Regulamentul DORA

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

Aplicare

- **REGULAMENTUL (UE) 2022/2554** 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 **(Regulamentul DORA) a intrat in vigoare în data de 17 ianuarie 2023 și urmează să se aplice de la data 17 ianuarie 2025.**
- Regulamentul DORA
  - este obligatoriu în toate elementele sale
  - se aplică direct în toate statele membre

Context

- Deși utilizarea extensivă a sistemelor TIC și gradul ridicat de digitalizare și conectivitate sunt în prezent caracteristicile de bază ale activităților entităților financiare din Uniune, reziliența digitală a acestora trebuie încă să fie mai bine abordată și integrată în cadrele lor operaționale mai ample.
- **Creșterea gradului de digitalizare și de interconectare amplifică, de asemenea, riscurile TIC, ceea ce face ca societatea în ansamblu – și sistemul financiar, în special – să fie mai vulnerabilă la amenințările cibernetice sau la perturbările din domeniul TIC.**

Context

- **Breșele grave de securitate a TIC care au loc în sectorul financiar nu afectează doar entitățile financiare luate separat. Acestea facilitează, de asemenea, propagarea vulnerabilităților** localizate la nivelul canalelor de transmisie financiară și **pot avea consecințe negative asupra stabilității sistemului financiar în ansamblu**, cum ar fi generarea de retrageri masive de lichiditate și o pierdere generală a încrederii în piețele financiare.
- **Comitetul european pentru risc sistemic (ESRB) a reafirmat într-un raport din 2020 care abordează riscul cibernetic sistemic modul în care nivelul ridicat existent de interconectare dintre entitățile financiare, piețele financiare și infrastructurile pieței financiare și, în special, interdependențele dintre sistemele lor TIC ar putea constitui o vulnerabilitate sistemică, deoarece incidentele cibernetice localizate s-ar putea răspândi rapid de la oricare dintre entitățile financiare ale Uniunii la întregul sistem financiar, nestingherite de limitele geografice.**

Context

- Sectorul financiar al Uniunii este reglementat printr-un cadru unic de reglementare și este guvernat de un sistem european de supraveghere financiară.
- **Dispozițiile privind reziliența operațională digitală și securitatea TIC nu erau armonizate pe deplin sau în mod consecvent, în pofida faptului că reziliența operațională digitală este vitală pentru asigurarea stabilității financiare și a integrității pieței în era digitală**, **astfel a fost dezvoltat un cadru unic la nivel european de reglementare și de supraveghere pentru a acoperi și reziliența operațională digitală**, prin consolidarea mandatelor autorităților competente pentru a le permite să supravegheze gestionarea riscurilor TIC în sectorul financiar în vederea protejării integrității și eficienței piețelor financiare și pentru facilitarea funcționării organizate a acesteia.

Context

- **Regulamentul DORA urmărește să consolideze și să actualizeze cerințele privind riscurile TIC ca parte a cerințelor privind riscurile operaționale care, până la apariția regulamentului, au fost abordate separat în diferite acte juridice ale Uniunii.**
- Deși au acoperit principalele categorii de riscuri financiare (de exemplu, riscul de credit, riscul de piață, riscul de credit al contrapărții și riscul de lichiditate, riscul de conduită pe piață), actele respective nu au abordat în mod cuprinzător, la momentul adoptării lor, toate componentele rezilienței operaționale.

Context

- Atunci când au fost dezvoltate într-o mai mare măsură în actele juridice respective ale Uniunii, **normele privind riscul operațional** au favorizat, adesea, o **abordare cantitativă tradițională a riscurilor** (respectiv, stabilirea unei cerințe de capital pentru a acoperi riscurile TIC), **mai degrabă decât norme calitative specifice pentru protecția, detectarea, limitarea, recuperarea și repararea capacităților în cazul unor incidente legate de TIC sau referitoare la capacitățile de raportare și de testare digitală.**
- Regulamentul DORA urmărește să contribuie la creșterea gradului de conștientizare cu privire la riscurile TIC și la recunoașterea faptului că incidentele legate de TIC și o lipsă de reziliență operațională ar putea periclita soliditatea entităților financiare.

Context

- Regulamentul DORA sporește nivelul de armonizare în ceea ce privește diferitele componente ale rezilienței digitale, prin introducerea unor cerințe privind gestionarea riscurilor TIC și raportarea incidentelor legate de TIC, iar acest nivel sporit constituie o armonizare sporită și în comparație cu cerințele prevăzute în Directiva (UE) 2022/2555.
- **Prin urmare, Regulamentul DORA constituie *lex specialis* în raport cu Directiva (UE) 2022/2555 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).**

Descriere

- Regulamentul DORA stabilește cerințe uniforme privind securitatea rețelelor și a sistemelor informatice care sprijină procesele operaționale ale entităților financiare:
  i. cerințe aplicabile entităților financiare în legătură cu:
     - gestionarea riscurilor legate de tehnologia informației și comunicațiilor (TIC);
     - raportarea incidentelor majore legate de TIC și notificarea, în mod voluntar, a amenințărilor cibernetice semnificative către autoritățile competente;
     - testarea rezilienței operaționale digitale;
     - schimbul de informații și de date operative cu privire la amenințările cibernetice și vulnerabilități;
     - măsuri pentru buna gestionare a riscurilor TIC generate de părți terțe;
  ii. cerințe în legătură cu acordurile contractuale încheiate între furnizorii terți de servicii TIC și entitățile financiare;
  iii. reguli privind instituirea și desfășurarea cadrului de supraveghere pentru furnizorii terți esențiali de servicii TIC, atunci când furnizează servicii entităților financiare;
  iv. reguli privind cooperarea între autoritățile competente.

Domeniul de aplicare – Institutiile financiare sub incidența DORA, aflate în competența ASF

- Firmele de investiții;
- Depozitarii centrali de titluri de valoare;
- Contrapărțile centrale;
- Locurile de tranzacționare;
- Administratorii de fonduri de investiții alternative;
- Societățile de administrare;
- Furnizorii de servicii de raportare a datelor;
- Întreprinderile de asigurare și de reasigurare;
- Intermediarii de asigurări, intermediarii de reasigurări și intermediarii de asigurări auxiliare;
- Instituțiile pentru furnizarea de pensii ocupaționale;
- Administratorii de indici de referință critici;
- Furnizorii de servicii de finanțare participativă;
- Furnizorii terți de servicii TIC.

