Republica Moldova

Agenția Națională pentru Reglementare în Energetică
ANRE

str. Alexandr Pușkin 52/A, MD 2005 Chișinău, Tel: 022 823 955, anre@anre.md, http://www.anre.md

UE

CONSILIUL DE ADMINISTRAȚIE
HOTĂRÂRE nr.

din_____2026

mun. Chișinău

cu privire la aprobarea Codului de rețea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică

În temeiul art. 9 alin. (3) și art. 36 alin. (2) din Legea nr. 164/2025 cu privire la energia electrică (Monitorul Oficial al Republicii Moldova, 2025, nr. 437-440, art. 598), Consiliul de administrație al Agenției Naționale pentru Reglementare în Energetică

HOTĂRĂŞTE:

1. Se aprobă Codul de rețea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică (se anexează).
2. Prezenta hotărâre se publică în Monitorul Oficial al Republicii Moldova.
3. Controlul asupra executării prezentei hotărâri se pune în sarcina subdiviziunilor Agenției Naționale pentru Reglementare în Energetică.

Alexei TARAN
Director general

Constantin BOROSAN
Director

Eugen CARPOV
Director

Daniel MITITELU
Director

Alexandru URSU
Director

Aprobat
prin Hotărârea Consiliului de administrație
al ANRE nr. ___/2026

CODUL DE REȚEA
privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică

Prezenta hotărâre pune în aplicare parțial 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, CELEX: 32024R1366, publicat în Jurnalul Oficial al Uniunii Europene nr. L 2024/1366 din 24 mai 2024, așa cum a fost modificat ultima dată prin Regulamentul delegat (UE) 2025/1759 al Comisiei din 19 iunie 2025.

CAPITOLUL I
DISPOZIȚII GENERALE

Secțiunea 1
Obiectul de reglementare și domeniul de aplicare

1. Codul de rețea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică *(în continuare - Codul)* stabilește norme sectoriale specifice privind aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică, inclusiv cerințe minime comune, precum și norme privind planificarea, monitorizarea, raportarea și gestionarea crizelor.

2. Codul se aplică aspectelor legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică în activitatea următoarelor entități, în măsura în care acestea sunt identificate drept entități cu impact ridicat sau entități cu impact critic în conformitate cu prevederile prezentului Cod:

2.1. întreprinderile electroenergetice, în sensul art. 2 pct. 71 din Legea nr. 164/2025 cu privire la energia electrică *(în continuare - Legea nr. 164/2025)*;

2.2. operatorul pieței energiei electrice desemnat (OPEED), în sensul art. 2 pct. 83 din Legea nr. 164/2025;

2.3. piețele organizate, în sensul art. 2 pct. 99 din Legea nr. 164/2025, în măsura în care organizează tranzacții cu produse relevante pentru fluxurile transfrontaliere de energie electrică;

2.4. furnizorii critici de servicii TIC, astfel cum sunt definiți la pct. 8 subpct. 13;

2.5. părțile responsabile pentru echilibrare, în sensul art. 2 pct. 91 din Legea nr. 164/2025;

2.6. operatorii punctelor de reîncărcare, în sensul art. 2 pct. 115 din Legea nr. 164/2025;

2.7. centrele de coordonare regionale (RCC), în sensul art. 56 din Legea nr. 164/2025;

2.8. furnizorii de servicii de securitate gestionate (MSSP), în sensul pct. 2.11 din Hotărârea Guvernului nr. 860/2024 cu privire la identificarea furnizorilor de servicii;

2.9. orice altă entitate sau terț căruia i-au fost delegate ori atribuite responsabilități în temeiul prezentului Cod.

3. În limitele competențelor și mandatelor stabilite de legislație, următoarele autorități și entități sunt responsabile pentru exercitarea atribuțiilor prevăzute de prezentul Cod:

3.1. Agenția Națională pentru Reglementare în Energetică *(în continuare - ANRE sau Agenția)*, în calitate de autoritate competentă în domeniul energetic, potrivit art. 7 din Legea nr. 164/2025;

3.2. Ministerul Energiei, în calitate de organ central de specialitate al administrației publice în domeniul energeticii, potrivit art. 5 din Legea nr. 164/2025;

3.3. Ministerul Energiei, în calitate de autoritate competentă responsabilă de evaluarea riscurilor de securitate a aprovizionării cu energie electrică, de elaborare a planului de acțiuni, si de gestionarea crizelor de energie electrică, potrivit Hotărârii Guvernului nr. 820/2024 pentru aprobarea Regulamentului privind situațiile excepționale în sectorul electroenergetic și a Planului de acțiuni pentru situații excepționale în sectorul electroenergetic *(în continuare – Hotărârea Guvernului nr. 820/2024)*;

3.4. Agenția pentru Securitate Cibernetică *(în continuare - ASC)*, în calitate de echipă de răspuns la incidente de securitate cibernetică (CSIRT), potrivit art. 7 și 9 din Legea nr. 48/2023 privind securitatea cibernetică *(în continuare - Legea nr. 48/2023)* și pct. 1 din Hotărârea Guvernului nr. 1028/2023 cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică *(în continuare – Hotărârea Guvernului nr. 1028/2023*);

3.5. ASC, în calitate de autoritate de gestionare a crizelor cibernetice la nivel național, potrivit Hotărârii Guvernului nr. 1028/2023;

3.6. orice alte autorități sau terți cărora, în condițiile prezentului Cod, le-au fost delegate sau atribuite responsabilități privind elaborarea, consultarea, prezentarea sau implementarea termenilor și condițiilor, metodologiilor ori planurilor prevăzute în secțiunea 4.

4. Prezentul Cod se aplică, de asemenea, entităților care nu sunt stabilite în Republica Moldova, dar care prestează servicii unor entități stabilite în Republica Moldova, cu condiția ca acestea să fi fost identificate ca entități cu impact ridicat sau entități cu impact critic de către ANRE, în conformitate cu pct. 44.1.

5. Prezentul Cod nu aduce atingere responsabilității statului privind protejarea securității naționale și competenței acestuia de a proteja alte funcții esențiale ale statului, inclusiv asigurarea integrității teritoriale și menținerea ordinii publice, precum și responsabilității statului privind securitatea națională în domeniul activităților nucleare, în conformitate cu tratatele internaționale aplicabile.

6. Entitățile, ANRE, ASC și punctele unice de contact la nivel de entitate prelucrează datele cu caracter personal în măsura necesară realizării scopurilor prezentului Cod, cu respectarea Legii nr. 195/2024 privind protecția datelor cu caracter personal.

Secțiunea 2
Noțiuni

7. În sensul prezentului Cod, noțiunile „securitate cibernetică”, „amenințare cibernetică”, „incident cibernetic”, „risc” și „vulnerabilitate” au înțelesul prevăzut la art. 2 din Legea nr. 48/2023; noțiunile „flux transfrontalier de energie electrică” și „operatori de sistem” au înțelesul prevăzut la art. 2 pct. 51 și, respectiv, pct. 87 din Legea nr. 164/2025.

8. În sensul prezentului Cod, următoarele noțiuni principale semnifică:

8.1. *activ* - orice informație, orice produs software sau hardware din cadrul rețelelor și sistemelor informatice, corporal sau necorporal, care are valoare pentru o persoană fizică, o organizație sau o autoritate publică;

8.2. *activ cu impact critic* - activ necesar pentru desfășurarea unui proces cu impact critic;

8.3. *activ cu impact ridicat* - activ necesar pentru desfășurarea unui proces cu impact ridicat;

8.4. *alertă timpurie* - informații necesare pentru a indica dacă un incident cibernetic este suspectat a fi cauzat de acte ilegale sau răuvoitoare ori dacă acesta poate avea un impact transfrontalier;

8.5. *atac cibernetic* - incident cibernetic produs cu rea-credință prin tentativa unui actor amenințător de a distruge, expune, modifica, dezactiva, sustrage, obține ori utiliza fără drept un activ;

8.6. *autoritate competentă în domeniul pregătirii pentru riscuri* - Ministerul Energiei, potrivit Hotărârii Guvernului nr. 820/2024, responsabil de evaluarea riscurilor de securitate a aprovizionării cu energie electrică, elaborarea și actualizarea planurilor de acțiuni pentru situații excepționale în sectorul electroenergetic, precum și gestionarea crizelor de energie electrică, în cooperare cu Comisia pentru Situații Excepționale;

8.7. *autoritate de gestionare a crizelor cibernetice* - ASC, potrivit Hotărârii Guvernului nr. 1028/2023 și art. 9 din Legea nr. 48/2023;

8.8. *echipă de răspuns la incidente de securitate cibernetică (CSIRT)* - ASC, potrivit art. 7 din Legea nr. 48/2023 și Hotărârii Guvernului nr. 1028/2023;

8.9. *entitate* - orice persoană fizică sau juridică, publică ori privată, creată și recunoscută ca atare potrivit legislației naționale a locului său de stabilire, care poate, acționând în nume propriu, să exercite drepturi și să fie supusă unor obligații;

8.10. *entitate cu impact critic* - entitate care desfășoară un proces cu impact critic și care este identificată de ANRE în conformitate cu pct. 44;

8.11. *entitate cu impact ridicat* - entitate care desfășoară un proces cu impact ridicat și care este identificată de ANRE ca entitate cu impact ridicat în conformitate cu pct. 44;

8.12. *centru de operațiuni de securitate cibernetică (CSOC)* - centru dedicat în cadrul căruia o echipă tehnică formată din unul sau mai mulți experți, susținută de sisteme informatice de securitate cibernetică, îndeplinește sarcini legate de securitate, precum gestionarea atacurilor cibernetice și a erorilor de configurare a securității, monitorizarea securității, analiza jurnalelor de evenimente și detectarea atacurilor cibernetice;

8.13. *furnizor critic de servicii TIC* - entitate care furnizează un serviciu TIC sau un proces TIC necesar pentru un proces cu impact critic ori cu impact ridicat care afectează securitatea cibernetică a fluxurilor transfrontaliere de energie electrică și care, dacă este compromis, poate cauza un atac cibernetic al cărui impact depășește pragul de impact critic sau pragul de impact ridicat;

8.14. *gestionarea vulnerabilităților de securitate cibernetică* - practica de identificare și remediere a vulnerabilităților;

8.15. *indice de impact în materie de securitate cibernetică în domeniul energiei electrice (ECII)* - indice sau grilă de clasificare care ierarhizează consecințele potențiale ale atacurilor cibernetice asupra proceselor operaționale implicate în fluxurile transfrontaliere de energie electrică;

8.16. *inițiator* - entitatea care inițiază un eveniment de schimb de informații, de partajare de informații sau de stocare a informațiilor;

8.17. *matrice de impact al riscurilor* - matrice utilizată în procesul de evaluare a riscurilor pentru determinarea nivelului de impact al riscului rezultat pentru fiecare risc evaluat;

8.18. *criză simultană de energie electrică* - criză de energie electrică care afectează simultan mai multe părți contractante ale Comunității Energetice și/sau state membre ale Uniunii Europene;

8.19. *perimetru cu impact critic* - perimetru definit de o entitate, care cuprinde toate activele cu impact critic ale acesteia și în interiorul căruia accesul la aceste active poate fi controlat, delimitând domeniul de aplicare al controalelor avansate de securitate cibernetică;

8.20. *perimetru cu impact ridicat* - perimetru definit de o entitate, care cuprinde toate activele cu impact ridicat ale acesteia și în interiorul căruia accesul la aceste active poate fi controlat, delimitând domeniul de aplicare al controalelor minime de securitate cibernetică;

8.21. *prag de impact critic* - valorile indicilor ECII stabilite potrivit pct. 43.2.7., peste care un atac cibernetic asupra unui proces operațional determină perturbări critice ale fluxurilor transfrontaliere de energie electrică;

8.22. *prag de impact ridicat* - valorile indicilor ECII stabilite potrivit pct. 43.2.7., peste care un atac cibernetic reușit asupra unui proces operațional va cauza o perturbare ridicată a fluxurilor transfrontaliere de energie electrică;

8.23. *proces cu impact critic* - proces operațional desfășurat de o entitate, pentru care indicii ECII depășesc pragul de impact critic;

8.24. *proces cu impact ridicat* - proces operațional desfășurat de o entitate, pentru care indicii ECII depășesc pragul de impact ridicat;

8.25. *produs TIC, serviciu TIC, proces TIC* - au înțelesul prevăzut la art. 2 din Legea nr. 48/2023, aplicat prin analogie produselor, serviciilor și proceselor tehnologiei informației și comunicațiilor din sectorul electroenergetic, inclusiv dispozitivelor tehnice și programelor informatice care permit interacțiunea directă cu rețeaua electrică;

8.26. *punct național unic de contact* - ASC, potrivit art. 7 alin. (2) din Legea nr. 48/2023;

8.27. *punct unic de contact la nivel de entitate* - persoana sau structura desemnată de o entitate cu impact ridicat sau cu impact critic, în condițiile pct. 85.7, în scopul schimbului de informații privind securitatea cibernetică;

8.28. *parte interesată* - orice parte care are un interes în succesul și funcționarea continuă a unei entități sau a unui proces prevăzut de prezentul Cod, precum angajați, conducători, acționari sau fondatori, autorități de reglementare, asociații profesionale, furnizori și clienți;

8.29. *regiune de exploatare a sistemului* - regiunea de operare a sistemelor electroenergetice, în sensul art. 2 din Legea nr. 164/2025;

8.30. *specificații de achiziție* - specificațiile pe care entitățile le stabilesc pentru achiziția de produse TIC, procese TIC sau servicii TIC noi ori actualizate;

8.31. *sistem de gestionare a securității cibernetice* - politicile, procedurile, orientările și resursele, precum și activitățile asociate acestora, gestionate colectiv de o entitate în scopul protejării activelor sale informaționale împotriva amenințărilor cibernetice, prin stabilirea, implementarea, operarea, monitorizarea, revizuirea, întreținerea și îmbunătățirea sistematică a securității rețelelor și sistemelor informatice ale organizației;

8.32. *sistem european de certificare a securității cibernetice* - ansamblul cuprinzător de norme, cerințe tehnice, standarde și proceduri, stabilit la nivelul Uniunii Europene, care se aplică certificării sau evaluării conformității anumitor produse TIC, servicii TIC sau procese TIC;

8.33. *sistem informatic legacy (sistem TIC moștenit)* - sistem TIC care a ajuns la finalul ciclului său de viață, care nu permite actualizări sau remedieri din motive tehnologice ori comerciale sau care nu mai este susținut de furnizorul său ori de un furnizor terț de servicii TIC, dar care este încă utilizat și susține funcțiile entității;

8.34. *standard* - specificație tehnică adoptată de un organism de standardizare recunoscut, pentru aplicare repetată sau continuă, a cărei respectare nu este obligatorie;

8.35. *vulnerabilitate necorectată exploatată activ* - o vulnerabilitate care nu a fost încă adusă la cunoștința publicului și remediată și cu privire la care există dovezi credibile că a fost executat cod rău intenționat de către un actor asupra unui sistem fără permisiunea proprietarului acestuia;

8.36. *reprezentant* - persoană fizică sau juridică stabilită în Republica Moldova, desemnată în mod expres să acționeze în numele unei entități cu impact ridicat sau cu impact critic care nu este stabilită în Republica Moldova, dar care prestează servicii unor entități din Republica Moldova, și care poate fi contactată de ANRE ori de ASC în locul entității respective.

