acestea a unei amenințări cibernetice semnificative

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere 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 ([1]), în special articolul 20 al patrulea alineat,

întrucât:

(1) Pentru a se asigura că entitățile financiare raportează incidentele majore autorităților lor competente în mod consecvent și pentru a se asigura că furnizează autorităților respective date de bună calitate, ar trebui să se specifice câmpurile de date pe care entitățile financiare trebuie să le furnizeze în diferitele etape ale raportării menționate la articolul 19 alineatul (4) din Regulamentul (UE) 2022/2554. Este important ca aceste informații să fie prezentate într-un mod care să permită o imagine de ansamblu unică asupra incidentului. Prin urmare, este necesar să se stabilească un model unic de raportare în acest scop.

(2) Entitățile financiare ar trebui să completeze câmpurile de date din modelul de raportare care corespund cerințelor de informare aferente notificării sau raportului respectiv. Cu toate acestea, entităților financiare care dețin deja informații pe care urmează să le furnizeze într-o etapă ulterioară de raportare, și anume în raportul intermediar sau în raportul final, ar trebui să li se permită să realizeze cu anticipație transmiterea datelor respective.

(3) Întrucât incidentele multiple sau recurente pot constitui un incident major, astfel cum se menționează la articolul 8 din Regulamentul delegat (UE) 2024/1772 al Comisiei ([2]), modul de concepere a modelului de raportare și a câmpurilor de date ar trebui să permită entităților financiare să raporteze astfel de incidente recurente.

(4) Pentru a asigura informații exacte și actualizate, modelul de raportare ar trebui să permită entităților financiare, atunci când transmit raportul intermediar și raportul final, să actualizeze orice informații care au fost transmise anterior și, dacă este necesar, să reclasifice incidentele majore ca nefiind majore.

(5) Identificarea juridică a entităților ar trebui să fie aliniată la identificatorii specificați în standardele tehnice de punere în aplicare adoptate în temeiul articolului 28 alineatul (9) din Regulamentul (UE) 2022/2554.

(6) În cazul în care entitățile financiare externalizează obligațiile de raportare a incidentelor majore legate de TIC către o parte terță, autoritățile competente ar trebui să aibă cunoștință de identitatea părții terțe care efectuează raportarea în numele entității financiare înainte de transmiterea primei notificări sau raportări, pentru a verifica legitimitatea părții terțe care efectuează raportarea.

([1]) JO L 333, 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) Regulamentul delegat (UE) 2024/1772 al Comisiei din 13 martie 2024 de completare a Regulamentului (UE) 2022/2554 al Parlamentului European și al Consiliului în ceea ce privește standardele tehnice de reglementare care precizează criteriile de clasificare a incidentelor legate de TIC și a amenințărilor cibernetice, stabilesc pragurile de semnificație și detaliile rapoartelor privind incidentele majore (JO L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

(7) Pentru a identifica cu ușurință impactul unui incident care a avut loc la un furnizor terț sau a fost cauzat de acesta și care afectează mai multe entități financiare dintr-un singur stat membru și pentru a reduce efortul de raportare pentru entitățile financiare, modelul de raportare ar trebui să permită transmiterea unui raport agregat care să cuprindă informații agregate cu privire la impactul incidentului asupra tuturor entităților financiare afectate care au clasificat incidentul ca fiind major.

(8) Modelul de raportare ar trebui să fie conceput într-un mod neutru din punct de vedere tehnologic pentru a permite punerea sa în aplicare în diferite soluții de raportare a incidentelor care există deja sau care pot fi dezvoltate pentru punerea în aplicare a cerințelor Regulamentului (UE) 2022/2554.

(9) Modelul de raportare și câmpurile de date ar trebui să fie concepute astfel încât să faciliteze raportarea incidentelor majore legate de TIC de către părțile terțe cărora entitățile financiare le-au externalizat obligația de raportare în conformitate cu articolul 19 alineatul (5) din Regulamentul (UE) 2022/2554.

(10) Prezentul regulament se bazează pe proiectul de standarde tehnice de punere în aplicare pe care autoritățile europene de supraveghere l-au transmis Comisiei.

(11) Autoritățile europene de supraveghere au efectuat consultări publice deschise cu privire la proiectul de standarde tehnice de punere în aplicare pe care se bazează prezentul regulament, a analizat costurile și beneficiile potențiale aferente și a solicitat avizul Grupului părților interesate din domeniul bancar, instituit în conformitate cu articolul 37 din Regulamentele (UE) nr. 1093/2010 ([3]), (UE) nr. 1094/2010 ([4]) și (UE) nr. 1095/2010 ([5]) ale Parlamentului European și al Consiliului.

(12) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([6]) și a emis un aviz favorabil la 22 iulie 2024. Orice prelucrare a datelor cu caracter personal care intră în domeniul de aplicare al prezentului regulament ar trebui să se efectueze în conformitate cu principiile și dispozițiile aplicabile în materie de protecție a datelor prevăzute în Regulamentul (UE) 2018/1725,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Modelul pentru raportarea incidentelor majore legate de TIC

(1) Entitățile financiare utilizează modelul prevăzut în anexa I pentru a transmite notificarea inițială, raportul intermediar și raportul final menționate la articolul 19 alineatul (4) din Regulamentul (UE) 2022/2554, după cum urmează:

(a) entitățile financiare care transmit o notificare inițială completează câmpurile de date din model care corespund informațiilor care trebuie furnizate în conformitate cu articolul 2 din Regulamentul delegat (UE) 2025/301 al Comisiei ([7]) și pot, în cazul în care dețin deja informațiile respective, să completeze acele câmpuri de date a căror completare nu este necesară pentru o notificare inițială, însă este necesară pentru un raport intermediar sau final;

([3]) Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea bancară europeană), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/78/CE a Comisiei (JO L 331, 15.12.2010, p. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Regulamentul (UE) nr. 1094/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea europeană de asigurări și pensii ocupaționale), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/79/CE a Comisiei (JO L 331, 15.12.2010, p. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Regulamentul (UE) nr. 1095/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea europeană pentru valori mobiliare și piețe), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/77/CE a Comisiei (JO L 331, 15.12.2010, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) Regulamentul delegat (UE) xxx/xxx al Comisiei din 23 octombrie 2024 de completare a Regulamentului (UE) 2022/2554 al Parlamentului European și al Consiliului în ceea ce privește standardele tehnice de reglementare care precizează conținutul și termenele pentru notificarea inițială privind incidentele majore legate de TIC și pentru raportul intermediar și raportul final aferente, precum și conținutul notificării voluntare privind amenințările cibernetice semnificative (JO L, 2025/301, 20.2.2025, ELI: http://data.europa.eu/eli/reg_del/2025/301/oj).

(b) entitățile financiare care transmit un raport intermediar completează câmpurile de date din model care corespund informațiilor care trebuie furnizate în conformitate cu articolul 3 din Regulamentul delegat (UE) 2025/301 și pot, în cazul în care dețin deja informațiile relevante, să completeze acele câmpuri de date a căror completare nu este necesară pentru raportul intermediar, însă este necesară pentru raportul final;

(c) entitățile financiare care transmit un raport final completează câmpurile de date din model care corespund informațiilor care trebuie furnizate în conformitate cu articolul 4 din Regulamentul delegat (UE) 2025/301.

(2) Entitățile financiare se asigură că informațiile conținute în notificarea inițială, în raportul intermediar și în raportul final sunt complete și exacte.

(3) Entitățile financiare furnizează valori estimate pe baza altor date și informații disponibile, în măsura posibilului, în cazul în care nu sunt disponibile date exacte la momentul raportării pentru notificarea inițială sau pentru raportul intermediar.

(4) Atunci când transmit un raport intermediar sau final, entitățile financiare utilizează modelul prevăzut în anexa I pentru a transmite toate informațiile necesare și pentru a actualiza, după caz, informațiile care au fost furnizate anterior în notificarea inițială sau în raportul intermediar.

(5) Entitățile financiare respectă glosarul de date și instrucțiunile prevăzute în anexa II atunci când completează modelul prevăzut în anexa I.

Articolul 2

Transmiterea simultană a notificării inițiale, a raportului intermediar și a raportului final

Entitățile financiare pot combina transmiterea notificării inițiale, a raportului intermediar și a raportului final astfel încât să furnizeze două dintre aceste documente sau toate aceste documente în același timp, în cazul în care activitățile obișnuite s-au redresat sau s-a finalizat analiza cauzelor principale și cu condiția respectării termenelor prevăzute la articolul 5 din Regulamentul delegat (UE) 2025/301.

Articolul 3

Incidente recurente legate de TIC

Entitățile financiare care furnizează informații privind incidente recurente legate de TIC care nu se încadrează în categoria incidentelor majore și care îndeplinesc cumulativ condițiile pentru a fi considerate un singur incident major legat de TIC, astfel cum sunt prevăzute la articolul 8 alineatul (2) din Regulamentul delegat (UE) 2024/1772, furnizează informațiile respective într-o formă agregată.

Articolul 4

Utilizarea unor canale electronice securizate

(1) Entitățile financiare utilizează canalele electronice securizate puse la dispoziție de autoritatea lor competentă pentru a transmite notificarea inițială, raportul intermediar și raportul final.

(2) Entitățile financiare care nu pot utiliza canalele electronice securizate puse la dispoziție de autoritatea lor competentă își informează autoritatea competentă cu privire la un incident major legat de TIC prin alte mijloace securizate, în acord cu autoritatea competentă. Dacă autoritatea competentă solicită acest lucru, entitățile financiare retransmit notificarea inițială sau raportul intermediar ori final prin intermediul canalului electronic securizat pus la dispoziție de autoritatea lor competentă de îndată ce sunt în măsură să facă acest lucru.

Articolul 5

Reclasificarea incidentelor majore legate de TIC

În cazul în care, după o evaluare suplimentară, entitatea financiară concluzionează că incidentul legat de TIC raportat anterior ca fiind major nu a îndeplinit în niciun moment criteriile și pragurile de clasificare prevăzute la articolul 8 din Regulamentul delegat (UE) 2024/1772, entitatea financiară notifică autorității competente că a reclasificat incidentul legat de TIC considerat major ca nefiind major, furnizând informații cu privire la reclasificare în modelul prevăzut în anexa II la prezentul regulament în ceea ce privește câmpurile „Tipul de raport” și „Alte informații”.

Articolul 6

Notificarea externalizării obligațiilor de raportare

(1) Entitățile financiare care au externalizat obligația de a raporta incidentele majore legate de TIC în conformitate cu articolul 19 alineatul (5) din Regulamentul (UE) 2022/2554 își informează autoritatea competentă cu privire la acordul de externalizare respectiv de îndată ce acordul de externalizare a fost încheiat și cel târziu înainte de prima notificare sau raportare.

(2) Entitățile financiare furnizează autorității competente denumirea, datele de contact și codul de identificare al părții terțe care va transmite notificările sau rapoartele privind incidentele majore legate de TIC pentru acestea.

(3) Entitățile financiare își informează autoritatea competentă de îndată ce nu mai externalizează obligațiile de raportare astfel cum se menționează la articolul 19 alineatul (5) din Regulamentul (UE) 2022/2554.

Articolul 7

Raportarea agregată

(1) Un furnizor terț de servicii căruia i-au fost externalizate obligații de raportare, astfel cum se menționează la articolul 19 alineatul (5) din Regulamentul (UE) 2022/2554, poate utiliza modelul prevăzut în anexa I la prezentul regulament pentru a furniza informații agregate cu privire la un incident major legat de TIC care afectează mai multe entități financiare într-o singură notificare sau într-un singur raport și poate transmite notificarea sau raportul respectiv autorității competente în numele tuturor entităților financiare afectate, dacă sunt îndeplinite toate condițiile următoare:

(a) incidentul major legat de TIC care trebuie raportat provine de la un furnizor terț de servicii TIC sau este cauzat de acesta;

(b) respectivul furnizor terț de servicii furnizează serviciul TIC relevant mai multor entități financiare sau unui grup;

(c) incidentul legat de TIC este clasificat ca fiind major de către fiecare entitate financiară care face obiectul notificării sau al raportului agregat;

(d) incidentul major legat de TIC afectează entitățile financiare dintr-un singur stat membru, iar raportul agregat se referă la entități financiare care sunt supravegheate de aceeași autoritate competentă;

(e) autoritățile competente au permis în mod explicit acestui tip de entități financiare să realizeze o raportare agregată.

