2024/1366

24.5.2024

# REGULAMENTUL DELEGAT (UE) 2024/1366 AL COMISIEI

## din 11 martie 2024

## de completare a Regulamentului (UE) 2019/943 al Parlamentului European și al Consiliului prin stabilirea unui cod de rețea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică

**(Text cu relevanță pentru SEE)**

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2019/943 al Parlamentului European și al Consiliului din 5 iunie 2019 privind piața internă de energie electrică ([1]), în special articolul 59 alineatul (2) litera (e),

întrucât:

(1) Gestionarea riscurilor în materie de securitate cibernetică este esențială pentru menținerea securității aprovizionării cu energie electrică și pentru asigurarea unui nivel ridicat de securitate cibernetică în sectorul energiei electrice.

(2) Digitalizarea și securitatea cibernetică sunt decisive pentru furnizarea serviciilor esențiale și, prin urmare, au o relevanță strategică pentru infrastructura energetică critică.

(3) Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului ([2]) stabilește măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune. Regulamentul (UE) 2019/941 al Parlamentului European și al Consiliului ([3]) completează Directiva (UE) 2022/2555 prin asigurarea faptului că incidentele de securitate cibernetică din sectorul energiei electrice sunt identificate în mod corespunzător ca un risc și că măsurile luate pentru a le aborda sunt integrate în mod corespunzător în planurile de pregătire pentru riscuri. Regulamentul (UE) 2019/943 completează Directiva (UE) 2022/2555 și Regulamentul (UE) 2019/941 prin stabilirea unor norme specifice pentru sectorul energiei electrice la nivelul Uniunii. În plus, prezentul regulament delegat completează dispozițiile Directivei (UE) 2022/2555 în ceea ce privește sectorul energiei electrice, ori de câte ori sunt vizate fluxurile transfrontaliere de energie electrică.

(4) În contextul sistemelor digitalizate interconectate de energie electrică, prevenirea și gestionarea crizelor de energie electrică legate de atacurile cibernetice nu pot fi considerate o sarcină exclusiv națională. Este necesară cooperarea la nivel regional și la nivelul Uniunii pentru a dezvolta la întregul lor potențial măsuri mai eficiente și mai puțin costisitoare. Prin urmare, este nevoie de un cadru comun de norme și de proceduri mai bine coordonate pentru a se asigura faptul că statele membre și alți actori sunt în măsură să coopereze în mod eficace la nivel transfrontalier, într-un spirit de transparență, de încredere și de solidaritate sporite între statele membre și autoritățile competente responsabile cu energia electrică și cu securitatea cibernetică.

(5) Gestionarea riscurilor în materie de securitate cibernetică aflate sub incidența prezentului regulament necesită un proces structurat care să includă, printre altele, identificarea riscurilor pentru fluxurile transfrontaliere de energie electrică generate de atacurile cibernetice, procesele și perimetrele operaționale aferente, controalele de securitate cibernetică și mecanismele de verificare corespunzătoare. Deși calendarul întregului proces este eșalonat pe mai mulți ani, fiecare etapă a acestuia ar trebui să contribuie la un nivel comun ridicat de securitate cibernetică în sector și la atenuarea riscurilor de securitate cibernetică. Toți participanții la proces ar trebui să depună toate eforturile pentru a elabora și a conveni asupra unor metodologii cât mai curând posibil, fără întârzieri nejustificate și, în orice caz, fără a depăși termenele stabilite în prezentul regulament.

([1]) JO L 158, 14.6.2019, p. 54.

([2]) 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).

([3]) Regulamentul (UE) 2019/941 al Parlamentului European și al Consiliului din 5 iunie 2019 privind pregătirea pentru riscuri în sectorul energiei electrice și de abrogare a Directivei 2005/89/CE (JO L 158, 14.6.2019, p. 1).

(6) Evaluările riscurilor în materie de securitate cibernetică la nivelul Uniunii, al statelor membre, al regiunilor și al entităților, menționate în prezentul regulament, pot fi limitate la cele care rezultă din atacurile cibernetice, astfel cum sunt definite în Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului ([4]), excluzând, prin urmare, de exemplu, atacurile fizice, dezastrele naturale și întreruperile cauzate de pierderea de instalații sau de resurse umane. Riscurile la nivelul întregii Uniuni și riscurile regionale legate de atacuri fizice sau de dezastre naturale în domeniul energiei electrice sunt deja reglementate de alte acte legislative existente ale Uniunii, inclusiv de articolul 5 din Regulamentul (UE) 2019/941 sau de Regulamentul (UE) 2017/1485 al Comisiei ([5]) de stabilire a unei linii directoare privind operarea sistemului de transport al energiei electrice. În mod similar, Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului ([6]) privind reziliența entităților critice urmărește să reducă vulnerabilitățile și să consolideze reziliența fizică a entităților critice și acoperă toate riscurile relevante, atât pe cele naturale, cât și pe cele provocate de om, care pot afecta furnizarea serviciilor esențiale, inclusiv accidentele, dezastrele naturale, urgențele de sănătate publică, cum ar fi pandemiile, amenințările hibride sau alte amenințări antagoniste, inclusiv infracțiunile de terorism, infiltrarea unor elemente infracționale și sabotajul.

(7) Noțiunile de „entități cu impact ridicat” și „entități cu impact critic” din prezentul regulament sunt fundamentale pentru definirea sferei entităților care vor face obiectul obligațiilor descrise în prezentul regulament. Abordarea bazată pe riscuri descrisă în diferitele dispoziții urmărește să identifice procesele, activele de sprijin și entitățile care le exploatează și care afectează fluxurile transfrontaliere de energie electrică. În funcție de gradul de impact al unor eventuale atacuri cibernetice asupra operațiunilor lor legate de fluxurile transfrontaliere de energie electrică, aceste entități pot fi considerate „cu impact ridicat” sau „cu impact critic”. Articolul 3 din Directiva (UE) 2022/2555 stabilește noțiunile de entități esențiale și entități importante, precum și criteriile de identificare a entităților din aceste categorii. Deși multe dintre acestea vor fi considerate și identificate simultan ca fiind „esențiale” în sensul articolului 3 din Directiva (UE) 2022/2555 și „cu impact ridicat” sau „cu impact critic” în temeiul articolului 24 din prezentul regulament, criteriile stabilite în prezentul regulament se referă numai la rolul și la impactul lor în cadrul proceselor de energie electrică ce afectează fluxurile transfrontaliere, fără a lua în considerare criteriile definite la articolul 3 din Directiva (UE) 2022/2555.

(8) Entitățile aflate sub incidența prezentului regulament care sunt considerate cu impact ridicat sau cu impact critic în temeiul articolului 24 din prezentul regulament și care fac obiectul obligațiilor prevăzute în acesta sunt în primul rând entitățile care au un impact direct asupra fluxurilor transfrontaliere de energie electrică din UE.

(9) Prezentul regulament utilizează mecanismele și instrumentele existente, deja stabilite în alte acte legislative, pentru a asigura eficiența și a evita suprapunerile în atingerea obiectivelor.

(10) Atunci când aplică prezentul regulament, statele membre, autoritățile competente și operatorii de sisteme ar trebui să ia în considerare standardele europene și specificațiile tehnice convenite ale organizațiilor europene de standardizare și să acționeze în conformitate cu legislația Uniunii referitoare la introducerea pe piață sau la punerea în funcțiune a produselor care fac obiectul legislației respective a Uniunii.

([4]) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).

([5]) Regulamentul (UE) 2017/1485 al Comisiei din 2 august 2017 de stabilire a unei linii directoare privind operarea sistemului de transport al energiei electrice (JO L 220, 25.8.2017, p. 1).

([6]) Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului (JO L 333, 27.12.2022, p. 164).

(11) În vederea atenuării riscurilor în materie de securitate cibernetică, este necesar să se stabilească un cadru de reglementare detaliat, care să vizeze atât acțiunile părților interesate relevante ale căror activități au ca obiect aspecte legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică, cât și cooperarea dintre respectivele părți interesate, cu scopul de a asigura securitatea sistemului. Aceste norme organizatorice și tehnice ar trebui să asigure un tratament eficace, la nivel operațional, al majorității incidentelor din sectorul energiei electrice ale căror cauze principale sunt legate de securitatea cibernetică. Este necesar să se stabilească ce anume ar trebui să facă părțile interesate relevante pentru a preveni astfel de crize și ce măsuri pot lua în cazul în care normele privind funcționarea sistemului nu mai sunt suficiente. Prin urmare, este necesar să se stabilească un cadru comun de norme cu privire la modul de prevenire, de pregătire și de gestionare a crizelor simultane de energie electrică a căror cauză principală este legată de securitatea cibernetică. Acest lucru aduce mai multă transparență în etapa de pregătire și în timpul unei crize simultane de energie electrică și asigură faptul că măsurile sunt luate în mod coordonat și eficace, împreună cu autoritățile competente în domeniul securității cibernetice din statele membre. Statele membre și entitățile relevante ar trebui să aibă obligația de a coopera, la nivel regional și, după caz, la nivel bilateral, într-un spirit de solidaritate. Această cooperare și aceste norme sunt menite să asigure o mai bună pregătire pentru riscurile în materie de securitate cibernetică la un cost mai mic, în conformitate și cu obiectivele Directiva (UE) 2022/2555. De asemenea, pare necesar să se consolideze piața internă a energiei electrice prin creșterea nivelului de încredere în rândul statelor membre, în special prin atenuarea riscului de restricționare nejustificată a fluxurilor transfrontaliere de energie electrică, ceea ce va reduce riscul unor efecte colaterale negative asupra statelor membre învecinate.

(12) Siguranța alimentării cu energie electrică implică o cooperare eficace între statele membre, instituțiile, organismele, oficiile și agențiile Uniunii și părțile interesate relevante. Operatorii de sisteme de distribuție și operatorii de sisteme de transport joacă un rol esențial în asigurarea unui sistem de energie electrică sigur, fiabil și eficient, în conformitate cu articolele 31 și 40 din Directiva (UE) 2019/944 a Parlamentului European și a Consiliului ([7]). Diferitele autorități de reglementare și alte autorități naționale competente relevante joacă, de asemenea, un rol important în asigurarea și monitorizarea securității cibernetice în cadrul aprovizionării cu energie electrică, ca parte a sarcinilor care le revin în temeiul Directivelor (UE) 2019/944 și (UE) 2022/2555. Statele membre ar trebui să desemneze o entitate existentă sau una nouă drept autoritatea lor națională competentă pentru punerea în aplicare a prezentului regulament, cu scopul de a asigura participarea transparentă și incluzivă a tuturor actorilor implicați, pregătirea eficientă și punerea în aplicare corespunzătoare a prezentului regulament, cooperarea dintre diferitele părți interesate relevante și autoritățile competente din domeniul energiei electrice și al securității cibernetice, precum și facilitarea prevenirii și a evaluării *ex post* a crizelor de energie electrică ale căror cauze principale sunt legate de securitatea cibernetică, dar și a schimburilor de informații în legătură cu acestea.

(13) În cazul în care o entitate cu impact ridicat sau o entitate cu impact critic furnizează servicii în mai multe state membre sau are sediul sau un alt loc de desfășurare a activității ori un reprezentant într-un stat membru, dar rețelele și sistemele sale informatice sunt situate în unul sau mai multe alte state membre, statele membre în cauză ar trebui să își încurajeze autoritățile competente respective să depună toate eforturile pentru a coopera și a se sprijini reciproc, în funcție de necesități.

(14) Statele membre ar trebui să se asigure că autoritățile competente dispun de competențele necesare, în legătură cu entitățile cu impact ridicat și cu entitățile cu impact critic, pentru a promova respectarea prezentului regulament. Competențele respective ar trebui să le permită autorităților competente să efectueze inspecții la fața locului și activități de supraveghere în afara amplasamentului. Acestea pot include verificări aleatorii, efectuarea unor audituri periodice, a unor audituri de securitate specifice bazate pe evaluări ale riscurilor sau pe informațiile și pe scanările de securitate disponibile legate de riscuri, bazate pe criterii obiective, nediscriminatorii, echitabile și transparente de evaluare a riscurilor și care includ solicitarea informațiilor necesare pentru evaluarea măsurilor de securitate cibernetică adoptate de entitate. Informațiile respective ar trebui să includă politici documentate în materie de securitate cibernetică, date de acces, documente sau orice informații necesare pentru îndeplinirea sarcinilor lor de supraveghere, precum și dovezi ale punerii în aplicare a politicilor de securitate cibernetică, cum ar fi rezultatele auditurilor de securitate efectuate de un auditor calificat și dovezile subiacente corespunzătoare.

([7]) Directiva (UE) 2019/944 a Parlamentului European și a Consiliului din 5 iunie 2019 privind normele comune pentru piața internă de energie electrică și de modificare a Directivei 2012/27/UE (JO L 158, 14.6.2019, p. 125).

(15) Pentru a evita decalajele sau duplicările obligațiilor privind gestionarea riscurilor în materie de securitate cibernetică impuse entităților cu impact ridicat și celor cu impact critic, autoritățile naționale în temeiul Directivei (UE) 2022/2555 și autoritățile competente în temeiul prezentului regulament ar trebui să coopereze în ceea ce privește punerea în aplicare a măsurilor de gestionare a riscurilor în materie de securitate cibernetică și supravegherea respectării acestor măsuri la nivel național. Respectarea de către o entitate a cerințelor de gestionare a riscurilor în materie de securitate cibernetică prevăzute în prezentul regulament ar putea fi considerată de autoritățile competente în temeiul Directivei (UE) 2022/2555 drept respectare a cerințelor corespunzătoare prevăzute în directiva respectivă sau viceversa.

(16) O abordare comună a prevenirii și gestionării simultane a crizelor de energie electrică necesită o înțelegere comună între statele membre cu privire la ce anume constituie o criză simultană de energie electrică și la momentul în care un atac cibernetic devine un factor important în contextul crizei respective. În special, ar trebui facilitată coordonarea dintre statele membre și entitățile relevante în scopul abordării unei situații în care este prezent sau iminent riscul potențial de deficit semnificativ de energie electrică sau imposibilitatea de a furniza energie electrică clienților, iar acest lucru se datorează unui atac cibernetic.

(17) Considerentul (1) din Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului ([8]) recunoaște rolul vital al rețelelor și al sistemelor informatice, precum și al rețelelor și serviciilor de comunicații electronice în menținerea funcționării economiei în sectoare-cheie cum ar fi energia, în timp ce considerentul 44 explică faptul că Agenția Uniunii Europene pentru Securitate Cibernetică („ENISA”) ar trebui să colaboreze cu Agenția Uniunii Europene pentru Cooperarea Autorităților de Reglementare din Domeniul Energiei („ACER”).

(18) Regulamentul (UE) 2019/943 atribuie responsabilități specifice în ceea ce privește securitatea cibernetică operatorilor de sisteme de transport („OST”) și operatorilor de sisteme de distribuție („OSD”). Asociațiile lor europene, și anume Rețeaua europeană a operatorilor de sisteme de transport de energie electrică („ENTSO pentru energie electrică”) și entitatea europeană pentru OSD („entitatea OSD UE”), promovează securitatea cibernetică, în temeiul articolelor 30 și, respectiv, 55 din regulamentul menționat anterior, în cooperare cu autoritățile relevante și cu entitățile reglementate.

(19) O abordare comună în ceea ce privește prevenirea și gestionarea crizelor simultane de energie electrică ale căror cauze principale sunt legate de securitatea cibernetică impune, de asemenea, ca toate părțile interesate relevante să utilizeze metode și definiții armonizate pentru a identifica riscurile legate de securitatea cibernetică a aprovizionării cu energie electrică. De asemenea, este necesar ca părțile respective să aibă capacitatea de a compara efectiv performanțele lor din acest domeniu cu cele ale vecinilor lor. Prin urmare, este necesar să se stabilească procesele, rolurile și responsabilitățile pentru a elabora și a actualiza metodologii de gestionare a riscurilor, grile de clasificare a incidentelor și măsuri de securitate cibernetică adaptate la riscurile în materie de securitate cibernetică ce afectează fluxurile transfrontaliere de energie electrică.

(20) Statele membre, prin intermediul autorității competente desemnate pentru prezentul regulament, sunt responsabile cu identificarea entităților care îndeplinesc criteriile pentru a se califica drept entități cu impact ridicat și entități cu impact critic. Pentru a elimina divergențele dintre statele membre în această privință și pentru a garanta securitatea juridică în ceea ce privește măsurile de gestionare a riscurilor în materie de securitate cibernetică și obligațiile de raportare pentru toate entitățile relevante, ar trebui stabilit un set de criterii pentru a identifica entitățile care intră sub incidența prezentului regulament. Acest set de criterii ar trebui să fie definit și să fie actualizat periodic prin intermediul procesului de elaborare și de adoptare a termenilor, condițiilor și metodologiilor prevăzute în prezentul regulament.

(21) Dispozițiile prezentului regulament trebuie să nu aducă atingere dreptului Uniunii care prevede norme specifice privind certificarea produselor din domeniul tehnologiei informației și comunicațiilor („TIC”), a serviciilor TIC și a proceselor TIC, în special să nu aducă atingere Regulamentul (UE) 2019/881 în ceea ce privește cadrul pentru instituirea sistemelor europene de certificare a securității cibernetice. În contextul prezentului regulament, produsele TIC ar trebui să includă, de asemenea, dispozitive tehnice și software care să permită interacțiunea directă cu rețeaua electrotehnică, în special sisteme industriale de control care pot fi utilizate pentru transportul, distribuția și producția de energie, precum și pentru colectarea și transmiterea informațiilor conexe. Dispozițiile ar trebui să garanteze că produsele TIC, serviciile TIC și procesele TIC care urmează să fie achiziționate îndeplinesc obiectivele de securitate relevante prevăzute la articolul 51 din Regulamentul (UE) 2019/881.

([8]) Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 15).

(22) Atacurile cibernetice recente arată că entitățile devin tot mai frecvent ținta atacurilor asupra lanțurilor de aprovizionare. Aceste atacuri asupra lanțurilor de aprovizionare nu numai că au un impact asupra entităților individuale incluse în domeniul de aplicare, dar pot avea și un efect de cascadă asupra unor atacuri de mai mare amploare asupra entităților cu care sunt conectate acestea în rețeaua de energie electrică. Prin urmare, au fost adăugate dispoziții și recomandări pentru a contribui la atenuarea riscurilor în materie de securitate cibernetică asociate proceselor legate de lanțul de aprovizionare, în special achizițiile publice, cu impact asupra fluxurilor transfrontaliere de energie electrică.

(23) Întrucât exploatarea vulnerabilităților rețelelor și ale sistemelor informatice poate produce perturbări semnificative în sectorul energetic și prejudicii pentru economie și consumatori, aceste vulnerabilități ar trebui identificate și remediate rapid în vederea reducerii riscurilor. Pentru a facilita punerea în aplicare eficace a prezentului regulament, entitățile relevante și autoritățile competente ar trebui să coopereze pentru a face exerciții și a testa activități considerate adecvate în acest scop, inclusiv schimbul de informații privind amenințările cibernetice, atacurile cibernetice, vulnerabilitățile, instrumentele și metodele, tacticile, tehnicile și procedurile, pregătirea pentru gestionarea crizelor de securitate cibernetică și alte exerciții. Întrucât tehnologia evoluează constant, iar digitalizarea sectorului energiei electrice progresează rapid, punerea în aplicare a dispozițiilor adoptate nu ar trebui să se facă în detrimentul inovării și nu ar trebui să reprezinte un obstacol pentru accesul la piața energiei electrice și nici pentru utilizarea ulterioară a soluțiilor inovatoare care contribuie la eficiența și sustenabilitatea sistemului de energie electrică.

(24) Informațiile colectate în vederea monitorizării punerii în aplicare a prezentului regulament ar trebui limitate în mod rezonabil pe baza principiului necesității de a cunoaște. Părților interesate ar trebui să li se acorde termene realizabile și eficace pentru transmiterea acestor informații. Ar trebui evitată dubla notificare.

(25) Protecția securității cibernetice nu se oprește la frontierele Uniunii. Un sistem securizat necesită implicarea țărilor terțe învecinate. Uniunea și statele sale membre ar trebui să depună eforturi pentru a sprijini țările terțe învecinate a căror infrastructură de energie electrică este conectată la rețeaua europeană să aplice norme similare în materie de securitate cibernetică cu cele prevăzute în prezentul regulament.

(26) Pentru a îmbunătăți din timp coordonarea în materie de securitate și pentru a testa termenii, condițiile și metodologiile care vor deveni obligatorii în viitor, ENTSO pentru energie electrică, entitatea OSD UE și autoritățile competente ar trebui să înceapă să elaboreze orientări fără caracter obligatoriu imediat după intrarea în vigoare a prezentului regulament. Aceste orientări vor servi drept bază pentru elaborarea termenilor, condițiilor și metodologiilor viitoare. În paralel, autoritățile competente ar trebui să identifice entitățile care ar putea fi considerate drept entități cu impact ridicat și entități cu impact critic, pentru a începe, în mod voluntar, îndeplinirea obligațiilor.

(27) Prezentul regulament a fost elaborat în strânsă cooperare cu ACER, ENISA, ENTSO pentru energie electrică, entitatea OSD UE și alte părți interesate, în vederea adoptării unor norme eficace, echilibrate și proporționale într-un mod transparent și participativ.

(28) Prezentul regulament completează și consolidează măsurile de gestionare a crizelor stabilite în Cadrul UE de răspuns la crizele de securitate cibernetică, în conformitate cu Recomandarea (UE) 2017/1584 a Comisiei ([9]). Un atac cibernetic ar putea, de asemenea, să provoace, să contribuie la sau să coincidă cu o criză de energie electrică, astfel cum este definită la articolul 2 punctul 9 din Regulamentul (UE) 2019/941, care afectează fluxurile transfrontaliere de energie electrică. Respectiva criză de energie electrică ar putea conduce la o criză simultană de energie electrică, astfel cum este definită la articolul 2 punctul 10 din Regulamentul (UE) 2019/941. Un astfel de incident ar putea avea, de asemenea, un impact asupra altor sectoare care depind de securitatea aprovizionării cu energie electrică. În cazul în care un astfel de incident se intensifică și devine un incident de securitate cibernetică de mare amploare în sensul articolului 16 din Directiva (UE) 2022/2555, ar trebui să se aplice dispozițiile din articolul respectiv care instituie Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice („EU-CyCLONe"). Pentru gestionarea crizelor la nivelul Uniunii, părțile relevante ar trebui să se bazeze pe mecanismul integrat al Uniunii pentru un răspuns politic la crize (mecanismul „IPCR") în temeiul Deciziei de punere în aplicare (UE) 2018/1993 a Consiliului ([10]).