Secțiunea 3
Autoritatea competentă și cooperarea instituțională

9. ANRE este autoritatea competentă la nivel național pentru îndeplinirea atribuțiilor stabilite prin prezentul Cod, în calitatea sa de autoritate de reglementare desemnată potrivit art. 7 din Legea nr. 164/2025.

10. ANRE poate delega, prin hotărâre proprie sau prin dispoziții exprese ale prezentului Cod, exercitarea unor atribuții stabilite prin prezentul Cod către alte autorități naționale, cu excepția atribuțiilor de coordonare și cooperare instituțională prevăzute la pct. 13 și 14. ANRE monitorizează modul de aplicare a prezentului Cod de către autoritățile cărora le-a delegat atribuții și comunică Secretariatului Comunității Energetice, Comitetului de Reglementare al Comunității Energetice, Grupului de coordonare pentru securitatea aprovizionării și Grupului de coordonare al Comunității Energetice pentru securitate cibernetică și infrastructuri critice denumirea, datele de contact și atribuțiile delegate, precum și orice modificare ulterioară a acestora.

11. ASC, autoritate competentă la nivel național în domeniul securității cibernetice potrivit art. 7 din Legea nr. 48/2023 și Hotărârii Guvernului nr. 1028/2023, exercită, pentru domeniul reglementat de prezentul Cod, funcțiile de:

11.1. echipă de răspuns la incidente de securitate cibernetică (CSIRT) pentru sectorul electroenergetic;

11.2. punct național unic de contact, în sensul pct. 8.26;

11.3. autoritate de gestionare a crizelor cibernetice la nivel național, în sensul pct. 8.7.

12. ASC exercită atribuțiile prevăzute la pct. 11 în strânsă cooperare cu ANRE și cu Operatorul Sistemului de Transport *(în continuare - OST),* cu respectarea specificului sectorial al fluxurilor transfrontaliere de energie electrică.

13. ANRE și ASC asigură coordonarea și cooperarea corespunzătoare între ele, precum și cu Comisia pentru Situații Excepționale, cu Ministerul Energiei și cu OST, în scopul îndeplinirii obligațiilor relevante prevăzute de prezentul Cod. ANRE și ASC stabilesc, în termen de 6 luni de la intrarea în vigoare a prezentei hotărâri, printr-un protocol de cooperare, modalitatea de schimb de informații privind atacurile cibernetice, incidentele și amenințările cibernetice raportate potrivit pct. 83-96, procedura de coordonare a activităților de supraveghere, controalelor și inspecțiilor, precum și punctele de contact operaționale ale fiecărei autorități.

14. ANRE și ASC cooperează cu organismele și autoritățile relevante ale Comunității Energetice, atunci și în măsura în care asemenea organisme și autorități exercită atribuții față de Republica Moldova în domeniul reglementat de prezentul Cod, în scopul asigurării unor proceduri eficiente și al evitării dublării sarcinilor și obligațiilor.

Secțiunea 4

Termeni și condiții, metodologii și planuri

15. OST participă, prin intermediul ENTSO-E, la elaborarea termenilor, condițiilor sau metodologiilor (în continuare, împreună cu planurile - TCM) la nivel regional, în măsura în care astfel de procese sunt organizate de ENTSO-E, în temeiul calității de membru al OST, și elaborează și prezintă ANRE, spre aprobare, TCM la nivel național prevăzute de prezenta secțiune. TCM adoptate la nivelul Comunității Energetice și Agenției Uniunii Europene pentru Cooperarea Autorităților de Reglementare din Domeniul Energiei (ACER), în măsura în care acestea vor exercita o asemenea funcție față de Republica Moldova, se pun în aplicare prin hotărâre a ANRE, potrivit art. 39 alin. (9)-(14) din Legea nr. 164/2025.

16. Sunt supuse aprobării ANRE, ca TCM la nivel național:

16.1. metodologiile de evaluare a riscurilor de securitate cibernetică prevăzute la pct. 35-37;

16.2. raportul de evaluare a riscurilor de securitate cibernetică la nivel național prevăzut la pct. 43;

16.3. controalele minime și avansate de securitate cibernetică prevăzute la pct. 58, corespondența controalelor de securitate cibernetică cu standardele prevăzută la pct. 74, inclusiv controalele minime și avansate de securitate cibernetică în lanțul de aprovizionare prevăzute la pct. 69-70;

16.4. recomandarea privind achizițiile în domeniul securității cibernetice prevăzută la pct. 75;

16.5. metodologia scalei de clasificare a atacurilor cibernetice prevăzută la pct. 84.

17. Propunerea de plan regional de atenuare a riscurilor de securitate cibernetică prevăzută la pct. 41 este supusă aprobării tuturor autorităților competente relevante din regiunea de operare a sistemelor electroenergetice vizată, cu respectarea, atunci când sunt implicate mai multe autorități competente din regiunea respectivă, a pragului special de vot prevăzut la pct. 19.1.

18. Propunerile de TCM includ un calendar propus pentru implementarea acestora și o descriere a impactului preconizat asupra obiectivelor prezentului Cod. Operatorii sistemelor de distribuție sunt consultați de OST la elaborarea TCM, potrivit art. 39 alin. (2) din Legea nr. 164/2025. La elaborarea comună a TCM la nivel regional, atunci când astfel de procese sunt organizate de ENTSO-E, OST participanți cooperează îndeaproape cu ceilalți operatori ai sistemelor de transport.

18.1. Entitatea OSD UE, atunci când există un asemenea proces organizat la nivelul relevant, poate transmite OST un aviz motivat cu privire la propunerile de TCM cu până la trei săptămâni înainte de termenul de prezentare a acestora ANRE. OST ia în considerare avizul motivat înainte de transmiterea propunerii spre aprobare și prezintă o justificare în cazul în care acesta nu este luat în considerare.

19. Dacă OST din regiunea de operare a sistemelor electroenergetice nu ajung la un acord asupra unei propuneri de TCM la nivel regional organizate de ENTSO-E, propunerea se adoptă prin vot cu majoritate calificată, potrivit regulilor stabilite de ENTSO-E pentru acest proces, la care OST participă în temeiul calității sale de membru.

19.1. Pentru propunerile prevăzute la pct. 16 (metodologii și celelalte TCM la nivel național elaborate cu participarea mai multor operatori ai sistemelor de transport), majoritatea calificată se consideră întrunită dacă OST reprezintă cel puțin 55% dintre părțile la procesul respectiv și OST reprezintă părți care cuprind cel puțin 65% din populația zonei vizate, cu o minoritate de blocare formată din cel puțin 4 asemenea părți și cu un vot atribuit fiecărei părți. Pentru propunerea de plan regional de atenuare a riscurilor prevăzută la pct. 41, atunci când regiunea de operare a sistemelor electroenergetice este compusă din mai mult de cinci asemenea părți, majoritatea calificată se consideră întrunită dacă OST reprezintă cel puțin 72% dintre părțile vizate și OST reprezintă părți care cuprind cel puțin 65% din populația regiunii vizate, cu o minoritate de blocare formată din OST reprezentând peste 35% din populația părților participante, plus cel puțin un OST reprezentând o parte vizată suplimentară.

19.2. OST participă la procesul de vot prevăzut la pct. 19 și 19.1 potrivit regulilor stabilite prin acordurile de cooperare la care Republica Moldova sau OST sunt parte, inclusiv, dacă este cazul, în ceea ce privește distribuirea drepturilor de vot între mai mulți OST din Republica Moldova.

20. OST prezintă ANRE, spre aprobare, propunerile de TCM prevăzute la pct. 16, în termenele stabilite la pct. 35, 58, 68, 75 și 84. ANRE poate prelungi aceste termene, în situații excepționale, în special atunci când termenul nu poate fi respectat din cauze exterioare sferei de control a OST.

21. ANRE analizează propunerile de TCM prevăzute la pct. 16 și decide asupra acestora în termen de 6 luni de la primirea propunerii.

22. Dacă ANRE solicită o modificare a propunerii ca o condiție a aprobării, OST prezintă propunerea modificată în termen de 2 luni de la solicitare, iar ANRE decide asupra propunerii modificate în termen de 2 luni de la prezentarea acesteia.

23. Dacă OST nu prezintă o propunere inițială sau modificată în termenele stabilite la pct. 20 sau 22, ANRE poate, prin hotărâre proprie, să stabilească termenul definitiv de prezentare a propunerii, să solicite modificări, să revizuiască și să completeze proiectele existente sau, dacă este necesar pentru respectarea termenelor prevăzute de Cod, să definească și să aprobe direct TCM respectiv, informând OST cu privire la aceasta.

24. Potrivit art. 39 alin. (13) din Legea nr. 164/2025, hotărârile ANRE de aprobare a TCM se publică în Monitorul Oficial al Republicii Moldova, iar TCM aprobate se publică pe paginile web oficiale ale ANRE și OST, cu excepția informațiilor considerate confidențiale în conformitate cu pct. 124. ANRE poate solicita propuneri de modificare a TCM aprobate, stabilind un termen pentru prezentarea acestora. OST poate propune modificări și din proprie inițiativă, cu respectarea aceleiași proceduri.

25. La fiecare 3 ani de la prima adoptare a unui TCM, OST revizuiește eficacitatea acestuia și raportează concluziile revizuirii ANRE, fără întârzieri nejustificate.

26. OST consultă părțile interesate, inclusiv ANRE, cu privire la proiectele propunerilor de TCM prevăzute la pct. 16, pentru o perioadă de cel puțin o lună, propunerile se publică și se supun consultării publice la nivel național. Propunerile de TCM la nivel regional, atunci când sunt organizate de ENTSO-E, se supun consultării potrivit regulilor stabilite de aceasta.

27. OST ține seama în mod corespunzător de punctele de vedere ale părților interesate rezultate din consultări, înainte de prezentarea propunerii spre aprobare, și prezintă, împreună cu propunerea, o justificare temeinică pentru includerea sau neincluderea acestor puncte de vedere, publicată în timp util înainte de sau concomitent cu propunerea.

28. ANRE organizează implicarea părților interesate, inclusiv prin reuniuni periodice, pentru identificarea problemelor și formularea propunerilor de îmbunătățire legate de aplicarea prezentului Cod.

Secțiunea 5
Dispoziții comune privind costurile, monitorizarea și cooperarea

29. Costurile suportate de OST și de operatorii sistemelor de distribuție (în continuare - OSD) supuși reglementării prin tarife de rețea și care decurg din obligațiile prevăzute de prezentul Cod sunt evaluate de ANRE, în conformitate cu metodologia de calculare, aprobare și aplicare a tarifelor reglementate, prevăzută la art. 9 alin. (1) lit. k) din Legea nr. 164/2025. Costurile apreciate ca fiind rezonabile, eficiente și proporționale se recuperează prin tarifele de rețea sau prin alte mecanisme corespunzătoare, stabilite de ANRE. La cererea ANRE, OST și OSD prezintă, în termenul rezonabil stabilit, informațiile necesare pentru facilitarea evaluării costurilor.

30. ANRE monitorizează aplicarea prezentului Cod la nivel național. Atunci și în măsura în care Comitetul de Reglementare al Comunității Energetice exercită o funcție de monitorizare față de Republica Moldova în domeniul reglementat de prezentul Cod, ANRE, cu sprijinul OST, poate coopera cu acesta și îi poate transmite informațiile solicitate. Entitățile prevăzute la pct. 2 prezintă ANRE și ASC informațiile necesare pentru îndeplinirea atribuțiilor de monitorizare.

31. ANRE efectuează, în termen de 12 luni de la primirea sau, în lipsa acestuia, de la elaborarea unui ghid propriu, o analiză comparativă pentru a evalua dacă investițiile actuale în securitatea cibernetică atenuează riscurile cu impact asupra fluxurilor transfrontaliere de energie electrică, produc rezultatele dorite, generează câștiguri de eficiență pentru dezvoltarea sistemelor de energie electrică și sunt eficiente și integrate în achiziția generală de active și servicii.

31.1. În efectuarea analizei comparative, ANRE evaluează, în special, cheltuielile medii aferente securității cibernetice, prețurile medii ale serviciilor, sistemelor și produselor de securitate cibernetică, precum și comparabilitatea costurilor și funcțiilor acestora.

31.2. Analiza comparativă nu se face publică și se tratează în conformitate cu cerințele privind clasificarea informațiilor și confidențialitatea prevăzute de prezentul Cod.

32. În termen de 18 luni de la intrarea în vigoare a prezentului Cod, dacă OST face parte dintr-o regiune de operare a sistemelor electroenergetice vecină unei țări terțe, acesta depune diligențe pentru încheierea unor acorduri cu operatorii sistemelor de transport din țara

terță vecină, care să stabilească baza cooperării privind protecția securității cibernetice. OST informează ANRE cu privire la acordurile astfel încheiate.

33. Entitățile care nu au un sediu în Republica Moldova, dar care prestează servicii unor entități din Republica Moldova și au fost notificate ca fiind entități cu impact ridicat sau cu impact critic în conformitate cu pct. 45, desemnează, în scris, în termen de 3 luni de la notificare, un reprezentant stabilit în Republica Moldova și informează despre aceasta ANRE.

33.1. Reprezentantul este mandatat pentru a fi contactat de ANRE sau de ASC, în plus față de entitatea cu impact ridicat sau cu impact critic ori în locul acesteia. Entitatea îi asigură reprezentantului competențele necesare și resurse suficiente pentru a garanta cooperarea eficientă și în timp util a acestuia.

33.2. Entitatea se consideră a fi sub jurisdicția Republicii Moldova atunci când reprezentantul este stabilit pe teritoriul acesteia, în acest caz, entitatea notifică ANRE numele, adresa poștală, adresa de email și numărul de telefon ale reprezentantului său legal.

33.3. Reprezentantul legal desemnat poate fi tras la răspundere pentru nerespectarea obligațiilor prevăzute de prezentul Cod, fără a aduce atingere răspunderii entității cu impact ridicat sau cu impact critic însăși. În lipsa desemnării unui reprezentant, Republica Moldova poate întreprinde acțiuni legale împotriva entității pentru nerespectarea obligațiilor prevăzute de prezentul Cod. Desemnarea unui reprezentant legal nu constituie, prin ea însăși, stabilirea unui sediu în Republica Moldova.

34. Atunci și în măsura în care Comitetul de Reglementare al Comunității Energetice exercită o funcție de monitorizare a măsurilor de gestionare a riscurilor de securitate cibernetică prevăzute la pct. 49-53 și a obligațiilor de raportare prevăzute la pct. 54 și 85 față de Republica Moldova, ANRE cooperează cu acesta în exercitarea acestei funcții.

CAPITOLUL II
EVALUAREA RISCURILOR DE SECURITATE CIBERNETICĂ ȘI IDENTIFICAREA ENTITĂȚILOR

Secțiunea 1
Metodologiile de evaluare a riscurilor de securitate cibernetică

35. În termen de 4 luni de la intrarea în vigoare a prezentului Cod, OST, cu asistența ENTSO-E, prezintă ANRE propunerea de metodologii de evaluare a riscurilor de securitate cibernetică la nivel național, aprobată potrivit pct. 21. Metodologiile aprobate la nivelul Comunității Energetice sau, după caz, al Uniunii Europene se pun în aplicare prin hotărâre a ANRE, potrivit art. 39 alin. (14) din Legea nr. 164/2025, iar OST propune, după caz, actualizarea corespunzătoare a metodologiei naționale.

