GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. _____

din_____

pentru aprobarea Regulamentului cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice

În temeiul art. 18 alin. (3) și art. 19 alin. (5) din Legea nr. 48/2023 privind securitatea cibernetică (Monitorul Oficial al Republicii Moldova, 2023, nr. 151-153, art. 225), Guvernul HOTĂRĂȘTE:

1. Se aprobă Regulamentul cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice (se anexează).

2. Ministerul Dezvoltării Economice și Digitalizării, în comun cu Agenția pentru Securitate Cibernetică, în termen de 12 luni de la data publicării prezentei hotărâri, va elabora și va prezenta Guvernului pentru aprobare Metodologia privind controlul de stat asupra activității de întreprinzător în baza analizei riscurilor aferent domeniilor de competență ale Agenției pentru Securitate Cibernetică.

3. Prezenta hotărâre intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

4. Controlul asupra executării prezentei hotărâri se pune în sarcina Ministerului Dezvoltării Economice și Digitalizării.

Prim-ministru

Viceprim-ministru,
ministrul dezvoltării
economice și digitalizării

Aprobat prin
Hotărârea Guvernului nr._____/2025

REGULAMENTUL
cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice

Capitolul I. Dispoziții generale

1. Regulamentul cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice (în continuare – *Regulament*) stabilește cadrul juridic, organizatoric și procedural de exercitare de către Agenția pentru Securitate Cibernetică a funcției de supraveghere și control de stat al modului în care furnizorii de servicii în sectoarele critice asigură conformitatea cu prevederile cadrului normativ în domeniul securității cibernetice

2. În sensul prezentului Regulament se utilizează noțiunile definite în Legea nr. 48/2023 privind securitatea cibernetică și Legea nr. 131/2012 privind controlul de stat.

3. Supravegherea și controlul de stat asupra respectării de către furnizorii de servicii în sectoarele critice a prevederilor cadrului normativ în domeniul securității cibernetice se realizează de către Agenția pentru Securitate Cibernetică (în continuare - *Agenția*) în conformitate cu prevederile Legii nr. 48/2023 privind securitatea cibernetică, Legii nr. 131/2012 privind controlul de stat și a prezentului Regulament.

4. Agenția exercită controlul de stat asupra respectării de către furnizorii de servicii a cadrului normativ în domeniul securității cibernetice în baza rezultatelor evaluării riscurilor de securitate cibernetică la nivel național, sectorial/subsectorial, intersectorial sau pe tipuri de furnizori de servicii în conformitate cu cadrul metodologic aprobat în conformitate cu art. 16 alin. (2) din Legea nr. 131/2012 privind controlul de stat.

5. La solicitarea unei autorități de supraveghere și control a gestionarilor de infrastructură critică națională sau în baza constatărilor rapoartelor de evaluare a conformității (audit), Agenția efectuează un control inopinat al furnizorului de servicii în cauză și informează autoritatea de supraveghere și control de stat în

sectorul corespunzător despre încălcările constatate într-un termen care nu depășește 5 zile lucrătoare de la data finalizării controlului.

6. Principiile specifice supravegherii și controlului de stat asupra respectării cadrului normativ în domeniul securității cibernetice sunt:

6.1. *proporționalitatea* – măsurile adoptate în procesul de realizare a funcției de supraveghere și control de stat de către Agenție trebuie să fie echilibrate în raport cu scopul general de evaluare a respectării prevederilor cadrului normativ în domeniul securității cibernetice și cu obiectivele specifice ale activității de supraveghere și control, evitând astfel sarcini administrative excesive și nejustificate pentru furnizorii de servicii și asigurând adaptarea resurselor și a intensității activității de supraveghere și control de stat la riscurile, importanța și dimensiunea furnizorilor de servicii;

6.2. *eficacitatea* – măsurile de supraveghere și de asigurare a respectării legislației trebuie să fie capabile să producă efectul urmărit, asigurând conformarea continuă a furnizorilor de servicii;

6.3. *efectul de descurajare* – măsurile adoptate trebuie să reducă probabilitatea încălcării prevederilor cadrului normativ, prin certitudinea și proporționalitatea aplicării acestora;

6.4. *cooperarea* – Agenția promovează colaborarea permanentă cu alte autorități și instituții publice, cu furnizorii de servicii în sectoarele critice, în scopul prevenirii și reducerii riscurilor de securitate cibernetică;

6.5. *protecția drepturilor fundamentale* – în exercitarea atribuțiilor, Agenția asigură respectarea dreptului la viață privată, a protecției datelor cu caracter personal și a altor date ce constituie secret comercial pentru furnizorii de servicii în sectoarele critice, precum și a altor drepturi fundamentale stabilite de cadrul normativ.

Capitolul II. Supravegherea respectării cadrului normativ în domeniul securității cibernetice de către furnizorilor de servicii în sectoarele critice

7. Agenția realizează activitățile de supraveghere la furnizorii de servicii în sectoarele critice, în mod sistematic și continuu, cu scopul de a monitoriza respectarea obligațiilor prevăzute de Legea 48/2023 privind securitatea cibernetică și actelor normative de punere în aplicare a acesteia precum și de a monitoriza remedierea eventualelor deficiențe constatate, contribuind astfel la asigurarea oportună a unui nivel comun ridicat de securitate cibernetică la nivel național.