Domeniul de aplicare – Excepții

Regulamentul DORA nu se aplică următoarelor entități:

- administratorii de fonduri de investiții alternative, astfel cum sunt menționați la articolul 3 alineatul (2) din Directiva 2011/61/UE;
- întreprinderile de asigurare și de reasigurare, astfel cum sunt menționate la articolul 4 din Directiva 2009/138/CE;
- instituțiile pentru furnizarea de pensii ocupaționale care gestionează sisteme de pensii care împreună nu au mai mult de 15 membri în total;
- intermediarii de asigurări, intermediarii de reasigurări și intermediarii de asigurări auxiliare care sunt microîntreprinderi sau întreprinderi mici sau mijlocii.

Cadrul de guvernanță

Cadrul de guvernanță

- Entitățile financiare **dispun de un cadru intern de guvernanță și control** care asigură o gestionare eficace și prudentă a riscurilor TIC, cu scopul de a obține un nivel ridicat de reziliență operațională digitală.
- **Entitățile financiare pun în aplicare prevederile Regulamentului DORA în conformitate cu principiul proporționalității, luând în considerare dimensiunea și profilul lor general de risc și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor.**
- Entitățile financiare, altele decât microîntreprinderile, **stabilesc un rol pentru a monitoriza acordurile încheiate cu furnizorii terți de servicii TIC** cu privire la utilizarea serviciilor TIC sau desemnează un membru al conducerii de nivel superior drept responsabil de supravegherea expunerii la risc aferente și a documentației relevante.
- **Membrii organului de conducere** al entității financiare își **actualizează în mod activ cunoștințele și competențele** pentru a înțelege și a evalua riscurile TIC și impactul acestora asupra operațiunilor entității financiare, inclusiv prin frecventarea cu regularitate a unor cursuri de formare specifice, pe măsura riscurilor TIC gestionate.

Gestionarea riscurilor TIC

- **Organul de conducere al entității financiare definește, aprobă, supraveghează și este responsabil de punerea în aplicare a tuturor dispozițiilor legate de cadrul de gestionare a riscurilor TIC**
- **Organul de conducere**:
  - **poartă responsabilitatea finală pentru gestionarea riscurilor TIC** ale entității financiare;
  - **stabilește politici** menite să asigure menținerea unor standarde ridicate de disponibilitate, autenticitate, integritate și confidențialitate a datelor;
  - **stabilește roluri și responsabilități** clare pentru toate funcțiile legate de TIC și instituie mecanisme de guvernanță adecvate pentru a asigura comunicarea, cooperarea și coordonarea eficace și în timp util între aceste funcții;
  - **poartă responsabilitatea generală pentru stabilirea și aprobarea strategiei privind reziliența operațională digitală**, inclusiv pentru determinarea nivelului adecvat de toleranță la risc pentru riscurile TIC în cazul entității financiare;
  - **aprobă, supraveghează și verifică periodic punerea în aplicare a politicii de continuitate a activității TIC și a planurilor de răspuns și de recuperare** în domeniul TIC ale entității financiare, care pot fi adoptate sub forma unei politici specifice dedicate care să facă parte integrantă din politica generală de continuitate a activității și planul general de răspuns și de recuperare ale entității financiare;
  - **aprobă și verifică periodic planurile de audit intern TIC și auditurile TIC ale entității financiare**, precum și modificările semnificative aduse acestora;
  - **alocă și verifică periodic bugetul adecvat pentru a răspunde nevoilor de reziliență operațională digitală ale entității financiare** în ceea ce privește toate tipurile de resurse, inclusiv programe de conștientizare cu privire la securitatea TIC și cursuri de formare în domeniul rezilienței operaționale digitale relevante, precum și competențe TIC pentru toți membrii personalului;
  - **aprobă și verifică periodic politica** entității financiare cu privire la **acordurile privind utilizarea serviciilor TIC furnizate de furnizori terți de servicii TIC**;
  - **instituie, la nivel corporativ, canale de raportare** care să îi permită să fie informat în mod corespunzător cu privire la:
    - acordurile încheiate cu furnizorii terți de servicii TIC privind utilizarea serviciilor TIC;
    - orice modificări semnificative planificate relevante privind furnizorii terți de servicii TIC;
    - impactul potențial al unor astfel de modificări asupra funcțiilor critice sau importante care fac obiectul acordurilor respective, inclusiv un rezumat al analizei de risc pentru a evalua impactul modificărilor respective, și cel puțin incidentele majore legate de TIC și impactul acestora, precum și cu privire la măsurile de răspuns, de recuperare și corective.

Sisteme, protocoale și instrumente TIC

- Pentru a aborda și a gestiona riscurile TIC, entitățile financiare **utilizează și mențin sisteme, protocoale și instrumente TIC actualizate** care sunt:
  - **adecvate magnitudinii/amplorii operațiunilor** care sprijină desfășurarea activităților lor, în conformitate cu principiul proporționalității;
  - **fiabile**;
  - **dotate cu suficientă capacitate de a prelucra cu precizie datele** necesare pentru desfășurarea activităților și furnizarea serviciilor în timp util, precum și pentru a face față volumelor ridicate de ordine, mesaje sau tranzacții, după caz, inclusiv în cazul introducerii unor noi tehnologii;
  - **reziliente** din punct de vedere tehnologic pentru a face față în mod adecvat nevoilor suplimentare de prelucrare a informațiilor, calitate necesară în condiții de criză a pieței sau în alte situații adverse.