36. Metodologiile de evaluare a riscurilor de securitate cibernetică includ:

36.1. o listă a amenințărilor cibernetice care trebuie luate în considerare, incluzând cel puțin următoarele amenințări legate de lanțul de aprovizionare:

36.1.1. coruperea gravă și neașteptată a lanțului de aprovizionare;

36.1.2. indisponibilitatea produselor TIC, serviciilor TIC sau proceselor TIC din lanțul de aprovizionare;

36.1.3. atacurile cibernetice inițiate prin actori din lanțul de aprovizionare;

36.1.4. scurgerea de informații sensibile prin lanțul de aprovizionare, inclusiv trasabilitatea acestuia;

36.1.5. introducerea de vulnerabilități sau de uși ascunse („backdoors”) în produsele, serviciile sau procesele TIC prin actori din lanțul de aprovizionare;

36.2. criteriile de evaluare a impactului riscurilor de securitate cibernetică ca fiind ridicat sau critic, utilizând praguri definite pentru consecințe și pentru probabilitate;

36.3. o abordare pentru analiza riscurilor de securitate cibernetică care decurg din sisteme informatice legacy, din efectele în cascadă ale atacurilor cibernetice și din natura în timp real a sistemelor care operează rețeaua electrică;

36.4. o abordare pentru analiza riscurilor de securitate cibernetică care decurg din dependența de un furnizor unic de produse TIC, servicii TIC sau procese TIC;

36.5. descrierea modului în care se definesc valorile ECII pentru pragurile de impact ridicat și critic, astfel încât entitățile să poată estima, potrivit pct. 51.3.1., impactul riscurilor asupra proceselor lor operaționale.

37. În baza Metodologiilor de evaluare a riscurilor de securitate cibernetică se evaluează riscurile utilizând aceeași matrice de impact al riscurilor, care:

37.1. măsoară consecințele atacurilor cibernetice pe baza:

37.1.1. pierderii de sarcină;

37.1.2. reducerii producerii de energie electrică;

37.1.3. pierderii capacității în rezerva primară de frecvență;

37.1.4. pierderii capacității de restaurare fără sprijinul rețelei de transport externe („black start”);

37.1.5. duratei preconizate a unei întreruperi în aprovizionarea cu energie electrică, coroborată cu numărul de utilizatori afectați;

37.1.6. oricărui alt criteriu cantitativ sau calitativ care poate constitui un indicator rezonabil al efectului unui atac cibernetic asupra fluxurilor transfrontaliere de energie electrică;

37.2. măsoară, distinct de criteriile prevăzute la subpct. 37.1, probabilitatea unui incident, ca frecvență anuală a atacurilor cibernetice.

38. Atunci și în măsura în care ENTSO-E organizează o evaluare a riscurilor de securitate cibernetică la nivelul Comunității Energetice sau un raport cuprinzător privind fluxurile transfrontaliere de energie electrică, OST, cu asistența și în cadrul termenelor stabilite de ENTSO-E, contribuie la acest proces cu informațiile rezultate din raportul național prevăzut la pct. 43.1, cu respectarea confidențialității informațiilor potrivit pct. 123.

Secțiunea 2
Evaluarea națională a riscurilor de securitate cibernetică

39. Prin prezentul Cod, ANRE deleagă Agenției pentru Securitate Cibernetică exercitarea atribuției de evaluare a riscurilor de securitate cibernetică la nivel național, prevăzută la pct. 43, în condițiile pct. 10, și monitorizează modul de exercitare a acesteia.

40. Atunci și în măsura în care ENTSO-E organizează, în consultare cu centrul de coordonare regional relevant, o evaluare regională a riscurilor de securitate cibernetică pentru regiunea de operare a sistemelor electroenergetice din care face parte OST, acesta participă la procesul respectiv, punând la dispoziție informațiile rezultate din raportul național prevăzut la pct. 43.1.

41. Atunci și în măsura în care ENTSO-E organizează elaborarea unui plan regional de atenuare a riscurilor de securitate cibernetică pentru regiunea de operare a sistemelor electroenergetice din care face parte OST, acesta participă la procesul respectiv, cu asistența

ENTSO-E și în consultare cu centrul de coordonare regional relevant, iar propunerea rezultată este supusă aprobării ANRE, potrivit pct. 18.1.

41.1. Planul regional de atenuare a riscurilor de securitate cibernetică include controalele minime și avansate de securitate cibernetică pe care entitățile cu impact ridicat și cu impact critic trebuie să le aplice în regiunea de operare a sistemelor electroenergetice, precum și riscurile reziduale de securitate cibernetică rămase după aplicarea acestor controale.

41.2. OST actualizează, cu asistența ENTSO-E, planul regional de atenuare a riscurilor, atunci când acesta există, la fiecare 3 ani, cu excepția cazului în care circumstanțele impun actualizări mai frecvente.

42. Independent de existența unui plan regional de atenuare a riscurilor potrivit pct. 41, ANRE stabilește controalele minime și avansate de securitate cibernetică aplicabile la nivel național, potrivit pct. 58, pe baza raportului de evaluare a riscurilor de securitate cibernetică la nivel național prevăzut la pct. 43.1.

43. ASC efectuează evaluarea riscurilor de securitate cibernetică la nivel național asupra tuturor entităților cu impact ridicat și cu impact critic din Republica Moldova, utilizând metodologiile prevăzute la pct. 36-37, pentru a identifica și analiza riscurile atacurilor cibernetice care afectează securitatea operațională a sistemului electroenergetic și perturbă fluxurile transfrontaliere de energie electrică, fără a lua în considerare prejudiciul juridic, financiar sau reputațional al atacurilor cibernetice.

43.1. În termen de 12 luni de la aprobarea metodologiilor potrivit pct. 21 și, ulterior, o dată la trei ani, ASC, în cooperare cu ANRE, elaborează raportul de evaluare a riscurilor de securitate cibernetică la nivel național.

43.2.1. Raportul prevăzut la pct. 43.1 conține, pentru fiecare proces operațional cu impact ridicat și cu impact critic:

43.2.2. stadiul implementării controalelor minime și avansate de securitate cibernetică prevăzute la pct. 57-58;

43.2.3. **lista** tuturor atacurilor cibernetice raportate în ultimii trei ani potrivit pct. 86;

43.2.4. **sinteza** informațiilor privind amenințările cibernetice raportate în ultimii trei ani potrivit pct. 89;

43.2.5. pentru fiecare proces cu impact ridicat sau cu impact critic, estimarea riscurilor de compromitere a confidențialității, integrității și disponibilității informațiilor și activelor relevante;

43.2.6. dacă este necesar, lista entităților suplimentare identificate ca fiind cu impact ridicat sau cu impact critic potrivit pct. 44.2;

43.2.7. valorile ECII și pragurile de impact ridicat și de impact critic, stabilite pe baza metodologiilor prevăzute la pct. 36-37.

43.3. Raportul de evaluare a riscurilor de securitate cibernetică la nivel național ține cont de Planul de acțiuni pentru situații excepționale în sectorul electroenergetic, aprobat prin Hotărârea Guvernului nr. 820/2024.

43.4. Informațiile prevăzute la pct. 43.2.1. – 43.2.6. nu se corelează cu entități sau active specifice, iar raportul include, de asemenea, o evaluare a riscurilor derogărilor temporare acordate de ANRE în conformitate cu pct. 63-65.

43.5. ASC răspunde de corectitudinea și exactitatea informațiilor cuprinse în raport. ANRE aprobă raportul, potrivit pct. 16.2 și 21, și poate solicita informații suplimentare ASC în legătură cu conținutul acestuia.

Secțiunea 3
Identificarea entităților cu impact ridicat și cu impact critic

44. ANRE identifică, utilizând ECII și pragurile de impact ridicat și critic stabilite potrivit pct. 43.2.7., entitățile cu impact ridicat și cu impact critic din Republica Moldova implicate în procesele cu impact ridicat și cu impact critic. ANRE poate solicita informații de la o entitate pentru a determina valorile ECII ale acesteia.

44.1. ANRE identifică, utilizând aceleași ECII și praguri, entitățile cu impact ridicat și cu impact critic care nu sunt stabilite în Republica Moldova, în măsura în care acestea sunt active pe teritoriul acesteia, putând solicita informații acestora pentru determinarea ECII.

44.2. ANRE poate identifica entități suplimentare ca fiind cu impact ridicat sau cu impact critic dacă sunt îndeplinite cumulativ următoarele criterii:

44.2.1. entitatea face parte dintr-un grup de entități pentru care există un risc semnificativ de a fi afectate simultan de un atac cibernetic; și

44.2.2. ECII agregat la nivelul grupului de entități depășește pragul de impact ridicat sau critic. Dacă sunt identificate astfel de entități, toate procesele acestora pentru care ECII agregat la nivelul grupului depășește pragul de impact ridicat se consideră procese cu impact ridicat, iar cele pentru care ECII agregat depășește pragul de impact critic se consideră procese cu impact critic.

44.3. Dacă ANRE identifică entități aparținând unui grup din mai multe părți contractante ale Comunității Energetice și/sau state membre ale Uniunii Europene, informează celelalte autorități competente și, dacă este cazul, ENTSO-E, pentru o analiză a agregării. În cazul în care ECII agregat al grupului depășește pragul de impact ridicat sau critic, ANRE identifică entitățile din grupul respectiv, aflate în Republica Moldova, ca fiind cu impact ridicat sau cu impact critic.

44.4. În termen de 3 luni de la aprobarea raportului prevăzut la pct. 43.1, ANRE identifică entitățile cu impact ridicat și cu impact critic potrivit prezentei secțiuni.

45. În termen de o lună de la identificarea prevăzută la pct. 44.4, dar nu mai târziu de 31 decembrie 2029, ANRE notifică entităților de pe listă faptul că au fost identificate ca entități cu impact ridicat sau cu impact critic în Republica Moldova. Termenele stabilite prin raportare la notificarea entităților cu impact ridicat și cu impact critic prevăzute de prezentul Cod se calculează de la data la care ANRE efectuează această notificare.

46. Atunci când un furnizor de servicii este raportat ASC ca fiind furnizor critic de servicii TIC potrivit pct. 54.3., ASC notifică acest fapt autorităților competente ale părților contractante ale Comunității Energetice și/sau statelor membre ale Uniunii Europene pe teritoriul cărora se află sediul sau reprezentantul furnizorului respectiv.

Secțiunea 4
Sistemele naționale de verificare

47. ANRE, în cooperare cu ASC, poate stabili un sistem național de verificare pentru a verifica dacă entitățile cu impact critic identificate potrivit pct. 44 au implementat cadrul legislativ național, inclus în matricea de corespondență prevăzută la pct. 75. Sistemul național de verificare se poate baza pe o inspecție realizată de ANRE, pe audituri de securitate independente ale unor terți sau pe evaluări reciproce (peer review) realizate de entitățile cu impact critic, sub supravegherea ANRE.

48. Dacă ANRE decide să stabilească un sistem național de verificare, se asigură că verificarea se realizează cu respectarea următoarelor cerințe:

48.1. partea care efectuează evaluarea reciprocă, auditul sau inspecția este independentă de entitatea cu impact critic verificată și nu are conflicte de interese;

48.2. personalul care efectuează verificarea are cunoștințe demonstrabile privind securitatea cibernetică în sectorul electroenergetic, sistemele de management al securității cibernetice, principiile auditului, evaluarea riscurilor de securitate cibernetică, cadrul comun de securitate cibernetică prevăzut la pct. 56, cadrul legislativ și de reglementare național și standardele europene și internaționale relevante pentru domeniul verificării, precum și procesele cu impact critic vizate;

48.3. partea care efectuează verificarea dispune de timp suficient pentru aceasta;

48.4. sunt luate măsuri corespunzătoare pentru protejarea informațiilor colectate, potrivit nivelului lor de confidențialitate;

48.5. auditurile sau inspecțiile se realizează cel puțin o dată pe an și acoperă întreaga sferă de verificare cel puțin o dată la 3 ani.

Secțiunea 5

Gestionarea riscurilor de securitate cibernetică la nivel de entitate și raportarea

49. Fiecare entitate cu impact ridicat și cu impact critic identificată de ANRE potrivit pct. 44 efectuează gestionarea riscurilor de securitate cibernetică pentru toate activele sale incluse în perimetrele cu impact ridicat și cu impact critic, cel puțin o dată la 3 ani, parcurgând etapele:

49.1. stabilirea contextului;

49.2.evaluarea riscurilor de securitate cibernetică la nivel de entitate;

49.3.tratarea riscurilor de securitate cibernetică;

49.4.acceptarea riscurilor de securitate cibernetică.

50. În etapa de stabilire a contextului, fiecare entitate cu impact ridicat și cu impact critic:

50.1. definește domeniul de aplicare al evaluării riscurilor de securitate cibernetică, inclusiv procesele cu impact ridicat și cu impact critic identificate potrivit pct. 43, precum și alte procese care pot constitui ținte ale unor atacuri cibernetice cu impact ridicat sau cu impact critic asupra fluxurilor transfrontaliere de energie electrică;

50.2. definește criteriile de evaluare a riscurilor și criteriile de acceptare a riscurilor în conformitate cu matricea de impact al riscurilor prevăzută la pct. 37.

51. În etapa de evaluare a riscurilor de securitate cibernetică, fiecare entitate cu impact ridicat și cu impact critic:

51.1. identifică riscurile de securitate cibernetică, ținând seama de:

51.1.1. toate activele care susțin procesele cu impact ridicat și cu impact critic, inclusiv evaluarea posibilului impact asupra fluxurilor transfrontaliere de energie electrică în cazul compromiterii activului;

51.1.2. posibilele amenințări cibernetice, inclusiv amenințările identificate în cel mai recent raport de evaluare a riscurilor de securitate cibernetică la nivel național, precum și amenințările aferente lanțului de aprovizionare;

51.1.3. vulnerabilitățile existente, inclusiv vulnerabilitățile sistemelor informatice moștenite;

51.1.4. posibilele scenarii de atac cibernetic, inclusiv atacurile care afectează securitatea operațională a sistemului electroenergetic și perturbă fluxurile transfrontaliere de energie electrică;

51.1.5. evaluările coordonate ale riscurilor legate de lanțurile de aprovizionare critice, realizate la nivel european sau național, dacă există;

51.1.6. controalele existente implementate;

51.2. analizează probabilitatea și consecințele riscurilor de securitate cibernetică identificate și determină nivelul riscului utilizând matricea de impact al riscurilor prevăzută la pct. 37;

51.3. clasifică activele în funcție de posibilele consecințe ale compromiterii securității cibernetice și determină perimetrele cu impact ridicat și cu impact critic prin:

51.3.1. realizarea, pentru toate procesele supuse evaluării riscurilor de securitate cibernetică, a unei evaluări a impactului asupra activității utilizând ECII;

51.3.2. clasificarea unui proces ca proces cu impact ridicat sau cu impact critic dacă ECII depășește pragul de impact ridicat sau, respectiv, pragul de impact critic;

51.3.3. determinarea activelor cu impact ridicat și cu impact critic ca active necesare pentru procesele cu impact ridicat și, respectiv, pentru procesele cu impact critic;

51.3.4. definirea perimetrelor cu impact ridicat și cu impact critic care includ activele respective, astfel încât accesul la acestea să poată fi controlat;

51.4. evaluează și prioritizează riscurile de securitate cibernetică utilizând criteriile de evaluare și acceptare a riscurilor prevăzute la pct. 50.2.