8. Activitatea de supraveghere se realizează de către personalul Agenției. În exercitarea competenței sale de supraveghere, Agenția aplică măsuri care nu au caracter coercitiv și nu constituie forme ale controlului de stat, în scopul monitorizării și evaluării continue a modului în care prevederile cadrului normativ în domeniul securității cibernetice este aplicat de către furnizorii de servicii în sectoarele critice.

9. În cazul în care pe parcursul desfășurării activității de supraveghere se constată săvârșirea unor fapte care pot întruni elemente constitutive ale unor contravenții sau infracțiuni, Agenția în termen de 3 zile sesizează autoritățile competente. În exercitarea funcției de supraveghere, Agenția aplică următoarele măsuri de supraveghere:

9.1. monitorizarea continuă a spațiului cibernetic național pentru identificarea amenințărilor, riscurilor și vulnerabilităților de securitate cibernetică și *s*chimbul continuu de informații cu furnizorii de servicii prin emiterea de avertizări timpurii, alerte, anunțuri privind amenințările cibernetice, vulnerabilitățile și incidentele cibernetice în spațiul cibernetic național;

9.2. acordarea asistenței consultative furnizorilor de servicii în asigurarea conformității cu prevederile cadrului normativ în domeniul securității cibernetice, inclusiv prin furnizarea de orientări metodologice, inclusiv ghiduri, modele de proceduri și politici;

9.3. solicitarea informațiilor de către Agenție necesare pentru determinarea gradului de conformitate cu cadrul normativ și a nivelului de maturitate și reziliență a furnizorilor de servicii;

9.4. acordarea suportului consultativ furnizorilor de servicii în crearea mecanismelor de autoevaluare a conformității cu cerințele de securitate a rețelelor și sistemelor informatice stabilite de cadrul normativ;

9.5. evaluarea nivelului de conformitate a furnizorilor de servicii, inclusiv în baza rapoartelor de evaluare a riscurilor, a planurilor de tratare a riscurilor și a rapoartelor de evaluare a conformității, realizate de furnizorii de servicii în baza prevederilor normative aferente securității cibernetice;

9.6. înaintarea recomandărilor corespunzătoare furnizorilor de servicii, în baza rapoartelor de evaluare a riscurilor, a planurilor de tratare a riscurilor și a rapoartelor de evaluare a conformității, realizate de furnizorii de servicii în baza prevederilor normative;

9.7. organizarea de exerciții și simulări în materie de securitate cibernetică în vederea determinării nivelului de pregătire a furnizorilor de servicii în sectoarele critice în realizarea obligațiilor de asigurarea a securității cibernetice stabilite de cadrul normativ în acest domeniu;

9.8. organizarea și efectuarea de teste la stres, precum și, la solicitarea furnizorilor de servicii în sectoarele critice, a testelor de penetrare și a scanărilor rețelelor și sistemelor informatice ale acestora în vederea identificării vulnerabilităților și determinării măsurilor de securitate ce necesită a fi implementate.

10. Rezultatele măsurilor de supraveghere sunt utilizate de către Agenție pentru planificarea activității de control de stat în baza analizei riscurilor pe domeniile de competență ale acesteia.

Capitolul III. Controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către persoanele juridice de drept privat, identificate ca furnizori de servicii în sectoarele critice

Secțiunea 1. Planificarea controlului de stat

11. Agenția efectuează controale de stat în privința furnizorilor de servicii persoane juridice de drept privat (furnizori de servicii privați) în baza Legii nr. 131/2012 privind controlul de stat și în baza prezentei hotărâri.

12. Agenția efectuează controale inopinate în cazul în care a depistat și confirmă, în urma unei investigații preliminare, fapte ce constituie încălcări ale prevederilor Legii nr. 48/2023 privind securitatea cibernetică și/sau atunci când este sesizată despre încălcări, neîndeplinirea sau îndeplinirea necorespunzătoare a obligațiilor stabilite prin această lege de către furnizorul de servicii privat. Controlul inopinat se inițiază în condițiile art. 19 din Legea nr. 131/2012 privind controlul de stat.

13. Controlul de stat se efectuează în temeiul delegației de control de către cel puțin doi inspectori ai Agenției și se semnează de către conducere.

14. În procesul de efectuare a controlului, inspectorii pot coopta alți angajați ai Agenției cu experiență profesională în domeniul de activitate al furnizorului de servicii privat supus controlului, cu condiția includerii acestora în delegația de control.

15. Agenția la efectuarea controalelor, va implica, în caz de necesitate, alte autorități și instituții publice ce nu se regăsesc în anexa Legii nr. 131/2012 privind

controlul de stat, în măsura în care acestea sunt necesare la desfășurarea unor expertize, evaluări sau teste suplimentare ori dacă acestea au atribuții de implementare a legislației aferente domeniului de control în cauză.