(29) Prezentul regulament nu aduce atingere competenței statelor membre de a lua măsurile necesare pentru a asigura protecția intereselor lor esențiale în materie de securitate, pentru a apăra ordinea și siguranța publică și pentru a permite investigarea, detectarea și urmărirea infracțiunilor, în conformitate cu legislația Uniunii. În conformitate cu articolul 346 din TFUE, niciun stat membru nu are obligația de a furniza informații a căror divulgare o consideră contrară intereselor esențiale ale siguranței sale.

([9]) Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare (JO L 239, 19.9.2017, p. 36).

([10]) Decizia de punere în aplicare (UE) 2018/1993 a Consiliului din 11 decembrie 2018 privind mecanismul integrat al Uniunii pentru un răspuns politic la crize (JO L 320, 17.12.2018, p. 28).

(30) Deși prezentul regulament se aplică, în principiu, entităților care desfășoară activități în domeniul producției de energie electrică în centrale nucleare, unele dintre activitățile respective pot fi legate de securitatea națională.

(31) Legislația Uniunii privind protecția datelor și legislația Uniunii privind protecția confidențialității ar trebui să se aplice oricărei forme de prelucrare a datelor cu caracter personal în temeiul prezentului regulament. În special, prezentul regulament nu aduce atingere Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului ([11]), Directivei 2002/58/CE a Parlamentului European și a Consiliului ([12]) și Regulamentului (UE) 2018/1725 al Parlamentului European și al Consiliului ([13]). Prin urmare, prezentul regulament ar trebui să nu aducă atingere, printre altele, sarcinilor și competențelor autorităților competente de a monitoriza respectarea legislației aplicabile a Uniunii privind protecția datelor și privind protecția confidențialității.

(32) Având în vedere importanța cooperării internaționale în materie de securitate cibernetică, autoritățile competente responsabile cu îndeplinirea sarcinilor care le-au fost atribuite în temeiul prezentului regulament și desemnate de statele membre ar trebui să poată participa la rețelele de cooperare internațională. Prin urmare, în scopul îndeplinirii sarcinilor care le revin, autoritățile competente ar trebui să fie în măsură să facă schimb de informații, inclusiv de date cu caracter personal, cu autoritățile competente din țări terțe, cu condiția să fie îndeplinite condițiile prevăzute în legislația Uniunii privind protecția datelor pentru transferurile de date cu caracter personal către țări terțe, printre altele cele prevăzute la articolul 49 din Regulamentul (UE) 2016/679.

(33) Prelucrarea datelor cu caracter personal, în măsura necesară și proporțională în scopul asigurării securității activelor de către entitățile cu impact ridicat și entitățile cu impact critic, ar putea fi considerată legală pe baza faptului că o astfel de prelucrare respectă o obligație legală care îi revine operatorului, în conformitate cu cerințele de la articolul 6 alineatul (1) litera (c) și de la articolul 6 alineatul (3) din Regulamentul (UE) 2016/679. Prelucrarea datelor cu caracter personal poate fi, de asemenea, necesară pentru interesele legitime urmărite de entitățile cu impact ridicat și de entitățile cu impact critic, precum și de furnizorii de tehnologii și servicii de securitate care acționează în numele acestor entități, în temeiul articolului 6 alineatul (1) litera (f) din Regulamentul (UE) 2016/679, inclusiv în cazul în care o astfel de prelucrare este necesară pentru acordurile privind schimbul de informații în materie de securitate cibernetică sau pentru notificarea voluntară a informațiilor relevante în conformitate cu prezentul regulament. Măsurile legate de prevenirea, detectarea, identificarea, limitarea, analizarea și combaterea atacurilor cibernetice, măsurile de sensibilizare cu privire la amenințări cibernetice specifice, schimbul de informații în contextul remedierii vulnerabilităților și al divulgării coordonate a vulnerabilităților, schimbul voluntar de informații cu privire la atacurile cibernetice respective, precum și la amenințările și vulnerabilitățile cibernetice, indicatorii de compromitere, tacticile, tehnicile și procedurile, alertele de securitate cibernetică și instrumentele de configurare pot necesita prelucrarea anumitor categorii de date cu caracter personal, cum ar fi adrese IP, localizatoare uniforme de resurse (URL), nume de domenii, adrese de e-mail și, în cazul în care acestea dezvăluie date cu caracter personal, marcaje temporale. Prelucrarea datelor cu caracter personal de către autoritățile competente, punctele unice de contact și echipele CSIRT poate constitui o obligație legală sau poate fi considerată necesară pentru îndeplinirea unei sarcini de interes public sau în exercitarea autorității publice cu care este învestit operatorul de date în temeiul articolului 6 alineatul (1) litera (c) sau (e) și al articolului 6 alineatul (3) din Regulamentul (UE) 2016/679 sau pentru urmărirea unui interes legitim al entităților cu impact ridicat și al entităților cu impact critic, astfel cum se menționează la articolul 6 alineatul (1) litera (f) din respectivul regulament. În plus, legislația națională poate stabili norme care să permită autorităților competente, punctelor unice de contact și echipelor CSIRT, în măsura în care acest lucru este necesar și proporțional pentru a asigura securitatea rețelelor și a sistemelor informatice ale entităților cu impact ridicat sau ale entităților cu impact critic, să prelucreze categorii speciale de date cu caracter personal în conformitate cu articolul 9 din Regulamentul (UE) 2016/679, în special prin prevederea unor măsuri adecvate și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanelor fizice, inclusiv limitări tehnice privind reutilizarea acestor date și utilizarea unor măsuri de ultimă generație de securitate și de protejare a confidențialității, cum ar fi pseudonimizarea sau criptarea, în cazul în care anonimizarea poate afecta în mod semnificativ scopul urmărit.

([11]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

([12]) Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37).

([13]) 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).

(34) În multe cazuri, datele cu caracter personal sunt compromise în urma unor atacuri cibernetice. În acest context, autoritățile competente ar trebui să coopereze și să facă schimb de informații cu privire la toate aspectele relevante cu autoritățile menționate în Regulamentul (UE) 2016/679 și în Directiva 2002/58/CE.

(35) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 și a emis un aviz la 17 noiembrie 2023,

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

**DISPOZIȚII GENERALE**

*Articolul 1*

**Obiect**

Prezentul regulament stabilește un cod de rețea care prevede norme sectoriale specifice pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică, inclusiv norme privind cerințele minime comune, planificarea, monitorizarea, raportarea și gestionarea crizelor.

*Articolul 2*

**Domeniu de aplicare**

(1) Prezentul regulament se aplică aspectelor legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică în cadrul activităților următoarelor entități, dacă acestea sunt identificate ca entități cu impact ridicat sau ca entități cu impact critic în conformitate cu articolul 24:

(a) întreprinderi din domeniul energiei electrice, în sensul definiției de la articolul 2 punctul 57 din Directiva (UE) 2019/944;

(b) operatori ai pieței de energie electrică desemnați („OPEED”), în sensul definiției de la articolul 2 punctul 8 din Regulamentul (UE) 2019/943;

(c) „piețe organizate”, astfel cum sunt definite la articolul 2 punctul 4 din Regulamentul de punere în aplicare (UE) nr. 1348/2014 al Comisiei ([14]), care organizează tranzacții cu produse relevante pentru fluxurile transfrontaliere de energie electrică;

(d) furnizorii critici de servicii TIC, astfel cum sunt menționați la articolul 3 punctul 9 din prezentul regulament;

(e) ENTSO pentru energie electrică, instituită în temeiul articolului 28 din Regulamentul (UE) 2019/943;

(f) entitatea OSD UE, instituită în temeiul articolului 52 din Regulamentul (UE) 2019/943;

(g) părțile responsabile cu echilibrarea, în sensul definiției de la articolul 2 punctul 14 din Regulamentul (UE) 2019/943;

(h) operatorii unui punct de reîncărcare, astfel cum sunt definiți în anexa I la Directiva (UE) 2022/2555;

(i) centrele de coordonare regionale, instituite în temeiul articolului 35 din Regulamentul (UE) 2019/943;

(j) furnizorii de servicii de securitate gestionate, în sensul definiției de la articolul 6 punctul 40 din Directiva (UE) 2022/2555;

(k) orice altă entitate sau terț căruia i-au fost delegate sau atribuite responsabilități în temeiul prezentului regulament.

(2) Următoarele autorități sunt responsabile, în cadrul mandatelor lor actuale, cu îndeplinirea sarcinilor atribuite prin prezentul regulament:

(a) Agenția Uniunii Europene pentru Cooperarea Autorităților de Reglementare din Domeniul Energiei („ACER”), instituită prin Regulamentul (UE) 2019/942 al Parlamentului European și al Consiliului ([15]);

(b) autoritățile naționale competente responsabile cu îndeplinirea sarcinilor care le-au fost atribuite în temeiul prezentului regulament și desemnate de statele membre în temeiul articolului 4 sau „autorității competente”;

(c) autoritățile naționale de reglementare (denumite în continuare „ANR”) desemnate de fiecare stat membru în temeiul articolului 57 alineatul (1) din Directiva (UE) 2019/944;

([14]) Regulamentul de punere în aplicare (UE) nr. 1348/2014 al Comisiei din 17 decembrie 2014 privind raportarea de date, pentru punerea în aplicare a articolului 8 alineatele (2) și (6) din Regulamentul (UE) nr. 1227/2011 al Parlamentului European și al Consiliului privind integritatea și transparența pieței angro de energie (JO L 363, 18.12.2014, p. 121).

([15]) Regulamentul (UE) 2019/942 al Parlamentului European și al Consiliului din 5 iunie 2019 de instituire a Agenției Uniunii Europene pentru Cooperarea Autorităților de Reglementare din Domeniul Energiei (JO L 158, 14.6.2019, p. 22).

(d) autoritățile competente în domeniul pregătirii pentru riscuri („ANC-PR”), instituite în temeiul articolului 3 din Regulamentul (UE) 2019/941;

(e) echipele de intervenție în caz de incidente de securitate informatică („echipele CSIRT”), desemnate sau instituite în temeiul articolului 10 din Directiva (UE) 2022/2555;

(f) autoritățile competente responsabile cu securitatea cibernetică („ANC-SC”), desemnate sau instituite în temeiul articolului 8 din Directiva (UE) 2022/2555;

(g) Agenția Uniunii Europene pentru Securitate Cibernetică, instituită în temeiul Regulamentului (UE) 2019/881;

(h) orice alte autorități sau orice alți terți cărora li s-au delegat sau li s-au atribuit responsabilități în temeiul articolului 4 alineatul (3).

(3) Prezentul regulament se aplică, de asemenea, tuturor entităților care nu sunt stabilite în Uniune, dar care furnizează servicii unor entități din Uniune, cu condiția ca acestea să fi fost identificate ca entități cu impact ridicat sau ca entități cu impact critic de către autoritățile competente în conformitate cu articolul 24 alineatul (2).

(4) Prezentul regulament nu aduce atingere responsabilității statelor membre de a proteja securitatea națională și nici competenței acestora de a proteja alte funcții esențiale ale statului, inclusiv asigurarea integrității teritoriale a statului și menținerea ordinii publice.

(5) Prezentul regulament nu aduce atingere responsabilității statelor membre de a proteja securitatea națională în ceea ce privește activitățile de producție a energiei electrice în centralele nucleare, inclusiv activitățile din cadrul lanțului valoric nuclear, în conformitate cu tratatele.

(6) Entitățile, autoritățile competente, punctele unice de contact de la nivelul entităților și echipele CSIRT prelucrează datele cu caracter personal în măsura necesară pentru scopurile prezentului regulament și în conformitate cu Regulamentul (UE) 2016/679; în special această prelucrare se bazează pe articolul 6 din respectivul regulament.

*Articolul 3*

**Definiții**

Se aplică următoarele definiții:

1. „activ” înseamnă orice informații, software sau hardware din rețea și din sistemele informatice, fie ele corporale sau necorporale, care au valoare pentru o persoană fizică, o organizație sau o administrație publică;
2. „autoritate competentă în domeniul pregătirii pentru riscuri” înseamnă autoritatea competentă desemnată în temeiul articolului 3 din Regulamentul (UE) 2019/941;
3. „echipă de intervenție în caz de incidente de securitate informatică” înseamnă o echipă responsabilă cu gestionarea riscurilor și a incidentelor în conformitate cu articolul 10 din Directiva (UE) 2022/2555;
4. „activ cu impact critic” înseamnă un activ care este necesar pentru desfășurarea unui proces cu impact critic;
5. „entitate cu impact critic” înseamnă o entitate care desfășoară un proces cu impact critic și care este identificată de autoritățile competente în conformitate cu articolul 24;
6. „perimetru cu impact critic” înseamnă un perimetru definit de o entitate menționată la articolul 2 alineatul (1), care conține toate activele cu impact critic, în cadrul căruia accesul la aceste active poate fi controlat și care definește domeniul de aplicare al controalelor avansate de securitate cibernetică;
7. „proces cu impact critic” înseamnă un proces operațional desfășurat de o entitate în cazul căreia indicii de impact în materie de securitate cibernetică în domeniul energiei electrice depășesc pragul de impact critic;
8. „prag de impact critic” înseamnă valorile indicilor de impact în materie de securitate cibernetică în domeniul energiei electrice menționați la articolul 19 alineatul (3) litera (b), peste care un atac cibernetic asupra unui proces operațional va cauza perturbări critice ale fluxurilor transfrontaliere de energie electrică;
9. „furnizor critic de servicii TIC” înseamnă o entitate care furnizează un serviciu TIC sau un proces TIC care este necesar pentru un proces cu impact critic sau pentru un proces cu impact ridicat care afectează aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică și care, dacă este compromis, poate cauza un atac cibernetic al cărui impact ar depăși pragul de impact critic sau pragul de impact ridicat;
10. „flux transfrontalier de energie electrică” înseamnă un flux transfrontalier în sensul definiției de la articolul 2 punctul 3 din Regulamentul (UE) 2019/943;
11. „atac cibernetic” înseamnă un incident în sensul definiției de la articolul 3 punctul 14 din Regulamentul (UE) 2022/2554;
12. „securitate cibernetică” înseamnă securitate cibernetică astfel cum este definită la articolul 2 punctul 1 din Regulamentul (UE) 2019/881;

13. „control de securitate cibernetică” înseamnă acțiunile sau procedurile desfășurate cu scopul de a evita, de a detecta, de a contracara sau de a reduce la minimum riscurile în materie de securitate cibernetică;
14. „incident de securitate cibernetică” înseamnă un incident astfel cum este definit la articolul 6 punctul 6 din Directiva (UE) 2022/2555;
15. „sistem de gestionare a securității cibernetice” înseamnă politicile, procedurile, orientările și resursele și activitățile asociate, gestionate în mod colectiv de o entitate în vederea protejării activelor sale informaționale împotriva amenințărilor cibernetice, care instituie, pun în aplicare, operează, monitorizează, revizuiesc, întreține și îmbunătățesc în mod sistematic securitatea rețelelor și a sistemelor informatice ale unei organizații;
16. „centru de operațiuni de securitate cibernetică” înseamnă un centru special în care o echipă tehnică formată din unul sau mai mulți experți, sprijinită de sisteme informatice de securitate cibernetică, îndeplinește sarcini legate de securitate [servicii ale centrului de operațiuni de securitate cibernetică („CSOC”)], cum ar fi gestionarea atacurilor cibernetice și a erorilor de configurare a securității, monitorizarea securității, analiza jurnalelor și detectarea atacurilor cibernetice;
17. „amenințare cibernetică” înseamnă o amenințare cibernetică astfel cum este definită la articolul 2 punctul 8 din Regulamentul (UE) 2019/881;
18. „gestionarea vulnerabilităților în materie de securitate cibernetică” înseamnă practica de identificare și de soluționare a vulnerabilităților;
19. „entitate” înseamnă o entitate astfel cum este definită la articolul 6 punctul 38 din Directiva (UE) 2022/2555;
20. „alertă timpurie” înseamnă informațiile necesare pentru a se indica dacă incidentul semnificativ este suspectat de a fi cauzat de acte ilegale sau răuvoitoare sau ar putea avea un impact transfrontalier;
21. „indice de impact în materie de securitate cibernetică în domeniul energiei electrice” („ECII”) înseamnă un indice sau o grilă de clasificare care ierarhizează posibilele consecințe ale atacurilor cibernetice asupra proceselor operaționale implicate în fluxurile transfrontaliere de energie electrică;
22. „sistem european de certificare a securității cibernetice” înseamnă un sistem în sensul definiției de la articolul 2 punctul 9 din Regulamentul (UE) 2019/881;
23. „entitate cu impact ridicat” înseamnă o entitate care desfășoară un proces cu impact ridicat și care este identificată de autoritățile competente în conformitate cu articolul 24;
24. „proces cu impact ridicat” înseamnă un proces operațional desfășurat de o entitate pentru care indicii de impact în materie de securitate cibernetică în domeniul energiei electrice se situează peste pragul de impact ridicat;
25. „activ cu impact ridicat” înseamnă un activ care este necesar pentru desfășurarea unui proces cu impact ridicat;
26. „prag de impact ridicat” înseamnă valorile indicilor de impact în materie de securitate cibernetică în domeniul energiei electrice menționați la articolul 19 alineatul (3) litera (b), peste care un atac cibernetic reușit asupra unui proces operațional va cauza perturbări ridicate ale fluxurilor transfrontaliere de energie electrică;
27. „perimetru cu impact ridicat” înseamnă un perimetru definit de o entitate menționată la articolul 2 alineatul (1), care conține toate activele cu impact ridicat, în cadrul căruia accesul la aceste active poate fi controlat și care definește domeniul de aplicare al controalelor avansate de securitate cibernetică;
28. „produs TIC” înseamnă un produs TIC astfel cum este definit la articolul 2 punctul 12 din Regulamentul (UE) 2019/881;
29. „serviciu TIC” înseamnă un serviciu TIC astfel cum este definit la articolul 2 punctul 13 din Regulamentul (UE) 2019/881;
30. „proces TIC” înseamnă un proces TIC astfel cum este definit la articolul 2 punctul 14 din Regulamentul (UE) 2019/881;
31. „sistem moștenit” înseamnă un sistem TIC moștenit astfel cum este definit la articolul 3 punctul 3 din Regulamentul (UE) 2022/2554;
32. „punct unic de contact național” înseamnă punctul unic de contact desemnat sau instituit de fiecare stat membru în temeiul articolului 8 alineatul (3) din Directiva (UE) 2022/2555;
33. „autorități de gestionare a crizelor cibernetice NIS” înseamnă autoritățile desemnate sau instituite în temeiul articolului 9 alineatul (1) din Directiva (UE) 2022/2555;
34. „inițiator” înseamnă o entitate care inițiază un eveniment de schimb de informații, de partajare de informații sau de stocare a informațiilor;
35. „specificații privind achizițiile publice” înseamnă specificațiile pe care entitățile le definesc pentru achiziționarea de produse TIC, de procese TIC sau de servicii TIC noi sau actualizate;
36. „reprezentant” înseamnă o persoană fizică sau juridică stabilită în Uniune care este desemnată în mod explicit să acționeze în numele unei entități cu impact ridicat sau al unei entități cu impact critic care nu este stabilită în Uniune, dar care furnizează servicii unor entități din Uniune, persoană care poate fi contactată de o autoritate competentă sau de o echipă CSIRT în locul entității cu impact ridicat sau al entității cu impact critic înseși, în legătură cu obligațiile care îi revin entității respective în temeiul prezentului regulament;

37. „risc” înseamnă risc în sensul definiției de la articolul 6 punctul 9 din Directiva (UE) 2022/2555;

38. „matrice de evaluare a impactului riscurilor” înseamnă o matrice utilizată în timpul evaluării riscurilor pentru a determina nivelul de impact al riscului rezultat pentru fiecare risc evaluat;

39. „criză simultană de energie electrică” înseamnă o criză de energie electrică în sensul definiției de la articolul 2 punctul 10 din Regulamentul (UE) 2019/941;

40. „punct unic de contact la nivel de entitate” înseamnă un punct unic de contact la nivel de entitate, astfel cum este desemnat în temeiul articolului 38 alineatul (1) litera (c);

41. „parte interesată” înseamnă orice parte care are un interes în succesul și funcționarea continuă a unei organizații sau a unui proces, cum ar fi angajați, directori, acționari, autorități de reglementare, asociații, furnizori și clienți;

42. „standard” înseamnă un standard în sensul definiției de la articolul 2 punctul 1 litera (c) din Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului ([16]);

43. „regiune de exploatare a sistemului” înseamnă o regiune de exploatare a sistemului în sensul definiției din anexa I la Decizia ACER 05-2022 privind definirea regiunilor de exploatare a sistemului, stabilite în conformitate cu articolul 36 din Regulamentul (UE) 2019/943;

44. „operatori de sistem” înseamnă „operator de distribuție” și „operator de transport și de sistem” în sensul definițiilor de la articolul 2 punctele 29 și 35 din Directiva (UE) 2019/944;

45. „proces cu impact critic la nivelul Uniunii” înseamnă orice proces din sectorul energiei electrice care poate implica mai multe entități pentru care posibilul impact al unui atac cibernetic poate fi considerat critic în timpul efectuării evaluării riscurilor în materie de securitate cibernetică la nivelul Uniunii;

46. „proces cu impact ridicat la nivelul Uniunii” înseamnă orice proces din sectorul energiei electrice care poate implica mai multe entități pentru care posibilul impact al unui atac cibernetic poate fi considerat ridicat în timpul efectuării evaluării riscurilor în materie de securitate cibernetică la nivelul Uniunii;

47. „vulnerabilitate necorectată exploatată activ” înseamnă o vulnerabilitate care nu a fost încă divulgată și corectată în mod public și în cazul căreia există dovezi fiabile că executarea unui cod dăunător a fost efectuată de un actor asupra unui sistem fără permisiunea proprietarului sistemului;

48. „vulnerabilitate” înseamnă o vulnerabilitate în sensul definiției de la articolul 6 punctul 15 din Directiva (UE) 2022/2555.