Identificare

- Entitățile financiare **identifică, clasifică și documentează în mod corespunzător toate funcțiile operaționale și toate rolurile și responsabilitățile sprijinite de TIC**, **activele informaționale și activele TIC** care sprijină funcțiile respective, precum și **rolurile și dependențele lor în legătură cu riscurile TIC**. Entitățile financiare **revizuiesc după caz, dar cel puțin anual, caracterul adecvat** al acestei clasificări și al oricărei documentări relevante.
- Entitățile financiare **identifică în mod constant toate sursele de riscuri TIC**, în special expunerea la riscuri față de alte entități financiare și din partea altor entități financiare, și evaluează amenințările cibernetice și vulnerabilitățile TIC relevante pentru funcțiile lor operaționale sprijinite de TIC, activele lor informaționale și activele lor TIC. Entitățile financiare **revizuiesc în mod regulat și cel puțin o dată pe an scenariile de risc** care au un impact asupra lor.
- Entitățile financiare **identifică toate activele informaționale și activele TIC**, inclusiv cele din locații aflate la distanță, resursele de rețea și echipamentele hardware și le inventariază pe cele considerate esențiale. Acestea cartografiază configurația activelor informaționale și a activelor TIC și legăturile și interdependențele dintre diferitele active informaționale și active TIC.
- Entitățile financiare, altele decât microîntreprinderile, **efectuează o evaluare a riscurilor cu ocazia fiecărei modificări majore aduse infrastructurii rețelei și a sistemului informatic și proceselor sau procedurilor** care le afectează funcțiile operaționale sprijinite de TIC, activele informaționale sau activele TIC.
- Entitățile financiare **identifică și documentează toate procesele care depind de furnizori terți de servicii TIC** și identifică interconexiunile cu furnizori terți de servicii TIC care oferă servicii care sprijină funcții critice sau importante.
- Entitățile financiare, altele decât microîntreprinderile, **efectuează periodic și cel puțin o dată pe an o evaluare specifică a riscurilor TIC vizând toate sistemele TIC moștenite** și, în orice caz, înainte și după conectarea tehnologiilor, aplicațiilor sau sistemelor.

Protecție și prevenire

- În scopul protejării adecvate a sistemelor TIC și în vederea organizării măsurilor de răspuns, entitățile financiare **monitorizează și controlează în mod continuu securitatea și funcționarea sistemelor și a instrumentelor TIC și reduc la minimum impactul riscurilor TIC asupra sistemelor TIC** prin utilizarea unor instrumente, politici și proceduri de securitate TIC adecvate.
- Entitățile financiare **concep, achiziționează și pun în aplicare politici, proceduri, protocoale și instrumente în domeniul securității TIC** care vizează să asigure reziliența, continuitatea și disponibilitatea sistemelor TIC, în special pentru cele care sprijină funcții critice sau importante, precum și să mențină standarde înalte de disponibilitate, autenticitate, integritate și confidențialitate a datelor, indiferent dacă sunt în repaus, în uz sau în tranzit.
- **Entitățile financiare utilizează soluții și procese TIC care sunt adecvate** în conformitate cu principiul proporționalității. Respectivele soluții și procese TIC:
  - **asigură securitatea mijloacelor de transfer al datelor;**
  - **reduc la minimum riscul de corupere sau de pierdere a datelor, de acces neautorizat și de defecțiuni tehnice care pot împiedica derularea activităților;**
  - **previn lipsa disponibilității, deteriorarea autenticității și a integrității, încălcarea confidențialității și pierderea datelor;**
  - **asigură protecția datelor împotriva riscurilor care decurg din gestionarea datelor, inclusiv gestionarea deficitară, precum și împotriva riscurilor legate de prelucrare și a erorii umane**.

Protecție și prevenire

- Ca parte a cadrului de gestionare a riscurilor TIC, entitățile financiare:
  - **elaborează și documentează o politică de securitate a informațiilor** care definește norme de protecție a disponibilității, autenticității, integrității și confidențialității datelor, a activelor informaționale și a activelor TIC, inclusiv a celor ale clienților lor, după caz;
  - **stabilesc,** urmând o abordare bazată pe riscuri, **o structură de gestionare solidă a rețelei și a infrastructurii** care utilizează tehnici, metode și protocoale adecvate ce pot include punerea în aplicare a unor mecanisme automatizate pentru a izola activele informaționale afectate în cazul unor atacuri cibernetice;
  - **pun în aplicare politici care limitează accesul fizic sau logic la activele informaționale și activele TIC** la ceea ce este necesar exclusiv pentru funcții și activități legitime și aprobate și stabilesc în acest scop un set de politici, proceduri și controale care să vizeze drepturile de acces și o bună administrare a acestora;
  - **pun în aplicare politici și protocoale pentru mecanisme solide de autentificare**, bazate pe standarde relevante și sisteme de control specifice, precum și măsuri de protecție a cheilor criptografice, prin care datele sunt criptate în funcție de rezultatele proceselor aprobate de clasificare a datelor și de evaluare a riscurilor TIC;
  - **pun în aplicare politici, proceduri și controale documentate pentru gestionarea modificărilor la nivelul TIC**, inclusiv modificări la nivelul componentelor software, hardware, firmware, parametrii sistemelor sau de securitate, care sunt fondate pe o abordare bazată pe evaluarea riscurilor și fac parte integrantă din procesul general de gestionare a modificărilor din cadrul entității financiare, pentru a se asigura că toate modificările aduse sistemelor TIC sunt înregistrate, testate, evaluate, aprobate, puse în aplicare și verificate în mod controlat;
  - **dispun de politici documentate adecvate și cuprinzătoare pentru corecții și actualizări.**

Detectare

- Entitățile financiare **dispun de mecanisme pentru detectarea rapidă a activităților anormale**, inclusiv a problemelor legate de performanța rețelei TIC și a incidentelor legate de TIC, precum și pentru identificarea posibilelor puncte unice de defecțiune semnificative.
- **Toate mecanismele de detectare sunt testate cu regularitate**.
- **Mecanismele de detectare** menționate mai sus **permit niveluri multiple de control, definesc praguri de alertă și criterii de declanșare și inițiere a proceselor de răspuns la incidentele legate de TIC**, inclusiv mecanisme de alertă automată pentru personalul relevant responsabil de răspunsul la incidentele legate de TIC.
- Entitățile financiare **alocă suficiente resurse și capacități pentru a monitoriza activitatea utilizatorilor, apariția anomaliilor TIC și a incidentelor legate de TIC**, în special a atacurilor cibernetice.

Răspuns și recuperare

- Entitățile financiare **instituie o politică cuprinzătoare de continuitate a activității TIC**, care poate fi adoptată sub forma unei politici specifice dedicate, ca parte integrantă a politicii generale de continuitate a activității a entității financiare.
- Entitățile financiare **pun în aplicare politica de continuitate a activității TIC prin măsuri, planuri, proceduri și mecanisme specifice, adecvate și documentate** care vizează:
  - **asigurarea continuității funcțiilor critice sau importante** ale entității financiare;
  - **un răspuns rapid, adecvat și eficace la toate incidentele legate de TIC și soluționarea tuturor acestor incidente**, într-un mod care să limiteze daunele și să acorde prioritate reluării activităților și acțiunilor de recuperare;
  - **activarea fără întârziere a unor planuri specifice care permit aplicarea unor măsuri, procese și tehnologii de limitare adecvat**e pentru fiecare tip de incident legat de TIC și previn producerea unor daune suplimentare, precum și a unor proceduri de răspuns și de recuperare adaptate;
  - **estimarea efectelor, a daunelor și a pierderilor preliminare**;
  - **stabilirea unor măsuri de comunicare și de gestionare a crizelor** care să asigure faptul că informațiile actualizate sunt transmise tuturor membrilor personalului intern relevant și părților interesate externe relevante și raportarea către autoritățile competente.