16. Agenția aprobă planul controalelor pentru anul următor și îl publică pe site-ul său web oficial.

Secțiunea 2. Pregătirea și realizarea controlului

17. Agenția în exercitarea funcției de control:

18.1 realizează verificarea sistematică a modului de îndeplinire a obligațiilor privind respectarea măsurilor de securitate impuse de cadrul normativ;

18.2 constată abateri de la obligațiile prevăzute la pct. 18.1;

18.3 emite dispoziții cu caracter obligatoriu în vederea conformării și remedierii deficiențelor constatate în cursul activităților de control;

18.4 stabilește termene de conformitate cu măsurile de securitate impuse de cadrul normativ;

18. În cadrul sau în urma controlului de stat, la depistarea încălcărilor, inspectorul Agenției înaintează prescripții și recomandări, aplica măsuri restrictive și sancțiuni în limitele prevăzute de lege. Acțiunile și măsurile se selectează și se aplică în conformitate cu prevederile Legii nr. 131/2012 privind controlul de stat.

19. La începutul controlului, Agenția pune la dispoziția furnizorului de servicii privat supus controlului toate documentele în baza căruia se efectuează controlul, inclusiv delegația de control și alte materiale și documente întocmite sau deținute în legătură cu exercitarea controlului și a căror divulgare nu poate afecta procesul de control.

20. Controlul se efectuează fără a influența desfășurarea activităților curente a furnizorului de servicii privat supus controlului, cu excepția situațiilor impuse de natura controlului.

21. Drepturile și obligațiile inspectorilor și furnizorilor de servicii privați pe parcursul desfășurării controlului sunt stabilite de articolele 23 - 26 ale Legii nr. 131/2012 privind controlul de stat.

22. În cazul în care personalul furnizorului de servicii privat supus controlului se află în imposibilitate de a participa la procesul de control, controlul se realizează în lipsa acestuia conform art. 24 și 26 din Legea 131/2012 privind controlul de stat.

23. În cazul în care în timpul desfășurării controlului, inspectorii constată încălcări ce conțin semne ale unei infracțiuni, aceștia consemnează în procesul-verbal de control și sesizează în decurs de 3 zile organele de urmărire penală cu privire la încălcările constatate, respectând procedura stabilită de Legea nr. 131/2012 privind controlul de stat.

24. Agenția solicită declanșarea imediată a măsurilor de remediere a anumitor deficiențe în situații de risc major sau care impun măsuri urgente.

25. Pentru a contracara o amenințare cibernetică semnificativă imediate asupra securității rețelelor și sistemelor informatice sau a atenua consecințele unui incident cibernetic cu impact semnificativ, Agenția poate restricționa utilizarea ori accesul la una sau mai multe rețele sau sisteme informatice, dacă sunt îndeplinite condițiile stabilite la art. 15 alin. (2) din Legea nr. 48/2023 privind securitatea cibernetică.

26. În cazul care Agenția restricționează utilizarea unuia sau mai multe sisteme informatice sau accesul la acesta/acestea, urmare a îndeplinirii cumulative a condițiilor prevăzute la pct. 26, furnizorul de servicii privat este notificat imediat cu privire la aceasta.

Secţiunea 3. Finalizarea controlului

27. Constatările efectuate pe timpul verificărilor, concluziile și măsurile propuse se reflectă în procesul-verbal de control, care se semnează de toate persoanele cooptate pentru efectuarea controlului, inclusiv persoana supusă controlului.

28. Procedura de control se încheie prin întocmirea de către inspectori a unui proces-verbal de control în conformitate cu art. 28 din Legea nr. 131/2012 privind controlul de stat.

29. Persoana supusă controlului are dreptul, în termen de 10 zile lucrătoare de la semnarea procesului-verbal de control, să prezinte dezacordul cu actul în cauză, aducînd probe suplimentare ce confirmă poziţia sa. În caz de neprezentare se consideră că se susține observații emise.

30. Pe lângă prescripțiile emise și sancțiuni aplicate în temeiul procesului-verbal de control, Agenția poate:

31.1 emite avertismente cu privire la încălcarea prevederilor cadrului normativ în domeniul securității cibernetice;

31.2 emite instrucțiuni obligatorii prin care solicită furnizorilor de servicii privați să remedieze deficiențele și încălcările identificate;

31.3 dispune ca furnizorii de servicii privați să înceteze conduita prin care încalcă prevederile cadrului normativ în domeniul securității cibernetice și să se abțină de la repetarea conduitei respective;
31.4 dispune ca furnizorii de servicii privați să informeze persoanele fizice sau juridice, cărora le furnizează servicii privind o amenințare cibernetică semnificativă, inclusiv privind măsurile de protecție sau de remediere pe care le-ar putea lua persoanele fizice sau juridice în cauză ca răspuns la o amenințare cibernetică;
31.5 dispune ca furnizorii de servicii privați să pună în aplicare recomandările formulate în urma unui audit de securitate cibernetică într-un termen rezonabil;
31.6 solicită autorităților publice competente aplicarea, în conformitate cu cadrul normativ, a unei sancțiuni proporționale încălcării și impactului produs.
31. Procesul-verbal de control și anexele acestuia se secretizează dacă în conținutul acestora se regăsesc informații care presupun aplicarea prevederilor legale privind secretul de stat.
32. Procesul-verbal de control și anexele acestuia se comunică în decurs de 3 zile și organului de urmărire penală atunci când există indici cu privire la săvârșirea unei posibile infracțiuni, respectând prevederile legale în domeniu.