*Articolul 4*

**Autoritatea competentă**

(1) Cât mai curând posibil și, în orice caz, până la 13 decembrie 2024, fiecare stat membru desemnează o autoritate națională guvernamentală sau de reglementare responsabilă cu îndeplinirea sarcinilor care îi sunt atribuite prin prezentul regulament („autoritate competentă”). Până când autorității competente i se încredințează îndeplinirea sarcinilor prevăzute în prezentul regulament, autoritatea de reglementare desemnată de fiecare stat membru în temeiul articolului 57 alineatul (1) din Directiva (UE) 2019/944 îndeplinește sarcinile autorității competente în conformitate cu prezentul regulament.

(2) Statele membre notifică fără întârziere Comisia, ACER, ENISA, Grupul de cooperare NIS, instituit în temeiul articolului 14 din Directiva (UE) 2022/2555, și Grupul de coordonare în domeniul energiei electrice, instituit în temeiul articolului 1 din Decizia Comisiei din 15 noiembrie 2012 ([17]), și le comunică numele și datele de contact ale autorității competente pe care au desemnat-o în temeiul alineatului (1) din prezentul articol, precum și orice modificări ulterioare ale acestora.

([16]) Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului (JO L 316, 14.11.2012, p. 12).

([17]) Decizia Comisiei din 15 noiembrie 2012 de înființare a Grupului de coordonare în domeniul energiei electrice (JO C 353, 17.11.2012, p. 2).

(3) Statele membre pot permite autorității lor competente să delege altor autorități naționale sarcinile care îi sunt atribuite prin prezentul regulament, cu excepția sarcinilor enumerate la articolul 5. Fiecare autoritate competentă monitorizează aplicarea prezentului regulament de către autoritățile cărora le-a delegat sarcini. Autoritatea competentă comunică Comisiei, ACER, Grupului de coordonare în domeniul energiei electrice, ENISA și Grupului de cooperare NIS numele, datele de contact și sarcinile atribuite autorităților cărora li s-au delegat sarcini, precum și orice modificări ulterioare ale acestor elemente.

*Articolul 5*

**Cooperarea dintre autoritățile și organismele relevante de la nivel național**

Autoritățile competente coordonează și asigură o cooperare adecvată între autoritățile competente responsabile cu securitatea cibernetică, autoritățile de gestionare a crizelor cibernetice, ANR-uri, autoritățile competente în domeniul pregătirii pentru riscuri și echipele CSIRT, în scopul îndeplinirii obligațiilor relevante prevăzute în prezentul regulament. Autoritățile competente se coordonează, de asemenea, cu orice alte organisme sau autorități, astfel cum sunt stabilite de fiecare stat membru, pentru a asigura proceduri eficiente și pentru a evita duplicarea sarcinilor și a obligațiilor. Autoritățile competente trebuie să fie în măsură să instruiască ANR-urile respective să solicite un aviz în temeiul articolului 8 alineatul (3) din partea ACER.

*Articolul 6*

**Termeni și condiții sau metodologii ori planuri**

(1) OST elaborează, în cooperare cu entitatea OSD UE, propuneri de termeni și condiții sau metodologii în temeiul alineatului (2) ori propuneri de planuri în temeiul alineatului (3).

(2) Termenii și condițiile sau metodologiile următoare, precum și orice modificări ale acestora, fac obiectul aprobării de către toate autoritățile competente:

(a) metodologiile de evaluare a riscurilor în materie de securitate cibernetică, în temeiul articolului 18 alineatul (1);

(b) raportul cuprinzător de evaluare a riscurilor în materie de securitate cibernetică a fluxurilor transfrontaliere de energie electrică, în temeiul articolului 23;

(c) controalele minime și controalele avansate de securitate cibernetică în temeiul articolului 29, punerea în corespondență a controalelor de securitate cibernetică în domeniul energiei electrice cu standardele în temeiul articolului 34, inclusiv a controalelor minime și a controalelor avansate de securitate cibernetică din cadrul lanțului de aprovizionare, în conformitate cu articolul 33;

(d) o recomandare privind achizițiile publice în domeniul securității cibernetice, în temeiul articolului 35;

(e) metodologia grilei de clasificare a atacurilor cibernetice, în temeiul articolului 37 alineatul (8).

(3) Propunerile de planuri de atenuare a riscurilor în materie de securitate cibernetică la nivel regional, în temeiul articolului 22 fac obiectul aprobării de către toate autoritățile competente din regiunea în cauză de exploatare a sistemului.

(4) Propunerile de termeni și condiții sau metodologii enumerate la alineatul (2) ori propunerile de planuri menționate la alineatul (3) includ un calendar propus pentru implementarea lor și o descriere a impactului lor preconizat asupra obiectivelor prezentului regulament.

(5) Entitatea OSD UE poate furniza un aviz motivat OST în cauză cu până la trei săptămâni înainte de termenul de prezentare a propunerii de termeni și condiții sau metodologii ori a propunerii de planuri către autoritățile competente. OST responsabili cu prezentarea propunerii de termeni și condiții sau metodologii ori a propunerii de planuri iau în considerare avizul motivat al entității OSD UE înainte de a transmite propunerea respectivă, spre aprobare, autorităților competente. OST furnizează o justificare în cazul în care avizul entității OSD UE nu este luat în considerare.

(6) Atunci când elaborează împreună termeni, condiții și metodologii, precum și planuri, OST participanți cooperează îndeaproape. OST, cu sprijinul ENTSO pentru energie electrică și în cooperare cu entitatea OSD UE, informează periodic autoritățile competente și ACER cu privire la progresele înregistrate în ceea ce privește elaborarea termenilor și condițiilor sau metodologiilor ori a planurilor.

*Articolul 7*

**Modalități de vot pentru OST**

(1) În cazul în care nu reușesc să ajungă la un acord, OST care trebuie să decidă cu privire la propunerile de termeni și condiții sau metodologii decid prin vot cu majoritate calificată. În cazul unor astfel de propuneri, majoritatea calificată se calculează după cum urmează:

(a) OST reprezentând cel puțin 55 % dintre statele membre și

(b) OST reprezentând state membre care cuprind cel puțin 65 % din populația Uniunii.

(2) O minoritate de blocare pentru deciziile privind propunerile de termeni și condiții sau metodologii enumerate la articolul 6 alineatul (2) trebuie să includă OST reprezentând cel puțin patru state membre. În caz contrar, majoritatea calificată este considerată ca fiind întrunită.

(3) În cazul în care OST dintr-o regiune de exploatare a sistemului care trebuie să decidă cu privire la propunerile de planuri enumerate la articolul 6 alineatul (2) nu reușesc să ajungă la un acord și în cazul în care regiunea în cauză de exploatare a sistemului este compusă din mai mult de cinci state membre, OST decid prin vot cu majoritate calificată. Majoritatea calificată pentru propunerile enumerate la articolul 6 alineatul (2) se calculează după cum urmează:

(a) OST reprezentând cel puțin 72 % dintre statele membre vizate și

(b) OST reprezentând state membre care cuprind cel puțin 65 % din populația regiunii vizate.

(4) O minoritate de blocare în cazul deciziilor privind propunerile de planuri include cel puțin un număr minim de OST reprezentând peste 35 % din populația statelor membre participante, plus OST reprezentând cel puțin un stat membru vizat suplimentar. În caz contrar, majoritatea calificată este considerată ca fiind întrunită.

(5) În cazul deciziilor OST privind propunerile de termeni și condiții sau metodologii în temeiul articolului 6 alineatul (2), se atribuie câte un vot fiecărui stat membru. Dacă pe teritoriul unui stat membru există mai mulți OST, statul membru respectiv distribuie drepturile de vot între OST respectivi.

(6) În cazul în care nu prezintă autorităților competente relevante o propunere inițială sau modificată de termeni și condiții sau metodologii ori de planuri în termenele stabilite în prezentul regulament, OST, în cooperare cu entitatea OSD UE, furnizează autorităților competente relevante și ACER proiectele relevante de termeni și condiții sau metodologii ori de planuri. Ei explică de ce nu s-a ajuns la încheierea unui acord. Autoritățile competente iau împreună măsurile adecvate pentru adoptarea termenilor și condițiilor sau metodologiilor necesare sau a planurilor necesare. Acest lucru se poate realiza, de exemplu, prin solicitarea de modificări ale proiectelor în temeiul prezentului alineat, prin revizuirea și completarea proiectelor respective sau, în cazul în care nu au fost furnizate proiecte, prin definirea și aprobarea termenilor și condițiilor sau metodologiilor necesare ori a planurilor necesare.

*Articolul 8*

**Transmiterea propunerilor către autoritățile competente**

(1) OST transmit autorităților competente relevante, spre aprobare, propunerile de termeni și condiții sau metodologii ori de planuri în termenele corespunzătoare prevăzute la articolele 18, 23, 29, 33, 34, 35 și 37. Autoritățile competente pot prelungi împreună aceste termene în circumstanțe excepționale, în special în cazurile în care un termen nu poate fi respectat din cauza unor circumstanțe externe sferei OST sau a entității OSD UE.

(2) Propunerile de termeni și condiții sau metodologii ori de planuri în temeiul alineatului (1) se transmit spre informare către ACER, în același timp în care sunt transmise autorităților competente.

(3) La cererea comună a ANR-urilor, ACER emite un aviz cu privire la propunerea de termeni și condiții sau metodologii ori la propunerea de planuri în termen de șase luni de la primirea propunerilor de termeni și condiții sau metodologii ori de planuri și notifică avizul respectiv ANR-urilor și autorităților competente. ANR-urile, ANC-SC și orice alte autorități desemnate drept autorități competente se coordonează înainte ca ANR-urile să solicite un aviz din partea ACER. În avizul respectiv, ACER poate să includă recomandări. ACER consultă ENISA înainte de a emite un aviz cu privire la propunerile enumerate la articolul 6 alineatul (2).

(4) Autoritățile competente se consultă, cooperează îndeaproape și se coordonează pentru a ajunge la un acord cu privire la propunerile de termeni și condiții sau metodologii ori de planuri. Înainte de a aproba termenii și condițiile sau metodologiile ori planurile, autoritățile competente revizuiesc și completează propunerile, dacă este necesar, după consultarea ENTSO pentru energie electrică și a entității OSD UE, pentru a se asigura că propunerile sunt în conformitate cu prezentul regulament și contribuie la un nivel comun ridicat de securitate cibernetică în întreaga Uniune.

(5) Autoritățile competente decid cu privire la termeni și condiții sau metodologii ori la planuri în termen de șase luni de la primirea termenilor și condițiilor sau metodologiilor ori a planurilor de către autoritatea competentă relevantă sau, acolo unde este cazul, de către ultima autoritate competentă relevantă în cauză.

(6) În cazul în care ACER emite un aviz, autoritățile competente relevante țin seama de avizul respectiv și iau deciziile în termen de șase luni de la primirea avizului ACER.

(7) În cazul în care autoritățile competente solicită în comun o modificare a termenilor și condițiilor sau metodologiilor propuse ori a planurilor, pentru a le aproba, OST elaborează, în cooperare cu entitatea OSD UE, o propunere privind această modificare a termenilor și condițiilor sau metodologiilor ori a planurilor. OST prezintă propunerea modificată spre aprobare în termen de două luni de la solicitarea autorităților competente. Autoritățile competente decid cu privire la termenii și condițiile sau metodologiile ori la planurile modificate în termen de două luni de la transmiterea acestora.

(8) În cazul în care nu au reușit să ajungă la un acord în termenul menționat la alineatul (5) sau (7), autoritățile competente informează Comisia în acest sens. Comisia poate lua măsurile corespunzătoare pentru a face posibilă adoptarea termenilor și condițiilor sau metodologiilor ori a planurilor necesare.

(9) OST, cu sprijinul ENTSO pentru energie electrică, și entitatea OSD UE publică termenii și condițiile sau metodologiile ori planurile pe site-urile lor după aprobarea de către autoritățile competente relevante, cu excepția cazului în care aceste informații sunt considerate confidențiale în conformitate cu articolul 47.

(10) Autoritățile competente pot solicita în comun OST și entității OSD UE propuneri de modificare a termenilor și condițiilor sau metodologiilor aprobate ori a planurilor aprobate și pot stabili un termen pentru prezentarea propunerilor respective. OST, în cooperare cu entitatea OSD UE, pot propune modificări autorităților competente și din proprie inițiativă. Propunerile de modificare a termenilor și condițiilor sau metodologiilor ori a planurilor se elaborează și se aprobă în conformitate cu procedura prevăzută la prezentul articol.

(11) Cel puțin o dată la trei ani de la prima adoptare a termenilor și condițiilor sau metodologiilor respective ori de la adoptarea planurilor respective, OST, în cooperare cu entitatea OSD UE, reexaminează eficacitatea termenilor și condițiilor sau metodologiilor adoptate ori a planurilor adoptate și raportează constatările reexaminării autorităților competente și ACER fără întârzieri nejustificate.

*Articolul 9*

**Consultare**

(1) OST, cu sprijinul ENTSO pentru energie electrică și în cooperare cu entitatea OSD UE, consultă părțile interesate, inclusiv ACER, ENISA și autoritatea competentă a fiecărui stat membru, cu privire la proiectele de propuneri de termeni și condiții sau metodologii enumerate la articolul 6 alineatul (2) și la proiectele de propuneri de planuri menționate la articolul 6 alineatul (3). Consultarea durează cel puțin o lună.

(2) Propunerile de termeni și condiții sau metodologii enumerate la articolul 6 alineatul (2) care sunt transmise de OST, în cooperare cu entitatea OSD UE, se publică și se supun consultării la nivelul Uniunii. Propunerile de planuri enumerate la articolul 6 alineatul (3) care sunt transmise de OST relevanți, în cooperare cu entitatea OSD UE, la nivel regional, se publică și se supun consultării cel puțin la nivel regional.

(3) OST, cu sprijinul ENTSO pentru energie electrică, și entitatea OSD UE responsabilă cu propunerea de termeni și condiții sau metodologii ori cu propunerea de planuri țin seama în mod corespunzător de opiniile părților interesate care rezultă în urma consultărilor întreprinse în conformitate cu alineatul (1), înainte de a fi transmise spre aprobare autorităților de reglementare. În toate cazurile, alături de propunerea prezentată, trebuie transmisă și o justificare solidă a includerii sau a neincluderii opiniilor rezultate în urma consultării, care trebuie publicată în timp util, înainte de sau simultan cu propunerea de termeni și condiții sau metodologii.

*Articolul 10*

**Implicarea părților interesate**

ACER, în strânsă cooperare cu ENTSO pentru energie electrică și cu entitatea OSD UE, organizează implicarea părților interesate, inclusiv reuniuni periodice cu părțile interesate, pentru a identifica problemele și a propune îmbunătățiri legate de punerea în aplicare a prezentului regulament.

*Articolul 11*

**Recuperarea costurilor**

(1) Costurile suportate de OST și de OSD care fac obiectul reglementării tarifelor de rețea și care decurg din obligațiile prevăzute în prezentul regulament, inclusiv costurile suportate de ENTSO pentru energie electrică și de entitatea OSD UE, sunt evaluate de ANR relevantă din fiecare stat membru.

(2) Costurile evaluate ca fiind rezonabile, eficiente și proporționale se recuperează prin tarife de rețea sau prin alte mecanisme adecvate, astfel cum sunt stabilite de ANR relevantă.

(3) La cererea ANR-urilor relevante, OST și OSD menționați la alineatul (1) furnizează, într-un termen rezonabil stabilit de ANR, informațiile necesare pentru a facilita evaluarea costurilor suportate.

*Articolul 12*

**Monitorizare**

(1) ACER monitorizează punerea în aplicare a prezentului regulament în conformitate cu articolul 32 alineatul (1) din Regulamentul (UE) 2019/943 și cu articolul 4 alineatul (2) din Regulamentul (UE) 2019/942. În contextul efectuării acestei monitorizări, ACER poate coopera cu ENISA și poate solicita sprijin din partea ENTSO pentru energie electrică și a entității OSD UE. ACER informează periodic Grupul de coordonare în domeniul energiei electrice și Grupul de cooperare NIS cu privire la punerea în aplicare a prezentului regulament.

(2) ACER publică un raport cel puțin o dată la trei ani după intrarea în vigoare a prezentului regulament pentru:

(a) a reexamina stadiul punerii în aplicare a măsurilor aplicabile de gestionare a riscurilor în materie de securitate cibernetică în ceea ce privește entitățile cu impact ridicat și entitățile cu impact critic;

(b) a identifica dacă este posibil să fie necesare norme suplimentare privind cerințele comune, planificarea, monitorizarea, raportarea și gestionarea crizelor pentru a preveni riscurile la adresa sectorului energiei electrice și

(c) a identifica domeniile în care se pot aduce îmbunătățiri în vederea revizuirii prezentului regulament sau a stabili domeniile nedescoperite și noile priorități care pot apărea ca urmare a evoluțiilor tehnologice.

(3) Până la data de 13 iunie 2025, ACER, în cooperare cu ENISA și după consultarea ENTSO pentru energie electrică și a entității OSD UE, poate emite orientări cu privire la informațiile relevante care trebuie comunicate ACER în scopul monitorizării, precum și cu privire la procesul de colectare și la frecvența acesteia, pe baza indicatorilor de performanță definiți în conformitate cu alineatul (5).

(4) Autoritățile competente pot avea acces la informațiile relevante deținute de ACER, pe care aceasta le-a colectat în conformitate cu prezentul articol.

(5) ACER, în cooperare cu ENISA și cu sprijinul ENTSO pentru energie electrică și al entității OSD UE, emite indicatori de performanță fără caracter obligatoriu pentru evaluarea fiabilității operaționale, care se referă la aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică.

(6) Entitățile enumerate la articolul 2 alineatul (1) din prezentul regulament transmit ACER informațiile necesare pentru ca ACER să își îndeplinească atribuțiile enumerate la alineatul (2).

*Articolul 13*

**Analiză comparativă**

(1) Până la data de 13 iunie 2025, ACER, în cooperare cu ENISA, stabilește un ghid fără caracter obligatoriu de analiză comparativă în materie de securitate cibernetică. Ghidul le explică ANR-urilor principiile de analiză comparativă a controalelor de securitate cibernetică implementate în temeiul alineatului (2) din prezentul articol, luând în considerare costurile implementării controalelor și eficacitatea funcției îndeplinite de procesele, produsele, serviciile, sistemele și soluțiile utilizate pentru implementarea acestor controale. ACER ține seama de rapoartele de analiză comparativă existente atunci când elaborează ghidul fără caracter obligatoriu de analiză comparativă în materie de securitate cibernetică. ACER transmite spre informare ANR-urilor ghidul fără caracter obligatoriu de analiză comparativă în materie de securitate cibernetică.

(2) În termen de 12 luni de la elaborarea ghidului de analiză comparativă în temeiul alineatului (1), ANR-urile efectuează o analiză comparativă pentru a evalua dacă investițiile actuale în securitatea cibernetică:

(a) atenuează riscurile care au un impact asupra fluxurilor transfrontaliere de energie electrică;

(b) conduc la rezultatele dorite și generează câștiguri în materie de eficiență pentru dezvoltarea sistemelor de energie electrică;

(c) sunt eficiente și integrate în achizițiile publice globale de active și servicii.

(3) Pentru efectuarea analizei comparative, ANR-urile pot lua în considerare ghidul fără caracter obligatoriu de analiză comparativă în materie de securitate cibernetică elaborat de ACER și evaluează în special:

(a) cheltuielile medii legate de securitatea cibernetică pentru atenuarea riscurilor care au un impact asupra fluxurilor transfrontaliere de energie electrică, în special în ceea ce privește entitățile cu impact ridicat și entitățile cu impact critic;

(b) în cooperare cu ENTSO pentru energie electrică și cu entitatea OSD UE, prețurile medii ale serviciilor, sistemelor și produselor de securitate cibernetică ce contribuie în mare măsură la îmbunătățirea și menținerea măsurilor de gestionare a riscurilor în materie de securitate cibernetică în diferitele regiuni de exploatare a sistemului;

(c) existența și nivelul de comparabilitate ale costurilor și funcțiilor aferente serviciilor, sistemelor și soluțiilor de securitate cibernetică adecvate pentru punerea în aplicare a prezentului regulament, identificând eventualele măsuri necesare pentru a promova eficiența în materie de cheltuieli, în special în cazul în care ar putea fi necesare investiții tehnologice în domeniul securității cibernetice.

(4) Toate informațiile referitoare la analiza comparativă sunt tratate și prelucrate în conformitate cu cerințele de clasificare a datelor din prezentul regulament, cu controalele minime de securitate cibernetică și cu raportul de evaluare a riscurilor în materie de securitate cibernetică a fluxurilor transfrontaliere de energie electrică. Analiza comparativă menționată la alineatele (2) și (3) nu se publică.

(5) Fără a aduce atingere cerințelor de confidențialitate de la articolul 47 și nici necesității de a proteja securitatea entităților care fac obiectul dispozițiilor din prezentul regulament, analiza comparativă menționată la alineatele (2) și (3) din prezentul articol este comunicată tuturor ANR-urilor, tuturor autorităților competente, ACER, ENISA și Comisiei.