Răspuns și recuperare

- **Entitățile financiare pun în aplicare planuri de răspuns și de recuperare în domeniul TIC** care, în cazul altor entități financiare decât microîntreprinderile, sunt **supuse unor evaluări de audit intern independente.**
- **Entitățile financiare instituie, mențin și testează periodic planuri de continuitate a activității TIC adecvate, în special în ceea ce privește funcțiile critice sau importante externalizate sau contractate prin acorduri cu furnizori terți de servicii TIC**.
- Ca parte a politicii generale de continuitate a activității, **entitățile financiare efectuează o analiză a impactului asupra activității (AIA)** al expunerilor lor la perturbări grave ale activității.
- În conformitate cu AIA, entitățile financiare **evaluează impactul potențial al perturbărilor grave ale activității cu ajutorul unor criterii cantitative și calitative, utilizând date interne și externe și analize de scenarii**, după caz. AIA ia în considerare caracterul critic al funcțiilor operaționale identificate și cartografiate, al proceselor de sprijin, al dependențelor față de terți și al activelor informaționale, precum și interdependențele acestora.
- Entitățile financiare **se asigură că activele TIC și serviciile TIC sunt proiectate și utilizate în deplină conformitate cu AIA,** în special în ceea ce privește asigurarea în mod adecvat a redundanței tuturor componentelor critice.

Răspuns și recuperare

- Ca parte a gestionării lor cuprinzătoare a riscurilor TIC, entitățile financiare:
  - **testează planurile de continuitate a activității TIC și planurile de răspuns și de recuperare în domeniul** TIC în legătură cu sistemele TIC care sprijină toate funcțiile **cel puțin o dată pe an, precum și în caz de eventuale modificări substanțiale ale sistemelor TIC** care sprijină funcții critice sau importante;
  - **testează planurile de comunicare în situații de criză**.
- Entitățile financiare **își revizuiesc periodic politica de continuitate a activității TIC și planurile de răspuns și de recuperare în domeniul TIC**, ținând seama de rezultatele testelor efectuate, precum și de recomandările care decurg din evaluările de audit sau procesele de supraveghere.
- Entitățile financiare altele decât microîntreprinderile **au o funcție de gestionare a crizelor**, care, în caz de activare a planurilor lor de continuitate a activității TIC sau a planurilor lor de răspuns și de recuperare în domeniul TIC, **stabilește, printre altele, proceduri clare de gestionare a comunicărilor interne și externe în situații de criză**.
- Entitățile financiare **păstrează o evidență ușor accesibilă a activităților înainte și în timpul evenimentelor perturbatoare** atunci când sunt activate planurile lor de continuitate a activității TIC și planurile lor de răspuns și de recuperare în domeniul TIC.
- Entitățile financiare, altele decât microîntreprinderile, r**aportează autorităților competente, la cererea acestora, o estimare a costurilor și a pierderilor anuale agregate cauzate de incidente majore legate de TIC.**

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

- Pentru a asigura restaurarea sistemelor TIC și a datelor cu o perioadă de indisponibilitate minimă și o perturbare și o pierdere limitate, ca parte a cadrului lor de gestionare a riscurilor TIC, **entitățile financiare elaborează și documentează**:
  - **politici și proceduri privind copiile de rezervă** care precizează sfera de acoperire a datelor care fac obiectul copierii de rezervă, precum și frecvența minimă a copierii de rezervă, pe baza caracterului critic al informațiilor sau al nivelului de confidențialitate al datelor;
  - **proceduri și metode de restaurare și recuperare**.
- Entitățile financiare **instituie sisteme de rezervă care pot fi activate în conformitate cu politicile și procedurile privind copiile de rezervă, precum și cu procedurile și metodele de restaurare și recuperare**. Activarea sistemelor de rezervă nu pune în pericol securitatea rețelelor și a sistemelor informatice sau disponibilitatea, autenticitatea, integritatea ori confidențialitatea datelor. **Periodic se efectuează testarea procedurilor privind copiile de rezervă și a procedurilor și metodelor de restaurare și recuperare**.
- Atunci când restaurează date de rezervă pe baza sistemelor proprii, entitățile financiare utilizează sisteme TIC care sunt separate fizic și logic de sistemul TIC sursă. Sistemele TIC sunt securizate împotriva oricărui acces neautorizat sau a deteriorării TIC și permit restaurarea în timp util a serviciilor care utilizează copii de rezervă ale datelor și sistemelor, după caz.

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

- Entitățile financiare, altele decât microîntreprinderile, **mențin capacități TIC redundante dotate cu resurse, capacități și funcții care sunt adecvate pentru a acoperi nevoile operaționale.** Microîntreprinderile evaluează necesitatea menținerii unor astfel de capacități TIC redundante pe baza profilului lor de risc.
- Depozitarii centrali de titluri de valoare mențin cel puțin o unitate de prelucrare secundară, dotată cu resurse adecvate, capacități, funcții și resurse umane pentru a acoperi nevoile operaționale.
- **Pentru a stabili obiectivele cu privire la intervalele de timp și momentele de la care se pot recupera datele** în urma unei întreruperi și intervalele maxime de recuperare în urma unei întreruperi, pentru fiecare funcție, **entitățile financiare iau în considerare dacă este vorba de o funcție critică sau importantă și impactul potențial global asupra eficienței pieței**.
- **În cazul recuperării în urma unui incident legat de TIC**, **entitățile financiare efectuează verificări necesare, inclusiv verificări și reconcilieri multiple, pentru a se asigura că nivelul de integritate a datelor este cel mai ridicat.** Aceste verificări se efectuează, de asemenea, atunci când sunt reconstituite date de la părțile interesate externe, pentru a se asigura că toate datele sunt coerente între sisteme.