(2) Alineatul (1) nu se aplică instituțiilor de credit care sunt considerate a avea o relevanță semnificativă, astfel cum se menționează la articolul 2 punctul 16 din Regulamentul (UE) nr. 468/2014 al Băncii Centrale Europene ([8]), operatorilor locurilor de tranzacționare și contrapărților centrale, care utilizează modelul din anexa I numai pentru a transmite notificări sau rapoarte privind incidentele majore legate de TIC în mod individual autorității lor competente.

(3) În cazul în care autoritățile competente solicită informații privind impactul individual al incidentului major legat de TIC asupra unei singure entități financiare, la cererea autorității competente, entitatea financiară transmite o notificare individuală sau un raport individual privind incidentul major legat de TIC.

([8]) Regulamentul (UE) nr. 468/2014 al Băncii Centrale Europene din 16 aprilie 2014 de instituire a cadrului de cooperare la nivelul Mecanismului unic de supraveghere între Banca Centrală Europeană și autoritățile naționale competente și cu autoritățile naționale desemnate (Regulamentul-cadru privind MUS) (BCE/2014/17) (JO L 141, 14.5.2014, p. 1, ELI: http://data.europa.eu/eli/reg/2014/468/oj).

Articolul 8

Notificarea privind amenințările cibernetice semnificative

(1) Entitățile financiare care notifică autorităților competente amenințările cibernetice semnificative în conformitate cu articolul 19 alineatul (2) din Regulamentul (UE) 2022/2554 utilizează modelul prevăzut în anexa III la prezentul regulament și urmează glosarul de date și instrucțiunile prevăzute în anexa IV la prezentul regulament.

(2) Entitățile financiare se asigură că informațiile conținute în notificarea privind amenințările cibernetice semnificative sunt complete și exacte.

Articolul 9

Intrarea în vigoare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Luxemburg, 23 octombrie 2024.

Pentru Comisie
Președinta
Ursula VON DER LEYEN

ANEXA I

MODELE PENTRU RAPORTAREA INCIDENTELOR MAJORE

Numărul câmpului	Câmpul de date	
Informații generale despre entitatea financiară		
1.1	Tipul de transmitere	
1.2	Denumirea entității care transmite raportul	
1.3	Codul de identificare al entității care transmite raportul	
1.4	Tipul de entitate financiară afectată	
1.5	Denumirea entității financiare afectate	
1.6	Codul LEI al entității financiare afectate	
1.7	Numele persoanei de contact principale	
1.8	Adresa de e-mail a persoanei de contact principale	
1.9	Numărul de telefon al persoanei de contact principale	
1.10	Numele persoanei de contact secundare	
1.11	Adresa de e-mail a persoanei de contact secundare	
1.12	Numărul de telefon al persoanei de contact secundare	
1.13	Denumirea societății-mamă de cel mai înalt rang	
1.14	Codul LEI al societății-mamă de cel mai înalt rang	
1.15	Moneda de raportare	
Conținutul notificării inițiale		
2.1	Codul de referință al incidentului atribuit de entitatea financiară	
2.2	Data și ora detectării incidentului major legat de TIC	
2.3	Data și ora clasificării incidentului legat de TIC ca fiind major	
2.4	Descrierea incidentului major legat de TIC	
2.5	Criteriile de clasificare care au declanșat raportul privind incidentul	
2.6	Praguri de semnificație pentru criteriul de clasificare „Întindere geografică”	
2.7	Descoperirea incidentului major legat de TIC	

Numărul câmpului	Câmpul de date	
2.8	Informații din care să reiasă dacă incidentul major legat de TIC provine de la un furnizor terț sau de la o altă entitate financiară	
2.9	Activarea planului de continuitate a activității, dacă este activat	
2.10	Alte informații relevante	
Conținutul raportului intermediar		
3.1	Codul de referință al incidentului furnizat de autoritatea competentă	
3.2	Data și ora producerii incidentului major legat de TIC	
3.3	Data și ora la care s-au reluat serviciile, activitățile sau operațiunile	
3.4	Numărul clienților afectați	
3.5	Procentul clienților afectați	
3.6	Numărul contrapărților financiare afectate	
3.7	Procentul contrapărților financiare afectate	
3.8	Impactul asupra clienților sau a contrapărților financiare relevante	
3.9	Numărul tranzacțiilor afectate	
3.10	Procentul tranzacțiilor afectate	
3.11	Valoarea tranzacțiilor afectate	
3.12	Informații din care să reiasă dacă cifrele sunt reale sau reprezintă estimări sau dacă nu a existat niciun impact	
3.13	Impactul asupra reputației	
3.14	Informații contextuale cu privire la impactul asupra reputației	
3.15	Durata incidentului major legat de TIC	
3.16	Perioada de indisponibilitate a serviciului	
3.17	Informații din care să reiasă dacă cifrele privind durata și perioada de indisponibilitate a serviciului sunt reale sau reprezintă estimări	
3.18	Tipurile de impact în statele membre	
3.19	Descrierea modului în care incidentul major legat de TIC are un impact în alte state membre	
3.20	Praguri de semnificație pentru criteriul de clasificare „Pierderi de date”	
3.21	Descrierea pierderilor de date	

Numărul câmpului	Câmpul de date	
3.22	Criteriul de clasificare „Servicii critice afectate”	
3.23	Tipul de incident major legat de TIC	
3.24	Alte tipuri de incidente	
3.25	Amenințări și tehnici utilizate de actorul care generează amenințarea	
3.26	Alte tipuri de tehnici	
3.27	Informații despre domeniile funcționale și procesele operaționale afectate	
3.28	Componente de infrastructură afectate care sprijină procesele operaționale	
3.29	Informații privind componentele de infrastructură afectate care sprijină procesele operaționale	
3.30	Impactul asupra intereselor financiare ale clienților	
3.31	Raportarea către alte autorități	
3.32	Precizarea „altor” autorități	
3.33	Acțiuni/măsuri temporare luate sau planificate în vederea redresării în urma incidentului	
3.34	Descrierea oricăror acțiuni și măsuri temporare luate sau planificate în vederea redresării în urma incidentului	
3.35	Indicatori de compromitere	
Conținutul raportului final		
4.1	Clasificarea de nivel înalt a cauzelor principale ale incidentului	
4.2	Clasificarea detaliată a cauzelor principale ale incidentului	
4.3	Clasificarea suplimentară a cauzelor principale ale incidentului	
4.4	Alte tipuri de cauze principale	
4.5	Informații privind cauzele principale ale incidentului	
4.6	Rezumatul modului de soluționare a incidentului	
4.7	Data și ora la care a fost contracarată cauza principală a incidentului	
4.8	Data și ora la care s-a soluționat incidentul	
4.9	Informații din care să reiasă dacă data soluționării definitive a incidentului diferă de data de punere în aplicare planificată inițial	
4.10	Evaluarea riscului pentru funcțiile critice în scopul rezoluției	
4.11	Informații relevante pentru autoritățile de rezoluție	

Numărul câmpului	Câmpul de date	
4.12	Pragul de semnificație pentru criteriul de clasificare „Impactul economic”	
4.13	Cuantumul costurilor și pierderilor directe și indirecte brute	
4.14	Cuantumul recuperărilor financiare	
4.15	Informații din care să reiasă dacă incidentele care nu se încadrează în categoria incidentelor majore au fost recurente	
4.16	Data și ora producerii incidentelor recurente	

ANEXA II

GLOSAR DE DATE ȘI INSTRUCȚIUNI PENTRU RAPORTAREA INCIDENTELOR MAJORE

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
Informații generale despre entitatea financiară					
1.1. Tipul de transmitere	A se indica tipul de notificare sau de raport privind incidentul transmis autorității competente	Da	Da	Da	Opțiuni: — notificare inițială — raport intermediar — raport final — incident major reclasificat ca nefiind major
1.2. Denumirea entității care transmite raportul	Denumirea juridică completă a entității care transmite raportul	Da	Da	Da	Alfanumeric
1.3. Codul de identificare al entității care transmite raportul	Codul de identificare al entității care transmite raportul În cazul în care entitățile financiare transmit notificarea/raportul, codul de identificare este un identificator al entității juridice (LEI), care este un cod unic format din 20 de caractere alfanumerice, bazat pe ISO 17442-1:2020. Un furnizor terț care transmite un raport pentru o entitate financiară poate utiliza un cod de identificare, astfel cum se specifică în standardele tehnice de punere în aplicare adoptate în temeiul articolului 28 alineatul (9) din Regulamentul (UE) 2022/2554.	Da	Da	Da	Alfanumeric
1.4. Tipul de entitate financiară afectată	Tipul de entitate menționată la articolul 2 alineatul (1) literele (a)-(t) din Regulamentul (UE) 2022/2554 pentru care se transmite raportul. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, se vor selecta diferitele tipuri de entități financiare vizate de raportul agregat.	Da	Da	Da	Opțiuni (cu posibilitate de selecție multiplă): — instituție de credit; — instituție de plată; — instituție de plată exceptată; — prestator de servicii de informare cu privire la conturi; — instituție emitentă de monedă electronică; — instituție emitentă de monedă electronică exceptată; — firmă de investiții; — prestator de servicii de criptoactive; — emitent de tokenuri raportate la active; — depozitar central de titluri de valoare; — contraparte centrală; — loc de tranzacționare; — registru central de tranzacții;

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
					— administrator de fonduri de investiții alternative; — societate de administrare; — furnizor de servicii de raportare a datelor; — întreprindere de asigurare și de reasigurare; — intermediar de asigurări, intermediar de reasigurări și intermediar de asigurări auxiliare; — instituție pentru furnizarea de pensii ocupaționale; — agenție de rating de credit; — administrator de indici de referință critici; — furnizor de servicii de finanțare participativă; — registru central de securitizări.
1.5. Denumirea entității financiare afectate	Denumirea juridică completă a entității financiare afectate de incidentul major legat de TIC care are obligația de a raporta incidentul major autorității sale competente în temeiul articolului 19 din Regulamentul (UE) 2022/2554. În cazul raportării agregate: (a) lista tuturor denumirilor entităților financiare afectate de incidentul major legat de TIC, separate prin punct și virgulă; (b) enumerarea de către furnizorul terț care transmite o notificare sau un raport privind un incident major sau în mod agregat, astfel cum se menționează la articolul 7 din prezentul regulament, a denumirilor tuturor entităților financiare afectate de incident, separate prin punct și virgulă.	Da, dacă entitatea financiară afectată de incident este diferită de entitatea care transmite raportul și în cazul raportării agregate	Da, dacă entitatea financiară afectată de incident este diferită de entitatea care transmite raportul și în cazul raportării agregate	Da, dacă entitatea financiară afectată de incident este diferită de entitatea care transmite raportul și în cazul raportării agregate	Alfanumeric
1.6. Codul LEI al entității financiare afectate	Identificatorul entității juridice (LEI) al entității financiare afectate de incidentul major legat de TIC, atribuit potrivit Organizației Internaționale de Standardizare. În cazul raportării agregate: (a) o listă a tuturor codurilor LEI ale entităților financiare afectate de incidentul major legat de TIC, separate prin punct și virgulă;	Da, dacă entitatea financiară afectată de incidentul major legat de TIC este	Da, dacă entitatea financiară afectată de incidentul major legat de TIC este diferită de entitatea care	Da, dacă entitatea financiară afectată de incidentul major legat de TIC este diferită	Cod unic format din 20 de caractere alfanumerice, bazat pe ISO 17442-1:2020