*Articolul 14*

**Acorduri cu OST din afara Uniunii**

(1) În termen de 18 luni de la intrarea în vigoare a prezentului regulament, OST dintr-o regiune de exploatare a sistemului care este învecinată cu o țară terță depun eforturi pentru a încheia cu OST din respectiva țară terță învecinată acorduri care să fie în conformitate cu dreptul relevant al Uniunii și care să pună bazele cooperării în domeniul protecției securității cibernetice și ale mecanismelor de cooperare în materie de securitate cibernetică cu OST respectivi.

(2) OST informează autoritatea competentă cu privire la acordurile încheiate în temeiul alineatului (1).

*Articolul 15*

**Reprezentanți legali**

(1) Entitățile care nu au un sediu în Uniune, dar care furnizează servicii unor entități din Uniune și care au fost notificate ca fiind entități cu impact ridicat sau entități cu impact critic în conformitate cu articolul 24 alineatul (6), desemnează în scris un reprezentant în Uniune și informează în consecință autoritatea competentă care a transmis notificarea, în termen de trei luni de la notificare.

(2) Acest reprezentant este mandatat cu scopul de a fi contactat de orice autoritate competentă sau echipă CSIRT din Uniune, pe lângă entitatea cu impact ridicat sau entitatea cu impact critic sau în locul acesteia, în ceea ce privește obligațiile care îi revin entității în temeiul prezentului regulament. Entitatea cu impact ridicat sau entitatea cu impact critic îi conferă reprezentantului său legal competențele necesare și îi furnizează resurse suficiente pentru a garanta cooperarea sa eficientă și în timp util cu autoritățile competente sau echipele CSIRT relevante.

(3) Reprezentantul se stabilește în unul dintre statele membre în care entitatea își oferă serviciile. Entitatea este considerată a fi sub jurisdicția statului membru în care este stabilit reprezentantul. Entitățile cu impact ridicat sau entitățile cu impact critic notifică numele, adresa poștală, adresa de e-mail și numărul de telefon ale reprezentantului lor legal autorității competente din statul membru în care își are reședința sau în care este stabilit respectivul reprezentant legal.

(4) Reprezentantul legal desemnat poate fi tras la răspundere pentru nerespectarea obligațiilor prevăzute în prezentul regulament, fără a se aduce atingere răspunderii și acțiunilor în justiție care ar putea fi introduse împotriva entității cu impact ridicat sau a entității cu impact critic înseși.

(5) În absența unui reprezentant în Uniune desemnat în temeiul prezentului articol, orice stat membru în care entitatea prestează servicii poate introduce acțiuni în justiție împotriva entității respective pentru nerespectarea obligațiilor care îi revin în temeiul prezentului regulament.

(6) Desemnarea unui reprezentant legal Uniune în temeiul alineatului (1) nu este echivalentă stabilirii în Uniune.

*Articolul 16*

**Cooperarea dintre ENTSO pentru energie electrică și entitatea OSD UE**

(1) ENTSO pentru energie electrică și entitatea OSD UE cooperează în vederea efectuării evaluărilor riscurilor în materie de securitate cibernetică în temeiul articolelor 19 și 21, în special pentru îndeplinirea următoarelor sarcini:

(a) elaborarea de metodologii de evaluare a riscurilor în materie de securitate cibernetică, în temeiul articolului 18 alineatul (1);

(b) elaborarea raportului cuprinzător de evaluare a riscurilor în materie de securitate cibernetică a fluxurilor transfrontaliere de energie electrică, în temeiul articolului 23;

(c) elaborarea cadrului comun de securitate cibernetică în domeniul energiei electrice în temeiul capitolului III;

(d) elaborarea unei recomandări privind achizițiile publice în domeniul securității cibernetice, în temeiul articolului 35;

(e) elaborarea metodologiei grilei de clasificare a atacurilor cibernetice, în temeiul articolului 37 alineatul (8);

(f) elaborarea indicelui provizoriu de impact în materie de securitate cibernetică în domeniul energiei electrice („ECII") în temeiul articolului 48 alineatul (1) litera (a);

(g) elaborarea listei provizorii consolidate a entităților cu impact ridicat și a entităților cu impact critic în conformitate cu articolul 48 alineatul (3);

(h) elaborarea listei provizorii consolidate a proceselor cu impact ridicat și a proceselor cu impact critic la nivelul Uniunii, în conformitate cu articolul 48 alineatul (4);

(i) elaborarea listei provizorii de standarde și controale europene și internaționale în conformitate cu articolul 48 alineatul (6);

(j) efectuarea evaluării riscurilor în materie de securitate cibernetică la nivelul Uniunii în temeiul articolului 19;

(k) efectuarea evaluării riscurilor în materie de securitate cibernetică la nivel regional în temeiul articolului 21;

(l) definirea planurilor regionale de atenuare a riscurilor în materie de securitate cibernetică în temeiul articolului 22;

(m) elaborarea de orientări privind sistemele europene de certificare a securității cibernetice pentru achiziționarea de produse TIC, servicii TIC și procese TIC în conformitate cu articolul 36;

(n) elaborarea de orientări pentru punerea în aplicare a prezentului regulament, în consultare cu ACER și ENISA.

(2) Cooperarea dintre ENTSO pentru energie electrică și entitatea OSD UE poate lua forma unui grup de lucru privind riscurile în materie de securitate cibernetică.

(3) ENTSO pentru energie electrică și entitatea OSD UE informează periodic ACER, ENISA, Grupul de cooperare NIS și Grupul de coordonare în domeniul energiei electrice cu privire la progresele înregistrate în ceea ce privește implementarea evaluărilor riscurilor în materie de securitate cibernetică la nivelul Uniunii și la nivel regional în temeiul articolelor 19 și 21.

*Articolul 17*

**Cooperarea dintre ACER și autoritățile competente**

ACER, în cooperare cu fiecare autoritate competentă:

1. monitorizează punerea în aplicare a măsurilor de gestionare a riscurilor în materie de securitate cibernetică în temeiul articolului 12 alineatul (2) litera (a) și a obligațiilor de raportare în temeiul articolelor 27 și 39 și

2. monitorizează procesul de adoptare și implementarea termenilor și condițiilor sau metodologiilor ori a planurilor în temeiul articolului 6 alineatele (2) și (3). Cooperarea dintre ACER, ENISA și fiecare autoritate competentă poate lua forma unui organism de monitorizare a riscurilor în materie de securitate cibernetică.

CAPITOLUL II

**EVALUAREA RISCURILOR ȘI IDENTIFICAREA RISCURILOR RELEVANTE ÎN MATERIE DE SECURITATE CIBERNETICĂ**

*Articolul 18*

**Metodologii de evaluare a riscurilor în materie de securitate cibernetică**

(1) Până la data de 13 martie 2025, OST, cu asistență din partea ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE și în urma unei consultări cu Grupul de cooperare NIS prezintă o propunere de metodologii de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii, la nivel regional și la nivel de stat membru.

(2) Metodologiile de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii, la nivel regional și la nivel de stat membru includ:

(a) o listă a amenințărilor cibernetice care trebuie avute în vedere, care să includă cel puțin următoarele amenințări la nivelul lanțului de aprovizionare:

  (i) o corupere gravă și neașteptată a lanțului de aprovizionare;

  (ii) indisponibilitatea produselor TIC, a serviciilor TIC sau a proceselor TIC din lanțul de aprovizionare;

(iii) atacuri cibernetice inițiate prin intermediul actorilor din lanțul de aprovizionare;

(iv) scurgeri de informații sensibile prin intermediul lanțului de aprovizionare, inclusiv urmărirea lanțului de aprovizionare;

(v) introducerea unor deficiențe sau a unor uși secrete în produsele TIC, serviciile TIC sau procesele TIC prin intermediul actorilor din lanțul de aprovizionare;

(b) criteriile de evaluare ca ridicat sau critic a impactului riscurilor în materie de securitate cibernetică, utilizând praguri definite pentru consecințe și probabilitate;

(c) o abordare pentru a analiza riscurile în materie de securitate cibernetică generate de sistemele moștenite, de efectele de cascadă ale atacurilor cibernetice și de funcționarea în timp real a sistemelor care operează rețeaua;

(d) o abordare pentru a analiza riscurile în materie de securitate cibernetică generate de dependența de un singur furnizor de produse TIC, de servicii TIC sau de procese TIC.

(3) Metodologiile de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii, la nivel regional și la nivel de stat membru evaluează riscurile în materie de securitate cibernetică utilizând aceeași matrice de evaluare a impactului riscurilor. Matricea de evaluare a impactului riscurilor:

(a) măsoară consecințele atacurilor cibernetice pe baza următoarelor criterii:

(i) pierderea în sarcină;

(ii) reducerea producției de energie electrică;

(iii) pierderea de capacitate în rezerva de frecvențe de bază;

(iv) pierderea capacității de repunere în funcțiune a unei rețele electrice fără a se baza pe rețeaua externă de transport pentru a se redresa după o oprire totală sau parțială (denumită și „pornire fără alimentare din sistem”);

(v) durata preconizată a unei întreruperi a alimentării cu energie electrică care afectează clienții, în combinație cu amploarea întreruperii exprimată ca număr de clienți și

(vi) orice alte criterii cantitative sau calitative care ar putea acționa în mod rezonabil ca indicatori ai efectului unui atac cibernetic asupra fluxurilor transfrontaliere de energie electrică;

(b) măsurarea probabilității unui incident ca frecvență anuală a atacurilor cibernetice.

(4) Metodologiile de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii descriu modul în care vor fi definite valorile ECII pentru pragurile de impact ridicat și pentru pragurile de impact critic. ECII permite entităților să estimeze, cu ajutorul criteriilor menționate la alineatul (2) litera (b), impactul riscurilor asupra procesului lor operațional în timpul evaluărilor impactului operațional pe care le efectuează în temeiul articolului 26 alineatul (4) litera (c) punctul (i).

(5) ENTSO pentru energie electrică, în coordonare cu entitatea OSD UE, informează Grupul de coordonare în domeniul energiei electrice cu privire la propunerile de metodologii de evaluare a riscurilor în materie de securitate cibernetică care sunt elaborate în temeiul alineatului (1).

*Articolul 19*

**Evaluarea riscurilor în materie de securitate cibernetică la nivelul Uniunii**

(1) În termen de 9 luni de la aprobarea metodologiilor de evaluare a riscurilor în materie de securitate cibernetică în temeiul articolului 8 și, ulterior, o dată la trei ani, ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE și în consultare cu Grupul de cooperare NIS, efectuează, fără a aduce atingere articolului 22 din Directiva (UE) 2022/2555, o evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii și elaborează un proiect de raport de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii. În acest scop, organismele respective vor utiliza metodologiile elaborate în temeiul articolului 18 și aprobate în temeiul articolului 8 pentru a identifica, a analiza și a evalua posibilele consecințe ale atacurilor cibernetice care afectează securitatea operațională a sistemului de energie electrică și care perturbă fluxurile transfrontaliere de energie electrică. Evaluarea riscurilor în materie de securitate cibernetică la nivelul Uniunii nu ia în considerare daunele juridice, financiare sau reputaționale cauzate de atacurile cibernetice.

(2) Raportul de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii include următoarele elemente:

(a) procesele cu impact ridicat la nivelul Uniunii și procesele cu impact critic la nivelul Uniunii;

(b) o matrice de evaluare a impactului riscurilor pe care entitățile și autoritățile competente o vor utiliza pentru a evalua riscurile în materie de securitate cibernetică identificate în evaluarea riscurilor în materie de securitate cibernetică la nivel de stat membru, efectuată în temeiul articolului 20, și în evaluarea riscurilor în materie de securitate cibernetică la nivel de entitate în temeiul articolului 26 alineatul (2) litera (b).

(3) În ceea ce privește procesele cu impact ridicat la nivelul Uniunii și procesele cu impact critic la nivelul Uniunii, raportul de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii include:

(a) o evaluare a posibilelor consecințe ale unui atac cibernetic utilizând indicatorii definiți în metodologia de evaluare a riscurilor în materie de securitate cibernetică elaborată în temeiul articolului 18 alineatele (2), (3) și (4) și aprobată în temeiul articolului 8;

(b) ECII și pragurile de impact ridicat și pragurile de impact critic pe care autoritățile competente le vor utiliza în temeiul articolului 24 alineatele (1) și (2) pentru a identifica entitățile cu impact ridicat și entitățile cu impact critic implicate în procesele cu impact ridicat la nivelul Uniunii și în procesele cu impact critic la nivelul Uniunii.

(4) ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE, transmite ACER, spre avizare, proiectul de raport de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii, împreună cu rezultatele evaluării riscurilor în materie de securitate cibernetică la nivelul Uniunii. ACER emite un aviz cu privire la proiectul de raport în termen de trei luni de la primirea acestuia. ENTSO pentru energie electrică și entitatea OSD UE țin seama în cea mai mare măsură de avizul ACER atunci când finalizează raportul respectiv.

(5) În termen de trei luni de la primirea avizului ACER, ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE, notifică ACER, Comisiei, ENISA și autorităților competente raportul final de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii.

*Articolul 20*

**Evaluarea riscurilor în materie de securitate cibernetică la nivel de stat membru**

(1) Fiecare autoritate competentă efectuează o evaluare a riscurilor în materie de securitate cibernetică la nivelul statului membru în cauză cu privire la toate entitățile cu impact ridicat și la toate entitățile cu impact critic din statul membru respectiv, utilizând metodologiile elaborate în temeiul articolului 18 și aprobate în temeiul articolului 8. Evaluarea riscurilor în materie de securitate cibernetică la nivel de stat membru identifică și analizează riscurile de atacuri cibernetice care afectează securitatea operațională a sistemului de energie electrică, perturbând fluxurile transfrontaliere de energie electrică. Evaluarea riscurilor în materie de securitate cibernetică la nivel de stat membru nu ia în considerare daunele juridice, financiare sau reputaționale cauzate de atacurile cibernetice.

(2) În termen de 21 de luni de la notificarea entităților cu impact ridicat și a entităților cu impact critic în temeiul articolului 24 alineatul (6) și, ulterior, o dată la trei ani și după consultarea ANC-SC responsabilă cu energia electrică, fiecare autoritate competentă, sprijinită de echipa CSIRT, prezintă ENTSO pentru energie electrică și entității OSD UE un raport de evaluare a riscurilor în materie de securitate cibernetică la nivel de stat membru, care conține următoarele informații pentru fiecare proces operațional cu impact ridicat și pentru fiecare proces operațional cu impact critic:

(a) stadiul implementării controalelor minime și a controalelor avansate de securitate cibernetică în temeiul articolului 29;

(b) o listă a tuturor atacurilor cibernetice raportate în ultimii trei ani în temeiul articolului 38 alineatul (3);

(c) o sinteză a tuturor informațiilor referitoare la amenințări cibernetice raportate în ultimii trei ani în temeiul articolului 38 alineatul (6);

(d) pentru fiecare proces cu impact ridicat sau proces cu impact critic la nivelul Uniunii, o estimare a riscurilor de compromitere a confidențialității, a integrității și a disponibilității informațiilor și activelor relevante;

(e) dacă este necesar, o listă a entităților suplimentare identificate ca fiind cu impact ridicat sau cu impact critic în temeiul articolului 24 alineatele (1), (2), (3) și (5).

(3) Raportul de evaluare a riscurilor în materie de securitate cibernetică la nivel de stat membru ține seama de planul de pregătire pentru riscuri elaborat de statul membru respectiv în temeiul articolului 10 din Regulamentul (UE) 2019/941.

(4) Informațiile cuprinse în raportul de evaluare a riscurilor în materie de securitate cibernetică la nivel de stat membru în temeiul alineatului (2) literele (a)-(d) nu sunt legate de entități sau active specifice. Raportul de evaluare a riscurilor în materie de securitate cibernetică la nivel de stat membru include, de asemenea, o evaluare a riscurilor legate de derogările temporare emise de autoritățile competente din statele membre în temeiul articolului 30.

(5) ENTSO pentru energie electrică și entitatea OSD UE pot solicita informații suplimentare de la autoritățile competente în legătură cu sarcinile specificate la alineatul (2) literele (a) și (c).

(6) Autoritățile competente se asigură că informațiile pe care le furnizează sunt exacte și corecte.

*Articolul 21*

**Evaluarea riscurilor în materie de securitate cibernetică la nivel regional**

(1) ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE și în consultare cu centrul regional de coordonare relevant, efectuează o evaluare a riscurilor în materie de securitate cibernetică la nivel regional pentru fiecare regiune de exploatare a sistemului, utilizând metodologiile elaborate în temeiul articolului 19 și aprobate în temeiul articolului 8, pentru a identifica, a analiza și a evalua riscurile de atacuri cibernetice care afectează securitatea operațională a sistemului de energie electrică și perturbă fluxurile transfrontaliere de energie electrică. Evaluările riscurilor în materie de securitate cibernetică la nivel regional nu iau în considerare daunele juridice, financiare sau reputaționale cauzate de atacurile cibernetice.

(2) În termen de 30 de luni de la notificarea entităților cu impact ridicat și a entităților cu impact critic în temeiul articolului 24 alineatul (6) și, ulterior, o dată la trei ani, ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE și în consultare cu Grupul de cooperare NIS, întocmește un raport de evaluare a riscurilor în materie de securitate cibernetică la nivel regional pentru fiecare regiune de exploatare a sistemului.

(3) Raportul de evaluare a riscurilor în materie de securitate cibernetică la nivel regional ține seama de informațiile relevante cuprinse în rapoartele de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii și în rapoartele de evaluare a riscurilor în materie de securitate cibernetică ale statelor membre.

(4) Evaluarea riscurilor în materie de securitate cibernetică la nivel regional ia în considerare scenariile regionale de criză de energie electrică legate de securitatea cibernetică, identificate în temeiul articolului 6 din Regulamentul (UE) 2019/941.

*Articolul 22*

**Planuri de atenuare a riscurilor în materie de securitate cibernetică la nivel regional**

(1) În termen de 36 de luni de la notificarea entităților cu impact ridicat și a entităților cu impact critic în temeiul articolului 24 alineatul (6) și nu mai târziu de 13 iunie 2031 și o dată la trei ani după această dată, OST, cu sprijinul ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE și în consultare cu centrele de coordonare regionale și cu Grupul de cooperare NIS, elaborează un plan de atenuare a riscurilor în materie de securitate cibernetică la nivel regional pentru fiecare regiune de exploatare a sistemului.

(2) Planurile de atenuare a riscurilor în materie de securitate cibernetică la nivel regional includ:

(a) controale minime și controale avansate de securitate cibernetică pe care entitățile cu impact ridicat și entitățile cu impact critic le aplică în regiunea de exploatare a sistemului;

(b) riscurile reziduale în materie de securitate cibernetică în regiunile de exploatare a sistemului după aplicarea controalelor menționate la litera (a).

(3) ENTSO pentru energie electrică prezintă operatorilor de sisteme de transport relevanți, autorităților competente și Grupului de coordonare în domeniul energiei electrice planurile de atenuare a riscurilor la nivel regional. Grupul de coordonare în domeniul energiei electrice poate recomanda modificări.

(4) OST, cu sprijinul ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE și în consultare cu Grupul de cooperare NIS, actualizează o dată la trei ani planurile de atenuare a riscurilor la nivel regional, cu excepția cazului în care circumstanțele impun actualizări mai frecvente.

*Articolul 23*

**Raportul cuprinzător de evaluare a riscurilor în materie de securitate cibernetică a fluxurilor transfrontaliere de energie electrică**

(1) În termen de 40 de luni de la notificarea entităților cu impact ridicat și a entităților cu impact critic în temeiul articolului 24 alineatul (6) și, ulterior, o dată la trei ani, OST, cu sprijinul ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE și în consultare cu Grupul de cooperare NIS, furnizează Grupului de coordonare în domeniul energiei electrice un raport privind rezultatul evaluării riscurilor în materie de securitate cibernetică în ceea ce privește fluxurile transfrontaliere de energie electrică („raportul cuprinzător de evaluare a riscurilor în materie de securitate cibernetică a fluxurilor transfrontaliere de energie electrică”).

(2) Raportul cuprinzător de evaluare a riscurilor în materie de securitate cibernetică a fluxurilor transfrontaliere de energie electrică se bazează pe raportul de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii, pe rapoartele de evaluare a riscurilor în materie de securitate cibernetică ale statelor membre și pe rapoartele de evaluare a riscurilor în materie de securitate cibernetică la nivel regional și include următoarele informații:

(a) lista proceselor cu impact ridicat și a proceselor cu impact critic la nivelul Uniunii, identificate în raportul de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii în conformitate cu articolul 19 alineatul (2) litera (a), inclusiv estimarea probabilității și a impactului riscurilor în materie de securitate cibernetică evaluate în cursul rapoartelor de evaluare a riscurilor în materie de securitate cibernetică la nivel regional în temeiul articolului 21 alineatul (2) și al articolului 19 alineatul (3) litera (a);

(b) amenințările cibernetice actuale, cu un accent special pe amenințările și riscurile emergente pentru sistemul de energie electrică;

(c) atacurile cibernetice pentru perioada anterioară la nivelul Uniunii, oferind o imagine de ansamblu critică asupra modului în care astfel de atacuri cibernetice ar fi putut avea un impact asupra fluxurilor transfrontaliere de energie electrică;

(d) stadiul general al implementării măsurilor de securitate cibernetică;

(e) stadiul implementării fluxurilor de informații în temeiul articolelor 37 și 38;

(f) lista informațiilor sau a criteriilor specifice pentru clasificarea informațiilor în temeiul articolului 46;

(g) riscurile identificate și evidențiate care pot decurge din gestionarea nesigură a lanțului de aprovizionare;

(h) rezultatele și experiențele acumulate în urma exercițiilor regionale și transregionale de securitate cibernetică organizate în temeiul articolului 44;

(i) o analiză a evoluției riscurilor transfrontaliere globale în materie de securitate cibernetică în sectorul energiei electrice de la ultimele evaluări ale riscurilor în materie de securitate cibernetică la nivel regional;

(j) orice alte informații care pot fi utile pentru a identifica posibile îmbunătățiri ale prezentului regulament sau necesitatea unei revizuiri a prezentului regulament sau a oricăruia dintre instrumentele sale și

(k) informații agregate și anonimizate privind derogările acordate în temeiul articolului 30 alineatul (3).