Învățăminte și perspective de dezvoltare

- Entitățile financiare **dispun de capacități și de personal pentru a colecta informații cu privire la vulnerabilități, amenințări cibernetice și incidente legate de TIC, în special atacuri cibernetice, și pentru a analiza impactul pe care acestea l-ar putea avea asupra rezilienței lor operaționale digitale**.
- Entitățile financiare **instituie verificări ulterioare incidentelor legate de TIC după ce un incident major** legat de TIC le perturbă activitățile de bază, **analizând cauzele perturbării și identificând îmbunătățirile necesare** pentru operațiunile TIC sau în cadrul politicii de continuitate a activității TIC
- Entitățile financiare, altele decât microîntreprinderile, comunică autorităților competente, la cerere, modificările care au fost operate în urma verificărilor ulterioare incidentelor legate de TIC, astfel cum sunt menționate la primul paragraf.
- Verificările ulterioare incidentelor legate de TIC **stabilesc dacă procedurile instituite au fost urmate și dacă măsurile luate au fost eficace**, inclusiv în ceea ce privește următoarele:
  - **promptitudinea reacției la alertele de securitate** și determinarea impactului și a gravității incidentelor legate de TIC;
  - **calitatea și rapiditatea efectuării unei analize judiciare**, acolo unde se consideră necesar;
  - **eficacitatea activării nivelurilor succesive de intervenție** (incident escalation) în caz de incidente în cadrul entității financiare;
  - **eficacitatea comunicării interne și externe**.
- Învățămintele desprinse în urma testării rezilienței operaționale digitale, precum și în urma incidentelor reale legate de TIC, în special a atacurilor cibernetice, alături de provocările întâmpinate la activarea planurilor de continuitate a activității TIC și a planurilor de răspuns și de recuperare în domeniul TIC, împreună cu informațiile relevante schimbate cu contrapărțile și evaluate în timpul proceselor de supraveghere, sunt încorporate în mod corespunzător și continuu în procesul de evaluare a riscurilor TIC. Constatările respective stau la baza unor revizuiri corespunzătoare ale componentelor relevante ale cadrului de gestionare a riscurilor TIC.

Învățăminte și perspective de dezvoltare

- Entitățile financiare **monitorizează eficacitatea punerii în aplicare a strategiei lor privind reziliența operațională digitală**. Acestea cartografiază evoluția riscurilor TIC de-a lungul timpului, analizează frecvența, tipurile, magnitudinea/amploarea și evoluția incidentelor legate de TIC, în special a atacurilor cibernetice și a modelelor lor, în vederea înțelegerii nivelului expunerii la riscurile TIC, în special în legătură cu funcțiile critice sau importante, și a consolidării gradului de maturitate și de pregătire cibernetică a entității financiare.
- **Personalul de nivel superior din domeniul TIC raportează cel puțin o dată pe an către organul de conducere cu privire la rezultatele desprinse în urma testării rezilienței operaționale digitale și propune recomandări.**
- Entitățile financiare **elaborează programe de conștientizare cu privire la securitatea TIC și cursuri de formare în domeniul rezilienței operaționale digitale** ca module obligatorii în cadrul programelor lor de formare a personalului. Respectivele programe și cursuri de formare se aplică tuturor angajaților și personalului de conducere de nivel superior și au un nivel de complexitate proporțional cu sfera de competență a funcțiilor lor. După caz, entitățile financiare includ, de asemenea, furnizorii terți de servicii TIC în programele lor de formare relevante.
- Entitățile financiare altele decât microîntreprinderile **monitorizează evoluțiile tehnologice relevante în mod continuu,** inclusiv pentru a înțelege posibilul impact al implementării unor astfel de noi tehnologii asupra cerințelor în materie de securitate TIC și a rezilienței operaționale digitale. Acestea trebuie să aibă informații actualizate cu privire la cele mai recente procese de gestionare a riscurilor TIC, cu scopul de a contracara cu eficacitate formele existente sau noi de atacuri cibernetice.

Comunicare

- Ca parte a cadrului de gestionare a riscurilor TIC entitățile financiare **instituie planuri de comunicare în situații de criză care permit o informare responsabilă a clienților și a contrapărților, precum și a publicului**, după caz, cu privire la, cel puțin, incidentele majore sau vulnerabilitățile legate de TIC.
- Entitățile financiare **pun în aplicare politici de comunicare pentru personalul intern și pentru părțile interesate externe**. Politicile de comunicare pentru personal țin seama de necesitatea de a face distincția între personalul implicat în gestionarea riscurilor TIC, în special personalul responsabil pentru răspuns și recuperare, și personalul care trebuie să fie informat.
- **Cel puțin o persoană din entitatea financiară este însărcinată cu punerea în aplicare a strategiei de comunicare pentru incidentele legate de TIC și îndeplinește în acest scop funcția de legătură cu publicul și mass-media**.

Procesul de gestionare a incidentelor legate de TIC

Procesul de gestionare a incidentelor legate de TIC

- Entitățile financiare **definesc, instituie și pun în aplicare un proces de gestionare a incidentelor legate de TIC pentru a detecta, a gestiona și a notifica incidentele legate de TIC.**
- Entitățile financiare **înregistrează toate incidentele legate de TIC și amenințările cibernetice semnificative**. Entitățile financiare **instituie proceduri și procese adecvate pentru a garanta monitorizarea, tratarea și urmărirea consecventă și integrată a incidentelor legate de TIC, pentru a asigura identificarea, documentarea și abordarea cauzelor lor principale**, astfel încât să se prevină apariția unor astfel de incidente.
- Procesul de gestionare a incidentelor legate de TIC:
  - **instituie indicatori de avertizare timpurie**;
  - **stabilește proceduri pentru identificarea, urmărirea, înregistrarea, indicarea categoriei și clasificarea incidentelor legate de TIC** în funcție de prioritatea și de gravitatea lor și în funcție de caracterul critic al serviciilor afectate, în conformitate cu criteriile stabilite;
  - **alocă roluri și responsabilități care trebuie activate pentru diferite tipuri și scenarii de incidente legate de TIC**;
  - **stabilește planuri pentru comunicarea cu personalul, cu părțile interesate externe și cu mass-media și pentru notificarea clienților**, proceduri interne de activare a nivelurilor succesive de intervenție (escalation), inclusiv în cazul unor plângeri din partea clienților legate de TIC, precum și pentru furnizarea de informații entităților financiare care acționează în calitate de contrapărți, după caz;
  - **asigură că cel puțin incidentele majore legate de TIC sunt raportate conducerii superioare relevante și informează organul de conducere cu privire la cel puțin incidentele majore legate de TIC**, explicând impactul, răspunsul și controalele suplimentare care urmează să fie instituite ca urmare a unor astfel de incidente legate de TIC;
  - **stabilește proceduri de răspuns la incidentele legate de TIC** în vederea atenuării efectelor și a asigurării faptului că serviciile devin operaționale și sigure în timp util.