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
	(b) enumerarea de către furnizorul terț care transmite o notificare sau un raport privind un incident major sau în mod agregat, astfel cum se menționează la articolul 7 din prezentul regulament, a codurilor LEI ale tuturor entităților financiare afectate de incident, separate prin punct și virgulă. Ordinea de prezentare a codurilor LEI și a denumirilor entităților financiare trebuie să fie identică.	diferită de entitatea care transmite raportul și în cazul raportării agregate	transmite raportul și în cazul raportării agregate	de entitatea care transmite raportul și în cazul raportării agregate	
1.7. Numele persoanei de contact principale	Prenumele și numele persoanei de contact principale a entității financiare În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, a se indica numele persoanei de contact principale a entității care transmite raportul agregat.	Da	Da	Da	Alfanumeric
1.8. Adresa de e-mail a persoanei de contact principale	Adresa de e-mail a persoanei de contact principale care poate fi utilizată de autoritatea competentă pentru comunicarea ulterioară. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, a se indica adresa de e-mail a persoanei de contact principale a entității care transmite raportul agregat.	Da	Da	Da	Alfanumeric
1.9. Numărul de telefon al persoanei de contact principale	Numărul de telefon al persoanei de contact principale care poate fi utilizat de autoritatea competentă pentru comunicarea ulterioară. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, a se indica numărul de telefon al persoanei de contact principale a entității care transmite raportul agregat. Numărul de telefon se raportează cu toate prefixele internaționale (de exemplu, +33XXXXXXXXX).	Da	Da	Da	Alfanumeric
1.10. Numele persoanei de contact secundare	Prenumele și numele persoanei de contact secundare sau numele echipei responsabile a entității financiare sau a unei entități care transmite raportul în numele entității financiare	Da	Da	Da	Alfanumeric
1.11. Adresa de e-mail a persoanei de contact secundare	Adresa de e-mail a persoanei de contact secundare sau o adresă de e-mail funcțională a echipei care poate fi utilizată de autoritatea competentă pentru comunicarea ulterioară.	Da	Da	Da	Alfanumeric

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
1.12. Numărul de telefon al persoanei de contact secundare	Numărul de telefon al persoanei de contact secundare sau al unei echipe care poate fi utilizat de autoritatea competentă pentru comunicarea ulterioară. Numărul de telefon se raportează cu toate prefixele internaționale (de exemplu, +33XXXXXXXXX).	Da	Da	Da	Alfanumeric
1.13. Denumirea societății-mamă de cel mai înalt rang	Denumirea societății-mamă de cel mai înalt rang a grupului din care face parte entitatea financiară afectată, după caz	Da, dacă entitatea financiară aparține unui grup	Da, dacă entitatea financiară aparține unui grup	Da, dacă entitatea financiară aparține unui grup	Alfanumeric
1.14. Codul LEI al societății-mamă de cel mai înalt rang	Codul LEI al societății-mamă de cel mai înalt rang a grupului din care face parte entitatea financiară afectată, după caz – atribuit potrivit Organizației Internaționale de Standardizare	Da, dacă entitatea financiară aparține unui grup	Da, dacă entitatea financiară aparține unui grup	Da, dacă entitatea financiară aparține unui grup	Cod unic format din 20 de caractere alfanumerice, bazat pe ISO 17442-1:2020
1.15. Moneda de raportare	Moneda utilizată pentru raportarea incidentelor	Da	Da	Da	Opțiune completată utilizând codurile monedelor ISO 4217
Conținutul notificării inițiale					
2.1. Codul de referință al incidentului atribuit de entitatea financiară	Codul unic de referință emis de entitatea financiară, care identifică fără echivoc incidentul major legat de TIC În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, a se indica respectivul cod de referință al incidentului atribuit de furnizorul terț.	Da	Da	Da	Alfanumeric
2.2. Data și ora detectării incidentului legat de TIC	Data și ora la care entitatea financiară a luat cunoștință de incidentul legat de TIC Pentru incidentele recurente, a se indica data și ora la care a fost detectat ultimul incident legat de TIC.	Da	Da	Da	Standardul ISO 8601 UTC (AAAA-LL-ZZ Thh:mm:ss)

	Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
2.3.	Data și ora clasificării incidentului ca fiind major	Data și ora la care incidentul legat de TIC a fost clasificat ca fiind major în conformitate cu criteriile de clasificare stabilite în Regulamentul delegat (UE) 2024/1772.	Da	Da	Da	Standardul ISO 8601 UTC (AAAA-LL-ZZ Thh:mm:ss)
2.4.	Descrierea incidentului legat de TIC	Descrierea celor mai relevante aspecte ale incidentului major legat de TIC Entitățile financiare furnizează o imagine de ansamblu de nivel înalt a următoarelor informații, cum ar fi cauzele posibile, efectele imediate, sistemele afectate și altele. Entitățile financiare includ, în cazul în care aceste aspecte sunt cunoscute sau preconizate în mod rezonabil, informații din care să reiasă dacă incidentul afectează furnizorii terți sau alte entități financiare, tipul de furnizor sau de entitate financiară, denumirea acestora, codurile de identificare ale acestora și tipul codului de identificare (de exemplu, LEI sau EUID). În rapoartele ulterioare, conținutul câmpului poate evolua în timp pentru a reflecta înțelegerea continuă a incidentului legat de TIC și pentru a descrie orice alte informații relevante cu privire la incidentul legat de TIC care nu sunt incluse în câmpurile de date, inclusiv evaluarea internă a gravității efectuată de entitatea financiară (de exemplu, foarte scăzută, scăzută, medie, ridicată, foarte ridicată) și o mențiune cu privire la nivelul și denumirea celor mai importante structuri de decizie care au fost implicate în răspunsul la incidentul legat de TIC.	Da	Da	Da	Alfanumeric
2.5.	Criteriile de clasificare care au declanșat raportul privind incidentul	Criteriile de clasificare în temeiul Regulamentului delegat (UE) 2024/1772 care au determinat încadrarea incidentului legat de TIC drept incident major și notificarea și raportarea ulterioare. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, a se indica criteriile de clasificare care au determinat încadrarea incidentului legat de TIC drept incident major pentru cel puțin una sau mai multe entități financiare.	Da	Da	Da	Opțiuni (multiple): — clienți, contrapărți financiare și tranzacții afectate; — impactul asupra reputației; — durata incidentului și perioada de indisponibilitate a serviciului; — întinderea geografică; — pierderile de date; — serviciile critice afectate; — impactul economic.
2.6.	Praguri de semnificație pentru criteriul de clasificare „Întindere geografică”	Statele membre ale SEE afectate de incidentul major legat de TIC Atunci când evaluează impactul incidentului major legat de TIC în alte state membre, entitățile financiare țin seama de articolele 4 și 12 din Regulamentul delegat (UE) 2024/1772	Da, dacă este atins pragul de „întindere geografică”	Da, dacă este atins pragul de „întindere geografică”	Da, dacă este atins pragul de „întindere geografică”	Opțiuni (multiple) completate utilizând standardul ISO 3166 ALPHA-2 pentru țările afectate

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
2.7. Descoperirea incidentului major legat de TIC	Indicarea modului în care a fost descoperit incidentul major legat de TIC	Da	Da	Da	Opțiuni: — securitatea informatică; — personalul; — auditul intern; — auditurile externe; — clienții; — contrapărțile financiare; — un furnizor terț; — atacatorul; — sistemele de monitorizare; — o autoritate/o agenție/un organism de aplicare a legii; — altele.
2.8. Informații din care să reiasă dacă incidentul provine de la un furnizor terț sau de la o altă entitate financiară	Informații din care să reiasă dacă incidentul major legat de TIC provine de la un furnizor terț sau de la o altă entitate financiară. Entitățile financiare indică dacă incidentul major legat de TIC provine de la un furnizor terț sau de la o altă entitate financiară (inclusiv de la entități financiare care aparțin aceluiași grup precum entitatea raportoare), precum și denumirea, codul de identificare al furnizorului terț sau al entității financiare și tipul codului de identificare (de exemplu, LEI sau EUID).	Da, dacă incidentul provine de la un furnizor terț sau de la o altă entitate financiară	Da, dacă incidentul provine de la un furnizor terț sau de la o altă entitate financiară	Da, dacă incidentul provine de la un furnizor terț sau de la o altă entitate financiară	Alfanumeric
2.9. Activarea planului de continuitate a activității, dacă este activat	Informații din care să reiasă dacă a existat o activare oficială a măsurilor de răspuns privind continuitatea activității ale entității financiare.	Da	Da	Da	Boolean (Da sau Nu)
2.10. Alte informații relevante	Orice alte informații care nu sunt incluse în model Entitățile financiare care au reclasificat un incident major legat de TIC ca nefiind major descriu motivele pentru care incidentul legat de TIC nu îndeplinește și nu se preconizează că va îndeplini criteriile pentru a fi considerat incident major legat de TIC.	Da, dacă există alte informații care nu sunt incluse în model sau	Da, dacă există alte informații care nu sunt incluse în model sau dacă	Da, dacă există alte informații care nu sunt incluse în model	Alfanumeric

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
		dacă incidentul major legat de TIC a fost reclasificat ca nefiind major	incidentul major legat de TIC a fost reclasificat ca nefiind major	sau dacă incidentul major legat de TIC a fost reclasificat ca nefiind major	
Conținutul raportului intermediar					
3.1. Codul de referință al incidentului furnizat de autoritatea competentă	Codul unic de referință atribuit de autoritatea competentă în momentul primirii notificării inițiale pentru a identifica fără echivoc incidentul major legat de TIC.	Nu	Da, dacă este cazul	Da, dacă este cazul	Alfanumeric
3.2. Data și ora producerii incidentului	Data și ora la care a avut loc incidentul major legat de TIC, dacă diferă de momentul la care entitatea financiară a luat cunoștință de incidentul major legat de TIC. Pentru incidentele majore recurente legate de TIC, a se indica data și ora la care a avut loc ultimul incident major legat de TIC.	Nu	Da	Da	Standardul ISO 8601 UTC (AAAA-LL-ZZ Thh:mm:ss)
3.3. Data și ora la care s-au reluat serviciile, activitățile sau operațiunile	Informații privind data și ora reluării serviciilor, a activităților sau a operațiunilor afectate de incidentul major legat de TIC.	Nu	Da, dacă câmpul de date 3.16. „Perioada de indisponibilitate a serviciului” a fost completată	Da, dacă câmpul de date 3.16. „Perioada de indisponibilitate a serviciului” a fost completată	Standardul ISO 8601 UTC (AAAA-LL-ZZ Thh:mm:ss)
3.4. Numărul clienților afectați	Numărul clienților afectați de incidentul major legat de TIC care utilizează serviciul furnizat de entitatea financiară Atunci când evaluează numărul clienților afectați, entitățile financiare țin seama, în evaluarea lor, de articolul 1 alineatul (1) și de articolul 9 alineatul (1) litera (b) din Regulamentul delegat (UE) 2024/1772. O entitate financiară care nu poate determina numărul real al clienților afectați utilizează estimări bazate pe datele disponibile din perioade de referință comparabile. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, a se indica numărul total al clienților afectați la nivelul tuturor entităților financiare.	Nu	Da	Da	Număr întreg

Câmpul de date		Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
3.5.	Procentul clienților afectați	Procentul clienților afectați de incidentul major legat de TIC în raport cu numărul total al clienților care utilizează serviciul afectat furnizat de entitatea financiară În cazul în care sunt afectate mai multe servicii, serviciile se furnizează în mod agregat. Entitățile financiare țin seama, în evaluarea lor, de articolul 1 alineatul (1) și de articolul 9 alineatul (1) litera (a) din Regulamentul delegat (UE) 2024/1772. O entitate financiară care nu poate determina procentul real al clienților afectați utilizează estimări bazate pe datele disponibile din perioade de referință comparabile. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, o entitate financiară împarte suma tuturor clienților afectați la numărul total al clienților tuturor entităților financiare afectate.	Nu	Da	Da	Dacă valoarea este exprimată în procente – orice valoare de maximum cinci caractere numerice, inclusiv maximum o zecimală, exprimată în procente (de exemplu, 2,4 în loc de 2,4 %). Dacă are peste o zecimală, valoarea trebuie rotunjită în sus de contrapărțile care efectuează raportarea.
3.6.	Numărul contrapărților financiare afectate	Numărul contrapărților financiare afectate de incidentul major legat de TIC care au încheiat un contract cu entitatea financiară. Atunci când evaluează numărul contrapărților financiare afectate, entitățile financiare țin seama, în evaluarea lor, de articolul 1 alineatul (2) din Regulamentul delegat (UE) 2024/1772. O entitate financiară care nu poate determina numărul real al contrapărților financiare afectate utilizează estimări bazate pe datele disponibile din perioade de referință comparabile. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, a se indica numărul total al contrapărților financiare afectate la nivelul tuturor entităților financiare.	Nu	Da	Da	Număr întreg

	Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
3.7.	Procentul contrapărților financiare afectate	Procentul contrapărților financiare afectate de incidentul major legat de TIC în raport cu numărul total al contrapărților financiare care au încheiat un contract cu entitatea financiară. Atunci când evaluează procentul contrapărților financiare afectate, entitățile financiare țin seama, în evaluarea lor, de articolul 1 alineatul (1) și de articolul 9 alineatul (1) litera (c) din Regulamentul delegat (UE) 2024/1772. O entitate financiară care nu poate determina procentul real al contrapărților financiare afectate utilizează estimări bazate pe datele disponibile din perioade de referință comparabile. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, a se indica suma tuturor contrapărților financiare afectate împărțită la numărul total al contrapărților financiare ale tuturor entităților financiare afectate.	Nu	Da	Da	Dacă valoarea este exprimată în procente – orice valoare de maximum cinci caractere numerice, inclusiv maximum o zecimală, exprimată în procente (de exemplu, 2,4 în loc de 2,4 %). Dacă are peste o zecimală, valoarea trebuie rotunjită în sus de contrapărțile care efectuează raportarea.
3.8.	Impactul asupra clienților sau a contrapărților financiare relevante	Orice impact identificat asupra clienților sau asupra contrapărților financiare relevante, astfel cum se menționează la articolul 1 alineatul (3) și la articolul 9 alineatul (1) litera (f) din Regulamentul delegat (UE) 2024/1772.	Nu	Da, dacă este atins pragul „Relevanța clienților și a contrapărților financiare”	Da, dacă este atins pragul „Relevanța clienților și a contrapărților financiare”	Boolean (Da sau Nu)
3.9.	Numărul tranzacțiilor afectate	Numărul tranzacțiilor afectate de incidentul major legat de TIC Atunci când evaluează impactul asupra tranzacțiilor, entitățile financiare țin seama de articolul 1 alineatul (4) din Regulamentul delegat (UE) 2024/1772, inclusiv de toate tranzacțiile interne și transfrontaliere afectate care implică o valoare monetară și în care cel puțin o parte a tranzacției se desfășoară în Uniune.	Nu	Da, dacă o tranzacție a fost afectată de incident.	Da, dacă o tranzacție a fost afectată de incident.	Număr întreg

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
	O entitate financiară care nu poate determina numărul real al tranzacțiilor afectate utilizează estimări bazate pe datele disponibile din perioade de referință comparabile. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, a se indica numărul total al tranzacțiilor afectate la nivelul tuturor entităților financiare.				
3.10. Procentul tranzacțiilor afectate	Procentul tranzacțiilor afectate în raport cu numărul mediu zilnic de tranzacții interne și transfrontaliere efectuate de entitatea financiară în legătură cu serviciul afectat. Entitățile financiare țin seama de articolul 1 alineatul (4) și de articolul 9 alineatul (1) litera (d) din Regulamentul delegat (UE) 2024/1772. O entitate financiară care nu poate determina procentul real al tranzacțiilor afectate utilizează estimări. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, o entitate financiară însumează numărul tuturor tranzacțiilor afectate și împarte suma la numărul total al tranzacțiilor tuturor entităților financiare afectate.	Nu	Da, dacă o tranzacție a fost afectată de incident.	Da, dacă o tranzacție a fost afectată de incident.	Dacă valoarea este exprimată în procente – orice valoare de maximum cinci caractere numerice, inclusiv maximum o zecimală, exprimată în procente (de exemplu, 2,4 în loc de 2,4 %). Dacă are peste o zecimală, valoarea trebuie rotunjită în sus de contrapărțile care efectuează raportarea.
3.11. Valoarea tranzacțiilor afectate	Valoarea totală a tranzacțiilor afectate de incidentul major legat de TIC se evaluează în conformitate cu articolul 1 alineatul (4) și cu articolul 9 alineatul (1) litera (e) din Regulamentul delegat (UE) 2024/1772. O entitate financiară care nu poate determina valoarea reală a tranzacțiilor afectate utilizează estimări bazate pe datele disponibile din perioade de referință comparabile. O entitate financiară raportează valoarea monetară ca valoare pozitivă. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, a se indica valoarea totală a tranzacțiilor afectate la nivelul tuturor entităților financiare.	Nu	Da, dacă tranzacțiile au fost afectate de incident.	Da, dacă o tranzacție a fost afectată de incident.	Monetar Entitățile financiare raportează punctul de date în unități, cu o precizie minimă echivalentă cu miile de unități (de exemplu, 2,5 în loc de 2 500 EUR).

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
3.12. Informații din care să reiasă dacă cifrele sunt reale sau reprezintă estimări sau dacă nu a existat niciun impact	Informații din care să reiasă dacă valorile raportate în câmpurile de date 3.4-3.11 sunt reale sau reprezintă estimări sau dacă nu a existat niciun impact.	Nu	Da	Da	Opțiuni (multiple): — cifre reale privind clienții afectați; — cifre reale privind contrapărțile financiare afectate; — cifre reale privind tranzacțiile afectate; — estimări privind clienții afectați; — estimări privind contrapărțile financiare afectate; — estimări privind tranzacțiile afectate; — niciun impact asupra clienților; — niciun impact asupra contrapărților financiare; — niciun impact asupra tranzacțiilor.
3.13. Impactul asupra reputației	Informații privind impactul asupra reputației care rezultă din incidentul major legat de TIC, astfel cum se menționează la articolele 2 și 10 din Regulamentul delegat (UE) 2024/1772. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, a se indica respectivele categorii de impact asupra reputației care se aplică cel puțin unei entități financiare.	Nu	Da, dacă este îndeplinit criteriul „Impactul asupra reputației”	Da, dacă este îndeplinit criteriul „Impactul asupra reputației”	Opțiuni (multiple): — incidentul major legat de TIC a fost reflectat în mass-media; — incidentul major legat de TIC a dus la formularea unor plângeri repetitive din partea unor clienți diferiți sau a unor contrapărți financiare diferite cu privire la serviciile care presupun contact direct cu clienții sau la relații de afaceri critice; — entitatea financiară nu va fi în măsură sau este probabil că nu va fi în măsură să îndeplinească cerințele reglementare ca urmare a incidentului major legat de TIC; — entitatea financiară va pierde sau este probabil că va pierde clienți sau contrapărți financiare, ceea ce va avea un impact semnificativ asupra activității sale ca urmare a incidentului major legat de TIC.
3.14. Informații contextuale cu privire la impactul asupra reputației	Informații care descriu modul în care incidentul major legat de TIC a afectat sau ar putea afecta reputația entității financiare, inclusiv încălcări ale legislației, cerințe de reglementare neîndeplinite, numărul de plângeri ale clienților și altele.	Nu	Da, dacă este îndeplinit criteriul „Impactul asupra reputației”	Da, dacă este îndeplinit criteriul „Impactul asupra reputației”	Alfanumeric

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
	Informațiile contextuale includ tipul de mass-media (de exemplu, mass-media tradițională și digitală, bloguri, platforme de streaming) și acoperirea mediatică, inclusiv nivelul de acoperire mediatică (local, național, internațional). În acest context, acoperirea mediatică nu înseamnă câteva comentarii negative din partea urmăritorilor sau a utilizatorilor rețelelor sociale. Entitatea financiară indică, de asemenea, dacă acoperirea mediatică a evidențiat riscuri semnificative pentru clienții săi în legătură cu incidentul major legat de TIC, inclusiv riscul de insolvență a entității financiare sau riscul de pierdere a fondurilor. Entitățile financiare indică, de asemenea, dacă au furnizat informații mass-mediei care au servit la informarea fiabilă a publicului cu privire la incidentul major legat de TIC și la consecințele acestuia. Entitățile financiare pot indica, de asemenea, dacă au existat informații false în mass-media în legătură cu incidentul legat de TIC, inclusiv informații bazate pe dezinformare deliberată răspândite de actorii care generează amenințări sau informații care au legătură cu site-ul web al entității financiare sau care ilustrează vandalizarea acestuia.				
3.15. Durata incidentului	Entitățile financiare măsoară durata incidentului major legat de TIC din momentul în care a survenit incidentul major legat de TIC până în momentul în care incidentul a fost soluționat. Entitățile financiare care nu sunt în măsură să stabilească momentul în care a survenit incidentul major legat de TIC măsoară durata incidentului major legat de TIC din momentul în care entitatea financiară a detectat incidentul sau din momentul în care entitatea financiară a înregistrat incidentul în jurnalele de rețea sau de sistem sau în alte surse de date, în funcție de care dintre aceste momente a intervenit mai devreme. Entitățile financiare care nu cunosc încă momentul în care va fi soluționat incidentul major legat de TIC aplică estimări. Valoarea se exprimă în zile, ore și minute. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, entitățile financiare măsoară cea mai lungă durată a incidentului major legat de TIC dacă există diferențe între entitățile financiare.	Nu	Da	Da	ZZ: HH: MM

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
3.16. Perioada de indisponibilitate a serviciului	Perioada de indisponibilitate a serviciului măsurată din momentul în care serviciul este total sau parțial indisponibil pentru clienți, pentru contrapărțile financiare sau pentru alți utilizatori interni sau externi până în momentul în care activitățile sau operațiunile obișnuite au fost readuse la nivelul serviciului care a fost furnizat înainte de incident. În cazul în care perioada de indisponibilitate a serviciului cauzează o întârziere în furnizarea serviciului după restabilirea activităților sau a operațiunilor obișnuite, entitățile financiare măsoară perioada de indisponibilitate de la începutul incidentului major legat de TIC până în momentul în care serviciul întârziat este furnizat. Entitățile financiare care nu sunt în măsură să stabilească momentul în care a început perioada de indisponibilitate a serviciului măsoară perioada de indisponibilitate a serviciului din momentul în care incidentul a fost detectat sau din momentul în care acesta a fost înregistrat, în funcție de care dintre aceste momente a intervenit mai devreme. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, entitățile financiare măsoară cea mai lungă durată a perioadei de indisponibilitate a serviciului dacă există diferențe între entitățile financiare.	Nu	Da, dacă incidentul a cauzat o perioadă de indisponibilitate a serviciului	Da, dacă incidentul a cauzat o perioadă de indisponibilitate a serviciului	ZZ: HH: MM
3.17. Informații din care să reiasă dacă cifrele privind durata și perioada de indisponibilitate a serviciului sunt reale sau reprezintă estimări.	Informații din care să reiasă dacă valorile raportate în câmpurile de date 3.15 și 3.16 sunt reale sau reprezintă estimări.	Nu	Da, dacă este îndeplinit criteriul „Durata și perioada de indisponibilitate a serviciului”	Da, dacă este îndeplinit criteriul „Durata și perioada de indisponibilitate a serviciului”	Opțiuni: — cifre reale; — estimări; — cifre reale și estimări; — informații indisponibile.
3.18. Tipurile de impact în statele membre	Tipul de impact în statele membre ale SEE respective Se indică dacă incidentul major legat de TIC a avut un impact în alte state membre ale SEE (altele decât statul membru al autorității competente căreia i se raportează direct incidentul), în conformitate cu articolul 4 din Regulamentul delegat (UE) 2024/1772, în special în ceea ce privește importanța impactului în legătură cu: (a) clienții și contrapărțile financiare afectate din alte state membre; sau	Nu	Da, dacă este atins pragul de „întindere geografică”	Da, dacă este atins pragul de „întindere geografică”	Opțiuni (multiple): — clienții; — contrapărțile financiare; — sucursala entității financiare; — entitățile financiare din cadrul grupului care desfășoară activități în statul membru respectiv; — infrastructura pieței financiare; — furnizorii terți care pot fi comuni cu alte entități financiare.