52. În etapa de tratare a riscurilor de securitate cibernetică, fiecare entitate cu impact ridicat și cu impact critic stabilește un plan de atenuare a riscurilor la nivel de entitate prin selectarea măsurilor adecvate pentru gestionarea riscurilor și identificarea riscurilor reziduale. În etapa de acceptare a riscurilor de securitate cibernetică, fiecare entitate cu impact ridicat și cu impact critic decide acceptarea riscurilor reziduale pe baza criteriilor de acceptare a riscurilor stabilite potrivit pct. 50.2

53. Fiecare entitate cu impact ridicat și cu impact critic înregistrează activele identificate potrivit prezentei secțiuni într-un inventar al activelor, care nu face parte din raportul de evaluare a riscurilor. ANRE și/sau ASC, în limitele competențelor stabilite prin prezentul Cod, pot inspecta activele incluse în inventar în cadrul inspecțiilor efectuate.

54. În termen de 12 luni de la notificarea entităților cu impact ridicat și cu impact critic potrivit pct. 45 și, ulterior, o dată la 3 ani, fiecare entitate cu impact ridicat și cu impact critic transmite ANRE un raport care conține:

54.1. lista controalelor selectate pentru planul de atenuare a riscurilor la nivel de entitate, stabilit potrivit pct. 52, împreună cu stadiul actual al implementării fiecărui control;

54.2. pentru fiecare proces cu impact ridicat sau cu impact critic, o estimare a riscului de compromitere a confidențialității, integrității și disponibilității informațiilor și activelor relevante, realizată în conformitate cu matricea de impact al riscurilor prevăzută la pct. 37;

54.3. lista furnizorilor critici de servicii TIC pentru procesele cu impact critic ale entității.

55. ANRE pune la dispoziția ASC informațiile relevante din rapoartele prevăzute la prezentul punct, prin protocolul de cooperare prevăzut la pct. 13, în scopul exercitării atribuției delegate potrivit pct. 39.

CAPITOLUL III
CADRUL COMUN DE SECURITATE CIBERNETICĂ ÎN SECTORUL ELECTROENERGETIC

Secțiunea 1
Componența, funcționarea și revizuirea cadrului comun

56. Cadrul comun de securitate cibernetică în sectorul electroenergetic este compus din următoarele controale și din sistemul de management al securității cibernetice:

56.1. controalele minime de securitate cibernetică, elaborate potrivit pct. 58;

56.2.controalele avansate de securitate cibernetică, elaborate potrivit pct. 57;

56.3. matricea de corespondență, elaborată potrivit pct. 75, care corelează controalele prevăzute la 56.1. și 56.2. cu standardele europene și internaționale selectate și cu cadrul legislativ sau de reglementare național;

56.4.sistemul de management al securității cibernetice, instituit potrivit pct. 68.

57. Toate entitățile cu impact ridicat aplică controalele minime de securitate cibernetică prevăzute la pct. 56.1. în cadrul perimetrului cu impact ridicat; toate entitățile cu impact critic aplică controalele avansate de securitate cibernetică prevăzute la pct. 56.2. în cadrul perimetrului cu impact critic.

58. În termen de 7 luni de la aprobarea raportului de evaluare a riscurilor de securitate cibernetică la nivel național prevăzut la pct. 43.1, OST, cu asistența ENTSO-E, elaborează și prezintă ANRE, spre aprobare, o propunere privind controalele minime și controalele avansate de securitate cibernetică, inclusiv controalele minime și avansate în lanțul de aprovizionare prevăzute la pct. 70-71.

Secțiunea 2
Controalele minime și controalele avansate de securitate cibernetică

59. Controalele minime și controalele avansate de securitate cibernetică pot fi verificate:

59.1. prin participarea la sistemul național de verificare, potrivit pct. 47; sau

59.2. prin audituri de securitate efectuate de terți independenți, potrivit cerințelor prevăzute la pct. 48.1. – 48.5..

60. Controalele minime de securitate cibernetică includ controale destinate protejării informațiilor schimbate potrivit pct. 123.

61. La 3 ani de la aprobarea inițială și ori de câte ori este necesar, în special pe baza rapoartelor de evaluare a riscurilor ulterioare prevăzute la pct. 43.1, OST propune ANRE o modificare a controalelor minime și avansate de securitate cibernetică și, după caz, a matricei de corespondență prevăzute la pct. 75.

62. În termen de 12 luni de la aprobarea controalelor minime și a controalelor avansate de securitate cibernetică potrivit pct. 16.3 și 21, precum și după fiecare actualizare a acestora, entitățile identificate ca fiind cu impact ridicat și cu impact critic potrivit pct. 44 aplică, în timpul elaborării planului de atenuare a riscurilor la nivel de entitate prevăzut la pct. 52, controalele minime de securitate cibernetică în perimetrul cu impact ridicat și controalele avansate de securitate cibernetică în perimetrul cu impact critic.

Secțiunea 3
Derogări de la controalele de securitate cibernetică și verificarea cadrului comun de securitate cibernetică

63. Entitățile prevăzute la pct. 2 pot solicita ANRE acordarea unei derogări de la obligația de a aplica controalele minime și controalele avansate de securitate cibernetică

prevăzute la pct. 62 ANRE poate acorda o astfel de derogare pe unul dintre următoarele temeiuri:

63.1. în circumstanțe excepționale, atunci când entitatea demonstrează că implementarea controalelor de securitate cibernetică corespunzătoare presupune costuri care depășesc semnificativ beneficiile;

63.2. atunci când entitatea prezintă un plan de tratare a riscurilor la nivel de entitate care atenuează riscurile de securitate cibernetică prin controale alternative la un nivel acceptabil, în conformitate cu criteriile de acceptare a riscurilor prevăzute la pct. 50.2.

64. În termen de 3 luni de la primirea cererii prevăzute la pct. 62, ANRE decide dacă acordă derogarea. Derogările se acordă pentru o perioadă de maximum 3 ani, cu posibilitatea reînnoirii.

65. Informațiile agregate și anonimizate privind derogările acordate se includ într-un raport anual al ANRE privind aplicarea prezentului Cod. OST actualizează lista aferentă, atunci când este necesar.

66. În termen de cel mult 24 de luni de la adoptarea controalelor prevăzute la pct. 56.1. – 56.3. și de la instituirea sistemului de management al securității cibernetice prevăzut la pct. 56.4., fiecare entitate cu impact critic identificată potrivit pct. 44 este în măsură să demonstreze, la solicitarea ANRE, conformitatea cu sistemul de management al securității cibernetice și cu controalele minime sau controalele avansate de securitate cibernetică, prin efectuarea unor audituri de securitate de către terți independenți, în conformitate cu cerințele prevăzute la pct. 48.1. – 48.5., sau prin participarea la sistemul național de verificare prevăzut la pct. 47.

67. Verificarea conformității unei entități cu impact critic acoperă toate activele incluse în perimetrul cu impact critic al acesteia și se repetă periodic, cel târziu la 36 de luni de la finalizarea primei verificări și, ulterior, o dată la fiecare 3 ani. Fiecare entitate cu impact critic demonstrează respectarea acestor cerințe prin transmiterea către ANRE a rezultatului verificării conformității.

Secțiunea 4
Sistemul de gestionare a securității cibernetice

68. În termen de 24 de luni de la notificarea prevăzută la pct. 45, fiecare entitate cu impact ridicat și fiecare entitate cu impact critic stabilește un sistem de gestionare a securității cibernetice și îl revizuiește ulterior o dată la fiecare 3 ani, pentru a:

68.1. stabili domeniul de aplicare al sistemului, ținând seama de interfețele și dependențele față de alte entități;

68.2. asigura informarea conducerii de nivel superior cu privire la obligațiile legale relevante și contribuția activă a acesteia la implementarea sistemului prin decizii prompte și reacții rapide;

68.3. asigura disponibilitatea resurselor necesare funcționării sistemului;

68.4. institui o politică de securitate cibernetică documentată și comunicată în cadrul entității și către părțile afectate de riscurile de securitate;

68.5. atribui și comunica responsabilitățile pentru rolurile relevante în domeniul securității cibernetice;

68.6. realiza gestionarea riscurilor de securitate cibernetică la nivel de entitate, potrivit pct. 49-52;

68.7. determina și asigura resursele necesare pentru implementarea, menținerea și îmbunătățirea continuă a sistemului;

68.8. determina comunicarea internă și externă relevantă pentru securitatea cibernetică;

68.9. crea, actualiza și controla informațiile documentate referitoare la sistem;

68.10 evalua performanța și eficacitatea sistemului;

68.11. efectua audituri interne la intervale planificate;

68.12. revizui implementarea sistemului la intervale planificate și controla și corecta neconformitățile.

69. Domeniul de aplicare al sistemului de gestionare a securității cibernetice include toate activele din perimetrul cu impact ridicat și din perimetrul cu impact critic ale entităților cu impact ridicat și cu impact critic. ANRE încurajează, fără a impune sau discrimina în favoarea utilizării unui anumit tip de tehnologie, utilizarea standardelor și specificațiilor europene sau internaționale referitoare la sistemele de management și relevante pentru securitatea rețelelor și sistemelor informatice.

Secțiunea 5
Controalele de securitate cibernetică în lanțul de aprovizionare și matricea de corespondență

70. Odată cu propunerea prevăzută la pct. 57, OST, cu asistența ENTSO-E, elaborează o propunere de controale minime și avansate de securitate cibernetică în lanțul de aprovizionare, care acoperă întregul ciclu de viață al produselor, serviciilor și proceselor TIC din perimetrele cu impact ridicat sau cu impact critic.

71. Controalele minime în lanțul de aprovizionare constau în controale pentru entitățile cu impact ridicat și cu impact critic care:

71.1. includ recomandări pentru achiziția de produse, servicii și procese TIC cu referire la specificații de securitate cibernetică, acoperind cel puțin:

71.1.1. verificările prealabile ale personalului furnizorului implicat în lanțul de aprovizionare și cu acces la informații sensibile sau la activele cu impact ridicat/critic ale entității, efectuate în conformitate cu dreptul și procedurile naționale, inclusiv cu Legea nr. 195/2024 privind protecția datelor cu caracter personal, exclusiv în scopul evaluării riscului de securitate, proporțional cu cerințele comerciale, cu clasificarea informațiilor accesate și cu riscurile percepute, și care pot fi efectuate de entitate, de o societate externă de screening sau prin autorizație administrativă;

71.1.2. procesele de proiectare, dezvoltare și producție securizate și controlate, inclusiv proiectarea rețelelor și sistemelor informatice în care dispozitivele nu sunt considerate de încredere nici în interiorul unui perimetru securizat, cu verificarea tuturor cererilor și aplicarea principiului privilegiului minim;

71.1.3. accesul furnizorului la activele entității;

71.1.4. obligațiile contractuale ale furnizorului privind protejarea și restricționarea accesului la informațiile sensibile ale entității;

71.1.5. transpunerea specificațiilor de achiziție de securitate cibernetică către subcontractanții furnizorului;

71.1.6. trasabilitatea aplicării specificațiilor de securitate cibernetică de la dezvoltare până la livrare;

71.1.7. suportul pentru actualizări de securitate pe întreaga durată de viață a produsului, serviciului sau procesului TIC;

71.1.8. dreptul de audit al securității cibernetice în procesele de proiectare, dezvoltare și producție ale furnizorului;

71.1.9. evaluarea profilului de risc al furnizorului;

71.2. impun entităților să țină cont de recomandările de achiziție menționate la subpct. 71.1 la încheierea contractelor cu furnizorii, partenerii de colaborare și alte părți din lanțul de aprovizionare, inclusiv pentru livrările obișnuite de produse TIC, servicii TIC și procese TIC, precum și pentru situații neprevăzute, inclusiv rezilierea și tranziția contractelor în caz de neglijență a partenerului contractual;

71.3. impun entităților să țină cont, dacă există, de rezultatele evaluărilor coordonate de securitate ale lanțurilor de aprovizionare critice realizate la nivel european;

71.4. includ criterii pentru selectarea și contractarea furnizorilor care pot îndeplini specificațiile de securitate cibernetică și care dispun de un nivel de securitate cibernetică adecvat riscurilor produsului, serviciului sau procesului TIC furnizat;

71.5. includ criterii pentru diversificarea surselor de aprovizionare și reducerea riscului de dependență de un singur furnizor;

71.6. includ criterii pentru monitorizarea, revizuirea sau auditarea periodică a specificațiilor de securitate cibernetică pentru procesele operaționale interne ale furnizorului, pe întregul ciclu de viață al produsului, serviciului sau procesului TIC.

72. Pentru specificațiile de securitate cibernetică prevăzute la pct. 71.1, entitățile cu impact ridicat sau cu impact critic utilizează principiile aplicabile în materia achizițiilor publice potrivit Legii nr. 325/2025 privind achizițiile publice sau își definesc propriile specificații pe baza rezultatelor evaluării riscurilor de securitate cibernetică la nivel de entitate.

73. Controalele avansate în lanțul de aprovizionare includ, pentru entitățile cu impact critic, controale pentru a verifica, în cadrul achiziției, că produsele, serviciile și procesele TIC care vor fi utilizate ca active cu impact critic satisfac specificațiile de securitate cibernetică, prin intermediul unui sistem european de certificare a securității cibernetice sau prin activități de verificare selectate și organizate de entitate. Profunzimea și acoperirea acestor activități trebuie să fie suficiente pentru a asigura că produsul, serviciul sau procesul TIC poate fi utilizat pentru atenuarea riscurilor identificate în evaluarea la nivel de entitate, iar entitatea documentează măsurile luate.

74. Controalele minime și avansate din lanțul de aprovizionare se aplică proceselor de achiziție ale entităților cu impact ridicat și cu impact critic care încep la 6 luni de la adoptarea sau actualizarea controalelor prevăzute la pct. 70-71.

75. Odată cu propunerea prevăzută la pct. 58, OST, cu asistența ENTSO-E, elaborează o propunere de matrice care corelează controalele prevăzute la pct. 56.1. și 56.2. cu standardele europene și internaționale selectate, precum și cu specificațiile tehnice relevante („matricea de corespondență”), documentând echivalența controalelor cu standardele respective. Propunerea de matrice se prezintă ANRE spre aprobare odată cu propunerea prevăzută la pct. 58, potrivit pct. 16.3 și 21. ANRE poate furniza, pentru integrare în matrice, o corelare a acestor controale cu cadrul legislativ sau de reglementare național, inclusiv standardele naționale relevante.

CAPITOLUL IV

RECOMANDĂRI PRIVIND ACHIZIȚIILE ÎN DOMENIUL SECURITĂȚII CIBERNETICE

76. OST, cu asistența ENTSO-E, elaborează, printr-un program de lucru actualizat la fiecare actualizare a raportului de evaluare a riscurilor de securitate cibernetică la nivel național, seturi de recomandări neobligatorii privind achizițiile în domeniul securității cibernetice, pe care entitățile cu impact ridicat și cu impact critic le pot utiliza ca bază pentru achiziția de produse, servicii și procese TIC în perimetrele cu impact ridicat și cu impact critic. Programul de lucru include:

76.1. o descriere și clasificare a tipurilor de produse, servicii și procese TIC utilizate de entitățile cu impact ridicat și cu impact critic;

76.2. o listă a tipurilor de produse, servicii și procese TIC pentru care se elaborează seturi de recomandări, pe baza raportului de evaluare a riscurilor de securitate cibernetică și a priorităților entităților cu impact ridicat și cu impact critic.