Clasificarea incidentelor legate de TIC și a amenințărilor cibernetice

- Entitățile financiare **clasifică incidentele legate de TIC și determină impactul acestora pe baza următoarelor criterii:**
  - **numărul și/sau relevanța clienților sau a contrapărților financiare afectate** și, după caz, **cuantumul și numărul tranzacțiilor afectate de incidentul legat de TIC**, precum și eventualul impact al incidentului legat de TIC asupra reputației;
  - **durata incidentului legat de TIC**, inclusiv perioada de indisponibilitate a serviciului;
  - **întinderea geografică în ceea ce privește zonele afectate de incidentul legat de TIC**, în special în cazul în care acesta afectează mai mult de două state membre;
  - **pierderile de date pe care le implică incidentul legat de TIC**, în ceea ce privește disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor;
  - **caracterul critic al serviciilor afectate**, inclusiv al tranzacțiilor și operațiunilor entității financiare;
  - **impactul economic, în special costurile și pierderile directe și indirecte, ale incidentului legat de TIC**, în termeni atât absoluți, cât și relativi.
- Entitățile financiare **clasifică amenințările cibernetice ca fiind semnificative pe baza caracterului critic al serviciilor expuse riscului, inclusiv al tranzacțiilor și operațiunilor entității financiare, precum și pe baza numărului și/sau relevanței clienților sau a contrapărților financiare vizate și a întinderii geografice a zonelor expuse riscului.**

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

- **Entitățile financiare raportează incidentele majore legate de TIC autorității competente relevante.**
- Entitățile financiare **pot notifica, în mod voluntar, amenințările cibernetice semnificative către autoritatea competentă relevantă atunci când consideră că amenințarea este relevantă pentru sistemul financiar**, pentru utilizatorii serviciilor sau pentru clienți.
- **În cazul în care are loc un incident major legat de TIC care are un impact asupra intereselor financiare ale clienților lor, entitățile financiare îi informează pe aceștia**, fără întârzieri nejustificate, de îndată ce află despre incident, cu privire la producerea acestuia și la măsurile care au fost luate pentru a-i atenua efectele negative.

Cerințe generale pentru efectuarea testării rezilienței operaționale digitale

Cerințe generale pentru efectuarea testării rezilienței operaționale digitale

- În scopul evaluării nivelului de pregătire pentru gestionarea incidentelor legate de TIC, al identificării punctelor slabe, a deficiențelor și a lacunelor în ceea ce privește reziliența operațională digitală și al punerii în aplicare prompte a măsurilor corective, **entitățile financiare**, altele decât microîntreprinderile, **stabilesc, mențin și revizuiesc, un program solid și cuprinzător de testare a rezilienței operaționale digitale ca parte integrantă a cadrului de gestionare a riscurilor TIC**.
- **Programul de testare a rezilienței operaționale digitale include o serie de evaluări, teste, metodologii, practici și instrumente**.
- Atunci când desfășoară programul de testare a rezilienței operaționale digitale, entitățile financiare, altele decât microîntreprinderile, urmează o abordare bazată pe riscuri, ținând seama de principiul proporționalității și luând în considerare în mod corespunzător evoluția peisajului riscurilor TIC, orice riscuri specifice la care entitatea financiară în cauză este sau ar putea fi expusă, caracterul critic al activelor informaționale și al serviciilor furnizate, precum și orice alt factor pe care entitatea financiară îl consideră adecvat.
- Entitățile financiare, altele decât microîntreprinderile, **se asigură că testele sunt efectuate de părți independente, indiferent dacă sunt interne sau externe.** Atunci când testele sunt efectuate de o entitate internă, entitățile financiare alocă resurse suficiente și se asigură că sunt evitate conflictele de interese pe parcursul fazelor de proiectare și execuție ale testului.
- Entitățile financiare, altele decât întreprinderile, **stabilesc proceduri și politici care să prioritizeze, să clasifice și să remedieze toate aspectele identificate pe parcursul desfășurării testelor și stabilesc metodologii de validare internă** pentru a se asigura că toate punctele slabe, deficiențele sau lacunele identificate sunt abordate integral.
- Entitățile financiare, altele decât microîntreprinderile, **se asigură că se efectuează teste adecvate cel puțin o dată pe an asupra tuturor sistemelor și aplicațiilor TIC care sprijină funcții critice sau importante**.

Gestionarea riscurilor TIC generate de părți terțe

Gestionarea riscurilor TIC generate de părți terțe

- Entitățile financiare **gestionează riscurile TIC generate de părți terțe ca parte integrantă a riscurilor TIC în cadrul lor de gestionare a riscurilor TIC** în conformitate cu următoarele principii:
  - **entitățile financiare care au instituit acorduri contractuale pentru utilizarea serviciilor TIC în scopul desfășurării operațiunilor lor rămân în orice moment pe deplin responsabile de respectarea și de îndeplinirea tuturor obligațiilor**;
  - gestionarea de către entitățile financiare a riscurilor TIC generate de părți terțe este pusă în aplicare din perspectiva principiului proporționalității, luând în considerare:
    - natura, amploarea, complexitatea și importanța dependențelor legate de TIC;
    - riscurile care decurg din acordurile contractuale privind utilizarea serviciilor TIC încheiate cu furnizori terți de servicii TIC, ținând seama de caracterul critic sau importanța serviciului, procesului sau funcției respective, precum și de impactul potențial asupra continuității și disponibilității serviciilor și activităților financiare, la nivel individual și la nivel de grup.
- Entitățile financiare, altele decât entitățile cărora li se aplică cadrul simplificat și altele decât microîntreprinderile, **adoptă și revizuiesc periodic o strategie privind riscurile TIC generate de părți terțe, ținând seama de strategia privind existența mai multor furnizori.**
- Entitățile financiare **mențin și actualizează la nivel de entitate și la nivel subconsolidat și consolidat un registru de informații în legătură cu toate acordurile contractuale privind utilizarea serviciilor TIC oferite de furnizori terți de servicii TIC**. Acordurile contractuale sunt documentate în mod corespunzător, făcându-se distincția între cele care acoperă servicii TIC de sprijinire a funcțiilor critice sau importante și cele care nu le acoperă.
- Entitățile financiare **raportează cel puțin o dată pe an autorităților competente cu privire la numărul de noi acorduri privind utilizarea serviciilor TIC, categoriile de furnizori terți de servicii TIC, tipurile de acorduri contractuale și serviciile și funcțiile TIC care sunt oferite.**
- Entitățile financiare **pot încheia acorduri contractuale numai cu furnizori terți de servicii TIC care respectă standarde adecvate de securitate a informațiilor**. În cazul în care acordurile contractuale respective se referă la funcții critice sau importante, entitățile financiare, înainte de încheierea acordurilor, țin seama în mod corespunzător de utilizarea de către furnizorii terți de servicii TIC a celor mai recente și de cea mai înaltă calitate standarde de securitate a informațiilor.