Secţiunea 4. Monitorizarea măsurilor stabilite

33. Nivelul de realizare a implementării măsurilor pentru remedierea deficiențelor și îmbunătățirea activității furnizorului de servicii privat se comunică Agenției în conformitate cu termenii stabiliți în anexa la procesul-verbal de control.
34. În cazul în care anumite măsuri prevăzute în anexa la procesul-verbal de control nu pot fi realizate în termen, furnizorul de servicii privat poate solicita Agenției extinderea termenului de realizare.
35. Decizia cu privire la extinderea termenului de realizare a măsurilor prevăzute în anexa la procesul-verbal de control se aprobă de Directorul Agenției.
36. Verificarea nivelului de realizare a măsurilor se realizează în baza rapoartelor de evaluare transmise de entitatea supusă controlului, prin solicitarea de informații suplimentare sau prin realizarea activităților de supraveghere.

Capitolul IV. Controlul de stat al respectării cadrului normativ în domeniul securității cibernetice de către persoanele juridice de drept public, identificate ca furnizori de servicii în sectoarele critice

Secțiunea 1. Planificarea controlului

37. Controlul respectării de către furnizorii de servicii în sectoarele critice care sunt persoane juridice de drept public (*în continuare - furnizorii de servicii publici*) se efectuează de Agenție în conformitate cu Planul anual al controlului respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii publici (în continuare - Planul).

38. Planul se aprobă de către Directorul Agenției și se publică pe site-ul web oficial al acesteia nu mai târziu de data de 15 a lunii care precedă perioada de gestiune.

39. Planificarea controalelor furnizorilor de servicii publici se efectuează în funcție de:

39.1. rezultatele evaluărilor de riscuri la nivel național, intersectorial, sectorial, și subsectorial;

39.2. categoria și nivelul de criticitate al furnizorului de servicii public;

39.3. rezultatele auditurilor de securitate cibernetică efectuate în conformitate cu anexa la Regulamentul cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice, aprobat prin Hotărârea Guvernului nr. 562/2025;

39.4. rezultatele aplicării măsurilor de supraveghere prevăzute la punctul 10;

40. Planul cuprinde cel puțin, următoarele părți componente:

40.1. furnizorul de servicii public supus controlului;

40.2. obiectivele controlului;

40.3. perioada controlului.

41. Planul poate fi revizuit pe parcursul anului atunci când apar modificări semnificative ale riscurilor, incidente cibernetice cu impact semnificativ sau crize cibernetice.

42. Controlul inopinat al furnizorului de servicii public poate fi efectuat în următoarele cazuri:

42.1. producerea unui incident cibernetic în rețelele și sistemele informatice deținute de furnizorul de servicii respectiv;

42.2. deținerea de către Agenție a unor informații veridice privind existența unei amenințări cibernetice semnificative asupra rețelelor și sistemelor informatice deținute de furnizorul de servicii public;

42.3. deținerea de către Agenție a informațiilor privind neîndeplinirea sau îndeplinirea necorespunzătoare de către furnizorul de servicii public a obligațiilor de

asigurare a securității cibernetice care prezintă un pericol iminent și imediat pentru viața și sănătatea persoanelor, pentru securitatea națională sau ordinea publică.

42.4. deținerea de către Agenție a informațiilor privind neîndeplinirea sau îndeplinirea necorespunzătoare de către furnizorul de servicii public a obligațiilor de raportare a incidentelor cibernetice cu impact semnificativ.

42.5. solicitarea din partea organului ierarhic superior sau a autorității publice care exercită supravegherea administrativă și controlul administrativ al furnizorului de servicii public.

43. Controlul inopinat se motivează. Nota de motivare se anexează la delegația de control și se înregistrează în Registrul de stat al controalelor în modul stabilit;

Secțiunea 2. Pregătirea și realizarea controlului

44. Controlul se inițiază și se efectuează în temeiul delegației de control semnată de conducerea Agenției și se înregistrează în Registrul de stat al controalelor în termenul stabilit;.

45. Delegația de control trebuie să conțină cel puțin:

45.1. numărul și data înregistrării;

45.2. temeiul controlului;

45.3. numele prenumele persoanelor ce vor efectua controlul;

45.4. denumirea furnizorului de servicii public și numele și prenumele conducătorului acestuia;

45.5. scopul controlului;

45.6. data începerii și durata preconizată a controlului.

46. Controlul se realizează de către cel puțin doi angajați ai Agenției (în continuare – echipa de control).

47. Furnizorul de servicii public este notificat în prealabil de către Agenție cu privire la controlul planificat cu cel puțin 5 zile lucrătoare înaintea începerii acestuia.

48. În cazul unui control inopinat, la începutul controlului echipa de control înmânează un exemplar al delegației de control furnizorului de servicii public.

49. În procesul de efectuare a controlului, Agenția poate solicita suportul altor autorități sau instituții publice cu competențe în domeniul securității cibernetice.

50. Activitatea de control se documentează în modul stabilit de cadrul normativ.

51. Odată cu recepționarea notificării remise de către Agenție cu privire la controlul preconizat, furnizorul de servicii public întreprinde măsurile necesare de

pregătire pentru efectuarea controlul, inclusiv a personalului care urmează a fi implicat în procesul controlului.

52. Până la începerea nemijlocită a controlului, echipa de control informează furnizorul de servicii public despre actele normative, în baza cărora urmează a fi evaluată conformitatea în cadrul controlului, precum și pune la dispoziția furnizorului de servicii public orice alte documente în baza cărora se realizează controlul sau care urmează a fi utilizate în cadrul controlului.