77. OST se asigură că seturile de recomandări privind achizițiile în domeniul securității cibernetice:

77.1. acoperă cel puțin specificațiile prevăzute la pct. 71.1;

77.2. respectă principiile achizițiilor publice potrivit Legii nr. 325/2025 privind achizițiile publice; și

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

78. Recomandările neobligatorii privind achizițiile în domeniul securității cibernetice pot include orientări sectoriale privind utilizarea sistemelor europene de certificare a securității cibernetice, ori de câte ori este disponibil un asemenea sistem pentru un tip de produs, serviciu sau proces TIC utilizat de entitățile cu impact critic. OST, cu asistența ENTSO-E, cooperează cu ENISA pentru elaborarea acestor orientări, atunci și în măsura în care există un mecanism de cooperare aplicabil Republicii Moldova.

CAPITOLUL V
FLUXURI INFORMAȚIONALE, ATACURI CIBERNETICE ȘI GESTIONAREA CRIZELOR

Secțiunea 1
Reguli privind schimbul de informații

79. În cazul în care ANRE primește informații referitoare la un atac cibernetic raportabil, aceasta:

79.1. evaluează nivelul de confidențialitate al informațiilor respective și informează entitatea cu privire la rezultatul evaluării, fără întârzieri nejustificate și în cel mult 24 de ore de la primirea informațiilor;

79.2. este responsabilă de eliminarea secretelor comerciale și de anonimizarea informațiilor, în conformitate cu normele naționale relevante;

79.3. diseminează informațiile privind atacul cibernetic, după anonimizare și eliminarea secretelor comerciale, entităților cu impact critic și entităților cu impact ridicat din Republica Moldova, fără întârzieri nejustificate și în cel mult 24 de ore de la primirea informațiilor, precum și informații actualizate periodic care să permită acestora organizarea eficientă a apărării;

79.4. poate solicita entității raportoare cu impact ridicat sau cu impact critic să disemineze în continuare, în mod securizat, informațiile privind atacul cibernetic raportabil către alte entități care pot fi afectate, în scopul creării unei conștientizări situaționale la nivelul sectorului electroenergetic;

79.5. atunci și în măsura în care există un canal securizat de schimb cu Agenția Uniunii Europene pentru Securitate Cibernetică *(în continuare - ENISA)* potrivit unui acord încheiat conform pct. 101, transmite ENISA un raport de sinteză privind informațiile referitoare la atacul cibernetic, după anonimizare și eliminarea secretelor comerciale.

80. În cazul în care ia cunoștință de o vulnerabilitate necorectată exploatată activ, ASC:

80.1. comunică ENISA, atunci și în măsura în care există un canal securizat de schimb de informații potrivit unui acord încheiat conform pct. 101;

80.2. sprijină entitatea vizată să obțină din partea producătorului sau furnizorului o gestionare eficientă, coordonată și rapidă a vulnerabilității necorectate exploatate activ sau măsuri de atenuare eficiente și eficace;

80.3. face schimb de informații disponibile cu furnizorul și solicită producătorului sau furnizorului, atunci când este posibil, să identifice echipele CSIRT din alte părți contractante ale Comunității Energetice și/sau state membre ale Uniunii Europene afectate care trebuie informate;

80.4. comunică informațiile disponibile echipelor CSIRT identificate potrivit 80.3., pe baza principiului necesității de a cunoaște;

80.5. comunică, atunci când există, strategiile și măsurile de atenuare pentru vulnerabilitatea necorectată exploatată activ raportată.

81. În cazul în care ia cunoștință de o vulnerabilitate necorectată exploatată activ, ANRE comunică, atunci când există, strategiile și măsurile de atenuare, în coordonare cu ASC, și transmite informațiile ASC.

82. În cazul în care ia cunoștință de o vulnerabilitate necorectată fără dovezi privind exploatarea activă a acesteia, ANRE se coordonează, fără întârzieri nejustificate, cu ASC în scopul divulgării coordonate a vulnerabilităților.

83. În cazul în care primește informații privind amenințări cibernetice de la una sau mai multe entități cu impact ridicat sau cu impact critic potrivit prezentului Cod, ASC disemnează informațiile respective sau orice alte informații relevante pentru prevenirea, detectarea, răspunsul sau atenuarea riscului asociat entităților cu impact critic și entităților cu impact ridicat din Republica Moldova, fără întârzieri nejustificate și în cel mult 4 ore de la primirea informațiilor. În cazul în care ANRE ia cunoștință de asemenea informații, le transmite ASC.

84. OST, cu asistența ENTSO-E, elaborează metodologia scalei de clasificare a atacurilor cibernetice, supusă aprobării ANRE potrivit pct. 16.5, odată cu propunerea prevăzută la pct. 58. Metodologia prevede clasificarea gravității unui atac cibernetic pe o scală de 5 niveluri, dintre care cele mai înalte două sunt „ridicat” și „critic”, pe baza evaluării:

84.1. impactului potențial, având în vedere activele și perimetrele expuse, determinate potrivit pct. 51.3.4.; și

84.2. gravității atacului cibernetic.

Secțiunea 2

Rolul entităților cu impact ridicat și cu impact critic în privința schimbului de informații

85. Fiecare entitate cu impact ridicat și fiecare entitate cu impact critic:

85.1. stabilește, pentru toate activele din perimetrul său de securitate cibernetică determinat potrivit pct. 51.3.4, cel puțin capacitățile unui centru de operațiuni de securitate cibernetică (CSOC), pentru:

85.1.1. a asigura că rețelele, sistemele informatice și aplicațiile relevante furnizează jurnale de securitate pentru monitorizarea securității, care permit detectarea anomaliilor și colectarea informațiilor privind atacurile cibernetice;

85.1.2. efectuarea monitorizării securității, inclusiv detectarea intruziunilor și evaluarea vulnerabilităților rețelelor și sistemelor informatice;

85.1.3. analizarea și, după caz, întreprinderea tuturor măsurilor necesare, în limita responsabilităților și competențelor sale, pentru protejarea entității;

85.1.4. participarea la colectarea și schimbul de informații prevăzute în prezenta secțiune;

85.2. are dreptul să achiziționeze, integral sau parțial, capacitățile prevăzute la subpct. 85.1 prin intermediul furnizorilor de servicii de securitate gestionate (MSSP), rămânând responsabilă pentru activitatea acestora și supraveghind serviciile prestate;

85.3. desemnează un punct unic de contact la nivelul entității în scopul schimbului de informații.

86. Fiecare entitate cu impact ridicat și fiecare entitate cu impact critic face schimb de informații relevante referitoare la un atac cibernetic raportabil cu ASC și cu ANRE, fără întârzieri nejustificate și în termen de cel mult 4 ore din momentul în care ia cunoștință că incidentul este raportabil.

87. Informațiile referitoare la un atac cibernetic se consideră raportabile atunci când entitatea afectată evaluează atacul cibernetic ca având un nivel de criticitate cuprins între „ridicat” și „critic”, potrivit metodologiei scalei de clasificare a atacurilor cibernetice prevăzute la pct. 84. Punctul unic de contact desemnat potrivit pct. 85.3 comunică clasificarea incidentului.

88. Notificarea unui incident semnificativ, efectuată de o entitate în temeiul art. 12 din Legea nr. 48/2023, constituie raportarea informațiilor prevăzute la pct. 86, dacă notificarea conține informațiile relevante prevăzute la punctul respectiv. Termenul de 4 ore prevăzut la pct. 86 se aplică, ca normă specială, atacurilor cibernetice raportabile în sensul prezentului Cod, iar notificarea efectuată în acest termen satisface și obligația de notificare prevăzută la art. 12 din Legea nr. 48/2023, fără a fi necesară o notificare separată în termenul general prevăzut de legea respectivă.

89. În cazul în care o entitate cu impact critic sau o entitate cu impact ridicat notifică ASC informații relevante privind vulnerabilități necorectate exploatate activ, aceasta poate transmite informațiile ANRE. Având în vedere nivelul de sensibilitate al informațiilor notificate, ASC poate reține informațiile sau poate întârzia transmiterea acestora din motive justificate legate de securitatea cibernetică.

90. Fiecare entitate cu impact critic și fiecare entitate cu impact ridicat furnizează, fără întârzieri nejustificate, ASC orice informații referitoare la o amenințare cibernetică raportabilă care poate avea efecte transfrontaliere. Informațiile referitoare la o amenințare cibernetică se consideră raportabile atunci când este îndeplinită cel puțin una dintre următoarele condiții:

90.1. furnizează informații relevante pentru alte entități cu impact critic și entități cu impact ridicat în scopul prevenirii, detectării, răspunsului sau atenuării impactului riscului;

90.2. tehnicile, tacticile și procedurile identificate în contextul unui atac conduc la informații precum adrese URL compromise, adrese IP compromise, valori hash sau orice alte atribute utile pentru contextualizarea și corelarea atacului;

90.3. amenințarea cibernetică poate fi evaluată și contextualizată suplimentar pe baza informațiilor furnizate de prestatori de servicii sau de terți care nu intră sub incidența prezentului Cod.

91. La transmiterea informațiilor potrivit prezentei secțiuni, fiecare entitate cu impact critic și fiecare entitate cu impact ridicat precizează:

91.1 că informațiile sunt transmise în temeiul prezentului Cod;

91.2 dacă informațiile se referă la un atac cibernetic raportabil, la vulnerabilități necorectate exploatate activ care nu sunt cunoscute publicului sau la o amenințare cibernetică raportabilă;

91.3 în cazul unui atac cibernetic raportabil, nivelul atacului cibernetic stabilit potrivit metodologiei scalei de clasificare, precum și informațiile care au condus la această clasificare, inclusiv cel puțin nivelul de criticitate al atacului.

92. Fiecare entitate cu impact critic și fiecare entitate cu impact ridicat raportează ANRE sau ASC, identificând în mod clar informațiile specifice care urmează să fie comunicate exclusiv uneia dintre acestea, în cazurile în care schimbul de informații ar putea constitui sursa unui atac cibernetic. Fiecare entitate are dreptul să furnizeze ASC o versiune neconfidențială a informațiilor.

Secțiunea 3
Detectarea atacurilor cibernetice și gestionarea informațiilor aferente

93. Entitățile cu impact critic și entitățile cu impact ridicat dezvoltă capacitățile necesare pentru gestionarea atacurilor cibernetice detectate, cu sprijinul necesar din partea ANRE, ASC și, dacă este cazul, al ENTSO-E, și implementează procese eficiente pentru identificarea, clasificarea și răspunsul la atacurile cibernetice care afectează sau pot afecta fluxurile transfrontaliere de energie electrică, în scopul reducerii la minimum a impactului acestora.

94. Entitățile cu impact critic și entitățile cu impact ridicat:

94.1. 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 ASC sau de la ANRE;

94.2. notifică ANRE și ASC o listă a punctelor unice de contact pentru securitate cibernetică la nivel de entitate;

94.3. instituie proceduri de gestionare a atacurilor cibernetice, inclusiv roluri și responsabilități, sarcini și măsuri de răspuns, pe baza evoluției observabile a atacului cibernetic în cadrul perimetrelor cu impact critic și cu impact ridicat;

94.4. 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 poate fi realizat în cadrul exercițiilor periodice prevăzute la pct. 104-108, orice activitate reală de răspuns la un atac cibernetic cu o consecință clasificată cel puțin la nivelul 2 al scalei prevăzute la pct. 84 și a cărei cauză principală este identificată ca fiind legată de securitatea cibernetică poate constitui testul anual al planului de răspuns.

95. Guvernul, la propunerea ANRE, poate decide delegarea sarcinilor prevăzute la pct. 92 centrelor de coordonare regionale.

Secțiunea 4
Gestionarea crizelor de securitate cibernetică și planurile de gestionare și răspuns la crize

96. Determinarea legăturii dintre o criză de energie electrică și un atac cibernetic se realizează în cadrul mecanismului prevăzut la art. 36 alin. (3) din Legea nr. 164/2025 și Hotărârea Guvernului nr. 820/2024:

96.1. criza de energie electrică se constată de OST și se confirmă de Comisia pentru Situații Excepționale;

96.2. determinarea legăturii cu un atac cibernetic se realizează de ANRE și ASC, împreună cu Ministerul Energiei, în cadrul aceluiași mecanism.

97. Atunci când o criză de energie electrică legată de un atac cibernetic are impact asupra mai multor părți contractante ale Comunității Energetice și/sau state membre ale Uniunii Europene, ANRE și ASC cooperează cu autoritățile competente din părțile afectate, în măsura în care există un cadru de cooperare aplicabil, pentru:

97.1. coordonarea obținerii eficiente și diseminării ulterioare a tuturor informațiilor relevante de securitate cibernetică către entitățile implicate în procesul de gestionare a crizei;

97.2. organizarea comunicării între toate entitățile afectate de criză și autoritățile competente;

97.3. furnizarea, în cooperare cu echipele CSIRT competente, a expertizei necesare, inclusiv consiliere operațională privind implementarea unor posibile măsuri de atenuare;

97.4. notificarea și furnizarea de actualizări periodice privind situația incidentului Secretariatului Comunității Energetice, atunci când este cazul, cu respectarea principiilor de protecție prevăzute la pct. 124;

97.5. solicitarea de consultanță din partea autorităților, agențiilor sau entităților relevante care ar putea contribui la atenuarea crizei de energie electrică.

98. În cazul în care atacul cibernetic se califică sau se estimează că se va califica drept criză în domeniul securității cibernetice de mare amploare, în sensul art. 9 alin. (3) lit. f) din Legea nr. 48/2023, ASC informează imediat autoritățile naționale relevante, precum și, dacă este cazul, Secretariatul Comunității Energetice.

99. Entitățile cu impact critic și entitățile cu impact ridicat dezvoltă și mențin capacități, orientări interne, planuri de pregătire și personal pentru participarea la detectarea și atenuarea crizelor cu efect transfrontalier. Entitatea cu impact critic sau entitatea cu impact ridicat afectată de o criză simultană a energiei electrice investighează cauza principală a acesteia în cooperare cu ANRE, pentru a determina măsura în care criza este legată de un atac cibernetic. Guvernul, la propunerea ANRE, poate decide delegarea sarcinilor prevăzute la prezentul punct centrelor de coordonare regionale.

100. ANRE elaborează un plan național de gestionare și răspuns la crizele de securitate cibernetică pentru fluxurile transfrontaliere de energie electrică, ținând cont de Planul de acțiuni pentru situații excepționale în sectorul electroenergetic, aprobat prin Hotărârea Guvernului nr. 820/2024, și se coordonează cu entitățile cu impact critic și cu impact ridicat și cu Ministerul Energiei. Planul se elaborează în termen de 12 luni de la intrarea în vigoare a prezentului Cod și se actualizează cel puțin o dată la 3 ani și ori de câte ori este necesar.