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
	(b) sucursalele sau alte entități financiare din cadrul grupului care desfășoară activități în alte state membre; sau (c) infrastructurile pieței financiare sau furnizorii terți, care pot afecta entitățile financiare din alte state membre cărora le furnizează servicii.				
3.19. Descrierea modului în care incidentul are un impact în alte state membre	Descrierea impactului și a gravității incidentului major legat de TIC în fiecare stat membru afectat, inclusiv o evaluare a impactului și a gravității cu privire la: (a) clienți; (b) contrapărțile financiare; (c) sucursalele entității financiare; (d) alte entități financiare din cadrul grupului care desfășoară activități în statul membru respectiv; (e) infrastructurile piețelor financiare; (f) furnizorii terți care pot fi comuni cu alte entități financiare, după caz, în alt stat membru (alte state membre).	Nu	Da, dacă este atins pragul de „întindere geografică”	Da, dacă este atins pragul de „întindere geografică”	Alfanumeric
3.20. Praguri de semnificație pentru criteriul de clasificare „Pierderi de date”	Tipul de pierderi de date pe care le implică incidentul major legat de TIC în ceea ce privește disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor. Entitățile financiare țin seama, în evaluarea lor, de articolele 5 și 13 din Regulamentul delegat (UE) 2024/1772. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, a se indica pierderile de date care afectează cel puțin o entitate financiară.	Nu	Da, dacă este îndeplinit criteriul „Pierderi de date”	Da, dacă este îndeplinit criteriul „Pierderi de date”	Opțiuni (multiple): — disponibilitatea; — autenticitatea; — integritatea; — confidențialitatea.
3.21. Descrierea pierderilor de date	Descrierea impactului incidentului major legat de TIC asupra disponibilității, a autenticității, a integrității și a confidențialității datelor critice, în conformitate cu articolele 5 și 13 din Regulamentul delegat (UE) 2024/1772. Informații privind impactul asupra punerii în aplicare a obiectivelor de activitate ale entității financiare sau asupra îndeplinirii cerințelor reglementare. În cadrul informațiilor furnizate, entitățile financiare indică dacă datele afectate sunt date privind clienții, date ale altor entități (de exemplu, ale contrapărților financiare) sau date ale entității financiare înseși.	Nu	Da, dacă este îndeplinit criteriul „Pierderi de date”	Da, dacă este îndeplinit criteriul „Pierderi de date”	Alfanumeric

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
	Entitatea financiară poate indica, de asemenea, tipul de date implicate în incident – în special dacă datele sunt confidențiale și ce tip de confidențialitate a fost implicată (de exemplu, confidențialitatea comercială/de afaceri, date cu caracter personal, secretul profesional: secretul bancar, secretul în domeniul asigurărilor, secretul serviciilor de plată etc.). Informațiile pot include, de asemenea, posibilele riscuri asociate pierderilor de date, cum ar fi dacă datele afectate de incident pot fi utilizate pentru a identifica persoane și dacă acestea ar putea fi utilizate de către actorul care generează amenințarea pentru a obține credite sau împrumuturi fără consimțământul lor, pentru a desfășura atacuri de spear-phishing sau pentru a face publice informații. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, a se indica o descriere generală a impactului incidentului asupra entităților financiare afectate. În cazul în care există diferențe în ceea ce privește impactul, descrierea impactului indică în mod clar impactul specific asupra diferitelor entități financiare.				
3.22. Criteriul de clasificare „Servicii critice afectate”	Informații referitoare la criteriul „Servicii critice afectate” Entitățile financiare țin seama, în evaluarea lor, de articolul 6 din Regulamentul delegat (UE) 2024/1772, inclusiv de informații cu privire la: — serviciile sau activitățile afectate care necesită autorizare, înregistrare sau care sunt supravegheate de autoritățile competente; sau — serviciile TIC sau rețelele și sistemele informatice care sprijină funcții critice sau importante ale entității financiare; și — natura accesului rău-intenționat și neautorizat la rețeaua și la sistemele informatice ale entității financiare. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, a se indica impactul asupra serviciilor critice care se aplică cel puțin unei entități financiare.	Nu	Da	Da	Alfanumeric

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
3.23. Tipul de incident	Clasificarea incidentelor în funcție de tipul acestora	Nu	Da	Da	Opțiuni (multiple): — incident legat de securitatea cibernetică; — disfuncționalitate a procesului; — disfuncționalitate a sistemului; — eveniment extern; — incident legat de plăți; — altele (a se preciza).
3.24. Alte tipuri de incidente	Alte tipuri de incidente legate de TIC: entitățile financiare care au selectat opțiunea „altele” în legătură cu tipurile de incidente în câmpul de date 3.23 specifică tipul de incident legat de TIC.	Nu	Da, dacă în câmpul de date 3.23 s-a selectat opțiunea „altele” în legătură cu tipurile de incidente	Da, dacă în câmpul de date 3.23 s-a selectat opțiunea „altele” în legătură cu tipurile de incidente	Alfanumeric
3.25. Amenințări și tehnici utilizate de actorul care generează amenințarea	A se indica amenințările și tehnicile utilizate de actorul care generează amenințarea, inclusiv: (a) ingineria socială, inclusiv phishing-ul; (b) atacuri (D)DoS; (c) furtul de identitate; (d) criptarea datelor pentru impact, inclusiv ransomware; (e) deturnarea resurselor; (f) exfiltrarea și manipularea datelor, exclusiv furtul de identitate; (g) distrugerea datelor; (h) vandalizarea; (i) atacuri asupra lanțului de aprovizionare; (j) altele (a se preciza).	Nu	Da, dacă tipul de incident legat de TIC din câmpul 3.23 este un „incident legat de securitatea cibernetică”	Da, dacă tipul de incident legat de TIC din câmpul 3.23 este un „incident legat de securitatea cibernetică”	Opțiuni (multiple): — ingineria socială, inclusiv phishing-ul; — atacuri (D)DoS; — furtul de identitate; — criptarea datelor pentru impact, inclusiv ransomware; — deturnarea resurselor; — exfiltrarea și manipularea datelor, exclusiv furtul de identitate; — distrugerea datelor; — vandalizarea; — atacuri asupra lanțului de aprovizionare; — altele (a se preciza).
3.26. Alte tipuri de tehnici	Alte tipuri de tehnici Entitățile financiare care au selectat opțiunea „altele” în legătură cu tipurile de tehnici în câmpul de date 3.25 specifică tipul de tehnică.	Nu	Da, dacă în câmpul de date 3.25 s-a selectat opțiunea „altele” în legătură cu tipurile de tehnici	Da, dacă în câmpul de date 3.25 s-a selectat opțiunea „altele” în legătură cu tipurile de tehnici	Alfanumeric

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
3.27. Informații despre domeniile funcționale și procesele operaționale afectate	Indicarea domeniilor funcționale și a proceselor operaționale care sunt afectate de incident, inclusiv a produselor și a serviciilor Domeniile funcționale includ, fără a se limita la: (a) marketing și dezvoltarea afacerilor; (b) serviciul pentru clienți; (c) managementul produselor; (d) conformitatea cu reglementările; (e) gestionarea riscurilor; (f) finanțe și contabilitate; (g) resurse umane și servicii generale; (h) tehnologia informației. Procesele operaționale includ, dar nu se limitează la: — furnizarea de servicii de informare cu privire la conturi; — servicii de actuariat; — acceptarea de operațiuni de plată; — autentificare/autorizare; — autoritate; — integrarea clienților; — administrarea beneficiilor; — gestionarea plăților beneficiilor; — cumpărarea și vânzarea de pachete de polițe de asigurare între asigurări; — plăți cu cardul; — administrarea numerarului; — plasamente sau retrageri de numerar; — gestionarea creanțelor de asigurare; — gestionarea procesului de despăgubire în asigurări; — compensare; — conglomerate de împrumuturi pentru întreprinderi; — asigurări colective; — transferuri de credite; — custodia și păstrarea în siguranță a activelor; — integrarea clienților; — încorporarea datelor; — prelucrarea datelor; — debitări directe; — asigurări pentru exporturi; — finalizarea tranzacțiilor/operațiunilor; — plasarea de instrumente financiare; — contabilitatea fondurilor;	Nu	Da	Da	Alfanumeric

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
	— fonduri în valută; — consultanță de investiții; — administrarea investițiilor; — emiterea de instrumente de plată; — gestionarea împrumuturilor; — gestionarea procesului de plată a asigurărilor de viață; — remiterea de bani; — calculul activului net; — emiterea ordinelor; — furnizarea de servicii de inițiere a plății; — subscrierea de asigurări; — administrarea de portofolii; — încasarea primelor; — recepție/transmitere/executare; — reasigurare; — decontare; — monitorizarea tranzacțiilor. În cazul raportării agregate, astfel cum se menționează articolul 7 din prezentul regulament, a se indica domeniile funcționale și procesele operaționale afectate care au fost afectate în cel puțin o entitate financiară.				
3.28. Componente de infrastructură afectate care sprijină procesele operaționale	Informații din care să reiasă dacă respectivele componente de infrastructură (servere, sisteme de operare, software, servere de aplicații, middleware, componente de rețea, alte elemente) care sprijină procesele operaționale au fost afectate de incidentul major legat de TIC.	Nu	Da	Da	Opțiuni: — Da — Nu — Informație indisponibilă
3.29. Informații privind componentele de infrastructură afectate care sprijină procesele operaționale	Descrierea impactului incidentului major legat de TIC asupra componentelor de infrastructură care sprijină procesele operaționale, inclusiv asupra hardware-ului și software-ului. Hardware-ul include serverele, calculatoarele, centrele de date, switch-urile, routerele și hub-urile. Software-ul include sistemele de operare, aplicațiile, bazele de date, instrumentele de securitate, componentele de rețea și alte elemente (a se preciza). Descrierile trebuie să prezinte sau să numească componentele sau sistemele de infrastructură afectate și, dacă sunt disponibile: (a) informațiile privind versiunea; (b) infrastructura internă/externalizată parțial/externalizată integral – denumirea furnizorului terț;	Nu	Da, dacă incidentul a afectat componente de infrastructură care sprijină procesele operaționale	Da, dacă incidentul a afectat componente de infrastructură care sprijină procesele operaționale	Alfanumeric

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
	(c) dacă infrastructura este utilizată sau partajată la nivelul mai multor funcții operaționale; (d) mecanismele relevante în materie de reziliență/continuitate/recuperare/substituibilitate instituite.				
3.30. Impactul asupra intereselor financiare ale clienților	Informații din care să reiasă dacă incidentul major legat de TIC a afectat interesele financiare ale clienților.	Nu	Da	Da	Opțiuni: — Da — Nu — Informație indisponibilă
3.31. Raportarea către alte autorități	Precizarea autorităților care au fost informate cu privire la incidentul major legat de TIC Ținând seama de diferențele care rezultă din legislația națională a statelor membre, conceptul de autorități de aplicare a legii este înțeles de entitățile financiare în sens larg pentru a include autoritățile publice abilitate să urmărească penal criminalitatea informatică, inclusiv poliția, agențiile de aplicare a legii și procurorii.	Nu	Da	Da	Opțiuni (multiple): — poliția/autoritățile de aplicare a legii; — CSIRT; — autoritate pentru protecția datelor; — agenția națională pentru securitate cibernetică; — niciuna; — altele (a se preciza).
3.32. Precizarea „altor” autorități	Precizarea „altor” tipuri de autorități informate cu privire la incidentul major legat de TIC Dacă în câmpul de date 3.31. s-a selectat opțiunea „altele”, descrierea trebuie să includă informații mai detaliate cu privire la autoritatea căreia entitatea financiară i-a transmis informații cu privire la incidentul major legat de TIC.	Nu	Da, dacă entitatea financiară a informat „alte” tipuri de autorități cu privire la incidentul major legat de TIC	Da, dacă entitatea financiară a informat „alte” tipuri de autorități cu privire la incidentul major legat de TIC	Alfanumeric
3.33. Acțiuni/măsuri temporare luate sau planificate în vederea redresării în urma incidentului	Informații din care să reiasă dacă entitatea financiară a pus în aplicare (sau planifică să pună în aplicare) orice acțiune temporară care a fost întreprinsă (sau planificată a fi întreprinsă) în vederea redresării în urma incidentului major legat de TIC.	Nu	Da	Da	Boolean (Da sau Nu)