(3) Entitățile enumerate la articolul 2 alineatul (1) pot contribui la elaborarea raportului cuprinzător de evaluare a riscurilor în materie de securitate cibernetică a fluxurilor transfrontaliere de energie electrică, respectând confidențialitatea informațiilor în conformitate cu articolul 47. OST, cu sprijinul ENTSO pentru energie electrică și în cooperare cu entitatea OSD UE, consultă aceste entități încă dintr-un stadiu incipient.

(4) Raportul cuprinzător de evaluare a riscurilor în materie de securitate cibernetică a fluxurilor transfrontaliere de energie electrică face obiectul normelor privind protecția schimbului de informații în temeiul articolului 46. Fără a aduce atingere articolului 10 alineatul (4) și articolului 47 alineatul (4), ENTSO pentru energie electrică și entitatea OSD UE publică o versiune accesibilă publicului a raportului respectiv, care nu trebuie să conțină informații care pot cauza prejudicii entităților enumerate la articolul 2 alineatul (1). Versiunea accesibilă publicului a acestui raport se publică numai cu acordul Grupului de cooperare NIS și al Grupului de coordonare în domeniul energiei electrice. ENTSO pentru energie electrică, în coordonare cu entitatea OSD UE, este responsabilă de compilarea și publicarea versiunii accesibile publicului a raportului.

*Articolul 24*

**Identificarea entităților cu impact ridicat și a entităților cu impact critic**

(1) Fiecare autoritate competentă identifică, utilizând pragurile ECII, precum și pragurile de impact ridicat și pragurile de impact critic incluse în raportul de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii în temeiul articolului 19 alineatul (3) litera (b), entitățile cu impact ridicat și entitățile cu impact critic din statul său membru care sunt implicate în procesele cu impact ridicat și în procesele cu impact critic la nivelul Uniunii. Autoritățile competente pot solicita informații de la o entitate din statul lor membru pentru a determina valorile ECII pentru entitatea respectivă. În cazul în care ECII determinat al unei entități depășește pragul de impact ridicat sau pragul de impact critic, entitatea identificată este inclusă în raportul de evaluare a riscurilor în materie de securitate cibernetică la nivel de stat membru, menționat la articolul 20 alineatul (2).

(2) Fiecare autoritate competentă identifică, utilizând pragurile ECII, precum și pragurile de impact ridicat și pragurile de impact critic incluse în raportul de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii în temeiul articolului 19 alineatul (3) litera (b), entitățile cu impact ridicat și entitățile cu impact critic care nu sunt stabilite în Uniune, în măsura în care acestea își desfășoară activitatea în Uniune. Autoritatea competentă poate solicita informații de la o entitate care nu este stabilită în Uniune pentru a determina valorile ECII pentru entitate.

(3) Fiecare autoritate competentă poate identifica entități suplimentare din statul său membru ca entități cu impact ridicat sau entități cu impact critic dacă sunt îndeplinite următoarele criterii:

(a) entitatea face parte dintr-un grup de entități supuse unui risc semnificativ de a fi afectate simultan de un atac cibernetic;

(b) ECII agregate la nivelul grupului de entități se situează peste pragul de impact ridicat sau peste pragul de impact critic.

(4) În cazul în care o autoritate competentă identifică entități suplimentare în conformitate cu alineatul (3), toate procesele din cadrul acestor entități pentru care ECII agregate în cadrul grupului depășesc pragul de impact ridicat sunt considerate procese cu impact ridicat, iar toate procesele din cadrul acestor entități pentru care ECII agregate în cadrul grupului depășesc pragurile de impact critic sunt considerate procese cu impact critic.

(5) În cazul în care identifică entități menționate la alineatul (3) litera (a) în mai multe state membre, autoritatea competentă informează celelalte autorități competente, ENTSO pentru energie electrică și entitatea OSD UE. ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE, pe baza informațiilor primite de la toate autoritățile competente, furnizează autorităților competente o analiză a agregării entităților din mai multe state membre care pot crea o perturbare distribuită a fluxurilor transfrontaliere de energie electrică și care pot duce la un atac cibernetic. În cazul în care un grup de entități din mai multe state membre este identificat ca fiind o agregare al cărei ECII depășește pragul de impact ridicat sau pragul de impact critic, toate autoritățile competente în cauză identifică entitățile din acest grup ca entități cu impact ridicat sau ca entități cu impact critic pentru statul lor membru respectiv, pe baza ECII agregate pentru grupul de entități, iar entitățile identificate trebuie enumerate în raportul de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii.

(6) În termen de nouă luni de la notificarea ENTSO pentru energie electrică și a entității OSD UE cu privire la raportul de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii în temeiul articolului 19 alineatul (5) și, în orice caz, nu mai târziu de 13 iunie 2028, fiecare autoritate competentă notifică entităților de pe listă faptul că au fost identificate ca entități cu impact ridicat sau ca entități cu impact critic în statul său membru.

(7) În cazul în care un furnizor de servicii este raportat unei autorități competente ca fiind un furnizor critic de servicii TIC în temeiul articolului 27 litera (c), autoritatea competentă respectivă notifică acest lucru autorităților competente din statele membre pe teritoriul cărora se află sediul sau reprezentantul acestui furnizor. Această din urmă autoritate competentă notifică furnizorului de servicii faptul că a fost identificat ca fiind un furnizor critic de servicii TIC.

*Articolul 25*

**Sisteme naționale de verificare**

(1) Autoritățile competente pot institui un sistem național de verificare pentru a verifica dacă entitățile cu impact critic identificate în temeiul articolului 24 alineatul (1) au pus în aplicare cadrul legislativ național care este inclus în matricea de corespondență menționată la articolul 34. Sistemul național de verificare se poate baza pe o inspecție efectuată de autoritatea competentă, pe audituri de securitate independente sau pe evaluări reciproce *inter pares* efectuate de entități cu impact critic din același stat membru, supravegheate de autoritatea competentă.

(2) În cazul în care decide să instituie un sistem național de verificare, autoritatea competentă se asigură că verificarea se efectuează în conformitate cu următoarele cerințe:

(a) orice parte care efectuează evaluarea *inter pares*, auditul sau inspecția este independentă de entitatea cu impact critic verificată și nu se află în conflict de interese;

(b) personalul care efectuează evaluarea *inter pares*, auditul sau inspecția are cunoștințe demonstrabile cu privire la:

(i) securitatea cibernetică în sectorul energiei electrice;

(ii) sistemele de gestionare a securității cibernetice;

(iii) principiile auditului;

(iv) evaluarea riscurilor în materie de securitate cibernetică;

(v) cadrul comun de securitate cibernetică în domeniul energiei electrice;

(vi) cadrul național legislativ și de reglementare și standardele europene și internaționale care fac obiectul verificării;

(vii) procesele cu impact critic care fac obiectul verificării;

(c) partea care efectuează evaluarea *inter pares*, auditul sau inspecția are la dispoziție suficient timp pentru a desfășura aceste activități;

(d) partea care efectuează evaluarea *inter pares*, auditul sau inspecția ia măsurile adecvate pentru a proteja informațiile pe care le colectează în timpul verificării, în conformitate cu nivelul de confidențialitate al acestora și

(e) evaluările *inter pares*, auditurile sau inspecțiile se efectuează cel puțin o dată pe an și acoperă întreaga sferă a verificării cel puțin o dată la trei ani.

(3) În cazul în care o autoritate competentă decide să instituie un sistem național de verificare, aceasta raportează anual ACER cu privire la frecvența cu care a efectuat inspecții în cadrul sistemului respectiv.

*Articolul 26*

**Gestionarea riscurilor în materie de securitate cibernetică la nivel de entitate**

(1) Fiecare entitate cu impact ridicat și fiecare entitate cu impact critic identificată de autoritățile competente în temeiul articolului 24 alineatul (1) efectuează gestionarea riscurilor în materie de securitate cibernetică pentru toate activele sale în perimetrul său cu impact ridicat și în perimetrul său cu impact critic. Fiecare entitate cu impact ridicat și fiecare entitate cu impact critic trebuie să efectueze o gestionare a riscurilor care să conțină etapele de la alineatul (2) o dată la trei ani.

(2) Fiecare entitate cu impact ridicat și fiecare entitate cu impact critic își bazează gestionarea riscurilor în materie de securitate cibernetică pe o abordare care urmărește să le protejeze rețelele și sistemele informatice și care cuprinde următoarele etape:

(a) stabilirea contextului;

(b) evaluarea riscurilor în materie de securitate cibernetică la nivel de entitate;

(c) tratarea riscurilor în materie de securitate cibernetică;

(d) acceptarea riscurilor în materie de securitate cibernetică.

(3) În etapa de stabilire a contextului, fiecare entitate cu impact ridicat și fiecare entitate cu impact critic:

(a) definește sfera evaluării riscurilor în materie de securitate cibernetică, inclusiv procesele cu impact ridicat și procesele cu impact critic identificate de ENTSO pentru energie electrică și de entitatea OSD UE, precum și alte procese care pot fi vizate de atacuri cibernetice cu impact ridicat sau cu impact critic asupra fluxurilor transfrontaliere de energie electrică, și

(b) definește criteriile de evaluare a riscurilor și criteriile de acceptare a riscurilor în conformitate cu matricea de evaluare a impactului riscurilor pe care entitățile și autoritățile competente trebuie să o utilizeze pentru a evalua riscurile în materie de securitate cibernetică din metodologiile de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii, la nivel regional și la nivel de stat membru, elaborate de ENTSO pentru energie electrică și de entitatea OSD UE în conformitate cu articolul 19 alineatul (2).

(4) În cursul etapei de evaluare a riscurilor în materie de securitate cibernetică, fiecare entitate cu impact ridicat și fiecare entitate cu impact critic:

(a) identifică riscurile în materie de securitate cibernetică, ținând seama de:

(i) toate activele care sprijină procesele cu impact ridicat și procesele cu impact critic la nivelul Uniunii, cu o evaluare a impactului posibil asupra fluxurilor transfrontaliere de energie electrică în cazul în care activul este compromis;

(ii) posibilele amenințări cibernetice, ținând seama de amenințările cibernetice identificate în cel mai recent raport cuprinzător de evaluare a riscurilor în materie de securitate cibernetică a fluxurilor transfrontaliere de energie electrică la care se face referire la articolul 23, precum și de amenințările la adresa lanțului de aprovizionare;

(iii) vulnerabilitățile, inclusiv vulnerabilitățile sistemelor moștenite;

(iv) posibilele scenarii de atac cibernetic, inclusiv atacuri cibernetice care afectează securitatea operațională a sistemului de energie electrică și care perturbă fluxurile transfrontaliere de energie electrică;

(v) evaluările relevante ale riscurilor și evaluările relevante efectuate la nivelul Uniunii, inclusiv evaluări coordonate ale riscurilor legate de lanțurile de aprovizionare critice, în conformitate cu articolul 22 din Directiva (UE) 2022/2555, și

(vi) controalele existente implementate;

(b) analizează probabilitatea și consecințele riscurilor în materie de securitate cibernetică identificate la litera (a) și determină nivelul de risc de securitate cibernetică utilizând matricea de evaluare a impactului riscurilor utilizată pentru a evalua riscurile în materie de securitate cibernetică din metodologiile de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii, la nivel regional și la nivel de stat membru, elaborate de OST, cu sprijinul ENTSO pentru energie electrică și în cooperare cu entitatea OSD UE în conformitate cu articolul 19 alineatul (2);

(c) clasifică activele în funcție de posibilele consecințe atunci când este compromisă securitatea cibernetică și determină perimetrul cu impact ridicat și perimetrul cu impact critic utilizând următoarele etape:

(i) efectuează, pentru toate procesele care fac obiectul evaluării riscurilor în materie de securitate cibernetică, o evaluare a impactului asupra activității utilizând ECII;

(ii) clasifică un proces ca având un impact ridicat sau un impact critic dacă ECII se situează peste pragul de impact ridicat sau, respectiv, peste pragul de impact critic;

(iii) determină toate activele cu impact ridicat și toate activele cu impact critic ca fiind activele necesare pentru procesele cu impact ridicat și, respectiv, pentru procesele cu impact critic;

(iv) definesc perimetrele cu impact ridicat și perimetrele cu impact critic care conțin toate activele cu impact ridicat și, respectiv, toate activele cu impact critic, astfel încât accesul la perimetre să poată fi controlat;

(d) evaluează riscurile în materie de securitate cibernetică, ierarhizându-le prin intermediul criteriilor de evaluare a riscurilor și al criteriilor de acceptare a riscurilor menționate la alineatul (3) litera (b).

(5) În cursul etapei de tratare a riscurilor în materie de securitate cibernetică, fiecare entitate cu impact ridicat și fiecare entitate cu impact critic stabilește un plan de atenuare a riscurilor la nivel de entitate prin selectarea opțiunilor de tratare a riscurilor adecvate pentru gestionarea riscurilor și pentru identificarea riscurilor reziduale.

(6) În cursul etapei de acceptare a riscului în materie de securitate cibernetică, fiecare entitate cu impact ridicat și fiecare entitate cu impact critic decide dacă acceptă riscul rezidual pe baza criteriilor de acceptare a riscurilor, stabilite la alineatul (3) litera (b).

(7) Fiecare entitate cu impact ridicat și fiecare entitate cu impact critic trebuie să înregistreze activele identificate la alineatul (1) într-un inventar al activelor. Acest inventar al activelor nu face parte din raportul de evaluare a riscurilor.

(8) Autoritatea competentă poate inspecta activele inventarului în timpul inspecțiilor.

*Articolul 27*

**Raportarea cu privire la evaluarea riscurilor la nivel de entitate**

Fiecare entitate cu impact ridicat și fiecare entitate cu impact critic transmite autorității competente, în termen de 12 luni de la notificarea entităților cu impact ridicat și a entităților cu impact critic în temeiul articolului 24 alineatul (6) și, ulterior, o dată la trei ani, un raport care conține următoarele informații:

1. o listă a controalelor selectate pentru planul de atenuare a riscurilor la nivel de entitate în temeiul articolului 26 alineatul (5), însoțită de stadiul actual de implementare a fiecărui control;

2. pentru fiecare proces cu impact ridicat sau proces cu impact critic la nivelul Uniunii, o estimare a riscului de compromitere a confidențialității, integrității și disponibilității informațiilor și ale activelor relevante. Estimarea acestui risc se face în conformitate cu matricea de evaluare a impactului riscurilor de la articolul 19 alineatul (2);

3. o listă a furnizorilor critici de servicii TIC pentru procesele lor cu impact critic.

CAPITOLUL III

**CADRUL COMUN DE SECURITATE CIBERNETICĂ ÎN DOMENIUL ENERGIEI ELECTRICE**

*Articolul 28*

**Componența, funcționarea și revizuirea cadrului comun de securitate cibernetică în domeniul energiei electrice**

(1) Cadrul comun de securitate cibernetică în domeniul energiei electrice este compus din următoarele controale și din sistemul de gestionare a securității cibernetice:

(a) controalele minime de securitate cibernetică, elaborate în conformitate cu articolul 29;

(b) controalele avansate de securitate cibernetică, elaborate în conformitate cu articolul 29;

(c) matricea de corespondență, elaborată în conformitate cu articolul 34, care corelează controalele menționate la literele (a) și (b) cu standardele europene și internaționale selectate și cu cadrele legislative sau de reglementare naționale;

(d) sistemul de gestionare a securității cibernetice instituit în temeiul articolului 32.

(2) Toate entitățile cu impact ridicat aplică controalele minime de securitate cibernetică în temeiul alineatului (1) litera (a) în perimetrul lor cu impact ridicat.

(3) Toate entitățile cu impact critic aplică controalele avansate de securitate cibernetică în temeiul alineatului (1) litera (b) în perimetrul lor cu impact critic.

(4) În termen de 7 luni de la transmiterea primului proiect de raport de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii în temeiul articolului 19 alineatul (4), cadrul comun de securitate cibernetică în domeniul energiei electrice menționat la alineatul (1) este completat de controale minime și de controale avansate de securitate cibernetică în lanțul de aprovizionare, elaborate în temeiul articolului 33.

*Articolul 29*

**Controale minime și controale avansate de securitate cibernetică**

(1) În termen de 7 luni de la transmiterea primului proiect de raport de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii în temeiul articolului 19 alineatul (4), OST, cu sprijinul ENTSO de energie electrică și în cooperare cu entitatea OSD UE, elaborează o propunere pentru controalele minime și pentru controalele avansate de securitate cibernetică.

(2) În termen de 6 luni de la elaborarea fiecărui raport de evaluare a riscurilor în materie de securitate cibernetică la nivel regional în temeiul articolului 21 alineatul (2), OST, cu sprijinul ENTSO pentru energie electrică și în cooperare cu entitatea OSD UE, propun autorității competente o modificare a controalelor minime și a controalelor avansate de securitate cibernetică. Propunerea se va realiza în conformitate cu articolul 8 alineatul (10) și va ține seama de riscurile identificate în evaluarea riscurilor la nivel regional.

(3) Controalele minime și controalele avansate de securitate cibernetică trebuie să poată fi verificate prin participarea la un sistem național de verificare în conformitate cu procedura prevăzută la articolul 31 sau prin efectuarea de audituri de securitate de către terți independenți în conformitate cu cerințele enumerate la articolul 25 alineatul (2).

(4) Controalele de securitate cibernetică inițiale, atât cele minime, cât și cele avansate, elaborate în temeiul alineatului (1), se bazează pe riscurile identificate în raportul de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii menționat la articolul 19 alineatul (5). Controalele de securitate cibernetică modificate, atât cele minime, cât și cele avansate, elaborate în temeiul alineatului (2), se bazează pe raportul de evaluare a riscurilor în materie de securitate cibernetică la nivel regional menționat la articolul 21 alineatul (2).

(5) Controalele minime de securitate cibernetică includ controale menite să protejeze informațiile schimbate în temeiul articolului 46.

(6) În termen de 12 luni de la aprobarea controalelor minime și a controalelor avansate de securitate cibernetică în temeiul articolului 8 alineatul (5) sau după fiecare actualizare în temeiul articolului 8 alineatul (10), entitățile enumerate la articolul 2 alineatul (1) și identificate ca entități cu impact critic și ca entități cu impact ridicat în temeiul articolului 24 aplică, în timpul elaborării planului de atenuare a riscurilor la nivel de entitate în temeiul articolului 26 alineatul (5), controalele minime de securitate cibernetică în perimetrul cu impact ridicat și controalele avansate de securitate cibernetică în perimetrul cu impact critic.

*Articolul 30*

**Derogări de la controalele minime și de la controalele avansate de securitate cibernetică**

(1) Entitățile enumerate la articolul 2 alineatul (1) pot solicita autorității competente respective să acorde o derogare de la obligația de a aplica controalele minime și controalele avansate de securitate cibernetică menționate la articolul 29 alineatul (6). Autoritatea competentă poate acorda o astfel de derogare pe baza unuia dintre următoarele motive:

(a) în circumstanțe excepționale, atunci când entitatea poate demonstra că implementarea controalelor de securitate cibernetică adecvate presupune costuri care depășesc în mod semnificativ beneficiile. ACER și ENTSO pentru energie electrică, în cooperare cu entitatea OSD, pot elabora în comun orientări pentru estimarea costurilor controalelor de securitate cibernetică pentru a ajuta entitățile;

(b) în cazul în care entitatea furnizează un plan de tratare a riscurilor la nivel de entitate care atenuează riscurile de securitate cibernetică utilizând controale alternative la un nivel acceptabil în conformitate cu criteriile de acceptare a riscurilor menționate la articolul 26 alineatul (3) litera (b).

(2) În termen de trei luni de la primirea cererii menționate la alineatul (1), fiecare autoritate competentă decide dacă trebuie acordată o derogare de la controalele minime și de la controalele avansate de securitate cibernetică. Derogările de la controalele minime sau de la controalele avansate de securitate cibernetică se acordă pentru o perioadă maximă de trei ani, cu posibilitatea de reînnoire.

(3) Informațiile agregate și anonimizate pentru derogările acordate se includ ca anexă la raportul cuprinzător de evaluare a riscurilor în materie de securitate cibernetică a fluxurilor transfrontaliere de energie electrică menționat la articolul 23. ENTSO pentru energie electrică și entitatea OSD UE actualizează în comun lista, dacă este necesar.

*Articolul 31*

**Verificarea cadrului comun de securitate cibernetică în domeniul energiei electrice**

(1) În termen de maximum 24 de luni de la adoptarea controalelor menționate la articolul 28 alineatul (1) literele (a)-(c) și de la instituirea sistemului de gestionare a securității cibernetice menționat la litera (d) de la articolul respectiv, fiecare entitate cu impact critic identificată în conformitate cu articolul 24 alineatul (1) trebuie să fie în măsură să demonstreze, la cererea autorității competente, conformitatea cu sistemul de gestionare a securității cibernetice și cu controalele minime sau controalele avansate de securitate cibernetică.

(2) Fiecare entitate cu impact critic îndeplinește obligația menționată la alineatul (1) prin efectuarea de audituri de securitate de către terți independenți, în conformitate cu cerințele enumerate la articolul 25 alineatul (2), sau prin participarea la un sistem național de verificare în conformitate cu articolul 25 alineatul (1).

(3) Verificarea faptului că o entitate cu impact critic respectă sistemul de gestionare a securității cibernetice și controalele minime sau controalele avansate de securitate cibernetică vizează toate activele din perimetrul cu impact critic al entității cu impact critic.

(4) Verificarea faptului că o entitate cu impact critic respectă sistemul de gestionare a securității cibernetice și controalele minime sau controalele avansate de securitate cibernetică se repetă periodic cel târziu la 36 de luni de la încheierea primei verificări și, ulterior, o dată la trei ani.

(5) Fiecare entitate cu impact critic definită în conformitate cu articolul 24 demonstrează că respectă controalele menționate la articolul 28 alineatul (1) literele (a)-(c) și că a instituit sistemul de gestionare a securității cibernetice menționat la litera (d) de la articolul respectiv prin transmiterea rezultatului verificării conformității către autoritatea competentă.