100.1. Planul național prevăzut la pct. 100 este în concordanță cu planul național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice, elaborat de ASC potrivit art. 9 alin. (2) din Legea nr. 48/2023. Planul elaborat potrivit art. 9 alin. (2) din Legea nr. 48/2023 constituie plan național în sensul pct. 100, dacă include dispoziții privind gestionarea crizelor și răspunsul la acestea pentru fluxurile transfrontaliere de energie electrică.

100.2. Guvernul, la propunerea ANRE, poate decide delegarea sarcinilor prevăzute la pct. 99 centrelor de coordonare regionale.

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

100.3.1. au proceduri compatibile de gestionare a incidentelor cu efect transfrontalier, incluse în mod formal în planurile lor de gestionare a crizelor;

100.3.2. fac parte din activitățile generale de gestionare a crizelor.

100.4. În termen de 12 luni de la notificarea entităților cu impact ridicat și cu impact critic potrivit pct. 45 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, inclus în planurile generale de gestionare a crizelor. Planul include cel puțin:

100.4.1. regulile privind declararea crizei, potrivit Planului de acțiuni pentru situații excepționale în sectorul electroenergetic, aprobat prin Hotărârea Guvernului nr. 820/2024;

100.4.2. roluri și responsabilități clare pentru gestionarea crizelor, inclusiv rolul altor entități relevante cu impact critic și cu impact ridicat;

100.4.3. informații de contact actualizate, precum și reguli privind comunicarea și schimbul de informații în timpul unei situații de criză, inclusiv legătura cu ASC.

100.5. Măsurile de gestionare a crizelor adoptate de o entitate potrivit art. 11 din Legea nr. 48/2023 constituie plan de gestionare a crizelor la nivel de entitate în sensul pct. 100.4, dacă îndeplinesc cerințele prevăzute la punctul respectiv.

100.6. Planurile de gestionare a crizelor prevăzute la pct. 100.4 sunt testate în cadrul exercițiilor de securitate cibernetică prevăzute la pct. 104-108.

100.7. 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 cu impact ridicat, care includ:

100.7.1. procesele care depind de disponibilitatea, integritatea și fiabilitatea serviciilor informatice;

100.7.2. toate locațiile pentru asigurarea continuității activității, inclusiv locațiile pentru echipamente hardware și software;

100.7.3. toate rolurile și responsabilitățile interne asociate proceselor de continuitate a activității. Entitățile actualizează planurile de gestionare a crizelor la nivel de entitate cel puțin o dată la trei ani și ori de câte ori este necesar.

100.8. 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 cu impact ridicat, care includ:

100.8.1. procesele care depind de disponibilitatea, integritatea și fiabilitatea serviciilor informatice;

100.8.2. toate locațiile pentru asigurarea continuității activității, inclusiv locațiile pentru echipamente hardware și software;

100.8.3. toate rolurile și responsabilitățile interne asociate proceselor de continuitate a activității.

Entitățile actualizează planurile de gestionare a crizelor la nivel de entitate cel puțin o dată la trei ani și ori de câte ori este necesar.

100.9. Entitățile cu impact critic și entitățile cu impact ridicat testează planurile de continuitate a activității cel puțin o dată la trei ani sau după modificări majore ale unui proces cu impact critic, documentând rezultatele. Entitățile pot include testarea planurilor de continuitate a activității în exercițiile de securitate cibernetică și le actualizează ori de câte ori este necesar și cel puțin o dată la trei ani, ținând cont de rezultatele testării.

100.10.În cazul în care un test identifică deficiențe în planul de continuitate a activității, entitatea corectează deficiențele respective în termen de 180 de zile calendaristice de la testare și efectuează un nou test pentru a demonstra eficacitatea măsurilor corective. În cazul în care entitatea nu poate corecta deficiențele în acest termen, include motivele în raportul transmis ANRE potrivit pct. 54.

101. Autoritățile competente cooperează cu ENISA, inclusiv prin încheierea de acorduri, pentru dezvoltarea unor capacități de alertă timpurie de securitate cibernetică pentru sectorul electroenergetic *(în continuare - ECEAC)*, cu respectarea competențelor instituționale ale ENISA și ținând seama de faptul că o asemenea cooperare depinde de disponibilitatea proprie a ENISA de a o extinde către o parte contractantă a Comunității Energetice. Obligația ANRE și a ASC se limitează, în acest caz, la depunerea diligențelor necesare pentru inițierea și menținerea cooperării.

102. Atunci și în măsura în care ECEAC este accesibil Republicii Moldova, ASC, ANRE și entitățile prevăzute la pct. 2 pot transmite, în mod voluntar, prin intermediul acestuia, informații relevante pentru identificarea condițiilor de risc cibernetic aferente fluxurilor transfrontaliere de energie electrică, cu respectarea pct. 115-128.

103. ASC diseminează fără întârziere entităților vizate informațiile primite prin mecanismul prevăzut la pct. 100-101.

CAPITOLUL VI
CADRUL EXERCIȚIILOR DE SECURITATE CIBERNETICĂ ÎN SECTORUL ELECTROENERGETIC

Secțiunea 1
Exerciții de securitate cibernetică la nivel de entitate și la nivel național

104. Până la 31 decembrie a anului următor notificării entităților cu impact critic potrivit pct. 45 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 de atacuri cibernetice care afectează direct sau indirect fluxurile transfrontaliere de energie electrică și care sunt legate de riscurile identificate în cadrul evaluărilor riscurilor de securitate cibernetică la nivel național și la nivel de entitate, efectuate potrivit pct. 43 și pct. 49-52.

105. Prin derogare de la pct. 104, Ministerul Energiei, după consultarea ANRE și a ASC, poate decide organizarea unui exercițiu de securitate cibernetică la nivel național în locul exercițiului de securitate cibernetică la nivel de entitate. În acest caz, Ministerul Energiei informează:

105.1. toate entitățile cu impact critic din Republica Moldova, ANRE și ASC, cel târziu până la data de 30 iunie a anului care precedă exercițiul de securitate cibernetică la nivel de entitate;

105.2. fiecare entitate care participă la exercițiul de securitate cibernetică la nivel național, cel târziu cu șase luni înainte de desfășurarea exercițiului.

106. Ministerul Energiei, cu sprijinul tehnic al ASC, organizează exercițiul de securitate cibernetică la nivel național prevăzut la pct. 104, în mod independent sau în cadrul unui alt exercițiu de securitate cibernetică desfășurat în Republica Moldova, putând amâna cu un an exercițiul de securitate cibernetică la nivel național prevăzut la pct. 104, pentru a permite gruparea acestor exerciții.

107. Exercițiile de securitate cibernetică la nivel de entitate și la nivel național sunt compatibile cu cadrul național de gestionare a crizelor de securitate cibernetică, prevăzut la art. 9 din Legea nr. 48/2023.

108. OST, cu asistența ENTSO-E, pune la dispoziție un model de scenariu de exercițiu pentru efectuarea exercițiilor de securitate cibernetică la nivel de entitate și la nivel național, ținând seama de rezultatele celei mai recente evaluări a riscurilor de securitate cibernetică la nivel de entitate și la nivel național și incluzând criterii-cheie de succes.

Secțiunea 2

Exerciții regionale și interregionale de securitate cibernetică

109. Atunci și în măsura în care ENTSO-E organizează un exercițiu regional sau interregional de securitate cibernetică pentru regiunea de operare a sistemelor electroenergetice din care face parte OST, entitățile cu impact critic din Republica Moldova participă la exercițiul respectiv.

110. ENTSO-E, atunci când organizează un asemenea exercițiu, informează entitățile cu impact critic participante cu cel puțin șase luni înainte de desfășurarea exercițiului.

Secțiunea 3

Rezultatele exercițiilor de securitate cibernetică

111. La cererea unei entități cu impact critic, furnizorii critici de servicii participă la exercițiile de securitate cibernetică prevăzute la pct. 104, 105 și 109, atunci când aceștia furnizează servicii entității cu impact critic în domeniul corespunzător domeniului de aplicare al exercițiului relevant.

112. Organizatorii exercițiilor de securitate cibernetică prevăzute la pct. 104, 105 și 109 analizează și finalizează exercițiul relevant printr-un raport care sintetizează lecțiile învățate și care este transmis tuturor participanților. Raportul include:

112.1. scenariile exercițiului, rapoartele reuniunilor, pozițiile principale, rezultatele obținute și lecțiile învățate la orice nivel al lanțului valoric al energiei electrice;

112.2. măsura în care au fost îndeplinite criteriile-cheie de succes;

112.3. o listă de recomandări pentru entitățile participante, pentru corectarea, adaptarea sau modificarea proceselor și procedurilor de criză de securitate cibernetică, a modelelor de guvernanță asociate și a angajamentelor contractuale existente cu furnizorii critici de servicii.

113. Organizatorii exercițiilor partajează rezultatul exercițiului relevant cu ASC și, după caz, cu alte autorități sau entități prevăzute la pct. 3. Organizatorii comunică fiecărei

entități participante informațiile prevăzute la pct. 112.1. și 112.2., lista recomandărilor prevăzută la 112.3. se comunică exclusiv entităților cărora le sunt adresate recomandările.

114. Organizatorii exercițiilor urmăresc periodic, împreună cu entitățile participante, implementarea recomandărilor formulate potrivit pct. 112.3.

CAPITOLUL VII
PROTECȚIA INFORMAȚIILOR

Secțiunea 1
Principii pentru protecția informațiilor schimbate

115. Entitățile prevăzute la pct. 2 se asigură că informațiile furnizate, primite, schimbate sau transmise în temeiul prezentului Cod sunt accesibile numai pe baza principiului necesității de a cunoaște și cu respectarea normelor naționale privind securitatea informațiilor.

116. Entitățile prevăzute la pct. 2 se asigură că informațiile furnizate, primite, schimbate sau transmise în temeiul prezentului Cod sunt gestionate și urmărite pe întregul ciclu de viață al acestora și că pot fi făcute publice la finalul ciclului de viață numai după anonimizare.

117. Entitățile prevăzute la pct. 2 se asigură că sunt instituite toate măsurile de protecție necesare de natură organizațională și tehnică pentru protejarea confidențialității, integrității, disponibilității și nerepudierii informațiilor furnizate, primite, schimbate sau transmise în temeiul prezentului Cod, indiferent de mijloacele utilizate. Măsurile de protecție:

117.1. sunt proporționale;

117.2. iau în considerare riscurile de securitate cibernetică legate de amenințările cunoscute din trecut și cele emergente la care pot fi supuse astfel de informații;

117.3. în măsura posibilului, se bazează pe standarde și bune practici naționale, europene sau internaționale;

117.4. sunt documentate.

118. Entitățile prevăzute la pct. 2 se asigură că orice persoană căreia îi este acordat acces la informațiile furnizate, primite, schimbate sau transmise în temeiul prezentului Cod este informată cu privire la normele de securitate aplicabile la nivel de entitate și la măsurile și procedurile relevante pentru protecția informațiilor, și recunoaște responsabilitatea de a proteja informațiile potrivit instrucțiunilor primite.

119. Entitățile prevăzute la pct. 2 se asigură că accesul la informațiile furnizate, primite, schimbate sau transmise în temeiul prezentului Cod este limitat la persoanele:

119.1. autorizate să acceseze informațiile respective pe baza funcțiilor exercitate și numai în limita executării sarcinilor atribuite;

119.2. pentru care entitatea a fost în măsură să evalueze principiile etice și de integritate și pentru care nu există dovezi ale unui rezultat negativ în urma unei verificări a antecedentelor, efectuată în conformitate cu Legea nr. 195/2024 privind protecția datelor cu caracter personal, destinată evaluării fiabilității persoanei.

120. Entitățile prevăzute la pct. 2 obțin acordul scris al persoanei fizice sau juridice care a creat sau a furnizat inițial informațiile, înainte de a furniza aceste informații unei părți terțe care nu intră în domeniul de aplicare al prezentului Cod.

121. O entitate prevăzută la pct. 2 poate considera că informațiile trebuie transmise fără respectarea cerințelor prevăzute la pct. 115 și 119, pentru prevenirea unei crize simultane

a energiei electrice a cărei cauză principală este legată de securitatea cibernetică sau a unei crize transfrontaliere în alt sector. În acest caz, entitatea:

121.1. se consultă cu ANRE și este autorizată de aceasta să transmită informațiile respective;

121.2. anonimizează informațiile fără a elimina elementele necesare pentru informarea publicului cu privire la un risc iminent și grav pentru fluxurile transfrontaliere de energie electrică și la posibilele măsuri de atenuare;

121.3. protejează identitatea inițiatorului informațiilor și a entităților care au prelucrat astfel de informații.

122. Prin derogare de la pct. 119, ANRE poate furniza informațiile furnizate, primite, schimbate sau transmise în temeiul prezentului Cod unei părți terțe care nu este prevăzută la pct. 2, fără acordul scris prealabil al inițiatorului informațiilor, informându-l în cel mai scurt timp posibil, cu condiția să se asigure în mod rezonabil că partea terță cunoaște normele de securitate aplicabile și poate proteja informațiile primite în conformitate cu pct. 114-118, cu anonimizarea informațiilor și protejarea identității inițiatorului.

123. Pct. 119-121 nu se aplică entităților care nu sunt prevăzute la pct. 2 și care primesc informații în temeiul pct. 119; în acest caz se aplică pct. 120 sau ANRE poate furniza entității respective dispoziții scrise aplicabile.

Secțiunea 2
Confidențialitatea informațiilor

124. Orice informație furnizată, primită, schimbată sau transmisă în temeiul prezentului Cod este supusă condițiilor privind secretul profesional prevăzute la pct. 124-128 și cerințelor prevăzute la art. 104 din Legea nr. 164/2025, și este protejată ținând cont de nivelul de confidențialitate stabilit de inițiatorul informațiilor.

125. Obligația de păstrare a secretului profesional se aplică entităților prevăzute la pct. 2.

126. ANRE, ASC, Ministerul Energiei și Comisia pentru Situații Excepționale fac schimb de toate informațiile necesare pentru îndeplinirea atribuțiilor care le revin potrivit prezentului Cod.

127. Informațiile primite de orice entitate sau autoritate care intră sub incidența prezentului Cod, în exercitarea atribuțiilor sale, nu pot fi divulgate unei alte entități sau autorități, fără a aduce atingere cazurilor prevăzute de legislația națională sau altor dispoziții ale prezentului Cod. Fără a aduce atingere legislației naționale, o autoritate, entitate sau persoană fizică care primește informații în temeiul prezentului Cod nu le poate utiliza în alt scop decât pentru îndeplinirea atribuțiilor care îi revin în temeiul acestuia.

128. Informațiile confidențiale se transmit Secretariatului Comunității Energetice și altor autorități relevante ale Comunității Energetice numai atunci când un asemenea schimb este necesar pentru aplicarea prezentului Cod și există un cadru de cooperare aplicabil. Informațiile transmise se limitează la ceea ce este necesar și proporțional cu scopul schimbului respectiv, cu păstrarea confidențialității acestora și protejarea securității și intereselor comerciale ale entităților cu impact critic sau cu impact ridicat.

NOTA DE FUNDAMENTARE

la proiectul hotărârii Consiliului de administrație al ANRE cu privire la aprobarea Codului de rețea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică

1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ

Proiectul hotărârii Consiliului de administrație al ANRE cu privire la aprobarea Codului de rețea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică a fost elaborat de Agenția Națională pentru Reglementare în Energetică (în continuare Agenția/ANRE), Departamentul energie electrică și regenerabilă, Secția reglementări.