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
3.34. Descrierea oricăror acțiuni și măsuri temporare luate sau planificate în vederea redresării în urma incidentului	Informațiile descriu măsurile imediate luate, inclusiv izolarea incidentului la nivel de rețea, procedurile activate pentru depășirea situației intervenite, porturile USB blocate, locul de recuperare în caz de dezastru activat și orice altă măsură de securitate suplimentară instituită temporar. Entitățile financiare indică data și ora punerii în aplicare a acțiunilor temporare și data preconizată de întoarcere la locul principal de desfășurare a activității. Pentru orice acțiuni temporare care nu au fost puse în aplicare, dar care sunt încă planificate, se indică data până la care se preconizează punerea lor în aplicare. Dacă nu s-au întreprins acțiuni/măsuri temporare, vă rugăm să indicați motivul.	Nu	Da, în cazul în care s-au întreprins sau sunt planificate acțiuni/măsuri temporare (câmpul de date 3.33)	Da, în cazul în care s-au întreprins sau sunt planificate acțiuni/măsuri temporare (câmpul de date 3.33)	Alfanumeric
3.35. Indicatori de compromitere	Informații referitoare la incidentul major legat de TIC care pot contribui la identificarea activităților rău-intenționate în cadrul unei rețele sau al unui sistem informatic (indicatori de compromitere), după caz. Câmpul se aplică numai entităților financiare care intră în domeniul de aplicare al Directivei (UE) 2022/2555 a Parlamentului European și a Consiliului ([1]) și entităților financiare identificate ca fiind entități esențiale sau importante în temeiul normelor naționale de transpunere a articolului 3 din Directiva (UE) 2022/2555, după caz. Indicatorii de compromitere furnizați de entitatea financiară includ următoarele categorii de date: (a) adresele IP; (b) adresele URL; (c) domeniile; (d) valorile hash ale fișierelor; (e) datele privind programele malware (numele programelor malware, numele fișierelor și locațiile acestora, cheile de înregistrare specifice asociate activității malware); (f) datele privind activitatea de rețea (porturi, protocoale, adrese, referenți, agenți utilizatori, antete, jurnale specifice sau modele distinctive în traficul de rețea); (g) datele mesajului transmis prin e-mail (expeditor, destinatar, subiect, antet, conținut);	Nu	Da, dacă în câmpul de date 3.23 s-a selectat opțiunea „incident legat de securitatea cibernetică” pentru tipul de incident	Da, dacă în câmpul de date 3.23 s-a selectat opțiunea „incident legat de securitatea cibernetică” pentru tipul de incident	Alfanumeric

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
	(h) cererile DNS și configurațiile registrului; (i) activitățile din contul de utilizator (conectare, activitate privilegiată a contului de utilizator, escaladarea privilegiilor); (j) traficul bazei de date (citire/scriere), solicitări către același fișier. În practică, informațiile de acest tip pot include date referitoare, printre altele, la indicatori care descriu tiparele traficului de rețea care corespund atacurilor cunoscute/comunicațiilor botnet, adresele IP ale mașinilor infectate cu programe malware (boți), date referitoare la serverele de „comandă și control" utilizate de programele malware (de obicei domenii sau adrese IP) și URL-uri referitoare la site-uri de phishing sau site-uri web care găzduiesc programe malware sau exploatează kituri.				
Conținutul raportului final					
4.1. Clasificarea de nivel înalt a cauzelor principale ale incidentului	Clasificarea de nivel înalt a cauzei principale a incidentului major legat de TIC în cadrul tipurilor de incidente, cu includerea următoarelor categorii de nivel înalt: (a) acțiuni rău-intenționate; (b) disfuncționalitate a procesului; (c) disfuncționalitate a sistemului/funcționarea defectuoasă a sistemului; (d) eroare umană; (e) eveniment extern.	Nu	Nu	Da	Opțiuni (multiple): — acțiuni rău-intenționate; — disfuncționalitate a procesului; — disfuncționalitate a sistemului/ funcționarea defectuoasă a sistemului; — eroare umană; — eveniment extern.
4.2. Clasificarea detaliată a cauzelor principale ale incidentului	Clasificarea detaliată a cauzelor principale ale incidentului major legat de TIC în cadrul tipurilor de incidente, cu includerea următoarelor categorii detaliate legate de categoriile de nivel înalt raportate în câmpul de date 4.1: 1. **Acțiuni rău-intenționate** (dacă s-a selectat această categorie, alegeți una sau mai multe dintre următoarele opțiuni): (a) acțiuni interne deliberate; (b) deteriorare fizică deliberată/manipulare/furt; (c) acțiuni frauduloase. 2. **Disfuncționalitate a procesului** (dacă s-a selectat această categorie, alegeți una sau mai multe dintre următoarele opțiuni): (a) monitorizarea insuficientă sau disfuncționalitatea monitorizării și a controlului;	Nu	Nu	Da	Opțiuni (multiple): — acțiuni rău-intenționate: acțiuni interne deliberate; — acțiuni rău-intenționate: deteriorare fizică deliberată/manipulare/furt; — acțiuni rău-intenționate: acțiuni frauduloase; — disfuncționalitate a procesului: monitorizarea insuficientă sau disfuncționalitatea monitorizării și a controlului; — disfuncționalitate a procesului: roluri și responsabilități insuficiente/neclare; — disfuncționalitate a procesului: disfuncționalitatea procesului de gestionare a riscurilor TIC; — disfuncționalitate a procesului: insuficiența sau disfuncționalitatea operațiunilor TIC și a operațiunilor de securitate TIC;

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
	(b) roluri și responsabilități insuficiente/neclare; (c) disfuncționalitatea procesului de gestionare a riscurilor TIC; (d) insuficiența sau disfuncționalitatea operațiunilor TIC și a operațiunilor de securitate TIC; (e) gestionarea insuficientă a proiectelor TIC sau disfuncționalitatea gestionării acestora; (f) politici, proceduri și documente interne inadecvate; (g) achiziționarea, dezvoltarea sau întreținerea necorespunzătoare a sistemelor TIC; (h) altele (a se preciza). 3. **Disfuncționalitate a sistemului/funcționarea defectuoasă a sistemului** (dacă s-a selectat această categorie, alegeți una sau mai multe dintre următoarele opțiuni): (a) capacitatea și performanța hardware-ului: incidente majore legate de TIC cauzate de resurse hardware care se dovedesc inadecvate în ceea ce privește capacitatea sau performanța pentru a îndeplini cerințele legislative aplicabile; (b) întreținerea hardware-ului: incidentele majore legate de TIC care rezultă din întreținerea inadecvată sau insuficientă a componentelor hardware, altele decât în urma „uzurii morale/a învechirii hardware-ului”; (c) uzura morală/învechirea hardware-ului: acest tip de cauză principală implică incidente majore legate de TIC care rezultă ca urmare a utilizării unor componente hardware depășite sau învechite; (d) compatibilitatea/configurarea software-ului: incidentele majore legate de TIC cauzate de componente software care sunt incompatibile cu alte configurații de software sau de sistem, inclusiv incidente majore legate de TIC care rezultă din conflicte de software, setări incorecte sau parametri configurați greșit care afectează funcționalitatea generală a sistemului; (e) performanța software-ului: incidentele majore legate de TIC cauzate de componente software care prezintă performanțe slabe sau ineficiențe, din alte motive decât cele specificate în categoria „Compatibilitatea/configurarea software-ului”, inclusiv incidentele majore legate de TIC cauzate de timpii de răspuns lenți, de consumul excesiv de resurse sau de executarea ineficientă a interogărilor care afectează performanța software-ului sau a sistemului;				— disfuncționalitate a procesului: gestionarea insuficientă a proiectelor TIC sau disfuncționalitatea gestionării acestora; — disfuncționalitate a procesului: caracterul inadecvat al politicilor, procedurilor și documentelor interne; — disfuncționalitate a procesului: achiziționarea, dezvoltarea și întreținerea inadecvată a sistemelor TIC; — disfuncționalitate a procesului: altele (a se preciza); — disfuncționalitate a sistemului: capacitatea și performanța hardware-ului; — disfuncționalitate a sistemului: întreținerea hardware-ului; — disfuncționalitate a sistemului: uzura morală/învechirea hardware-ului; — disfuncționalitate a sistemului: compatibilitatea/configurarea software-ului; — disfuncționalitate a sistemului: performanța software-ului; — disfuncționalitate a sistemului: configurația rețelei; — disfuncționalitate a sistemului: deteriorare fizică; — disfuncționalitate a sistemului: altele (a se preciza); — eroare umană: omisiune; — eroare umană: greșeală; — eroare umană: competențe și cunoștințe; — eroare umană: resurse umane inadecvate; — eroare umană – probleme de comunicare; — eroare umană: altele (a se preciza); — eveniment extern: dezastre naturale/forță majoră; — eveniment extern: erori ale părților terțe; — eveniment extern: altele (a se preciza).

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
	(f) configurația rețelei: incidente majore legate de TIC cauzate de setări sau infrastructuri de rețea incorecte sau configurate greșit, inclusiv incidente majore legate de TIC cauzate de erori de configurare a rețelei, probleme de rutare, configurații greșite ale firewall-ului sau alte probleme legate de rețea care afectează conectivitatea sau comunicarea; (g) deteriorare fizică: incidentele majore legate de TIC cauzate de deteriorarea fizică a infrastructurii TIC, care conduc la disfuncționalități ale sistemului; (h) altele (a se preciza). 4. **Eroare umană** (dacă s-a selectat această categorie, alegeți una sau mai multe dintre următoarele opțiuni): (a) omisiune (neintenționată); (b) greșeală; (c) competențe și cunoștințe: incidentele majore legate de TIC cauzate de lipsa de cunoștințe de specialitate sau de competențe în gestionarea sistemelor sau proceselor TIC, care pot fi cauzate de o formare inadecvată, de cunoștințe insuficiente sau de lacune în ceea ce privește competențele necesare pentru a îndeplini sarcini specifice sau pentru a aborda probleme de ordin tehnic; (d) resurse umane inadecvate: incidentele majore legate de TIC cauzate de lipsa resurselor necesare, inclusiv a hardware-ului, a software-ului, a infrastructurii sau a personalului, inclusiv situațiile în care resursele insuficiente conduc la ineficiențe operaționale, la disfuncționalități ale sistemului sau la incapacitatea de a satisface cerințele operaționale; (e) probleme de comunicare; (f) altele (a se preciza). 5. **Eveniment extern** (dacă s-a selectat această categorie, alegeți una sau mai multe dintre următoarele opțiuni): (a) dezastre naturale/forță majoră; (b) erori ale părților terțe;				

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
	(c) altele (a se preciza). Entitățile financiare se asigură că, pentru incidentele majore recurente legate de TIC, se ia în considerare cauza principală aparentă specifică a incidentului și nu categoriile generale incluse în acest domeniu.				
4.3. Clasificarea suplimentară a cauzelor principale ale incidentului	Clasificarea suplimentară a cauzelor principale ale incidentului major legat de TIC în cadrul tipului de incident, cu includerea următoarelor categorii de clasificare suplimentare legate de categoriile detaliate care trebuie raportate în câmpul de date 4.2. Câmpul este obligatoriu pentru raportul final dacă în câmpul de date 4.2 se raportează categorii specifice care necesită o granularitate suplimentară. 2(a) **Monitorizarea insuficientă sau disfuncționalitatea monitorizării și a controlului:** (a) monitorizarea respectării politicilor; (b) monitorizarea furnizorilor terți de servicii; (c) monitorizarea și verificarea remedierii vulnerabilităților; (d) gestionarea identității și a accesului; (e) criptare și criptografie; (f) jurnalizare. 2(c) **Disfuncționalitatea procesului de gestionare a riscurilor TIC:** (a) nespecificarea nivelurilor exacte de toleranță la risc; (b) evaluări insuficiente ale vulnerabilității și amenințărilor; (c) măsuri inadecvate de gestionare a riscurilor; (d) gestionarea defectuoasă a riscurilor TIC reziduale. 2(d) **Insuficiența sau disfuncționalitatea operațiunilor TIC și a operațiunilor de securitate TIC:** (a) gestionarea vulnerabilităților și a corecțiilor; (b) gestionarea modificărilor; (c) gestionarea capacității și a performanței; (d) gestionarea activelor TIC și clasificarea informațiilor;	Nu	Nu	Da	Opțiuni (multiple): — monitorizarea respectării politicilor; — monitorizarea furnizorilor terți de servicii; — monitorizarea și verificarea remedierii vulnerabilităților; — gestionarea identității și a accesului; — criptare și criptografie; — jurnalizare; — nespecificarea nivelurilor exacte de toleranță la risc; — evaluări insuficiente ale vulnerabilității și amenințărilor; — măsuri inadecvate de gestionare a riscurilor; — gestionarea defectuoasă a riscurilor TIC reziduale; — gestionarea vulnerabilităților și a corecțiilor; — gestionarea modificărilor; — gestionarea capacității și a performanței; — gestionarea activelor TIC și clasificarea informațiilor; — copii de rezervă și restaurare; — gestionarea erorilor; — achiziționarea, dezvoltarea și întreținerea inadecvată a sistemelor TIC; — testarea insuficientă a software-ului sau disfuncționalități în testarea software-ului.