*Articolul 32*

**Sistemul de gestionare a securității cibernetice**

(1) Fiecare entitate cu impact ridicat și fiecare entitate cu impact critic, în termen de 24 de luni de la data la care autoritatea competentă i-a notificat faptul că a fost identificată drept entitate cu impact ridicat sau drept entitate cu impact critic în conformitate cu articolul 24 alineatul (6), instituie un sistem de gestionare a securității cibernetice și, ulterior, îl revizuiește o dată la trei ani în următoarele scopuri:

(a) ca să stabilească domeniul de aplicare al sistemului de gestionare a securității cibernetice, luând în considerare interfețele cu alte entități și dependențele față de acestea;

(b) ca să se asigure că toți membrii conducerii sale superioare sunt informați cu privire la obligațiile legale relevante și contribuie activ la implementarea sistemului de gestionare a securității cibernetice prin decizii rapide și reacții prompte;

(c) ca să asigure disponibilitatea resurselor necesare funcționării sistemului de gestionare a securității cibernetice;

(d) ca să instituie o politică de securitate cibernetică documentată și comunicată, accesibilă atât în cadrul entității, cât și părților afectate de riscurile de securitate;

(e) ca să atribuie și să comunice responsabilitățile pentru rolurile pertinente în securitatea cibernetică;

(f) ca să efectueze gestionarea riscurilor de securitate cibernetică la nivel de entitate, astfel cum este definită la articolul 26;

(g) ca să stabilească și să furnizeze resursele necesare pentru implementarea, întreținerea și îmbunătățirea continuă a sistemului de gestionare a securității cibernetice, ținând seama de competența necesară și de sensibilizarea cu privire la resursele de securitate cibernetică;

(h) ca să determine comunicarea internă și externă relevantă pentru securitatea cibernetică;

(i) ca să creeze, actualizeze și controleze informații documentate legate de sistemul de gestionare a securității cibernetice;

(j) ca să evalueze performanța și eficacitatea sistemului de gestionare a securității cibernetice;

(k) ca să efectueze audituri interne la intervale planificate pentru a se asigura că sistemul de gestionare a securității cibernetice este implementat și întreținut cu eficacitate;

(l) ca să revizuiască implementarea sistemului de gestionare a securității cibernetice la intervale planificate; și ca să controleze și corecteze neconformitatea resurselor și activităților cu politicile, procedurile și orientările din sistemul de gestionare a securității cibernetice.

(2) Domeniul de aplicare al sistemului de gestionare a securității cibernetice include toate activele din perimetrul cu impact ridicat și din perimetrul cu impact critic al entității cu impact ridicat și al entității cu impact critic.

(3) Fără a impune sau a face o discriminare în favoarea utilizării unui anumit tip de tehnologie, autoritățile competente încurajează utilizarea standardelor și specificațiilor europene sau internaționale referitoare la sistemele de management și relevante pentru securitatea rețelelor și a sistemelor informatice.

*Articolul 33*

**Controale minime și controale avansate de securitate cibernetică în lanțul de aprovizionare**

(1) În termen de șapte luni de la transmiterea primului proiect de raport de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii în temeiul articolului 19 alineatul (4), OST, cu sprijinul ENTSO pentru energie electrică și în cooperare cu entitatea OSD UE, elaborează o propunere de controale minime și de controale avansate de securitate cibernetică în lanțul de aprovizionare, care să atenueze riscurile legate de lanțul de aprovizionare identificate în evaluările riscurilor în materie de securitate cibernetică la nivelul Uniunii, completând controalele minime și controalele avansate de securitate cibernetică elaborate în temeiul articolului 29. Controalele minime și controalele avansate de securitate cibernetică în lanțul de aprovizionare se elaborează împreună cu controalele minime și cu controalele avansate de securitate cibernetică în temeiul articolului 29. Controalele minime și controalele avansate de securitate cibernetică în lanțul de aprovizionare acoperă întregul ciclu de viață al tuturor produselor TIC, serviciilor TIC și proceselor TIC din perimetrul cu impact ridicat sau din perimetrul cu impact critic al unei entități cu impact ridicat sau al unei entități cu impact critic. Grupul de cooperare NIS este consultat la elaborarea propunerii de controale minime și de controale avansate de securitate cibernetică în lanțul de aprovizionare.

(2) Controalele minime de securitate cibernetică în lanțul de aprovizionare constau în controale pentru entitățile cu impact ridicat și pentru entitățile cu impact critic care:

(a) să includă recomandări pentru achizițiile publice de produse TIC, de servicii TIC și de procese TIC referitoare la specificațiile în materie de securitate cibernetică, care să acopere cel puțin:

(i) verificările antecedentelor personalului furnizorului implicat în lanțul de aprovizionare și care se ocupă de informații sensibile sau de accesul la activele cu impact ridicat sau la activele cu impact critic ale entității. Verificarea antecedentelor poate include o verificare a identității și a antecedentelor personalului sau ale contractanților unei entități în conformitate cu dreptul și procedurile naționale și cu dreptul relevant și aplicabil al Uniunii, inclusiv cu Regulamentul (UE) 2016/679 și cu Directiva (UE) 2016/680 a Parlamentului European și a Consiliului ([18]). Verificările antecedentelor sunt proporționale și strict limitate la ceea ce este necesar. Acestea se efectuează exclusiv în scopul evaluării unui potențial risc de securitate pentru entitatea în cauză. Ele trebuie să fie proporționale cu cerințele comerciale, cu clasificarea informațiilor care trebuie accesate și cu riscurile percepute și pot fi efectuate de entitatea însăși, de o societate externă care efectuează o examinare sau prin intermediul unei autorizații administrative;

(ii) procesele de proiectare, dezvoltare și producție sigure și controlate de produse TIC, servicii TIC și procese TIC, care promovează proiectarea și dezvoltarea de produse TIC, servicii TIC și procese TIC, care includ măsuri tehnice adecvate pentru asigurarea securității cibernetice;

(iii) proiectarea rețelelor și a sistemelor informatice în care dispozitivele nu sunt fiabile nici atunci când se află într-un perimetru securizat, necesită verificarea tuturor cererilor pe care le primesc și aplică principiul celor mai mici privilegii;

(iv) accesul furnizorului la activele entității;

([18]) Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L 119, 4.5.2016, p. 89).

(v) obligațiile contractuale ale furnizorului de a proteja și restricționa accesul la informațiile sensibile ale entității;

(vi) specificațiile care stau la baza achizițiilor publice în materie de securitate cibernetică pentru subcontractanții furnizorului;

(vii) trasabilitatea aplicării specificațiilor de securitate cibernetică, de la dezvoltare la producție și la livrarea de produse TIC, servicii TIC sau procese TIC;

(viii) sprijinirea actualizărilor de securitate pe parcursul întregii durate de viață a produselor TIC, a serviciilor TIC sau a proceselor TIC;

(ix) dreptul de a audita securitatea cibernetică în procesele de proiectare, dezvoltare și producție ale furnizorului și

(x) evaluarea profilului de risc al furnizorului;

(b) impun acestor entități să țină seama de recomandările de achiziții menționate la litera (a) atunci când încheie contracte cu furnizorii, cu parteneri de colaborare și cu alte părți din lanțul de aprovizionare, care vizează livrările obișnuite de produse TIC, servicii TIC și procese TIC, precum și de evenimente și circumstanțe nesolicitate, cum ar fi rezilierea și tranziția contractelor în cazuri de neglijență a partenerului contractual;

(c) impun acestor entități să țină seama de rezultatele evaluărilor coordonate relevante ale riscurilor în materie de securitate ale lanțurilor de aprovizionare critice, efectuate în conformitate cu articolul 22 alineatul (1) din Directiva (UE) 2022/2555;

(d) includ criterii pentru selectarea și contractarea furnizorilor care pot îndeplini specificațiile de securitate cibernetică menționate la litera (a) și care dețin un nivel de securitate cibernetică adecvat riscurilor în materie de securitate cibernetică ale produsului TIC, serviciului TIC sau proceselor TIC pe care furnizorul le livrează;

(e) includ criterii de diversificare a surselor de aprovizionare pentru produsele TIC, serviciile TIC și procesele TIC și reduc riscul de dependență de furnizor;

(f) includ criterii de monitorizare, revizuire sau auditare periodică a specificațiilor de securitate cibernetică pentru procesele operaționale interne ale furnizorilor pe parcursul întregului ciclu de viață al fiecărui produs TIC, serviciu TIC și proces TIC.

(3) În ceea ce privește specificațiile de securitate cibernetică din recomandarea privind achizițiile în materie de securitate cibernetică menționată la alineatul (2) litera (a), entitățile cu impact ridicat sau entitățile cu impact critic utilizează principiile achizițiilor publice în temeiul Directivei 2014/24/UE a Parlamentului European și a Consiliului ([19]), în conformitate cu articolul 35 alineatul (4), sau își definesc propriile specificații pe baza rezultatelor evaluării riscurilor în materie de securitate cibernetică la nivel de entitate.

(4) Controalele avansate de securitate cibernetică din lanțul de aprovizionare includ controale pentru entitățile cu impact critic cu scopul de a verifica, în timpul achizițiilor publice, dacă produsele TIC, serviciile TIC și procesele TIC care vor fi utilizate ca active cu impact critic îndeplinesc specificațiile de securitate cibernetică. Produsul TIC, serviciul TIC sau procesul TIC se verifică fie prin intermediul unui sistem european de certificare a securității cibernetice menționat la articolul 31, fie prin activitățile de verificare selectate și organizate de entitate. Profunzimea și acoperirea activităților de verificare trebuie să fie suficiente pentru a oferi asigurarea că produsul TIC, serviciul TIC sau procesul TIC poate fi utilizat pentru a atenua riscurile identificate în evaluarea riscurilor la nivel de entitate. Entitatea cu impact critic trebuie să documenteze măsurile luate pentru a reduce riscurile identificate.

(5) Controalele minime și controalele avansate de securitate cibernetică din lanțul de aprovizionare se aplică achizițiilor de produse TIC, servicii TIC și procese TIC relevante. Controalele minime și controalele avansate în materie de securitate cibernetică ale lanțului de aprovizionare se vor aplica proceselor de achiziții publice din entitățile identificate ca fiind entități cu impact critic și entități cu impact ridicat în conformitate cu articolul 24, care încep la șase luni de la adoptarea sau actualizarea controalelor minime și controalelor avansate de securitate cibernetică menționate la articolul 29.

([19]) Directiva 2014/24/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind achizițiile publice și de abrogare a Directivei 2004/18/CE (JO L 94, 28.3.2014, p. 65).

(6) În termen de 6 luni de la elaborarea fiecărui raport de evaluare a riscurilor în materie de securitate cibernetică la nivel regional în temeiul articolului 21 alineatul (2), OST, cu sprijinul ENTSO pentru energie electrică și în cooperare cu entitatea OSD UE, propun autorității competente o modificare a controalelor minime și a controalelor avansate de securitate cibernetică din lanțul de aprovizionare. Propunerea se va realiza în conformitate cu articolul 8 alineatul (10) și va ține seama de riscurile identificate în evaluarea riscurilor la nivel regional.

*Articolul 34*

**Matricea de corespondență a controalelor de securitate cibernetică în domeniul energiei electrice în raport cu standardele**

(1) În termen de 7 luni de la transmiterea primului proiect de raport de evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii în temeiul articolului 19 alineatul (4), OST, cu sprijinul ENTSO pentru energie electrică și în cooperare cu entitatea OSD UE și în consultare cu ENISA, elaborează o propunere de matrice pentru punerea în corespondență a controalelor prevăzute la articolul 28 alineatul (1) literele (a) și (b) cu standardele europene și internaționale selectate, precum și cu specificațiile tehnice relevante („matricea de corespondență”). ENTSO pentru energie electrică și entitatea OSD UE documentează echivalența diferitelor controale cu controalele prevăzute la articolul 28 alineatul (1) literele (a) și (b).

(2) Autoritățile competente pot furniza ENTSO pentru energie electrică și entității OSD UE o punere în corespondență a controalelor prevăzute la articolul 28 alineatul (1) literele (a) și (b), cu o trimitere la cadrele legislative sau de reglementare naționale aferente, inclusiv la standardele naționale relevante ale statelor membre în temeiul articolului 25 din Directiva (UE) 2022/2555. În cazul în care autoritatea competentă a unui stat membru furnizează o astfel de punere în corespondență, ENTSO pentru energie electrică și entitatea OSD UE o integrează în matricea de corespondență.

(3) În termen de 6 luni de la elaborarea fiecărui raport de evaluare a riscurilor în materie de securitate cibernetică la nivel regional în temeiul articolului 21 alineatul (2), OST, cu sprijinul ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE și în consultare cu ENISA, propun autorității competente o modificare a matricei de corespondență. Propunerea se va realiza în conformitate cu articolul 8 alineatul (10) și va ține seama de riscurile identificate în evaluarea riscurilor la nivel regional.

CAPITOLUL IV

**RECOMANDĂRI PRIVIND ACHIZIȚIILE PUBLICE ÎN DOMENIUL SECURIĂȚII CIBERNETICE**

*Articolul 35*

**Recomandări privind achizițiile publice în domeniul securității cibernetice**

(1) OST, cu sprijinul ENTSO pentru energie electrică și în cooperare cu entitatea OSD UE, elaborează, în cadrul unui program de lucru care urmează să fie stabilit și actualizat de fiecare dată când se adoptă un raport de evaluare a riscurilor în materie de securitate cibernetică la nivel regional, seturi de recomandări fără caracter obligatoriu privind achizițiile în domeniul securității cibernetice pe care entitățile cu impact ridicat și entitățile cu impact critic le pot utiliza ca bază pentru achiziționarea de produse TIC, servicii TIC și procese TIC în perimetre cu impact ridicat și în perimetre cu impact critic. Programul de lucru cuprinde următoarele aspecte:

(a) o descriere și o clasificare a tipurilor de produse TIC, servicii TIC și procese TIC utilizate de entitățile cu impact ridicat și de entitățile cu impact critic în perimetrul cu impact ridicat și în perimetrul cu impact critic;

(b) o listă a tipurilor de produse TIC, servicii TIC și procese TIC pentru care se elaborează un set de recomandări în materie de securitate cibernetică fără caracter obligatoriu, pe baza rapoartelor relevante de evaluare a riscurilor în materie de securitate cibernetică la nivel regional și a priorităților entităților cu impact ridicat și ale entităților cu impact critic.

(2) În termen de 6 luni de la adoptarea sau actualizarea raportului de evaluare a riscurilor în materie de securitate cibernetică la nivel regional, ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE, furnizează ACER un rezumat al programului de lucru respectiv.

(3) OST, cu sprijinul ENTSO pentru energie electrică și în cooperare cu entitatea OSD UE, depun eforturi pentru a se asigura că recomandările fără caracter obligatoriu privind achizițiile în domeniul securității cibernetice elaborate pe baza evaluării relevante a riscurilor în materie de securitate cibernetică la nivel regional sunt similare sau comparabile între regiunile de exploatare a sistemului. Seturile de recomandări privind achizițiile în domeniul securității cibernetice acoperă cel puțin specificațiile menționate la articolul 33 alineatul (2) litera (a). Acolo unde este posibil, specificațiile trebuie selectate din standardele europene și internaționale.

(4) OST, cu sprijinul ENTSO pentru energie electrică și în cooperare cu entitatea OSD UE, se asigură că seturile de recomandări privind achizițiile în domeniul securității cibernetice:

(a) respectă principiile achizițiilor publice în temeiul Directivei 2014/24/UE și

(b) sunt compatibile cu cele mai recente sisteme europene de certificare a securității cibernetice disponibile, relevante pentru produsul TIC, serviciul TIC sau procesul TIC, și țin seama de acestea.

*Articolul 36*

**Orientări privind utilizarea sistemelor europene de certificare a securității cibernetice pentru achiziționarea de produse TIC, servicii TIC și procese TIC**

(1) Recomandările fără caracter obligatoriu privind achizițiile în domeniul securității cibernetice elaborate în temeiul articolului 35 pot include orientări sectoriale specifice privind utilizarea sistemelor europene de certificare a securității cibernetice, ori de câte ori este disponibil un sistem adecvat pentru un tip de produs TIC, serviciu TIC sau proces TIC utilizat de entități cu impact critic, fără a aduce atingere cadrului pentru instituirea sistemelor europene de certificare a securității cibernetice în temeiul articolului 46 din Regulamentul (UE) 2019/881.

(2) OST, cu sprijinul ENTSO pentru energie electrică și în cooperare cu entitatea OSD UE, cooperează îndeaproape cu ENISA la furnizarea orientărilor sectoriale incluse în recomandările fără caracter obligatoriu privind achizițiile în domeniul securității cibernetice în temeiul alineatului (1).

CAPITOLUL V

**FLUXURILE DE INFORMAȚII, ATACURILE CIBERNETICE ȘI GESTIONAREA CRIZELOR**

*Articolul 37*

**Norme privind schimbul de informații**

(1) În cazul în care primește informații referitoare la un atac cibernetic raportabil, o autoritate competentă are următoarele obligații:

(a) evaluează nivelul de confidențialitate al informațiilor respective și informează entitatea cu privire la rezultatul evaluării sale fără întârzieri nejustificate și nu mai târziu de 24 de ore de la primirea informațiilor;

(b) încearcă să găsească orice alt atac cibernetic similar în Uniune raportat altor autorități competente, pentru a corela informațiile primite în contextul atacului cibernetic raportabil cu informațiile furnizate în contextul altor atacuri cibernetice și pentru a îmbogăți informațiile existente, a consolida și a coordona răspunsurile în materie de securitate cibernetică;

(c) este responsabilă de eliminarea secretelor de afaceri și de anonimizarea informațiilor în conformitate cu normele relevante de la nivel național și de la nivelul Uniunii;

(d) comunică informațiile punctelor unice de contact naționale, echipelor CSIRT și tuturor autorităților competente ale altor state membre, desemnate în temeiul articolului 4, fără întârzieri nejustificate și în termen de cel mult 24 de ore de la primirea informațiilor referitoare la un atac cibernetic raportabil și furnizează periodic informații actualizate autorităților sau organismelor respective;

(e) diseminează informațiile privind atacul cibernetic, după anonimizarea și eliminarea secretelor de afaceri în temeiul alineatului (1) litera (c), entităților cu impact critic și entităților cu impact ridicat din statul său membru, fără întârzieri nejustificate și în termen de cel mult 24 de ore de la primirea informațiilor în conformitate cu alineatul (1) litera (a), și furnizează periodic informații actualizate care să permită entităților să își organizeze apărarea în mod eficace;

(f) poate solicita entității raportoare cu impact ridicat sau entității raportoare cu impact critic să disemineze în continuare informațiile raportabile privind atacurile cibernetice în mod securizat către alte entități care pot fi afectate, cu scopul de a genera conștientizarea situației de către sectorul energiei electrice și de a preveni materializarea unui risc care ar putea escalada, devenind un incident transfrontalier de securitate cibernetică în sectorul energiei electrice;

(g) transmite ENISA un raport de sinteză, după anonimizare și eliminarea secretelor de afaceri, cu informații privind atacul cibernetic.

(2) În cazul în care ia cunoștință de o vulnerabilitate necorectată exploatată activ, o echipă CSIRT are următoarele obligații:

(a) să o partajeze fără întârziere cu ENISA prin intermediul unui canal securizat adecvat de schimb de informații, cu excepția cazului în care se prevede altfel în alte acte legislative ale Uniunii;

(b) să sprijine entitatea în cauză să primească din partea producătorului sau a furnizorului o gestionare eficace, coordonată și rapidă a vulnerabilității necorectate exploatate activ sau a unor măsuri de atenuare eficace și eficiente;

(c) să facă schimb de informații disponibile cu vânzătorul și să solicite producătorului sau furnizorului, atunci când este posibil, să identifice o listă a CSIRT din statele membre vizate de vulnerabilitatea necorectată exploatată activ și care să fie informată;

(d) să partajeze informațiile disponibile cu echipele CSIRT identificate la litera anterioară, pe baza principiului necesității de a cunoaște;

(e) să partajeze, acolo unde există, strategiile și măsurile de atenuare cu vulnerabilitatea necorectată exploatată activ care a fost raportată.

(3) În cazul în care ia cunoștință de o vulnerabilitate necorectată exploatată activ, o autoritate competentă are următoarele obligații:

(a) să partajeze, în cazul în care există, strategiile și măsurile de atenuare cu vulnerabilitatea necorectată exploatată activ care a fost raportată, în coordonare cu echipele CSIRT din statul său membru;

(b) să comunice informațiile unei echipe CSIRT din statul membru în care a fost raportată vulnerabilitatea necorectată exploatată activ.

(4) În cazul în care ia cunoștință de o vulnerabilitate necorectată, fără a dovedi că a fost încă exploatată activ, autoritatea competentă se coordonează, fără întârzieri nejustificate, cu CSIRT în scopul divulgării coordonate a vulnerabilităților, astfel cum se prevede la articolul 12 alineatul (1) din Directiva (UE) 2022/2555.

(5) În cazul în care primește informații legate de amenințări cibernetice de la una sau mai multe entități cu impact ridicat sau de la una sau mai multe entități cu impact critic în temeiul articolului 38 alineatul (6), o echipă CSIRT diseminează informațiile respective sau orice alte informații importante pentru prevenirea, detectarea, răspunsul sau atenuarea riscului asociat entităților cu impact critic și entităților cu impact ridicat din statul său membru și, după caz, tuturor echipelor CSIRT vizate și punctului său unic de contact național, fără întârzieri nejustificate și în termen de cel mult patru ore de la primirea informațiilor.

(6) În cazul în care ia cunoștință de informații legate de amenințările cibernetice de la una sau mai multe entități cu impact ridicat sau cu impact critic, o autoritate competentă transmite aceste informații echipei CSIRT în sensul alineatului (5).