53. Echipa de control asigură desfășurarea controlului prin minimizarea caracterului intrusiv al activităților de control în activitatea curentă a furnizorului supus controlului. Delegația de control își pierde valabilitatea la expirarea termenului de 5 zile lucrătoare de la data începerii controlului, indiferent de temeiul efectuării acestuia și de tipul controlului.

54. Conducerea organului de control poate prelungi termenul prevăzut la pct. anterior cu încă 5 zile lucrătoare, în baza unei decizii motivate, care poate fi contestată de către persoana supusă controlului.

55. În procesul efectuării controlului, echipa de control are următoarele drepturi:

55.1. să pătrundă în orice încăpere utilizată de furnizorul de servicii în activitatea sa, care găzduiește rețele și sisteme informatice sau date relevante obiectului controlului, în măsura în care aceasta este parte a obiectului controlului.

55.2. să solicite și să obțină orice informații, documente sau alte tipuri de date relevante obiectului controlului;

55.3. să facă copii, înregistrări foto sau video ale documentelor sau ale altor obiecte purtătoare de informații relevante obiectului controlului.

56. În procesul efectuării controlului, echipa de control are următoarele obligații:

56.1. să se legitimeze și să informeze furnizorul de servicii public supus controlului despre drepturile și obligațiile acestuia;

56.2. să aprecieze obiectiv și echidistant toate aspectele ce țin de efectuarea controlului și să asigure integritatea bunurilor și a documentației furnizorului de servicii public suspus controlului;

56.3. să asigure controlul accesului la informațiile și documentele de care a luat cunoștință în procesul de realizare a controlului în conformitate cu cadrul normativ relevant;

56.4. să anexeze la actul de control orice documente sau copii ale acestora și explicații în scris ale furnizorului de servicii supus controlului și/sau ale angajaților acestuia.

57. În procesul efectuării controlului, furnizorul de servicii public are următoarele drepturi:

57.1. să verifice delegația de control și să ia cunoștință de legitimația de serviciu a inspectorilor;

57.2. să prezinte dovezi și explicații;

57.3. să ceară anexarea la actul de control a oricăror documente sau copii ale acestora, pe care are dreptul să aplice semnătura și să dea explicații în scris, precum și să ceară includerea în actul de control a informațiilor privind anumite fapte relevante procesului și procedurii de control;

57.4. să solicite Agenției suspendarea sau amânarea controlului pentru o altă perioadă, dacă continuarea controlului ar putea afecta continuitatea activității furnizorului de servicii public;

57.5. să ia cunoștință de actul de control și de alte acte și informații întocmite în cadrul controlului;

57.6. să asiste la acțiunile desfășurate în procesul realizării controlului de stat.

58. În procesul efectuării controlului de stat furnizorul de servicii public este obligat:

58.1. să prezinte documentele și informațiile ce țin de obiectul controlului, solicitate de echipa de control;

58.2. să permită accesul echipei de control în încăperile de serviciu;

59. În cazul în care personalul furnizorului de servicii public supus controlului se află în imposibilitate de a participa la activitățile desfășurate în cadrul controlului, acesta se realizează în lipsa personalului furnizorului de servicii public.

60. Agenția în decurs de 3 zile sesizează organele de urmărire penală cu privire la încălcări constatate ce conțin semne ale unei infracțiuni, respectând procedura stabilită de actele normative relevante.

61. În cazul în care toate aspectele vizate în delegația de control nu au fost atinse sau au apărut circumstanțe noi pentru a căror clarificare sunt necesare acțiuni suplimentare, perioada de desfășurare a controlului se poate prelungi până la realizarea acestora, cu aprobarea Directorului Agenției.

Secțiunea 3. Finalizarea controlului

62. Constatările efectuate în timpul verificărilor, concluziile și măsurile propuse de inspectori se reflectă în procesul-verbal de control, care se semnează de toți inspectorii și, după caz, angajații Agenției cooptați pentru efectuarea controlului.

63. Procesul-verbal cuprinde:

63.1. principalele realizări;

63.2. deficiențele, disfuncțiile, neregulile și măsurile de ordin organizatoric și administrativ;

63.3. concluziile echipei de supraveghere;

63.4. alte aspecte care pot contribui la creșterea eficacității și eficienței activităților evaluate.

63.5. Procesul-verbal de control include obligatoriu explicații și/sau obiecțiile furnizorului în privința măsurilor restrictive prescrise, anexate integral la proces;

64. Modelul procesului verbal de control al furnizorilor de servicii publici se aprobă de Directorul Agenției.

65. Procesul-verbal se aduce la cunoștință furnizorului de servicii supus controlului, confirmată prin semnătura persoanei care recepționează procesul-verbal.

66. Proiectul procesului-verbal se prezintă furnizorului de servicii, oferind un termen de 10 zile lucrătoare pentru prezentarea observațiilor, cu excepția cazurilor justificate în mod corespunzător, când sunt în desfășurare acțiuni imediate pentru a preveni sau răspunde la un incident.

67. O copie a procesului-verbal se înmânează furnizorului de servicii supus activității de supraveghere.

68. La procesul-verbal se anexează un plan de măsuri pentru remedierea deficiențelor și îmbunătățirea activității furnizorului de servicii, care include în mod obligatoriu termene limită pentru realizarea acestora.