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
	(e) copii de rezervă și restaurare; (f) gestionarea erorilor. 2(g) **Achiziționarea, dezvoltarea și întreținerea inadecvată a sistemelor TIC:** (a) achiziționarea, dezvoltarea și întreținerea inadecvată a sistemelor TIC; (b) testarea insuficientă a software-ului sau disfuncționalități în testarea software-ului.				
4.4. Alte tipuri de cauze principale	Entitățile financiare care au selectat opțiunea „altele” în legătură cu tipurile de cauze principale în câmpul de date 4.2 precizează alte tipuri de cauze principale.	Nu	Nu	Da, dacă în câmpul de date 4.2 s-a selectat opțiunea „altele” în legătură cu tipurile de cauze principale.	Alfanumeric
4.5. Informații privind cauzele principale ale incidentului	Descrierea succesiunii evenimentelor care au condus la incidentul major legat de TIC și descrierea modului în care incidentul major legat de TIC are o cauză principală aparentă similară dacă incidentul respectiv este clasificat drept incident recurent, inclusiv o descriere concisă a tuturor motivelor subiacente și a factorilor principali care au contribuit la apariția incidentului major legat de TIC. În cazul în care au existat acțiuni rău-intenționate, se vor descrie modul de operare al acțiunii rău-intenționate, inclusiv tacticile, tehnicile și procedurile utilizate, precum și vectorul de intrare al incidentului major legat de TIC, inclusiv investigațiile și analiza care au condus la identificarea cauzelor principale, dacă este cazul.	Nu	Nu	Da	Alfanumeric
4.6. Soluționarea incidentului	Informații suplimentare privind acțiunile/măsurile luate/planificate pentru soluționarea definitivă a incidentului major legat de TIC și pentru prevenirea repetării incidentului respectiv. Lecții învățate în urma incidentului major legat de TIC	Nu	Nu	Da	Alfanumeric

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
	Descrierea trebuie să conțină următoarele puncte: 1. **Descrierea acțiunilor întreprinse în vederea soluționării incidentului** (a) acțiunile întreprinse pentru soluționarea definitivă a incidentului major legat de TIC (cu excepția oricăror acțiuni temporare); (b) pentru fiecare acțiune întreprinsă, indicarea eventualei implicări a unui furnizor terț și a entității financiare; (c) informații din care să reiasă dacă procedurile au fost adaptate în urma incidentului major legat de TIC; (d) indicarea oricăror controale suplimentare care au fost instituite sau care sunt planificate, alături de calendarul de punere în aplicare aferent. Eventualele probleme identificate în ceea ce privește soliditatea sistemelor informatice afectate/sau în ceea ce privește procedurile sau controalele existente, dacă este cazul. Entitățile financiare indică în mod clar modul în care acțiunile de remediere avute în vedere vor aborda cauzele principale identificate și momentul în care se preconizează că incidentul major legat de TIC va fi soluționat definitiv. 2. **Lecții învățate** Entitățile financiare descriu constatările rezultate în urma analizei ulterioare incidentului.				
4.7. Data și ora la care a fost contracarată cauza principală a incidentului	Data și ora la care a fost contracarată cauza principală a incidentului	Nu	Nu	Da	Standardul ISO 8601 UTC (AAAA-LL-ZZ Thh:mm:ss)
4.8. Data și ora la care s-a soluționat incidentul	Data și ora la care s-a soluționat incidentul	Nu	Nu	Da	Standardul ISO 8601 UTC (AAAA-LL-ZZ Thh:mm:ss)

	Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
4.9.	Informații din care să reiasă dacă data soluționării definitive a incidentelor majore legate de TIC este diferită de data de punere în aplicare planificată inițial, după caz.	Descrieri ale motivului pentru care data soluționării definitive a incidentelor majore legate de TIC este diferită de data de punere în aplicare planificată inițial, după caz.	Nu	Nu	Da	Alfanumeric
4.10.	Evaluarea riscului pentru funcțiile critice în scopul rezoluției	Evaluarea măsurii în care incidentul major legat de TIC prezintă un risc pentru funcțiile critice în sensul articolului 2 alineatul (1) punctul 35 din Directiva 2014/59/UE a Parlamentului European și a Consiliului ([2]). Entitățile menționate la articolul 1 alineatul (1) din Directiva 2014/59/UE indică dacă incidentul prezintă un risc pentru funcțiile critice în sensul articolului 2 alineatul (1) punctul 35 din Directiva 2014/59/UE, raportate în macheta Z07.01 din Regulamentul de punere în aplicare (UE) 2018/1624 al Comisiei ([3]) și puse în corespondență cu entitatea specifică din macheta Z07.02.	Nu	Nu	Da, dacă incidentul prezintă un risc pentru funcțiile critice ale entităților financiare prevăzute la articolul 2 alineatul (1) punctul 35 din Directiva 2014/59/UE	Alfanumeric
4.11.	Informații relevante pentru autoritățile de rezoluție	Descrierea măsurii în care și, dacă este cazul, a modului în care incidentul major legat de TIC a afectat posibilitatea de rezoluție a entității sau a grupului. Entitățile menționate la articolul 1 alineatul (1) din Directiva 2014/59/UE furnizează informații din care să reiasă dacă și, după caz, modul în care incidentul major legat de TIC a afectat posibilitatea de rezoluție a entității sau a grupului. Entitățile respective indică, de asemenea, dacă incidentul major legat de TIC afectează solvabilitatea sau lichiditatea entității financiare și potențiala cuantificare a impactului. Entitățile respective furnizează, de asemenea, informații cu privire la impactul asupra continuității operaționale, impactul asupra posibilității de rezoluție a entității, orice impact suplimentar asupra costurilor și a pierderilor generate de incidentul major legat de TIC, inclusiv asupra poziției de capital a entității financiare, precum și dacă acordurile contractuale privind utilizarea serviciilor TIC sunt în continuare solide și pe deplin executorii în cazul rezoluției entității.	Nu	Nu	Da, dacă incidentul a afectat posibilitatea de rezoluție a entității sau a grupului.	Alfanumeric

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
4.12. Pragul de semnificație pentru criteriul de clasificare „Impactul economic”	Informații detaliate cu privire la pragurile atinse în cele din urmă de incidentul major legat de TIC în legătură cu criteriul „Impactul economic” menționat la articolele 7 și 14 din Regulamentul delegat (UE) 2024/1772.	Nu	Nu	Da	Alfanumeric
4.13. Cuantumul costurilor și pierderilor directe și indirecte brute	Cuantumul total al costurilor și pierderilor directe și indirecte brute suportate de entitatea financiară în urma incidentului major legat de TIC, inclusiv: (a) cuantumul fondurilor expropriate sau al activelor financiare pentru care este răspunzătoare entitatea financiară; (b) cuantumul costurilor de înlocuire sau mutare a software-ului, hardware-ului sau infrastructurii; (c) cuantumul costurilor cu personalul, inclusiv al costurilor asociate înlocuirii sau mutării personalului, angajării de personal suplimentar, remunerării orelor suplimentare și recuperării competențelor pierdute sau afectate ale personalului; (d) cuantumul taxelor datorate ca urmare a nerespectării obligațiilor contractuale; (e) cuantumul reparațiilor și despăgubirilor datorate clienților; (f) cuantumul pierderilor datorate veniturilor nerealizate; (g) cuantumul costurilor aferente comunicării interne și externe; (h) cuantumul costurilor de consiliere, inclusiv al costurilor aferente consilierii juridice și serviciilor de expertiză criminalistică și de remediere; (i) cuantumul altor costuri și pierderi, inclusiv: (i) al cheltuielilor directe, inclusiv al deprecierilor și al cheltuielilor de decontare, în contul de profit și pierdere și al reducerilor valorii contabile cauzate de incidentul major legat de TIC; (ii) al provizioanelor sau al rezervelor contabilizate în contul de profit și pierdere pentru pierderile probabile legate de incidentul major legat de TIC;	Nu	Nu	Da	Monetar

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
	(iii) al pierderilor latente, sub formă de pierderi generate de incidentul major legat de TIC, care sunt înregistrate temporar în conturi tranzitorii sau de așteptare și nu sunt încă reflectate în contul de profit și pierdere și care urmează să fie incluse în contul de profit și pierdere într-un termen proporțional cu dimensiunea și vechimea elementului latent; (iv) al veniturilor semnificative care nu au fost încasate, legate de obligațiile contractuale cu părțile terțe, inclusiv decizia de a despăgubi mai degrabă un client în urma incidentului major legat de TIC decât de a efectua o rambursare sau o plată directă, ajustând venitul prin renunțarea la taxele contractuale sau prin reducerea acestora într-o anumită perioadă de timp viitoare; (v) al pierderilor temporare, în cazul în care acestea acoperă o perioadă mai lungă decât un exercițiu financiar-contabil și generează un risc juridic. Entitățile financiare țin seama, în evaluarea lor, de articolul 7 alineatele (1) și (2) din Regulamentul delegat (UE) 2024/1772. Entitățile financiare nu includ în această cifră recuperări financiare de niciun tip. Entitățile financiare raportează valoarea monetară ca valoare pozitivă. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, entitățile financiare țin seama de cuantumul total al costurilor și pierderilor la nivelul tuturor entităților financiare. Entitățile financiare raportează punctul de date în unități, cu o precizie minimă echivalentă cu miile de unități.				
4.14. Cuantumul recuperărilor financiare	Cuantumul total al recuperărilor financiare Recuperările financiare se raportează la pierderea inițială cauzată de incident, independent de momentul în care se primesc recuperările financiare sub formă de fonduri sau intrări de beneficii economice.	Nu	Nu	Da	Monetar Entitățile financiare raportează punctul de date în unități, cu o precizie minimă echivalentă cu miile de unități.

Câmpul de date	Descriere	Obligatoriu pentru notificarea inițială	Obligatoriu pentru raportul intermediar	Obligatoriu pentru raportul final	Tipul de câmp
	Entitățile financiare raportează valoarea monetară ca valoare pozitivă. În cazul raportării agregate, astfel cum se menționează la articolul 7 din prezentul regulament, entitățile financiare țin seama de cuantumul total al recuperărilor financiare la nivelul tuturor entităților financiare.				
4.15. Informații din care să reiasă dacă incidentele care nu se încadrează în categoria incidentelor majore au fost recurente	Informații din care să reiasă dacă mai multe incidente legate de TIC care nu se încadrează în categoria incidentelor majore au fost recurente și sunt considerate împreună ca fiind un singur incident major în sensul articolului 8 alineatul (2) din Regulamentul delegat (UE) 2024/1772. Entitățile financiare indică dacă incidentele legate de TIC care nu se încadrează în categoria incidentelor majore au fost recurente și sunt considerate împreună ca fiind un singur incident major legat de TIC. Entitățile financiare indică, de asemenea, numărul de cazuri în care au survenit astfel de incidente legate de TIC care nu se încadrează în categoria incidentelor majore.	Nu	Nu	Da, dacă incidentul major cuprinde mai multe incidente recurente care nu se încadrează în categoria incidentelor majore.	Alfanumeric
4.16. Data și ora producerii incidentelor recurente	În cazul în care entitățile financiare raportează incidente recurente legate de TIC, data și ora la care a survenit primul incident legat de TIC.	Nu	Nu	Da, pentru incidente recurente	Standardul ISO 8601 UTC (AAAA-LL-ZZ Thh:mm:ss)

([1]) Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (JO L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([2]) Directiva 2014/59/UE a Parlamentului European și a Consiliului din 15 mai 2014 de instituire a unui cadru pentru redresarea și rezoluția instituțiilor de credit și a firmelor de investiții și de modificare a Directivei 82/891/CEE a Consiliului și a Directivelor 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE și 2013/36/UE ale Parlamentului European și ale Consiliului, precum și a Regulamentelor (UE) nr. 1093/2010 și (UE) nr. 648/2012 ale Parlamentului European și ale Consiliului (JO L 173, 12.6.2014, p. 190, ELI: http://data.europa.eu/eli/dir/2014/59/oj).