(7) Autoritățile competente pot delega integral sau parțial responsabilitățile prevăzute la alineatele (3) și (4) privind una sau mai multe entități cu impact ridicat sau cu impact critic care își desfășoară activitatea în mai multe state membre unei alte autorități competente dintr-unul dintre statele membre respective, în urma unui acord între autoritățile competente în cauză.

(8) OST, cu sprijinul ENTSO pentru energie electrică și în cooperare cu entitatea OSD UE, elaborează o metodologie a grilei de clasificare a atacurilor cibernetice până la 13 iunie 2025. OST, cu sprijinul ENTSO pentru energie electrică și al entității OSD UE, pot solicita autorităților competente să consulte ENISA și autoritățile lor competente responsabile cu securitatea cibernetică pentru asistență la elaborarea unei astfel de grile de clasificare. Metodologia prevede clasificarea gravității unui atac cibernetic în funcție de 5 niveluri, cele mai înalte două niveluri fiind „ridicat" și „critic". Clasificarea se bazează pe evaluarea următorilor parametri:

(a) impactul potențial având în vedere activele și perimetrele expuse, determinate în conformitate cu articolul 26 alineatul (4) litera (c) și

(b) gravitatea atacului cibernetic.

(9) Până la 13 iunie 2026, ENTSO pentru energie electrică, în colaborare cu entitatea OSD UE, efectuează un studiu de fezabilitate pentru a evalua posibilitatea și costurile financiare necesare dezvoltării unui instrument comun care să permită tuturor entităților să facă schimb de informații cu autoritățile naționale relevante.

(10) Studiul de fezabilitate abordează posibilitatea ca un astfel de instrument comun:

(a) să sprijine entitățile cu impact critic și entitățile cu impact ridicat furnizându-le informații relevante legate de securitatea operațiunilor legate de fluxuri transfrontaliere de energie electrică, cum ar fi raportarea în timp aproape real a atacurilor cibernetice, alertele timpurii legate de aspecte legate de securitatea cibernetică și vulnerabilitățile nedivulgate ale echipamentelor utilizate în sistemul de energie electrică;

(b) să fie menținut într-un mediu adecvat și foarte fiabil;

(c) să permită colectarea de date de la entități cu impact critic și de la entități cu impact ridicat și să faciliteze eliminarea informațiilor confidențiale și anonimizarea datelor, precum și diseminarea promptă a acestora către entitățile cu impact critic și entitățile cu impact ridicat.

(11) ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE:

(a) consultă ENISA și Grupul de cooperare NIS, punctele unice de contact naționale și reprezentanții principalelor părți interesate atunci când evaluează fezabilitatea;

(b) prezintă rezultatele studiului de fezabilitate ACER și Grupului de cooperare NIS.

(12) ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE, poate analiza și facilita inițiativele propuse de entitățile cu impact critic și de entitățile cu impact ridicat pentru a evalua și testa astfel de instrumente pentru schimbul de informații.

*Articolul 38*

**Rolul entităților cu impact ridicat și al entităților cu impact critic în ceea ce privește schimbul de informații**

(1) Fiecare entitate cu impact ridicat și fiecare entitate cu impact critic:

(a) stabilește, pentru toate activele din perimetrul său de securitate cibernetică stabilit în temeiul articolului 26 alineatul (4) litera (c), cel puțin capacitățile CSOC pentru:

(i) a se asigura că rețelele și sistemele informatice, precum și aplicațiile relevante furnizează jurnale de securitate pentru monitorizarea securității, care să permită detectarea anomaliilor și colectarea de informații privind atacurile cibernetice;

(ii) a efectua monitorizarea securității, inclusiv detectarea intruziunilor și evaluarea vulnerabilităților rețelelor și ale sistemelor informatice;

(iii) a analiza și, dacă este necesar, a întreprinde toate acțiunile necesare aflate sub responsabilitatea sa și aferente calității sale, în scopul protejării entității;

(iv) a participa la colectarea și la schimbul de informații descrise la prezentul articol;

(b) are dreptul de a achiziționa, integral sau parțial, aceste capacități în temeiul literei (a) prin intermediul MSSP-urilor. Entitățile cu impact critic și entitățile cu impact ridicat rămân responsabile pentru MSSP și supraveghează eforturile acestora;

(c) desemnează un punct unic de contact la nivel de entitate în scopul schimbului de informații.

(2) ENISA poate emite orientări fără caracter obligatoriu privind instituirea unor astfel de capacități sau subcontractarea serviciului către MSSP, ca parte a sarcinii definite la articolul 6 alineatul (2) din Regulamentul (UE) 2019/881.

(3) Fiecare entitate cu impact critic și fiecare entitate cu impact ridicat face schimb de informații relevante referitoare la un atac cibernetic raportabil cu echipele sale CSIRT și cu autoritatea sa competentă, fără întârzieri nejustificate și în termen de cel mult patru ore de la momentul în care a luat cunoștință de faptul că incidentul este raportabil.

(4) Informațiile referitoare la un atac cibernetic sunt considerate raportabile atunci când atacul cibernetic este evaluat de entitatea afectată ca având un nivel de criticalitate care variază de la „ridicat" la „critic" conform metodologiei de clasificare a atacurilor cibernetice în temeiul articolului 37 alineatul (8). Punctul unic de contact la nivel de entitate desemnat în temeiul alineatului (1) litera (c) comunică clasificarea incidentelor.

(5) În cazul în care entitățile cu impact critic și entitățile cu impact ridicat notifică unei echipe CSIRT informații relevante legate de vulnerabilitățile necorectate exploatate activ, aceasta din urmă poate transmite aceste informații autorității sale competente. Având în vedere nivelul de sensibilitate al informațiilor notificate, echipa CSIRT poate refuza transmiterea informațiilor sau poate întârzia transmiterea lor din motive justificate legate de securitatea cibernetică.

(6) Fiecare entitate cu impact critic și fiecare entitate cu impact ridicat furnizează fără întârzieri nejustificate echipelor sale CSIRT orice informații legate de o amenințare cibernetică raportabilă care ar putea avea un efect transfrontalier. Informațiile referitoare la o amenințare cibernetică sunt considerate raportabile atunci când este îndeplinită cel puțin una dintre următoarele condiții:

(a) furnizează informații relevante, pentru alte entități cu impact critic și pentru alte entități cu impact ridicat, legate de prevenirea, detectarea, răspunsul sau atenuarea impactului riscului;

(b) tehnicile, tacticile și procedurile identificate utilizate în contextul unui atac conduc la informații precum adrese URL sau IP compromise, hash-uri sau orice alt atribut util pentru contextualizarea și corelarea atacului;

(c) o amenințare cibernetică poate fi evaluată și contextualizată mai amănunțit cu ajutorul informațiilor suplimentare furnizate de prestatori de servicii sau terți care nu fac obiectul prezentului regulament.

(7) Atunci când face schimb de informații în temeiul prezentului articol, fiecare entitate cu impact critic și fiecare entitate cu impact ridicat specifică următoarele:

(a) că informațiile sunt transmise în temeiul prezentului regulament;

(b) dacă informațiile se referă la:

(i) un atac cibernetic raportabil menționat la alineatul (3);

(ii) vulnerabilitățile necorectate exploatate activ care nu sunt cunoscute public, menționate la alineatul (4);

(iii) o amenințare cibernetică raportabilă menționată la alineatul (5);

(c) în cazul unui atac cibernetic raportabil, nivelul atacului cibernetic în conformitate cu metodologia grilei de clasificare a atacurilor cibernetice menționată la articolul 37 alineatul (8), precum și informațiile care conduc la această clasificare, inclusiv cel puțin nivelul de criticalitate al atacului cibernetic.

(8) Atunci când o entitate critică sau o entitate cu impact ridicat notifică un incident semnificativ în temeiul articolului 23 din Directiva (UE) 2022/2555, iar raportarea incidentelor în temeiul articolului respectiv conține informații relevante, astfel cum se prevede la alineatul (3) din prezentul articol, raportarea entității în temeiul articolului 23 alineatul (1) din directiva respectivă constituie raportarea informațiilor în temeiul alineatului (3) din prezentul articol.

(9) Fiecare entitate cu impact critic și fiecare entitate cu impact ridicat raportează autorității sale competente sau echipei CSIRT, identificând clar informațiile specifice care trebuie comunicate autorității competente sau echipei CSIRT numai în cazurile în care schimbul de informații ar putea fi sursa unui atac cibernetic. Fiecare entitate cu impact critic și fiecare entitate cu impact ridicat are dreptul de a furniza echipei CSIRT competente o versiune neconfidențială a informațiilor.

*Articolul 39*

**Detectarea atacurilor cibernetice și tratarea informațiilor conexe**

(1) Entitățile cu impact critic și entitățile cu impact ridicat dezvoltă capacitățile necesare pentru a gestiona atacurile cibernetice detectate cu sprijinul necesar din partea autorității competente relevante, a ENTSO pentru energie electrică și a entității OSD UE. Entitățile cu impact critic și entitățile cu impact ridicat pot fi sprijinite de echipa CSIRT desemnată în statul lor membru respectiv ca parte a sarcinii atribuite echipelor CSIRT prin articolul 11 alineatul (5) litera (a) din Directiva (UE) 2022/2555. Entitățile cu impact critic și entitățile cu impact ridicat implementează procese eficace de identificare, clasificare și răspuns la atacurile cibernetice care vor afecta sau pot afecta fluxurile transfrontaliere de energie electrică, pentru a reduce la minimum impactul acestora.

(2) În cazul în care un atac cibernetic afectează fluxurile transfrontaliere de energie electrică, punctele unice de contact la nivel de entitate ale entităților cu impact critic și ale entităților cu impact ridicat afectate cooperează pentru a face schimb de informații, coordonate de autoritatea competentă a statului membru în care a fost raportat pentru prima dată atacul cibernetic.

(3) Entitățile cu impact critic și entitățile cu impact ridicat:

(a) se asigură că propriul punct unic de contact la nivel de entitate are acces, pe baza principiului necesității de a cunoaște, la informațiile primite de la punctul unic de contact național prin intermediul autorității lor competente;

(b) dacă nu s-a efectuat deja notificarea în temeiul articolului 3 alineatul (4) din Directiva (UE) 2022/2555, notifică autorității competente din statul membru în care sunt stabilite și punctului unic de contact național o listă a punctelor lor unice de contact în materie de securitate cibernetică la nivel de entitate:

(i) de la care autoritatea competentă și punctul unic național de contact se pot aștepta să primească informații despre atacuri cibernetice raportabile;

(ii) cărora autoritățile competente și punctele unice naționale de contact ar putea fi nevoite să le furnizeze informații;

(c) instituie proceduri de gestionare a atacurilor cibernetice în cazul atacurilor cibernetice, inclusiv roluri și responsabilități, sarcini și reacții pe baza evoluției observabile a atacului cibernetic în perimetrele cu impact critic și în perimetrele cu impact ridicat;

(d) testează procedurile generale de gestionare a atacurilor cibernetice cel puțin o dată pe an prin testarea a cel puțin unui scenariu care afectează direct sau indirect fluxurile transfrontaliere de energie electrică. Testul anual respectiv poate fi efectuat de entitățile cu impact critic și de entitățile cu impact ridicat în timpul exercițiilor periodice menționate la articolul 43. Orice activitate de răspuns la atacuri cibernetice în direct cu o consecință clasificată cel puțin la scara 2, în conformitate cu metodologia grilei de clasificare a atacurilor cibernetice menționată la articolul 37 alineatul (8), și a căror cauză principală este legată de securitatea cibernetică, poate servi drept test anual al planului de răspuns la atacurile cibernetice.

(4) Sarcinile menționate la alineatul (1) pot fi delegate de statele membre și centrelor de coordonare regionale, în conformitate cu articolul 37 alineatul (2) din Regulamentul (UE) 2019/943.

*Articolul 40*

**Gestionarea crizelor**

(1) Atunci când autoritatea competentă stabilește că o criză de energie electrică este legată de un atac cibernetic care afectează mai multe state membre, autoritățile competente din statele membre afectate, ANC-SC (autoritățile competente în domeniul securității cibernetice în sectorul energetic), ANC-PR (autoritățile competente în domeniul pregătirii pentru riscuri) și autoritățile de gestionare a crizelor cibernetice NIS din statele membre afectate creează în comun un grup ad-hoc de coordonare transfrontalieră a crizelor.

(2) Grupul ad-hoc de coordonare transfrontalieră a crizelor:

(a) coordonează recuperarea eficientă și diseminarea în continuare a tuturor informațiilor relevante în materie de securitate cibernetică către entitățile implicate în procesul de gestionare a crizelor;

(b) organizează comunicarea dintre toate entitățile afectate de criză și autoritățile competente, pentru a reduce suprapunerile și a spori eficiența analizelor și a răspunsurilor tehnice care să remedieze crizele simultane de energie electrică ale căror cauze principale sunt legate de securitatea cibernetică;

(c) furnizează, în cooperare cu echipele CSIRT competente, expertiza necesară, inclusiv consiliere operațională cu privire la implementarea unor posibile măsuri de atenuare în cadrul entităților afectate de incident;

(d) notifică și furnizează Comisiei și Grupului de coordonare în domeniul energiei electrice actualizări periodice cu privire la situația incidentului, respectând principiile de protecție prevăzute la articolul 46;

(e) solicită consiliere din partea autorităților, agențiilor sau entităților relevante care ar putea contribui la atenuarea crizei de energie electrică.

(3) În cazul în care atacul cibernetic se califică sau se preconizează că va fi calificat drept incident de securitate cibernetică de mare amploare, grupul ad-hoc de coordonare transfrontalieră a crizelor informează imediat autoritățile naționale de gestionare a crizelor cibernetice în conformitate cu articolul 9 alineatul (1) din Directiva (UE) 2022/2555 din statele membre afectate de incident, precum și Comisia și EU CyCLONe. Într-o astfel de situație, grupul ad-hoc de coordonare transfrontalieră a crizelor sprijină rețeaua EU CyCLONe în ceea ce privește particularitățile sectoriale.

(4) Entitățile cu impact critic și entitățile cu impact ridicat dezvoltă și au la dispoziție capacități, orientări interne, planuri de pregătire și personal care să participe la detectarea și la atenuarea crizelor transfrontaliere. Entitatea cu impact critic sau entitatea cu impact ridicat afectată de o criză simultană de energie electrică investighează cauza principală a unei astfel de crize în cooperare cu autoritatea sa competentă pentru a stabili măsura în care criza este legată de un atac cibernetic.

(5) Sarcinile menționate la alineatul (4) pot fi delegate de statele membre și centrelor de coordonare regionale, în conformitate cu articolul 37 alineatul (2) din Regulamentul (UE) 2019/943.

*Articolul 41*

**Planuri de gestionare și răspuns la crizele de securitate cibernetică**

(1) În termen de 24 de luni de la notificarea către ACER a raportului de evaluare a riscurilor la nivelul Uniunii, ACER, în strânsă cooperare cu ENISA, ENTSO pentru energie electrică, entitatea OSD UE, ANC-SC, autoritățile competente, ANC-PR, ANR și autoritățile naționale NIS de gestionare a crizelor cibernetice, elaborează un plan de gestionare și răspuns la crizele de securitate cibernetică la nivelul Uniunii pentru sectorul energiei electrice.

(2) În termen de 12 luni de la elaborarea de către ACER a planului de gestionare și răspuns la crizele de securitate cibernetică la nivelul Uniunii pentru sectorul energiei electrice în temeiul alineatului (1), fiecare autoritate competentă elaborează un plan național de gestionare și răspuns la crizele de securitate cibernetică pentru fluxurile transfrontaliere de energie electrică, ținând seama de planul de gestionare a crizelor de securitate cibernetică la nivelul Uniunii și de planul național de pregătire pentru riscuri instituit în conformitate cu articolul 10 din Regulamentul (UE) 2019/941. Acest plan trebuie să fie în concordanță cu planul de răspuns la incidente de securitate cibernetică de mare amploare și crize în temeiul articolului 9 alineatul (4) din Directiva (UE) 2022/2555. Autoritatea competentă se coordonează cu entitățile cu impact critic și cu entitățile cu impact ridicat, precum și cu ANC-PR din statul său membru.

(3) Planul național de răspuns la incidente de securitate cibernetică de mare amploare și crize, necesar în temeiul articolului 9 alineatul (4) din Directiva (UE) 2022/2555, este considerat un plan național de gestionare a crizelor de securitate cibernetică în temeiul prezentului articol dacă include dispoziții privind gestionarea crizelor și răspunsul la acestea pentru fluxurile transfrontaliere de energie electrică.

(4) Sarcinile enumerate la alineatele (1) și (2) pot fi delegate de statele membre și centrelor de coordonare regionale, în conformitate cu articolul 37 alineatul (2) din Regulamentul (UE) 2019/943.

(5) Entitățile cu impact critic și entitățile cu impact ridicat se asigură că procesele lor de gestionare a crizelor legate de securitatea cibernetică:

(a) au proceduri compatibile de gestionare a incidentelor de securitate cibernetică transfrontaliere, astfel cum este definită la articolul 6 punctul 8 din Directiva (UE) 2022/2555, incluse în mod oficial în planurile lor de gestionare a crizelor;

(b) fac parte din activitățile generale de gestionare a crizelor.

(6) În termen de 12 luni de la notificarea entităților cu impact ridicat și a entităților cu impact critic în temeiul articolului 24 alineatul (6) și, ulterior, o dată la trei ani, entitățile cu impact critic și entitățile cu impact ridicat elaborează un plan de gestionare a crizelor la nivel de entitate pentru o criză legată de securitatea cibernetică, care este inclus în planurile lor generale de gestionare a crizelor. Planul respectiv include cel puțin următoarele elemente:

(a) regulile privind declararea crizei, astfel cum se prevede la articolul 14 alineatele (2) și (3) din Regulamentul (UE) 2019/941;

(b) roluri și responsabilități clare pentru gestionarea crizelor, inclusiv rolul altor entități relevante cu impact critic și al altor entități cu impact ridicat;

(c) informații de contact actualizate, precum și norme privind comunicarea și schimbul de informații în timpul unei situații de criză, inclusiv conectarea cu echipele CSIRT.

(7) Măsurile de gestionare a crizelor în temeiul articolului 21 alineatul (2) litera (c) din Directiva (UE) 2022/2555 sunt considerate un plan de gestionare a crizelor la nivel de entitate pentru sectorul energiei electrice în temeiul prezentului articol dacă include toate cerințele enumerate la alineatul (6).

(8) Planurile de gestionare a crizelor sunt testate în cursul exercițiilor de securitate cibernetică menționate la articolele 43, 44 și 45.

(9) Entitățile cu impact critic și entitățile cu impact ridicat includ planurile lor de gestionare a crizelor la nivel de entitate în planurile lor de continuitate a activității pentru procesele cu impact critic și procesele cu impact ridicat. Planurile de gestionare a crizelor la nivel de entitate includ:

(a) procese în funcție de disponibilitatea, integritatea și fiabilitatea serviciilor informatice;

(b) toate locațiile de asigurare a continuității activității, inclusiv locațiile pentru hardware și software;

(c) toate rolurile și responsabilitățile interne legate de procesele de continuitate a activității.

(10) Entitățile cu impact critic și entitățile cu impact ridicat își actualizează planurile de gestionare a crizelor la nivel de entitate cel puțin o dată la trei ani și ori de câte ori este necesar.

(11) ACER actualizează planul de gestionare și răspuns la crizele de securitate cibernetică la nivelul Uniunii pentru sectorul energiei electrice, elaborat în temeiul alineatului (1), cel puțin o dată la trei ani și ori de câte ori este necesar.

(12) Fiecare autoritate competentă actualizează planul național de gestionare și răspuns la crizele de securitate cibernetică pentru fluxurile transfrontaliere de energie electrică, elaborat în temeiul alineatului (2), cel puțin o dată la trei ani și ori de câte ori este necesar.

(13) Entitățile cu impact critic și entitățile cu impact ridicat își testează planurile de continuitate a activității cel puțin o dată la trei ani sau după modificări majore în cadrul unui proces cu impact critic. Rezultatul testării planului de asigurare a continuității activității trebuie documentat. Entitățile cu impact critic și entitățile cu impact ridicat pot include testarea planului lor de continuitate a activității în exercițiile de securitate cibernetică.

(14) Entitățile cu impact critic și entitățile cu impact ridicat își actualizează planul de continuitate a activității ori de câte ori este necesar și cel puțin o dată la trei ani, ținând seama de rezultatul testului.

(15) În cazul în care un test identifică deficiențe în planul de continuitate a activității, entitatea cu impact critic și entitatea cu impact ridicat corectează deficiențele respective în termen de 180 de zile calendaristice de la testare și efectuează un nou test pentru a furniza dovezi că măsurile corective sunt eficace.

(16) În cazul în care nu poate corecta deficiențele în termen de 180 de zile calendaristice, o entitate cu impact critic sau o entitate cu impact ridicat include motivele în raportul care urmează să fie transmis autorității sale competente în conformitate cu articolul 27.

*Articolul 42*

**Capacități de alertă timpurie de securitate cibernetică în sectorul energiei electrice**

(1) Autoritățile competente cooperează cu ENISA pentru a dezvolta capacități de alertă timpurie de securitate cibernetică în sectorul energiei electrice (ECEAC), ca parte a asistenței acordate statelor membre în temeiul articolului 6 alineatul (2) și al articolului 7 din Regulamentul (UE) 2019/881.