69. Procesul-verbal și anexele acestuia se secretizează dacă în conținutul acestora se regăsesc informații care presupun aplicarea prevederilor legale privind secretul de stat.

70. Procesul-verbal și anexele acestuia se comunică în decurs de 3 zile organului de urmărire penală atunci când există indici cu privire la săvârșirea unei infracțiuni, respectând prevederile legale în domeniu.

Secţiunea 4
Monitorizarea măsurilor stabilite

71. Agenția monitorizează implementarea măsurilor stabilite pentru remedierea deficiențelor și îmbunătățirea activităților furnizorului de servicii, constatate în procesul de efectuare a controlului și incluse în anexă la procesul-verbal.

72. Nivelul de realizare a implementării măsurilor pentru remedierea deficiențelor și îmbunătățirea activităților furnizorului de servicii se comunică Agenției în conformitate cu termenii stabiliți în anexa la procesul-verbal.

73. În cazul în care anumite măsuri prevăzute în anexa la procesul-verbal nu pot fi realizate în termen, furnizorul de servicii solicită Agenției extinderea termenului de realizare.

74. Decizia cu privire la extinderea termenului de realizare a măsurilor prevăzute în anexa la procesul-verbal se aprobă de Directorul Agenției.

75. Verificarea nivelului de realizare a măsurilor se realizează prin evaluarea rapoartelor transmise de furnizorul de servicii public Agenției la solicitarea acesteia sau periodic conform termenelor stabilite în anexa la procesul-verbal.

Nota de fundamentare
la proiectul hotărârii Guvernului pentru aprobarea Regulamentului cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice

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

Proiectul hotărârii Guvernului este elaborat de către Ministerul Dezvoltării Economice și Digitalizării, în calitate de autoritate a administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice.

2. Condițiile ce au impus elaborarea proiectului actului normativ

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

Temeiul legal al elaborării și adoptării proiectului de act normativ îl constituie prevederile art. 18 alin. (3) și art. 19 alin. (5) din Legea nr. 48/2023 privind securitatea cibernetică (în continuare – Legea nr. 48/2023). Aceste norme stabilesc în competența Guvernului reglementarea:

- măsurilor de supraveghere și a modului de aplicare a acestora, și
- modului de efectuare a controlului de stat de către autoritatea competentă asupra respectării obligațiilor ce le revin acestora conform Legii nr. 48/2023 separat pentru furnizorii de servicii persoane juridice de drept privat și pentru furnizorii de servicii persoane juridice de drept public.

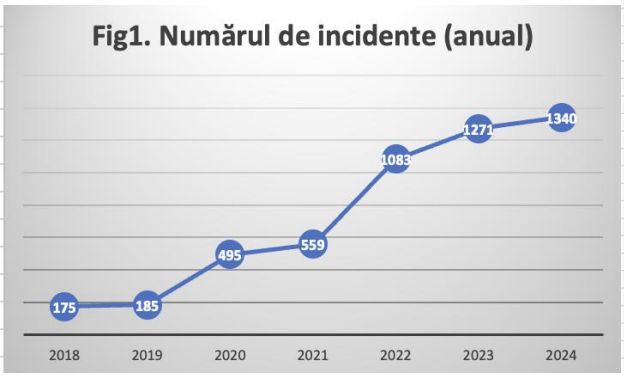
Elaborarea proiectului de act normativ propus spre examinare este prevăzută și de următoarele documente strategice ale Republicii Moldova:

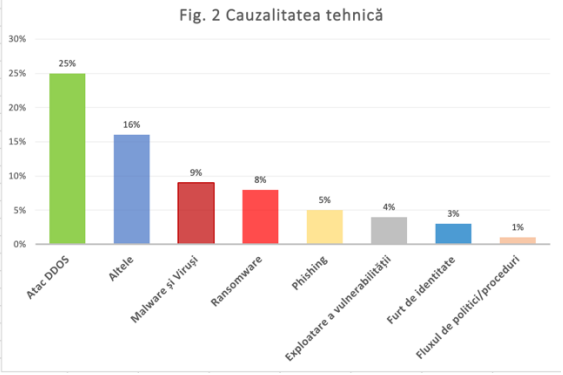
- Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029 (Hotărârea Guvernului nr. 306/2025) - punctul 53, proiectul nr. 38 din Capitolul 10 „Societatea informațională și mass-media" al Clusterului 3 „Competitivitate și creștere incluzivă";
- Agenda de reforme aferentă Planului de creștere al Republicii Moldova pentru 2025-2027 (Hotărârea Guvernului nr. 260/2025) - măsura 2.3.11, indicatorul (v) „delimitarea clară și transparentă a competențelor instituțiilor de securitate cibernetică ale MD, cu ajustarea mandatelor instituțiilor relevante în urma unei note a unui expert.";
- Foaia de parcurs privind „Statul de drept" (criteriu de referință în procesul de aderare a Republicii Moldova la Uniunea Europeană) (Hotărârea Guvernului nr. 275/2025) – acț. 4.1 și 4.3 din Rezultatul strategic nr. 4. „Consolidarea capacității de prevenire și combatere a criminalității cibernetice";
- Planul național de reglementări pentru anul 2025 (Hotărârea Guvernului nr. 841/2024) – acțiunea 18;
- Strategia de transformare digitală a Republicii Moldova (Hotărârea Guvernului nr. 650/2023) - Obiectivul general nr. 5. „Crearea unui mediu digital accesibil, sigur și incluziv direcții prioritare", direcția prioritară nr. 1) „Instituirea unei autorități competente în domeniul securității cibernetice la nivel național, cu funcții de punct unic de contact, echipă de răspuns la incidente de securitate cibernetică (CSIRT), dar și identificare, monitorizare și supraveghere, coordonare operațională a situațiilor de criză, de cooperare și interacțiune la nivel național și internațional."