Gestionarea riscurilor TIC generate de părți terțe

- În exercitarea drepturilor de acces, de inspecție și de audit **cu privire la furnizorul terț de servicii TIC**, entitățile financiare **stabilesc în prealabil, utilizând o abordare bazată pe riscuri, frecvența auditurilor și a inspecțiilor, precum și domeniile care urmează să fie auditate** prin aderarea la standardele de audit acceptate de comun acord, în concordanță cu instrucțiunile de supraveghere privind utilizarea și integrarea unor astfel de standarde de audit.
- **În cazul în care acordurile contractuale încheiate cu furnizori terți de servicii TIC privind utilizarea unor servicii TIC prezintă o complexitate tehnică ridicată**, entitatea financiară **verifică dacă auditorii, atât cei interni, cât și cei externi, sau un grup de auditori, dețin competențele și cunoștințele corespunzătoare pentru a efectua în mod eficace auditurile și evaluările relevante.**
- Entitățile financiare **se asigură că acordurile contractuale privind utilizarea serviciilor TIC pot fi reziliate în oricare dintre următoarele circumstanțe**:
  - **încălcarea semnificativă** de către furnizorul terț de servicii TIC a actelor cu putere de lege, **a reglementărilor sau a clauzelor contractuale aplicabile**;
  - **circumstanțe identificate** pe parcursul monitorizării riscurilor TIC generate de părți terțe **care sunt considerate capabile să modifice îndeplinirea funcțiilor oferite prin acordul contractual**, inclusiv modificările semnificative care afectează acordul sau situația furnizorului terț de servicii TIC;
  - **deficiențe demonstrate ale furnizorului terț de servicii TIC legate de gestionarea sa generală a riscurilor TIC** și, în special, legate de modul în care asigură disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor, fie date cu caracter personal sau date sensibile din alt punct de vedere, ori a datelor fără caracter personal;
  - **în cazul în care autoritatea competentă nu mai poate supraveghea în mod eficace entitatea financiară ca urmare a condițiilor acordului contractual respectiv sau a unor circumstanțe legate de acesta**.

Gestionarea riscurilor TIC generate de părți terțe

- **Pentru serviciile TIC care sprijină funcții critice sau importante, entitățile financiare instituie strategii de ieșire.** Strategiile de ieșire țin seama de riscurile care pot apărea la nivelul furnizorilor terți de servicii TIC, în special o posibilă deficiență din partea acestora, o deteriorare a calității serviciilor TIC oferite, orice perturbare a activității cauzată de furnizarea necorespunzătoare sau defectuoasă a serviciilor TIC sau orice riscuri semnificative care decurg din utilizarea adecvată și continuă a serviciului TIC respectiv ori încetarea acordurilor contractuale cu furnizorii terți de servicii TIC în oricare dintre situațiile enumerate anterior.
- **Entitățile financiare se asigură că pot să se retragă din acordurile contractuale fără:**
  - perturbarea activităților lor comerciale;
  - limitarea respectării cerințelor în materie de reglementare;
  - afectarea continuității și calității serviciilor furnizate către clienți.
- **Planurile de ieșire trebuie să fie cuprinzătoare, documentate și, în conformitate cu principiul proporționalității, trebuie să fie testate în mod suficient și revizuite periodic**.
- Entitățile financiare **identifică soluții alternative și dezvoltă planuri de tranziție care să le permită să elimine serviciile TIC contractate și datele relevante de la furnizorul terț de servicii TIC și să le transfere în condiții de siguranță și în integralitatea lo**r către furnizori alternativi sau să le reintegreze în sistemul propriu.

Evaluarea preliminară a riscului de concentrare a serviciilor TIC

- La identificarea și evaluarea riscurilor, entitățile **financiare iau în considerare, de asemenea, dacă încheierea preconizată a unui acord contractual în legătură cu servicii TIC care sprijină funcții critice sau importante ar conduce la oricare dintre următoarele situații**:
  - stabilirea unei relații contractuale cu un furnizor terț de servicii TIC care nu este ușor de înlocuit; sau
  - instituirea unor acorduri contractuale multiple cu privire la furnizarea de servicii TIC care sprijină funcții critice sau importante cu același furnizor terț de servicii TIC sau cu furnizori terți de servicii TIC strâns conectați.

Dispoziții contractuale esențiale

- **Drepturile și obligațiile care revin entității financiare și furnizorului terț de servicii TIC sunt clar atribuite și definite în scris**. Contractul complet include acordurile privind nivelul serviciilor și este consemnat într-un document scris care se află la dispoziția părților pe suport de hârtie sau într-un document având un alt format durabil, accesibil și care poate fi descărcat.
- **Acordurile contractuale privind utilizarea serviciilor TIC includ cel puțin următoarele elemente**:
  - **o descriere clară și completă a tuturor funcțiilor și serviciilor TIC** care urmează să fie furnizate de furnizorul terț de servicii TIC, **indicând dacă este permisă subcontractarea unui serviciu TIC care sprijină o funcție critică sau importantă sau părți semnificative ale acesteia** și, în caz afirmativ, condițiile aplicabile acestei subcontractări;
  - **locurile, și anume regiunile sau țările, în care urmează să fie furnizate funcțiile și serviciile TIC contractate sau subcontractate** și în care urmează să fie prelucrate datele, inclusiv locul stabilit pentru stocare, precum și cerința ca furnizorul terț de servicii TIC să informeze în prealabil entitatea financiară în cazul în care are în vedere modificarea acestor locuri;
  - **dispoziții privind disponibilitatea, autenticitatea, integritatea și confidențialitatea** în ceea ce privește protecția datelor, inclusiv a datelor cu caracter personal;
  - **dispoziții privind asigurarea accesului, a recuperării și a returnării într-un format ușor accesibil a datelor** cu caracter personal și a celor fără caracter personal prelucrate de entitatea financiară **în caz de insolvență, de rezoluție sau de încetare a activității furnizorului terț de servicii TIC sau în cazul încetării acordurilor contractuale**;
  - **descrieri la nivelul serviciilo**r, inclusiv actualizări și revizuiri ale acestora;
  - **obligația furnizorului terț de servicii TIC de a oferi asistență entității financiare fără costuri suplimentare sau la un cost stabilit ex ante**, atunci când survine un incident TIC care este legat de serviciul TIC furnizat entității financiare;
  - **obligația furnizorului terț de servicii TIC de a coopera pe deplin cu autoritățile competente și cu autoritățile de rezoluție ale entității financiare**, inclusiv cu persoanele numite de acestea;
  - **drepturile de încetare și perioadele minime de preaviz aferente pentru încetarea acordurilor contractuale**, în conformitate cu așteptările autorităților competente și ale autorităților de rezoluție;
  - **condițiile pentru participarea furnizorilor terți de servicii TIC la programele de conștientizare** cu privire la securitatea TIC ale entităților financiare și la cursurile de formare în domeniul rezilienței operaționale digitale.