2. Condițiile ce au impus elaborarea proiectului actului normativ

2.1. Temeiul legal sau, după caz, sursa proiectului actului normativ

Temeiul legal pentru elaborarea și aprobarea proiectului hotărârii Consiliului de administrație al Agenției Naționale pentru Reglementare în Energetică îl constituie prevederile art. 9 alin. (3) și art. 36 alin. (2) din Legea nr. 164/2025 cu privire la energia electrică, care stabilesc competențele Agenției în domeniul aprobării actelor normative de reglementare aplicabile sectorului electroenergetic.

Sursa elaborării proiectului o constituie necesitatea asigurării implementării obligațiilor asumate de Republica Moldova în calitate de parte contractantă a Tratatului de instituire a Comunității Energetice și alinierii cadrului normativ național la acquis-ul Comunității Energetice în domeniul securității cibernetice a fluxurilor transfrontaliere de energie electrică.

Proiectul hotărârii are ca obiect aprobarea Codului de rețea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică, elaborat în baza Regulamentului 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, astfel cum a fost modificat ultima dată prin Regulamentul delegat (UE) 2025/1759 al Comisiei din 19 iunie 2025 și rectificat, în versiunea în limba română, prin Rectificarea publicată în JO L din 19 mai 2026.

Precizăm că Regulamentul delegat (UE) 2024/1366 nu a fost, la data prezentei note, preluat în acquis-ul Comunității Energetice și nu există încă o decizie de adaptare și adoptare a acestuia aplicabilă părților contractante (constatare reținută și în Declarația de compatibilitate nr. 31/02-126-12023 din 11 septembrie 2026 a Centrului de Armonizare a Legislației), deși, potrivit Programului de lucru al Comunității Energetice pentru anii 2026-2027, adoptarea acestuia prin decizie a Consiliului ministerial este preconizată în anul 2026.

Totodată, Regulamentul (UE) 2019/943, pe care acesta îl completează, este deja inclus în acquis-ul Comunității Energetice prin Decizia Consiliului ministerial al Comunității Energetice nr. 2022/03/MC-EnC din 15 decembrie 2022. În consecință, proiectul pune în aplicare parțial, în mod unilateral, Regulamentul delegat (UE) 2024/1366, cu termene naționale proprii, calculate de la intrarea în vigoare a Hotărârii, fără a condiționa aplicarea obligațiilor naționale de adoptarea

unei viitoare decizii a Comunității Energetice. Exercițiul de armonizare figurează la acțiunea nr. 27-28 din Anexa A la Capitolul 15 "Energie", Clusterul 4 "Agenda verde și conectivitatea sustenabilă" al Programului Național de Aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029, aprobat prin Hotărârea Guvernului nr. 306/2025.

2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative

Securitatea cibernetică a sistemului electroenergetic a devenit un element esențial pentru asigurarea funcționării sigure și continue a pieței energiei electrice, în special în contextul creșterii interconectării sistemelor electroenergetice și al intensificării schimburilor transfrontaliere de energie electrică.

Totodată, digitalizarea proceselor operaționale, utilizarea sistemelor informatice și de comunicații pentru monitorizarea și controlul infrastructurilor energetice, precum și dependența tot mai mare de servicii și tehnologii digitale generează noi riscuri de securitate cibernetică, care pot afecta disponibilitatea, integritatea și funcționarea sistemului electroenergetic.

Cadrul normativ național relevant include prevederile Legii nr. 164/2025 cu privire la energia electrică, care stabilește atribuțiile Agenției Naționale pentru Reglementare în Energetică în domeniul reglementării sectorului electroenergetic, ale Legii nr. 48/2023 privind securitatea cibernetică, care instituie Agenția pentru Securitate Cibernetică (ASC) drept autoritate competentă națională, echipă de răspuns la incidente de securitate cibernetică (CSIRT) și punct național unic de contact, cu obligații generale de gestionare a riscurilor (art. 11) și de notificare a incidentelor semnificative (art. 12) pentru furnizorii de servicii din sectoarele critice, ale Hotărârii Guvernului nr. 1028/2023 cu privire la constituirea, organizarea și funcționarea ASC și ale Hotărârii Guvernului nr. 820/2024, care desemnează Ministerul Energiei drept autoritate competentă pentru pregătirea la riscuri în sectorul electroenergetic și aprobă Planul de acțiuni pentru situații excepționale în sectorul electroenergetic.

Cadrul general privind obligațiile de securitate cibernetică aplicabile entităților din sectoarele critice, stabilit prin Legea nr. 48/2023, prevede cerințe generale privind protecția sistemelor informatice și gestionarea riscurilor de securitate cibernetică, însă nu reglementează în mod detaliat particularitățile sectorului electroenergetic în ceea ce privește fluxurile transfrontaliere de energie electrică, nu operează cu noțiunile de "entitate cu impact ridicat"/"entitate cu impact critic", proprii Regulamentului delegat (UE) 2024/1366, și nu conține un mecanism specific de evaluare a riscurilor de securitate cibernetică a fluxurilor transfrontaliere, de identificare a entităților cu impact ridicat/critic sau de stabilire a unor controale minime/avansate de securitate cibernetică calibrate pentru rețeaua electrică.

Prin intervenția propusă urmează a fi soluționate, în principal, următoarele probleme: lipsa unui cadru sectorial unitar privind gestionarea riscurilor de securitate cibernetică în domeniul energiei electrice, entitățile relevante nedispunând, în prezent, de un set armonizat de obligații privind identificarea proceselor critice, evaluarea riscurilor, aplicarea controalelor de securitate cibernetică și monitorizarea măsurilor de reducere a riscurilor și necesitatea consolidării cooperării și a schimbului securizat de informații între autoritățile competente și entitățile din sectorul electroenergetic, riscurile cibernetice care afectează infrastructurile energetice putând avea efecte transfrontaliere care necesită mecanisme clare de cooperare, notificare și schimb de informații.

Prin urmare, aprobarea prezentului Cod de rețea reprezintă o măsură necesară pentru dezvoltarea cadrului de reglementare național în domeniul securității cibernetice a sectorului electroenergetic, asigurarea conformării cu obligațiile asumate în cadrul Comunității Energetice și creșterea rezilienței infrastructurii electroenergetice împotriva riscurilor cibernetice.

3. Obiectivele urmărite și soluțiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Proiectul Codului de rețea instituie un set de reguli sectoriale aplicabile domeniului electroenergetic, având ca scop asigurarea unui nivel ridicat de securitate cibernetică pentru infrastructurile, sistemele informatice și procesele operaționale care susțin funcționarea sigură a sistemului electroenergetic și realizarea schimburilor transfrontaliere de energie electrică. Proiectul introduce cerințe sectoriale specifice aplicabile entităților identificate ca entități cu impact ridicat sau entități cu impact critic.

Principalele elemente ale proiectului constau în:

1. Stabilirea cadrului instituțional și a responsabilităților entităților implicate. Codul repartizează atribuțiile astfel: Agenția exercită, în calitate de autoritate competentă desemnată potrivit art. 7 din Legea nr. 164/2025, atribuțiile prevăzute de Cod, inclusiv aprobarea termenilor, condițiilor și metodologiilor (TCM), identificarea entităților cu impact ridicat/critic, gestionarea derogărilor și, dacă decide astfel, un sistem național de verificare, prin pct. 39 din proiect, Agenția deleagă Agenției pentru Securitate Cibernetică, în condițiile pct. 10, exercitarea atribuției de evaluare a riscurilor de securitate cibernetică la nivel național (pct. 43), păstrând atribuția de monitorizare a acestei delegări - repartizare care constituie o adaptare instituțională națională, justificată de competențele atribuite ASC prin Legea nr. 48/2023, ASC exercită, de asemenea, funcțiile de CSIRT, punct național unic de contact și autoritate de gestionare a crizelor cibernetice, iar Ministerul Energiei exercită funcția de autoritate competentă pentru pregătirea la riscuri, potrivit Hotărârii Guvernului nr. 820/2024, inclusiv pentru organizarea exercițiilor de securitate cibernetică la nivel național.

2. Identificarea entităților și proceselor cu impact ridicat și critic. Proiectul introduce noțiunea de entități cu impact ridicat și entități cu impact critic (pct. 44-46), precum și obligația identificării proceselor operaționale și informatice care pot influența securitatea și continuitatea funcționării sistemului electroenergetic, permițând aplicarea unor măsuri proporționale cu nivelul de risc identificat.

3. Instituirea unui proces de evaluare a riscurilor de securitate cibernetică. Codul stabilește obligația efectuării evaluării riscurilor de securitate cibernetică la nivel național (pct. 35-43), cu participarea OST, cu asistența ENTSO-E, la procesele regionale organizate de aceasta, atunci și în măsura în care există.

4. Introducerea controalelor minime și avansate de securitate cibernetică (pct. 55-74), vizând gestionarea politicilor și procedurilor de securitate cibernetică, identificarea și protecția activelor critice, controlul accesului, gestionarea vulnerabilităților, monitorizarea evenimentelor de securitate, răspunsul la incidente și asigurarea securității lanțului de aprovizionare.

5. Stabilirea cerințelor privind sistemul de management al securității cibernetice (pct. 67-68), care asigură o abordare organizată și documentată a proceselor de identificare, evaluare, tratare și monitorizare a riscurilor.

6. Reglementarea securității lanțului de aprovizionare (pct. 69-73), cu cerințe privind evaluarea și gestionarea riscurilor provenite din relațiile cu furnizorii de produse, servicii și

tehnologii utilizate în infrastructurile energetice. Specificațiile de achiziție și recomandările privind achizițiile sunt corelate cu Legea nr. 325/2025 privind achizițiile publice (pct. 71, 76), aplicabilă de la 1 ianuarie 2027, înainte ca obligațiile privind lanțul de aprovizionare să devină aplicabile, iar verificarea antecedentelor personalului furnizorilor se efectuează cu respectarea Legii nr. 195/2024 (pct. 70.1 lit. a).

7. Introducerea unui mecanism sectorial de notificare a atacurilor cibernetice (pct. 78-91), inclusiv criterii de clasificare a acestora pe o scală de 5 niveluri (pct. 83), termene de raportare și schimbul de informații între entitățile competente. Pct. 87 din proiect instituie o clauză de echivalență: notificarea unui incident semnificativ efectuată potrivit art. 12 din Legea nr. 48/2023 constituie și raportarea impusă de prezentul Cod, evitând dubla raportare pentru entitățile care sunt, concomitent, furnizori de servicii în sensul Legii nr. 48/2023.

8. Reglementarea protecției informațiilor schimbate între entități (pct. 114-127), inclusiv accesul pe baza principiului necesității de a cunoaște, protejarea confidențialității, integrității și disponibilității informațiilor, anonimizarea și agregarea informațiilor, respectarea obligației de secret profesional.

9. Gestionarea crizelor de securitate cibernetică (pct. 95-99), cu mecanismul de constatare/confirmare a crizei corelat cu art. 36 alin. (3) din Legea nr. 164/2025 și Hotărârea Guvernului nr. 820/2024 (OST constată, Comisia pentru Situații Excepționale confirmă), și cu două clauze suplimentare de echivalență cu planul, respectiv măsurile de gestionare a crizelor adoptate potrivit art. 9 alin. (2) și art. 11 din Legea nr. 48/2023 (pct. 99.1, 99.5).

Elementele de mai sus constau în instituirea unui mecanism sectorial complet de securitate cibernetică aplicabil domeniului electroenergetic, care completează cadrul general național existent, stabilit prin Legea nr. 48/2023, cu cerințe specifice pentru protejarea infrastructurilor critice energetice, evitând totodată suprapunerea acestor cerințe prin clauzele de echivalență de la pct. 87, 99.1 și 99.5.

Stabilirea intrării în vigoare a hotărârii la data publicării în Monitorul Oficial al Republicii Moldova este necesară în vederea asigurării aplicării fără întârziere a prevederilor Codului și a realizării obligațiilor asumate de Republica Moldova în calitate de parte contractantă a Tratatului de instituire a Comunității Energetice. Stabilirea unei alte date de intrare în vigoare decât termenul general prevăzut de Legea nr. 100/2017 cu privire la actele normative este determinată de realizarea angajamentelor internaționale ale Republicii Moldova și este în conformitate cu prevederile art. 56 alin. (3) din legea precitată, care permite stabilirea unei date diferite de intrare în vigoare în cazul realizării angajamentelor internaționale ale Republicii Moldova.

3.2. Opțiunile alternative analizate și motivele pentru care acestea nu au fost luate în considerare

Opțiunea recomandată constă în elaborarea și aprobarea Codului de rețea, în conformitate cu obligațiile asumate de Republica Moldova în calitate de parte contractantă a Tratatului de instituire a Comunității Energetice și cu cadrul normativ național aplicabil în domeniul energiei electrice și al securității cibernetice.

A fost analizată opțiunea sincronizării proiectului cu o eventuală decizie viitoare a Consiliului ministerial al Comunității Energetice de adaptare a Regulamentului delegat (UE) 2024/1366. Această opțiune nu a fost reținută ca o condiție pentru adoptarea proiectului, întrucât, la data prezentei note, deși adoptarea unei asemenea decizii este preconizată în anul 2026, nu există încă o decizie adoptată și aplicabilă părților contractante, iar condiționarea termenelor și a

efectului util al obligațiilor naționale de adoptarea unei asemenea decizii ar afecta claritatea și previzibilitatea normei, cerută de Legea nr. 100/2017. S-a optat pentru punerea în aplicare unilaterală a Regulamentului, cu termene naționale proprii, fără a prejudicia o eventuală ajustare ulterioară a Codului ca urmare a unei decizii a Comunității Energetice.

A fost analizată, de asemenea, menținerea situației existente, fără intervenție normativă suplimentară, precum și reglementarea separată a unor aspecte privind securitatea cibernetică a fluxurilor transfrontaliere de energie electrică prin acte normative distincte. Menținerea situației existente nu a fost considerată o soluție viabilă, întrucât cadrul normativ general existent în domeniul securității cibernetice nu reglementează în mod suficient particularitățile sectorului electroenergetic. Elaborarea unor acte normative separate nu a fost considerată oportună, întrucât ar putea conduce la fragmentarea cadrului de reglementare și la suprapuneri de competențe.

Prin urmare, aprobarea unui act normativ unic, sub forma unui Cod de rețea sectorial, reprezintă soluția cea mai adecvată pentru asigurarea unui cadru clar, predictibil și armonizat.

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Aprobarea proiectului va avea un impact asupra sectorului public prin consolidarea cadrului instituțional aplicabil securității cibernetice în sectorul electroenergetic. Prin aplicarea Codului se instituie un cadru sectorial pentru cooperarea dintre Agenție, Ministerul Energiei, Agenția pentru Securitate Cibernetică și alte autorități competente, în limitele competențelor și mandatelor stabilite de legislația națională.

Pentru Agenție, aplicarea Codului presupune exercitarea atribuțiilor de autoritate competentă, inclusiv identificarea entităților cu impact ridicat și critic, aprobarea TCM și monitorizarea delegării către ASC a evaluării naționale a riscurilor. Pentru Ministerul Energiei și ASC, proiectul creează un cadru formal de cooperare privind pregătirea pentru riscuri, gestionarea situațiilor de criză cibernetică și schimbul de informații relevante.