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

Între 2018 și 2024, statele membre ale Uniunii Europene au raportat un total de 5108 de incidente cibernetice cu impact semnificativ[1], conform criteriilor stabilite de Directiva NIS1[2], Codul[3] european al comunicațiilor electronice și Regulamentul eIDAS[4] . Dintre acestea, 29 % au fost considerate acțiuni rău intenționate. Cel mai afectat sector a fost sectorul privat, în special domeniile comunicațiilor, bancar, sănătate, servicii de încredere, transporturi și energie.

Datele indică o tendință generală de creștere a numărului de incidente cu impact semnificativ (figura 1). Din cele 1402 de incidente rău intenționate raportate, majoritatea au fost clasificate ca infracțiuni cibernetice, conform graficului de cauzalitate tehnică prezentat în figura 2.





Sursa: Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)

Conform *raportului actualizat al IBM privind costul unei încălcări a securității datelor în 2024*[5] , impactul financiar al încălcărilor securității datelor este și mai mare pentru entitățile critice. Raportul indică faptul că, în 2024, costul mediu global al unei încălcări a securității datelor a atins un nivel record de 4,88 milioane de dolari SUA, înregistrând o creștere de 10% față de 2023

Studiul global realizat de compania McAfee[6] , care a evaluat pierderile economice cauzate de criminalitatea informatică, intitulat "Pierderi nete: estimarea costului global al criminalității informatice", oferă o estimare a impactului economic al criminalității informatice pentru diferite țări, exprimat ca procent din PIB. Graficul prezentat în figura 3 evidențiază țările cele mai grav afectate în funcție de proporția daunelor monetizate în raport cu PIB-ul lor. În medie, pierderile cauzate de criminalitatea cibernetică reprezintă aproximativ 0,3% din PIB. Extrapolând aceste date pentru Republica Moldova, având în vedere că produsul intern brut al țării a fost de aproximativ 16,5 miliarde de dolari americani în 2023, se poate estima un prejudiciu anual potențial de aproximativ 49 de milioane de dolari, pe baza mediei de 0,3% din PIB.

---

[1] https://ciras.enisa.europa.eu/ciras-consolidated-reporting

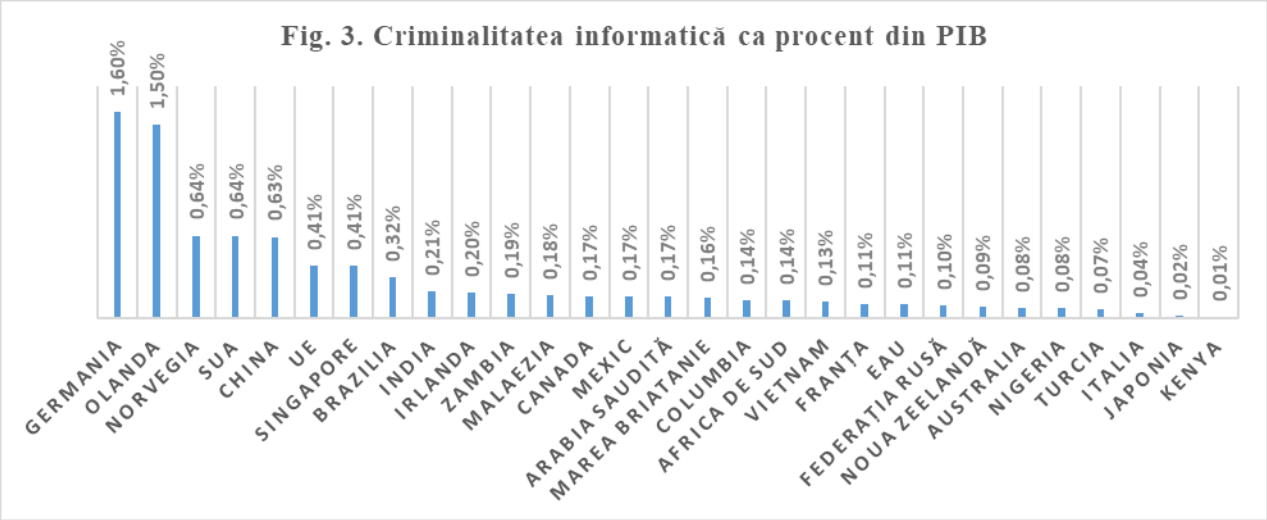
[2] Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32016L1148