([3]) Regulamentul de punere în aplicare (UE) 2018/1624 al Comisiei din 23 octombrie 2018 de stabilire a unor standarde tehnice de punere în aplicare cu privire la procedurile și formularele și machetele standard care trebuie utilizate pentru furnizarea informațiilor necesare în scopul planurilor de rezoluție pentru instituțiile de credit și firmele de investiții în temeiul Directivei 2014/59/UE a Parlamentului European și a Consiliului și de abrogare a Regulamentului de punere în aplicare (UE) 2016/1066 al Comisiei (JO L 277, 7.11.2018, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2018/1624/oj).

ANEXA III

MODELE PENTRU NOTIFICAREA PRIVIND AMENINȚĂRILE CIBERNETICE SEMNIFICATIVE

Numărul câmpului	Câmpul de date	
1	Denumirea entității care transmite notificarea	
2	Codul de identificare al entității care transmite notificarea	
3	Tipul de entitate financiară care transmite notificarea	
4	Denumirea entității financiare	
5	Codul LEI al entității financiare	
6	Numele persoanei de contact principale	
7	Adresa de e-mail a persoanei de contact principale	
8	Numărul de telefon al persoanei de contact principale	
9	Numele persoanei de contact secundare	
10	Adresa de e-mail a persoanei de contact secundare	
11	Numărul de telefon al persoanei de contact secundare	
12	Data și ora detectării amenințării cibernetice	
13	Descrierea amenințării cibernetice semnificative	
14	Informații privind impactul potențial	
15	Criterii de clasificare a incidentelor potențiale	
16	Starea amenințării cibernetice	
17	Acțiuni întreprinse pentru a preveni materializarea	
18	Notificarea altor părți interesate	
19	Indicatori de compromitere	
20	Alte informații relevante	

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

ANEXA IV

GLOSAR DE DATE ȘI INSTRUCȚIUNI PENTRU NOTIFICAREA PRIVIND AMENINȚĂRILE CIBERNETICE SEMNIFICATIVE

Câmpul de date	Descriere	Câmp obligatoriu	Tipul de câmp
1. Denumirea entității care transmite notificarea	Denumirea juridică completă a entității care transmite notificarea	Da	Alfanumeric
2. Codul de identificare al entității care transmite notificarea	Codul de identificare al entității care transmite notificarea În cazul în care entitățile financiare transmit notificarea/raportul, codul de identificare este un identificator al entității juridice (LEI), care este un cod unic format din 20 de caractere alfanumerice, bazat pe ISO 17442-1:2020. În cazul în care un furnizor terț transmite un raport pentru o entitate financiară, acesta poate utiliza un cod de identificare, astfel cum se specifică în standardele tehnice de punere în aplicare adoptate în temeiul articolului 28 alineatul (9) din Regulamentul (UE) 2022/2554.	Da	Alfanumeric
3. Tipul de entitate financiară care transmite raportul	Tipul de entitate menționată la articolul 2 alineatul (1) literele (a)-(t) din Regulamentul (UE) 2022/2554 care transmite raportul.	Da, dacă raportul nu este furnizat direct de entitatea financiară afectată.	Opțiuni (cu posibilitate de selecție multiplă): — instituție de credit; — instituție de plată; — instituție de plată exceptată; — prestator de servicii de informare cu privire la conturi; — instituție emitentă de monedă electronică; — instituție emitentă de monedă electronică exceptată; — firmă de investiții; — prestator de servicii de criptoactive; — emitent de tokenuri raportate la active; — depozitar central de titluri de valoare; — contraparte centrală; — loc de tranzacționare; — registru central de tranzacții; — administrator de fonduri de investiții alternative; — societate de administrare; — furnizor de servicii de raportare a datelor;

Câmpul de date		Descriere	Câmp obligatoriu	Tipul de câmp
				— întreprindere de asigurare și de reasigurare; — intermediar de asigurări, intermediar de reasigurări și intermediar de asigurări auxiliare; — instituție pentru furnizarea de pensii ocupaționale; — agenție de rating de credit; — administrator de indici de referință critici; — furnizor de servicii de finanțare participativă; — registru central de securitizări.
4.	Denumirea entității financiare	Denumirea juridică completă a entității financiare care notifică amenințarea cibernetică semnificativă	Da, dacă entitatea financiară este diferită de entitatea care transmite notificarea	Alfanumeric
5.	Codul LEI al entității financiare	Identificatorul entității juridice (LEI) al entității financiare care notifică amenințarea cibernetică semnificativă, atribuit potrivit Organizației Internaționale de Standardizare.	Da, dacă entitatea financiară care notifică amenințarea cibernetică semnificativă este diferită de entitatea care transmite raportul	Cod unic format din 20 de caractere alfanumerice, bazat pe ISO 17442-1:2020
6.	Numele persoanei de contact principale	Prenumele și numele persoanei de contact principale a entității financiare	Da	Alfanumeric
7.	Adresa de e-mail a persoanei de contact principale	Adresa de e-mail a persoanei de contact principale care poate fi utilizată de autoritatea competentă pentru comunicarea ulterioară.	Da	Alfanumeric
8.	Numărul de telefon al persoanei de contact principale	Numărul de telefon al persoanei de contact principale care poate fi utilizat de autoritatea competentă pentru comunicarea ulterioară. Numărul de telefon se raportează cu toate prefixele internaționale (de exemplu, +33XXXXXXXXX).	Da	Alfanumeric
9.	Numele persoanei de contact secundare	Prenumele și numele persoanei de contact secundare a entității financiare sau a unei entități care transmite notificarea în numele entității financiare, dacă sunt disponibile.	Da, dacă sunt disponibile prenumele și numele persoanei de contact secundare a entității financiare sau a unei entități care transmite notificarea în numele entității financiare	Alfanumeric

Câmpul de date	Descriere	Câmp obligatoriu	Tipul de câmp
10. Adresa de e-mail a persoanei de contact secundare	Adresa de e-mail a persoanei de contact secundare sau o adresă de e-mail funcțională a echipei care poate fi utilizată de autoritatea competentă pentru comunicarea ulterioară, dacă o astfel de adresă este disponibilă.	Da, dacă este disponibilă adresa de e-mail a persoanei de contact secundare sau o adresă de e-mail funcțională a echipei care poate fi utilizată de autoritatea competentă pentru comunicarea ulterioară	Alfanumeric
11. Numărul de telefon al persoanei de contact secundare	Numărul de telefon al persoanei de contact secundare care poate fi utilizat de autoritatea competentă pentru comunicarea ulterioară, dacă este disponibil. Numărul de telefon se raportează cu toate prefixele internaționale (de exemplu, +33XXXXXXXXX).	Da, dacă este disponibil numărul de telefon al persoanei de contact secundare care poate fi utilizat de autoritatea competentă pentru comunicarea ulterioară	Alfanumeric
12. Data și ora detectării amenințării cibernetice	Data și ora la care entitatea financiară a luat cunoștință de amenințarea cibernetică semnificativă	Da	Standardul ISO 8601 UTC (AAAA-LL-ZZ Thh: mm:ss)
13. Descrierea amenințării cibernetice semnificative	Descrierea celor mai relevante aspecte ale amenințării cibernetice semnificative Entitățile financiare furnizează: (a) o imagine de ansamblu de nivel înalt a celor mai relevante aspecte ale amenințării cibernetice semnificative; (b) riscurile conexe care decurg din aceasta, inclusiv vulnerabilitățile potențiale ale sistemelor entității financiare care pot fi exploatate; (c) informații cu privire la probabilitatea de materializare a amenințării cibernetice semnificative; și (d) date privind sursa de informații cu privire la amenințarea cibernetică.	Da	Alfanumeric
14. Informații privind impactul potențial	Informații privind impactul potențial al amenințării cibernetice asupra entității financiare, a clienților săi sau a contrapărților financiare, în cazul în care amenințarea cibernetică s-a materializat	Da	Alfanumeric
15. Criterii de clasificare a incidentelor potențiale	Criteriile de clasificare care ar fi putut conduce la un raport privind un incident major dacă amenințarea cibernetică s-ar fi materializat.	Da	Opțiuni (multiple): — clienți, contrapărți financiare și tranzacții afectate; — impactul asupra reputației; — durata incidentului și perioada de indisponibilitate a serviciului; — întinderea geografică; — pierderile de date; — serviciile critice afectate; — impactul economic.

Câmpul de date	Descriere	Câmp obligatoriu	Tipul de câmp
16. Starea amenințării cibernetice	Informații privind starea amenințării cibernetice la adresa entității financiare, precum și informații din care să reiasă dacă au avut loc modificări în activitatea de amenințare. În cazul în care amenințarea cibernetică a încetat să comunice cu sistemele informatice ale entității financiare, starea acesteia poate fi marcată ca fiind inactivă. În cazul în care entitatea financiară deține informații conform cărora amenințarea rămâne activă împotriva altor părți sau a sistemului financiar în ansamblu, starea sa se marchează ca fiind activă.	Da	Opțiuni: — activă — inactivă
17. Acțiuni întreprinse pentru a preveni materializarea	Informații de nivel înalt cu privire la acțiunile întreprinse de entitatea financiară pentru a preveni materializarea amenințărilor cibernetice semnificative, dacă este cazul.	Da	Alfanumeric
18. Notificarea altor părți interesate	Informații privind notificarea amenințării cibernetice către alte entități financiare sau autorități	Da, dacă alte entități financiare sau autorități au fost informate cu privire la amenințarea cibernetică	Alfanumeric
19. Indicatori de compromitere	Informații referitoare la amenințarea semnificativă care pot contribui la identificarea activităților rău-intenționate în cadrul unei rețele sau al unui sistem informatic (indicatori de compromitere), după caz. Indicatorii de compromitere furnizați de entitatea financiară includ, dar nu se limitează la următoarele categorii de date: (a) adresele IP; (b) adresele URL; (c) domeniile; (d) valorile hash ale fișierelor; (e) datele privind programele malware (numele programelor malware, numele fișierelor și locațiile acestora, cheile de înregistrare specifice asociate activității malware); (f) datele privind activitatea de rețea (porturi, protocoale, adrese, referenți, agenți utilizatori, antete, jurnale specifice sau modele distinctive în traficul de rețea); (g) datele mesajului transmis prin e-mail (expeditor, destinatar, subiect, antet, conținut); (h) cererile DNS și configurațiile registrului; (i) activitățile din contul de utilizator (conectare, activitate privilegiată a contului de utilizator, escaladarea privilegiilor); (j) traficul bazei de date (citire/scriere), solicitări către același fișier. Informațiile de acest tip pot include date referitoare la indicatori care descriu tiparele traficului de rețea care corespund atacurilor cunoscute/comunicațiilor botnet, adresele IP ale mașinilor infectate cu programe malware (boți), date referitoare la serverele de „comandă și control” utilizate de programele malware (de obicei domenii sau adrese IP) și URL-uri referitoare la site-uri de phishing sau site-uri web care găzduiesc programe malware sau exploatează kituri.	Da, dacă sunt disponibile informații cu privire la indicatorii de compromitere legați de amenințarea cibernetică)	Alfanumeric
20. Alte informații relevante	Orice alte informații relevante cu privire la amenințarea cibernetică semnificativă	Da, dacă este cazul și dacă există alte informații disponibile care nu sunt incluse în model	Alfanumeric