Implementarea prevederilor Codului nu necesită instituirea unor structuri administrative noi, ci asigură aplicarea într-o manieră sectorială și coordonată a atribuțiilor deja stabilite prin legislația națională.

4.2. Impactul financiar și argumentarea costurilor estimative

Implementarea prevederilor Codului nu presupune, la momentul elaborării proiectului, instituirea unor structuri administrative noi sau identificarea unor alocări bugetare suplimentare distincte. Costurile suportate de operatorul sistemului de transport și de operatorii sistemelor de distribuție care decurg din obligațiile prezentului Cod (pct. 29) sunt evaluate de Agenție și, în măsura în care sunt apreciate ca fiind rezonabile, eficiente și proporționale, se recuperează prin tarifele de rețea sau prin alte mecanisme corespunzătoare, stabilite de ANRE, fără a afecta bugetul public național.

4.3. Impactul asupra sectorului privat

Aprobarea Codului va avea impact asupra entităților private care desfășoară activități în sectorul electroenergetic și care sunt identificate drept entități cu impact ridicat sau entități cu impact critic. Impactul constă în instituirea unor cerințe sectoriale specifice privind gestionarea riscurilor de securitate cibernetică, protecția informațiilor, implementarea controalelor minime și

avansate de securitate cibernetică, gestionarea riscurilor aferente lanțului de aprovizionare, notificarea incidentelor și cooperarea cu autoritățile competente.

Proiectul prevede un mecanism de derogare (pct. 62-64), care poate fi acordată de Agenție, pentru cel mult 3 ani, cu posibilitatea reînnoirii, în circumstanțe excepționale în care costurile implementării controalelor depășesc semnificativ beneficiile sau atunci când entitatea prezintă un plan de tratare a riscurilor care le atenuează la un nivel acceptabil prin controale alternative.

4.4. Impactul social

Aprobarea Codului nu generează un impact social direct asupra populației și nu instituie obligații suplimentare pentru consumatorii finali de energie electrică. Implementarea prevederilor Codului va produce efecte sociale pozitive indirecte, prin consolidarea securității și rezilienței infrastructurii electroenergetice.

4.4.1. Impactul asupra datelor cu caracter personal

Implementarea prevederilor Codului implică prelucrarea datelor cu caracter personal în măsura necesară realizării atribuțiilor stabilite pentru entitățile și autoritățile prevăzute de Cod. Codul stabilește, la pct. 6, că entitățile, Agenția, ASC și punctele unice de contact la nivel de entitate prelucrează datele cu caracter personal numai în măsura necesară realizării scopurilor prevăzute de Cod, cu respectarea Legii nr. 195/2024 privind protecția datelor cu caracter personal, un temei specific similar este prevăzut la pct. 70.1 lit. a) pentru verificarea antecedentelor personalului furnizorilor din lanțul de aprovizionare. Prevederile Codului nu instituie categorii noi de date cu caracter personal și nu modifică regimul juridic aplicabil protecției datelor.

4.4.2. Impactul asupra echității și egalității de gen

Prevederile proiectului nu generează un impact direct asupra echității sau egalității de gen. Cerințele stabilite se aplică în mod uniform entităților și autorităților prevăzute în Cod, în funcție de atribuțiile, rolul și nivelul de impact al acestora, fără instituirea unor criterii sau condiții diferențiate în funcție de gen.

4.5. Impactul asupra mediului

Prevederile proiectului nu generează un impact direct asupra mediului, întrucât obiectul acestuia îl constituie stabilirea cerințelor privind securitatea cibernetică, protecția informațiilor și gestionarea riscurilor asociate funcționării sistemului electroenergetic.

4.6. Alte impacturi și informații relevante

Aprobarea Codului va avea un impact instituțional prin consolidarea mecanismelor de cooperare dintre autoritățile competente și entitățile implicate în asigurarea securității cibernetice a sectorului electroenergetic, contribuind la îndeplinirea angajamentelor asumate de Republica Moldova în calitate de parte contractantă a Comunității Energetice.

5. Compatibilitatea proiectului actului normativ cu legislația UE

5.1. Măsuri normative necesare pentru transpunerea actelor juridice ale UE în legislația națională

Elaborarea prezentului proiect derivă din obligațiile asumate de Republica Moldova în calitate de parte contractantă la Tratatul de instituire a Comunității Energetice. Prin Decizia Consiliului Ministerial al Comunității Energetice nr. 2022/03/MC-EnC din 15 decembrie 2022, Regulamentul (UE) 2019/943 privind piața internă de energie electrică a fost inclus în acquis-ul Comunității Energetice, în varianta adaptată și adoptată pentru Comunitatea Energetică.

Regulamentul delegat (UE) 2024/1366, care completează Regulamentul (UE) 2019/943 prin stabilirea prezentului cod de rețea, nu a fost însă, la data prezentei note, preluat în acquis-ul Comunității Energetice și nu există încă o decizie de adaptare și adoptare a acestuia aplicabilă părților contractante, potrivit evidenței oficiale a Secretariatului Comunității Energetice. Potrivit Programului de lucru al Comunității Energetice pentru anii 2026-2027, adoptarea sa prin decizie a Consiliului ministerial este preconizată în anul 2026.

În consecință, proiectul pune în aplicare parțial, în mod unilateral, actul Uniunii Europene, cu termene naționale proprii, calculate de la intrarea în vigoare a Hotărârii, iar nu o variantă adaptată a acestuia. Această soluție este susținută de împrejurarea că exercițiul este urmărit ca măsură de armonizare cu dreptul Uniunii Europene în cadrul Programului Național de Aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029 (Clusterul 4 "Agenda verde și conectivitatea sustenabilă", Capitolul 15 "Energie"), iar punerea în aplicare a prezentului Cod nu este condiționată de adoptarea unei viitoare decizii a Comunității Energetice.

Metoda de armonizare aplicată este punerea în aplicare prin măsuri naționale, iar gradul de compatibilitate atins este „pune în aplicare parțial", potrivit tabelului de concordanță anexat. Nu au putut fi transpuse dispozițiile care se adresează exclusiv arhitecturii instituționale proprii Uniunii Europene - ACER, ENISA, ENTSO pentru energie electrică și entitatea OSD UE ca entități reglementate distinct sau ca destinatare ale unor atribuții proprii -, calificate drept prevederi UE neaplicabile, precum și dispozițiile tranzitorii de la art. 48, calibrate pe un calendar al Uniunii Europene expirat (2024-2025), calificate drept prevedere UE netranspusă.

Proiectul introduce, fără corespondent literal în Regulament, delegarea expresă către ASC a evaluării naționale a riscurilor (pct. 39), trei clauze de echivalență cu Legea nr. 48/2023 (pct. 87, 99.1, 99.5) și calendarul național ancorat la intrarea în vigoare a Hotărârii, pentru motivele expuse la pct. 3.1 și 3.2 din prezenta notă.

Pentru dispozițiile Regulamentului care presupun exercitarea unor atribuții proprii instituțiilor și organismelor Uniunii Europene (ACER, ENISA, ENTSO pentru energie electrică, entitatea OSD UE) sau participarea la mecanisme europene ori regionale instituite în temeiul dreptului Uniunii, proiectul utilizează formule de aplicare condiționată ("atunci și în măsura în care" procesul este organizat sau există un mecanism de cooperare aplicabil Republicii Moldova - de exemplu, pct. 14, 30, 34, 38, 40, 41, 100 și 127). Această tehnică normativă nu extinde competențele autorităților naționale și nu atribuie instituțiilor Uniunii Europene competențe printr-un act normativ național.

În partea ce ține de art. 42 din Regulament, obligația de cooperare cu ENISA este instituită expres în sarcina autorităților naționale (pct. 100), cu precizarea că aceasta constă în depunerea diligențelor necesare, întrucât extinderea cooperării către o parte contractantă a Comunității Energetice depinde de ENISA; funcțiile proprii ale ENISA nu sunt preluate, iar pct. 101 reglementează exclusiv participarea voluntară a destinatarilor naționali.

Totodată, tehnica aplicării condiționate permite ca obligațiile OST și ale autorităților naționale să devină operaționale de îndată ce procesul european sau regional relevant există,

inclusiv după o eventuală decizie a Consiliului ministerial al Comunității Energetice, iar în acel caz Codul va fi reexaminat și, după caz, ajustat.

Este vorba despre o primă punere în aplicare: Regulamentul delegat (UE) 2024/1366 nu a mai constituit anterior obiect al armonizării în legislația Republicii Moldova.

5.2. Măsuri normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE

Prin aprobarea Codului se creează cadrul juridic necesar pentru:

- stabilirea domeniului de aplicare și a categoriilor de entități supuse cerințelor de securitate cibernetică aferente fluxurilor transfrontaliere de energie electrică;
- definirea responsabilităților autorităților competente și ale entităților implicate;
- instituirea mecanismelor de identificare a entităților cu impact ridicat și cu impact critic;
- stabilirea cerințelor privind evaluarea riscurilor, aplicarea controalelor minime și avansate de securitate cibernetică, gestionarea riscurilor aferente lanțului de aprovizionare și raportarea incidentelor;
- stabilirea regulilor privind protecția, confidențialitatea și schimbul securizat de informații;
- asigurarea mecanismelor de cooperare între autoritățile competente din domeniul energetic și cel al securității cibernetice.

Adoptarea prezentului proiect nu condiționează modificarea altor acte normative primare sau secundare.

Totodată, în vederea consolidării coerenței cadrului normativ primar, se apreciază oportun ca, cu prima ocazie de modificare a Legii nr. 164/2025, art. 39 să fie completat cu o mențiune expresă a Regulamentului delegat (UE) 2024/1366, în limitele competenței Parlamentului, o asemenea intervenție legislativă are caracter conex și nu constituie o condiție pentru adoptarea sau intrarea în vigoare a prezentului proiect.

6. Avizarea și consultarea publică a proiectului actului normativ

În conformitate cu prevederile art. 13 din Legea nr. 164/2025 cu privire la energia electrică și art. 8 din Legea nr. 239/2008 privind transparența în procesul decizional, proiectul Codului de rețea, tabelul de concordanță și prezenta notă de fundamentare au fost plasate pe pagina web oficială a Agenției (www.anre.md, secțiunea Transparența decizională / Proiecte supuse consultării, poziția nr. 2826 https://anre.md/consultari-publice-3-27) și supuse consultărilor publice, astfel încât orice persoană să aibă posibilitatea să prezinte propuneri și obiecții pe marginea lor, la adresa electronică a Agenției.

În rezultat Agenția a recepționat avize din partea Confederației Naționale a Sindicatelor din Moldova, Ministerului Energiei și S.A, „Termoelectrica". Propunerile expuse de părțile interesate au fost examinate și considerate în procesul de definitivare a proiectului de act normativ.

În baza avizelor primite de la părțile interesate, a fost elaborat tabelul de sinteză a obiecțiilor și propunerilor la proiectul dat, fiind plasat pe pagina oficială a Agenției la rubrica Transparență decizională/Proiecte supuse consultării publice.

7. Concluziile expertizelor

Proiectul a fost supus expertizei de compatibilitate cu legislația Uniunii Europene, potrivit Regulamentului privind armonizarea legislației Republicii Moldova cu legislația Uniunii

Europene, aprobat prin Hotărârea Guvernului nr. 1171/2018, efectuată de Centrul de Armonizare a Legislației (Declarația de compatibilitate nr. 31/02-126-12023 din 11 septembrie 2026, în conformitate cu art. 35 din Legea nr. 100/2017). Observațiile și recomandările formulate au fost analizate și reflectate în proiect, în tabelul de concordanță și în prezenta notă de fundamentare.

8. Modul de încorporare a actului în cadrul normativ existent

Pentru implementarea prevederilor proiectului nu este necesară, ca o condiție pentru intrarea în aplicare a Codului, modificarea sau abrogarea altor acte normative. Prin proiectul propus se instituie un cadru normativ sectorial specific în domeniul securității cibernetice aplicabil entităților relevante din sectorul electroenergetic, care se va integra în cadrul juridic existent privind funcționarea sectorului energiei electrice și asigurarea securității infrastructurilor critice.

Prevederile Codului urmează a fi aplicate în coroborare cu cadrul normativ existent, inclusiv cu prevederile Legii nr. 164/2025, care stabilește principiile de organizare și funcționare a sectorului electroenergetic, precum și competențele Agenției. Totodată, Codul completează cadrul normativ național în domeniul securității cibernetice, stabilit prin Legea nr. 48/2023 și actele normative subsecvente (Hotărârile Guvernului nr. 1028/2023 și nr. 820/2024), prin instituirea unor cerințe sectoriale specifice pentru entitățile implicate în fluxurile transfrontaliere de energie electrică, cu clauzele de echivalență de la pct. 87, 99.1 și 99.5 din proiect, care evită suprapunerea obligațiilor pentru entitățile care sunt, concomitent, furnizori de servicii în sensul Legii nr. 48/2023.

Concomitent, în contextul procesului de integrare europeană a Republicii Moldova și al obiectivelor stabilite prin Programul Național de Aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029, Clusterul 4 "Agenda verde și conectivitatea sustenabilă", Capitolul 15 "Energie", aprobarea prezentului Cod contribuie la alinierea cadrului de reglementare național la cerințele acquis-ului Uniunii Europene și ale Comunității Energetice.

9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

Implementarea prevederilor proiectului reprezintă o măsură de realizare a angajamentelor asumate de Republica Moldova în procesul de integrare europeană, inclusiv în conformitate cu acțiunile prevăzute în Programul Național de Aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029, Clusterul 4 "Agenda verde și conectivitatea sustenabilă", Capitolul 15 "Energie".

Implementarea prevederilor Codului va fi organizată etapizat, pe un calendar ancorat la data intrării în vigoare a Hotărârii și, ulterior, la data notificării de către Agenție a entităților cu impact ridicat/critic (pct. 45), care condiționează termenele relative ulterioare.

Ulterior aprobării actului normativ, implementarea prevederilor acestuia va fi asigurată prin:

- aplicarea de către entitățile prevăzute la pct. 2 din Cod a cerințelor privind gestionarea riscurilor de securitate cibernetică, protecția informațiilor, aplicarea controalelor de securitate și raportarea incidentelor;
- îndeplinirea de către Agenție a atribuțiilor privind identificarea și notificarea entităților cu impact ridicat și critic, aprobarea și monitorizarea aplicării TCM;

– asigurarea cooperării instituționale dintre Agenție, Ministerul Energiei, Agenția pentru Securitate Cibernetică și alte autorități competente.

Implementarea prevederilor Codului nu presupune, la nivelul actelor normative primare sau secundare, adoptarea unor acte normative suplimentare ca o condiție pentru intrarea în aplicare a Codului. Eventualele metodologii, TCM, planuri, matrice, recomandări și alte documente tehnice prevăzute de Cod vor fi elaborate și aprobate în condițiile și termenele stabilite de acesta, de autoritățile sau entitățile competente. Măsurile de implementare urmează a fi realizate în limitele competențelor și resurselor instituționale existente, iar eventualele costuri administrative suplimentare pentru autoritățile publice vor fi gestionate în limitele bugetelor aprobate și ale resurselor disponibile.

Alexandru URSU
Director