Acorduri privind schimbul de informații referitoare la informații și date operative privind amenințările cibernetice

Acorduri privind schimbul de informații referitoare la informații și date operative privind amenințările cibernetice

- Entitățile financiare **pot face schimb reciproc de informații și date operative privind amenințările cibernetice**, inclusiv de indicatori de compromitere, tactici, tehnici și proceduri, alerte de securitate cibernetică și instrumente de configurare, în măsura în care aceste schimburi de informații și date operative:
  - vizează sporirea rezilienței operaționale digitale a entităților financiare, în special prin creșterea gradului de conștientizarea cu privire la amenințările cibernetice, limitarea sau împiedicarea capacității de propagare a amenințărilor cibernetice, sprijinirea capacităților de apărare, tehnicile de detectare a amenințărilor, strategiile de atenuare sau etapele proceselor de răspuns și de recuperare;
  - au loc în cadrul unor comunități de încredere ale entităților financiare;
  - sunt puse în aplicare prin intermediul unor acorduri privind schimbul de informații care protejează natura potențial sensibilă a informațiilor partajate și care sunt reglementate de norme de conduită care respectă pe deplin secretul comercial, protecția datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 și orientările privind politica în domeniul concurenței.
- Acordurile privind schimbul de informații definesc condițiile de participare și, după caz, stabilesc detaliile privind implicarea autorităților publice și calitatea în care acestea pot fi asociate la acordurile privind schimbul de informații, implicarea furnizorilor terți de servicii TIC și elementele operaționale, inclusiv utilizarea platformelor informatice specifice.
- Entitățile financiare **informează autoritățile competente cu privire la participarea lor la acordurile privind schimbul de informații, în momentul validării sau, după caz, al încetării participării lor**, odată ce aceasta începe să producă efecte.

DORA@ASFROMANIA.RO

Anexa 1 – *Standardele tehnice aprobate*

- ***Standardele tehnice cu termen de elaborare 12 luni (17 ianuarie 2024)*** – au fost aprobate, publicate:
  - RTS privind cadrul de gestionare a riscurilor TIC și a cadrului simplificat de gestionare a riscurilor TIC (conform art. 15 și art. 16 din Regulamentul DORA)
  - ITS cu privire la modele standard pentru Registrele de Informații cu privire la acordurile contractuale privind utilizarea serviciilor TIC oferite de furnizori terți de servicii TIC (conform art. 28 alin. (9) din Regulamentul DORA)
  - RTS cu privire la criteriile de clasificare a incidentelor majore legate de TIC și a amenințărilor cibernetice semnificative (conform art. 18 din Regulamentul DORA)
  - RTS pentru detalierea conținutului politicilor cu privire la utilizarea serviciilor TIC în legătură cu acordurile contractuale de utilizare a serviciilor TIC cu privire la funcții critice sau importante, oferite de furnizorii terți de servicii TIC (conform art. 28 alin. (10) din Regulamentul DORA)

Anexa II – *Standardele tehnice în curs de aprobare*

- ***Standardele tehnice cu termen de elaborare 18 luni (17 iulie 2024)*** –urmează procesul de aprobare de către cele trei ESAs și ulterior CE:
  - RTS cu privire la armonizarea continutului raportărilor cu privire la cu privire la incidentele majore legate de TIC si la amenințările cibernetice (conform art. 20 lit. a) din Regulamentul DORA)
  - ITS pentru stabilirea formularelor, modelelor și procedurilor standard pentru raportarea de către entitățile financiare a unui incident major legat de TIC (conform art. 20 lit. b) din Regulamentul DORA)
  - RTS pentru testarea avansată a instrumentelor, sistemelor și proceselor TIC cu ajutorul TLPT (conform art. 26 alin. (11) din Regulamentul DORA)
  - RTS pentru dispozițiile contractuale cuprinse în acordurile contractuale privind utilizarea serviciilor TIC (Specificarea elementelor suplimentare pe care o entitate financiară trebuie să le identifice și monitorizeze atunci când subcontractează funcții critice sau importante) (conform art.30 din Regulamentul DORA)
  - Ghid cu privire la cooperarea dintre ESAs și autoritățile competente, precum și detalii privind schimburile de informații (conform art. 32 alin. (7) din Regulamentul DORA)
  - RTS pentru armonizarea condițiilor care permit desfășurarea activității de supraveghere (conform art. 41 din Regulamentul DORA)
  - Ghid cu privire la calculele anuale agregate (pierderi și câștiguri) ca urmare a incidentelor majore legate de TIC (conform art. 11 alin. (11) din Regulamentul DORA)

Anexa III – Acte delegate

- Comisia Europeană, cu sprijinul ESA trebuie să emită până la același termen, 17 iulie 2024, următoarele (acte delegate, care vin în sprijinul clarificării prevederilor din cuprinsul Regulamentului) :
  - Act delegat pentru desemnarea furnizorilor terți esențiali de servicii TIC (conform art. 31 alin. (6) din Regulamentul DORA)
  - Act delegat pentru stabilirea taxelor de supraveghere percepute de supraveghetorul principal (conform art. 43 alin. (2) din Regulamentul DORA)