(2) ECEAC permite ENISA, atunci când îndeplinește atribuțiile enumerate la articolul 7 alineatul (7) din Regulamentul (UE) 2019/881:

(a) să colecteze informații în sistem de schimb voluntar de la:

(i) echipele CSIRT, autoritățile competente;

(ii) entitățile menționate la articolul 2 din prezentul regulament;

(iii) orice altă entitate care dorește să facă schimb voluntar de informații relevante;

(b) să evalueze și să clasifice informațiile colectate;

(c) să evalueze informațiile la care ENISA are acces pentru identificarea condițiilor de risc cibernetic și a indicatorilor relevanți pentru aspectele fluxurilor transfrontaliere de energie electrică;

(d) să identifice condițiile și indicatorii care se corelează frecvent cu atacurile cibernetice din sectorul energiei electrice;

(e) să definească dacă se iau măsuri suplimentare de analiză și de prevenire prin evaluarea și identificarea factorilor de risc;

(f) să informeze autoritățile competente cu privire la riscurile identificate și la acțiunile preventive recomandate specifice entităților în cauză;

(g) să informeze toate entitățile relevante enumerate la articolul 2 cu privire la rezultatele informațiilor evaluate în conformitate cu literele (b), (c) și (d) de la prezentul alineat;

(h) să includă periodic informațiile relevante în raportul privind conștientizarea situației, elaborat în conformitate cu articolul 7 alineatul (6) din Regulamentul (UE) 2019/881;

(i) să obțină, acolo unde este posibil, date aplicabile care indică o potențială încălcare a securității sau un atac cibernetic („indicatori de compromitere”) din informațiile colectate.

(3) Echipele CSIRT diseminează fără întârziere informațiile primite de la ENISA către entitățile în cauză, în limitele atribuțiilor lor definite la articolul 11 alineatul (3) litera (b) din Directiva (UE) 2022/2555.

(4) ACER monitorizează eficacitatea ECEAC. ENISA acordă asistență ACER prin furnizarea tuturor informațiilor necesare, în temeiul articolului 6 alineatul (2) și al articolului 7 alineatul (1) din Regulamentul (UE) 2019/881. Analiza acestei activități de monitorizare face parte din monitorizarea prevăzută la articolul 12 din prezentul regulament.

CAPITOLUL VI

**CADRUL DE EXERCIȚII DE SECURITATE CIBERNETICĂ ÎN SECTORUL ENERGIEI ELECTRICE**

*Articolul 43*

**Exerciții de securitate cibernetică la nivelul entităților și al statelor membre**

(1) Până la 31 decembrie din anul următor notificării entităților cu impact critic și, ulterior, o dată la trei ani, fiecare entitate cu impact critic efectuează un exercițiu de securitate cibernetică care include unul sau mai multe scenarii cu atacuri cibernetice care afectează direct sau indirect fluxurile transfrontaliere de energie electrică și în legătură cu riscurile identificate în cursul evaluărilor riscurilor în materie de securitate cibernetică la nivel de stat membru și la nivel de entitate, în conformitate cu articolul 20 și cu articolul 27.

(2) Prin derogare de la alineatul (1), ANC-PR, după consultarea autorității competente și a autorității relevante de gestionare a crizelor cibernetice, astfel cum a fost desemnată sau stabilită în Directiva (UE) 2022/2555 în temeiul articolului 9, poate decide să organizeze un exercițiu de securitate cibernetică la nivel de stat membru, astfel cum se descrie la alineatul (1), în loc să efectueze exercițiul de securitate cibernetică la nivel de entitate. În acest sens, autoritatea competentă informează:

(a) toate entitățile cu impact critic din statul său membru, ANR, echipele CSIRT și ANC-SC cel târziu până la data de 30 iunie a anului care precedă exercițiul de securitate cibernetică la nivel de entitate;

(b) fiecare entitate care participă la exercițiul de securitate cibernetică la nivel de stat membru, cu cel puțin șase luni înainte de începerea exercițiului.

(3) ANC-PR, cu sprijinul tehnic al echipelor sale CSIRT, organizează exercițiul de securitate cibernetică descris la alineatul (2) la nivel de stat membru în mod independent sau în contextul unui alt exercițiu de securitate cibernetică în statul membru respectiv. Pentru a putea grupa aceste exerciții, ANC-PR poate amâna cu un an exercițiul de securitate cibernetică la nivel de stat membru menționat la alineatul (1).

(4) Exercițiile de securitate cibernetică la nivel de entitate și la nivel de stat membru trebuie să fie coerente cu cadrele naționale de gestionare a crizelor de securitate cibernetică, în conformitate cu articolul 9 alineatul (4) litera (d) din Directiva (UE) 2022/2555.

(5) Până la 31 decembrie 2026 și, ulterior, o dată la trei ani, ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE, pune la dispoziție un model de scenariu de exercițiu pentru efectuarea exercițiilor de securitate cibernetică la nivelul entității și al statelor membre, menționate la alineatul (1). Acest model ține seama de rezultatele celei mai recente evaluări a riscurilor în materie de securitate cibernetică la nivel de entitate și la nivel de stat membru și include principalele criterii de reușită. ENTSO pentru energie electrică și entitatea OSD UE implică ACER și ENISA în elaborarea unui astfel de model.

*Articolul 44*

**Exerciții regionale sau transregionale de securitate cibernetică**

(1) Până la 31 decembrie 2029 și, ulterior, o dată la trei ani, în fiecare regiune de exploatare a sistemului, ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE, organizează un exercițiu regional de securitate cibernetică. Entitățile cu impact critic din regiunea de exploatare a sistemului participă la exercițiul regional de securitate cibernetică. ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE, poate organiza, în locul unui exercițiu regional de securitate cibernetică, un exercițiu transregional de securitate cibernetică în mai multe regiuni de exploatare a sistemelor, în același interval de timp. Exercițiul ar trebui să țină seama de alte evaluări și scenarii existente ale riscurilor în materie de securitate cibernetică elaborate la nivelul Uniunii.

(2) ENISA sprijină ENTSO pentru energie electrică și entitatea OSD UE la pregătirea și organizarea exercițiului de securitate cibernetică la nivel regional sau transregional.

(3) ENTSO pentru energie electrică, în coordonare cu entitatea OSD UE, informează entitățile cu impact critic care participă la exercițiul regional sau transregional de securitate cibernetică cu șase luni înainte ca exercițiul să aibă loc.

(4) Organizatorul unui exercițiu periodic de securitate cibernetică la nivelul Uniunii în temeiul articolului 7 alineatul (5) din Regulamentul (UE) 2019/881 sau al oricărui exercițiu obligatoriu de securitate cibernetică legat de sectorul energiei electrice în același perimetru geografic poate invita ENTSO pentru energie electrică și entitatea OSD UE să participe. În astfel de cazuri, obligația prevăzută la alineatul (1) nu se aplică, cu condiția ca toate entitățile cu impact critic din regiunea de exploatare a sistemului să participe la același exercițiu.

(5) În cazul în care participă la un exercițiu de securitate cibernetică menționat la alineatul (4), ENTSO pentru energie electrică și entitatea OSD UE pot amâna cu un an exercițiul regional sau transregional de securitate cibernetică menționat la alineatul (1).

(6) Până la 31 decembrie 2027 și, ulterior, o dată la trei ani, ENTSO pentru energie electrică, în coordonare cu entitatea OSD UE, pune la dispoziție un model de exercițiu pentru efectuarea exercițiilor regionale și transregionale de securitate cibernetică. Acest model ține seama de rezultatele celei mai recente evaluări a riscurilor în materie de securitate cibernetică la nivel regional și include principalele criterii de reușită. ENTSO pentru energie electrică consultă Comisia și poate solicita consiliere din partea ACER, ENISA și a Centrului Comun de Cercetare cu privire la organizarea și executarea exercițiilor regionale și transregionale de securitate cibernetică.

*Articolul 45*

**Rezultatul exercițiilor de securitate cibernetică la nivel de entitate, de stat membru, la nivel regional sau la nivel transregional**

(1) La cererea unei entități cu impact critic, furnizorii de servicii critice participă la exercițiile de securitate cibernetică menționate la articolul 43 alineatele (1) și (2) și la articolul 44 alineatul (1) atunci când furnizează servicii entității cu impact critic în domeniul corespunzător domeniului de aplicare al exercițiului de securitate cibernetică relevant.

(2) Organizatorii exercițiilor de securitate cibernetică menționate la articolul 43 alineatele (1) și (2) și la articolul 44 alineatul (1), cu avizul ENISA, la cererea acestora și în temeiul articolului 7 alineatul (5) din Regulamentul (UE) 2019/881, analizează și finalizează exercițiul de securitate cibernetică relevant prin intermediul unui raport care sintetizează lecțiile învățate, adresat tuturor participanților. Raportul trebuie să conțină:

(a) scenariile de exercițiu, rapoartele de reuniune, principalele poziții, reușitele și lecțiile învățate la orice nivel al lanțului valoric al energiei electrice;

(b) dacă au fost îndeplinite principalele criterii de reușită;

(c) o listă de recomandări pentru entitățile care participă la exercițiul de securitate cibernetică relevant pentru a corecta, a adapta sau a modifica procesele de criză de securitate cibernetică, procedurile aferente, modelele de guvernanță asociate și orice angajamente contractuale existente cu furnizorii critici de servicii.

(3) La cererea rețelei CSIRT, a Grupului de cooperare NIS sau a EU CyCLONe, organizatorii exercițiilor de securitate cibernetică menționate la articolul 43 alineatele (1) și (2) și la articolul 44 alineatul (1) partajează rezultatul exercițiului de securitate cibernetică relevant. Organizatorii comunică fiecărei entități care participă la exerciții informațiile menționate la alineatul (2) literele (a) și (b) din prezentul articol. Organizatorii transmit lista de recomandări menționată la alineatul respectiv litera (c) numai entităților cărora li se adresează recomandările.

(4) Organizatorii exercițiilor de securitate cibernetică menționate la articolul 43 alineatele (1) și (2) și la articolul 44 alineatul (1) urmăresc periodic, împreună cu entitățile care participă la exerciții, punerea în aplicare a recomandărilor formulate în temeiul alineatului (2) litera (c) din prezentul articol.

CAPITOLUL VII

**PROTECȚIA INFORMAȚIILOR**

*Articolul 46*

**Principii pentru protecția informațiilor care fac obiectul schimbului**

(1) Entitățile enumerate la articolul 2 alineatul (1) se asigură că informațiile furnizate, primite, schimbate sau transmise în temeiul prezentului regulament sunt accesibile numai pe baza principiului necesității de a cunoaște și în conformitate cu normele relevante ale Uniunii și cu normele naționale privind securitatea informațiilor.

(2) Entitățile enumerate la articolul 2 alineatul (1) se asigură că informațiile furnizate, primite, schimbate sau transmise în temeiul prezentului regulament sunt manipulate și urmărite pe parcursul întregului ciclu de viață al informațiilor respective și că acestea pot fi publicate la sfârșitul ciclului lor de viață numai după ce au fost anonimizate.

(3) Entitățile enumerate la articolul 2 alineatul (1) se asigură că sunt instituite toate măsurile de protecție necesare de natură organizațională și tehnică pentru a proteja confidențialitatea, integritatea, disponibilitatea și nerepudierea informațiilor furnizate, primite, schimbate sau transmise în temeiul prezentului regulament, independent de mijloacele utilizate. Măsurile de protecție:

(a) trebuie să fie proporționale;

(b) iau în considerare riscurile în materie de securitate cibernetică legate de amenințările trecute și emergente cunoscute la care pot fi supuse astfel de informații în contextul prezentului regulament;

(c) în măsura posibilului, se bazează pe standarde și bune practici naționale, europene sau internaționale;

(d) sunt susținute de documente justificative.

(4) Entitățile enumerate la articolul 2 alineatul (1) se asigură că orice persoană căreia i se acordă acces la informațiile furnizate, primite, schimbate sau transmise în temeiul prezentului regulament este informată cu privire la normele de securitate aplicabile la nivel de entitate și cu privire la măsurile și procedurile relevante pentru protecția informațiilor. Entitățile respective se asigură că persoana în cauză își recunoaște responsabilitatea de a proteja informațiile, conform instrucțiunilor din timpul informării.

(5) Entitățile enumerate la articolul 2 alineatul (1) se asigură că accesul la informațiile furnizate, primite, schimbate sau transmise în temeiul prezentului regulament este limitat la persoanele:

(a) care sunt autorizate să acceseze informațiile respective pe baza funcțiilor lor și în limita executării sarcinilor atribuite;

(b) în privința cărora entitatea a fost în măsură să evalueze principiile etice și de integritate, precum și în privința cărora nu există dovezi ale unui rezultat negativ în urma unei verificări a antecedentelor pentru a evalua fiabilitatea persoanei în conformitate cu cele mai bune practici și cu cerințele standard de securitate ale entității și, dacă este necesar, cu legile și reglementările naționale.

(6) Entitățile enumerate la articolul 2 alineatul (1) au acordul scris al persoanei fizice sau juridice care a creat sau a furnizat inițial informațiile, înainte de a furniza informațiile respective unui terț care nu intră în domeniul de aplicare al prezentului regulament.

(7) O entitate menționată la articolul 2 alineatul (1) poate considera că aceste informații trebuie partajate fără a se respecta alineatele (1) și (4) din prezentul articol pentru a preveni o criză simultană de energie electrică a cărei cauză principală este legată de securitatea cibernetică sau orice criză transfrontalieră din Uniune într-un alt sector. În acest caz, entitatea:

(a) se consultă cu autoritatea competentă și este autorizată de aceasta să facă schimb de astfel de informații;

(b) anonimizează aceste informații fără a pierde elementele necesare pentru a informa publicul cu privire la un risc iminent și grav la adresa fluxurilor transfrontaliere de energie electrică și la posibilele măsuri de atenuare;

(c) garantează identitatea inițiatorului și a entităților care au prelucrat astfel de informații în temeiul prezentului regulament.

(8) Prin derogare de la alineatul (6) din prezentul articol, autoritățile competente pot transmite informațiile furnizate, primite, schimbate sau transmise în temeiul prezentului regulament unui terț care nu este menționat la articolul 2 alineatul (1) fără acordul prealabil scris al inițiatorului informațiilor, dar informându-l în cel mai scurt timp posibil. Înainte de a divulga orice informații furnizate, primite, schimbate sau transmise în temeiul prezentului regulament unui terț care nu este menționat la articolul 2 alineatul (1), autoritatea competentă în cauză se asigură în mod rezonabil că terțul în cauză are cunoștință de normele de securitate în vigoare și primește asigurări rezonabile că terțul în cauză poate proteja informațiile primite în conformitate cu alineatele (1)-(5) din prezentul articol. Autoritatea competentă anonimizează aceste informații fără a pierde elementele necesare pentru a informa publicul cu privire la un risc iminent și grav la adresa fluxurilor transfrontaliere de energie electrică și la posibilele măsuri de atenuare și garantează identitatea inițiatorului informațiilor. În acest caz, terțul care nu este enumerat la articolul 2 alineatul (1) protejează informațiile primite în conformitate cu dispozițiile aflate deja în vigoare la nivel de entitate sau, dacă acest lucru nu este posibil, cu dispozițiile și instrucțiunile furnizate de autoritatea competentă relevantă.

(9) Prezentul articol nu se aplică entităților care nu sunt enumerate la articolul 2 alineatul (1) și care primesc informații în temeiul alineatului (6) din prezentul articol. În acest caz, se aplică alineatul (7) din prezentul articol sau autoritatea competentă poate furniza entității respective dispoziții scrise care să se aplice în cazurile în care se primesc informații în temeiul prezentului regulament.

*Articolul 47*

**Confidențialitatea informațiilor**

(1) Orice informație furnizată, primită, schimbată sau transmisă în temeiul prezentului regulament face obiectul condițiilor privind secretul profesional prevăzute la alineatele (2)-(5) din prezentul articol al prezentului regulament și al cerințelor prevăzute la articolul 65 din Regulamentul (UE) 2019/943. Orice informații furnizate, primite, schimbate sau transmise între entitățile enumerate în articolul 2 din prezentul regulament, în scopul punerii în aplicare a prezentului regulament, sunt protejate, ținând cont de nivelul de confidențialitate al informațiilor aplicat de inițiator.

(2) Obligația de a păstra secretul profesional se aplică entităților enumerate la articolul 2.

(3) ANC-SC, ANR, ANC-PR și echipele CSIRT partajează toate informațiile necesare pentru îndeplinirea sarcinilor care le revin.

(4) Orice informații primite, schimbate sau transmise între entitățile enumerate la articolul 2 alineatul (1), în scopul punerii în aplicare a articolului 23, se anonimizează și se agregă.

(5) Informațiile primite de orice entitate sau autoritate care intră sub incidența prezentului regulament în timpul exercitării atribuțiilor sale nu pot fi divulgate niciunei alte entități sau autorități, fără a aduce atingere cazurilor reglementate de dreptul intern, celorlalte dispoziții ale prezentului regulament sau altor acte legislative relevante ale Uniunii.

(6) Fără a aduce atingere legislației naționale sau a Uniunii, o autoritate, o entitate sau o persoană fizică care primește informații în temeiul prezentului regulament nu le poate utiliza în niciun alt scop decât pentru îndeplinirea sarcinilor care îi revin în temeiul prezentului regulament.

(7) ACER, după consultarea ENISA, a tuturor autorităților competente, ENTSO pentru energie electrică și a entității OSD UE emit, până la 13 iunie 2025, orientări care abordează mecanismele prin care toate entitățile enumerate la articolul 2 alineatul (1) pot face schimb de informații, în special fluxurile de comunicare avute în vedere, precum și metodele de anonimizare și de agregare a informațiilor în scopul punerii în aplicare a prezentului articol.

(8) Informațiile care sunt confidențiale în temeiul normelor de drept intern sau al normelor UE fac obiectul unui schimb cu Comisia și cu alte autorități relevante numai în cazul în care un astfel de schimb este necesar pentru aplicarea prezentului regulament. Informațiile care fac obiectul schimbului se limitează la informații necesare și proporționale cu scopul respectivului schimb. Schimbul de informații păstrează confidențialitatea respectivelor informații și protejează securitatea și interesele comerciale ale entităților cu impact critic sau ale entităților cu impact ridicat.

CAPITOLUL VIII

**DISPOZIȚII FINALE**

*Articolul 48*

**Dispoziții temporare**

(1) Până la aprobarea termenilor și condițiilor sau a metodologiilor menționate la articolul 6 alineatul (2) sau a planurilor menționate la articolul 6 alineatul (3), ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE, elaborează orientări fără caracter obligatoriu cu privire la următoarele aspecte:

(a) un indice provizoriu de impact în materie de securitate cibernetică în domeniul energiei electrice („ECII") în temeiul alineatului (2) din prezentul articol;

(b) o listă provizorie a proceselor cu impact ridicat și a proceselor cu impact critic la nivelul Uniunii în temeiul alineatului (4) din prezentul articol și

(c) o listă provizorie a standardelor și controalelor europene și internaționale impuse de legislația națională relevantă pentru aspectele de securitate cibernetică a fluxurilor transfrontaliere de energie electrică în temeiul alineatului (6) din prezentul articol.

(2) Până la 13 octombrie 2024, ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE, elaborează o recomandare pentru un ECII provizoriu. ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE, notifică ECII provizoriu recomandat autorităților competente.

(3) La patru luni de la primirea ECII provizoriu recomandat sau cel târziu până la 13 februarie 2025, autoritățile competente identifică candidații pentru entitățile cu impact ridicat și pentru entitățile cu impact critic din statul lor membru pe baza ECII recomandați și elaborează o listă provizorie a entităților cu impact ridicat și a entităților cu impact critic. Entitățile cu impact ridicat și entitățile cu impact critic identificate în lista provizorie își pot îndeplini în mod voluntar obligațiile prevăzute în prezentul regulament, pe baza principiului precauției. Până la 13 martie 2025, autoritățile competente notifică entităților identificate în lista provizorie faptul că au fost identificate ca entități cu impact ridicat sau ca entități cu impact critic.

(4) Până la 13 decembrie 2024, ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE, elaborează o listă provizorie a proceselor cu impact ridicat și a proceselor cu impact critic la nivelul Uniunii. Entitățile notificate în temeiul alineatului (3) care decid în mod voluntar să își îndeplinească obligațiile prevăzute în prezentul regulament pe baza principiului precauției utilizează lista provizorie a proceselor cu impact ridicat și a proceselor cu impact critic pentru a determina perimetrele provizorii cu impact ridicat și cele cu impact critic și pentru a stabili activele care urmează să fie incluse în prima evaluare a riscurilor în materie de securitate cibernetică la nivel de entitate.

(5) Până la 13 septembrie 2024, fiecare autoritate competentă în conformitate cu articolul 4 alineatul (1) furnizează ENTSO pentru energie electrică și entității OSD UE o listă a legislației sale naționale relevante pentru aspectele de securitate cibernetică a fluxurilor transfrontaliere de energie electrică.

(6) Până la 13 iunie 2025, ENTSO pentru energie electrică, în cooperare cu entitatea OSD UE, pregătește o listă provizorie a standardelor și controalelor europene și internaționale impuse de legislația națională relevantă pentru aspectele de securitate cibernetică a fluxurilor transfrontaliere de energie electrică, ținând seama de informațiile furnizate de autoritățile competente.

(7) Lista provizorie a standardelor și controalelor europene și internaționale include:

(a) standardele europene și internaționale și legislația națională care furnizează orientări privind metodologiile de gestionare a riscurilor în materie de securitate cibernetică la nivel de entitate și

(b) controale de securitate cibernetică echivalente cu controalele care se preconizează că vor face parte din controalele minime și din controalele avansate de securitate cibernetică.

(8) ENTSO pentru energie electrică și entitatea OSD UE țin seama de opiniile exprimate de ENISA și ACER atunci când finalizează lista provizorie a standardelor. ENTSO pentru energie electrică și entitatea OSD UE publică lista tranzitorie a standardelor și controalelor europene și internaționale pe site-urile lor web.

(9) ENTSO pentru energie electrică și entitatea OSD UE consultă ENISA și ACER cu privire la propunerile de orientări fără caracter obligatoriu elaborate în temeiul alineatului (1).

(10) Până la elaborarea controalelor minime și a controalelor avansate de securitate cibernetică în temeiul articolului 29 și până la adoptarea acestora în temeiul articolului 8, toate entitățile enumerate la articolul 2 alineatul (1) depun eforturi pentru a aplica treptat orientările fără caracter obligatoriu elaborate în temeiul alineatului (1).

*Articolul 49*

**Intrare 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 Bruxelles, 11 martie 2024.

*Pentru Comisie*
*Președinta*
Ursula VON DER LEYEN