[3] Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:02018L1972-20241018

[4] Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:02014R0910-20241018

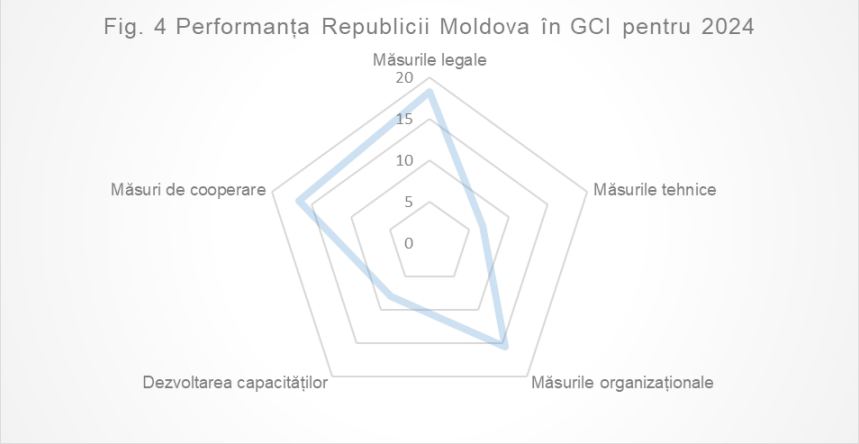
[5] https://www.ibm.com/reports/data-breach

[6] https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis



Sursa: Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)

Conform Indicelui Global de Securitate Cibernetică (GCI) al UIT pentru 2024, Republica Moldova are un scor general de 65,09, iar performanța țării este descrisă ca fiind de nivel 3 (nivelul 3 reprezintă țările care au obținut un scor general de cel puțin 55/100), demonstrând un angajament de bază în materie de securitate cibernetică, care include evaluarea, stabilirea sau implementarea anumitor măsuri de securitate cibernetică general acceptate, pe un număr moderat de piloni sau indicatori. Conform raportului UIT privind echipa națională de răspuns la incidente de securitate cibernetică, performanța Republicii Moldova pentru 2024, comparativ cu 2020, a înregistrat o creștere a măsurilor legale, organizaționale și de cooperare, însă o scădere notabilă a măsurilor tehnice și de dezvoltare a capacităților, dar acest lucru poate fi atribuit parțial ajustărilor metodologice și ponderilor GCI, precum și modificărilor aduse întrebărilor. Graficul de mai jos (Figura 4) evidențiază performanța Republicii Moldova în GCI pentru 2024, subliniind că măsurile tehnice și consolidarea capacităților sunt punctele slabe ale Republicii Moldova în acest domeniu. Cu toate acestea, acest indice poate fi îmbunătățit prin implementarea corespunzătoare a legislației naționale armonizate cu legislația UE.



Industria IT în Republica Moldova se dezvoltă rapid. În 2023, industria IT a atins o pondere de peste 5,3% din produsul intern brut, depășind 15 miliarde de lei în vânzări, ponderea sectorului TIC este de peste 8,3% din PIB, cu peste 25 de miliarde de lei în vânzări în 2023, realizate de aproximativ 3 200 de companii cu peste 35 000 de angajați. Creșterea în sectorul IT a fost generată de avantajele pe care Moldova le oferă ca destinație pentru externalizarea serviciilor IT, beneficiind de costuri competitive, amplasare geografică favorabilă și calificări ale forței de muncă, alături de un cadru fiscal și

administrativ facil pentru rezidenții Parcului IT Virtual Moldova. Rapoartele globale referitoare la digitalizare (cum ar fi Indicele UN DESA e-Guvernare, Indicele de Dezvoltare în Rețea NRI, Indicele Țării Digitale etc.), rapoartele emise de ANRCETI și sondajele anuale efectuate de Agenția de Guvernare Electronică (AGE) confirmă progresele semnificative ale Republicii Moldova în privința accesului la internet și utilizarea dispozitivelor IT, precum și dezvoltarea platformelor de e-guvernare.
Cu toate acestea, avansul rapid al tehnologiei informației și comunicațiilor electronice și al proceselor de transformare digitală, deși aduce beneficii incontestabile în diverse domenii, este însoțit de o creștere semnificativă și continuă a amenințărilor la adresa securității cibernetice. Reieșind din acestea, securitatea cibernetică a fost declarată ca fiind o prioritate la nivel național, acest aspect fiind reflectat într-un set de documente de politici, cum ar fi:

- ***Programul național de aderare a Republicii Moldova la Uniunea Europeană*** **pentru perioada 2025-2029**[7] acordă prioritate punerii în aplicare a Legii 48/2023 privind securitatea cibernetică, în special identificării furnizorilor de servicii critice și punerii în aplicare a cerințelor de securitate pentru rețele și sisteme informatice, precum și operaționalizării complete a Agenției pentru Securitate Cibernetică. Hotărârea Guvernului nr. 562/2025 „Cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice", care include în obiectul său de reglementare și cerințele de securitate pentru rețele și sisteme informatice, este în proces de promovare, urmând în timpul apropiat să fie supus examinării de către Guvern. Aceasta determină necesitatea consolidării capacităților furnizorilor de servicii din sectoarele critice, deoarece aceștia au nevoie de formare în ceea ce privește modul de punere în aplicare a cerințelor de securitate cibernetică și de respectare a cadrului normativ în domeniu.
- ***Strategia de transformare digitală a Republicii Moldova pentru anii 2023-2030***[8]***:*** unul dintre obiectivele acesteia este crearea unui mediu digital accesibil, sigur și incluziv, având ca scop asigurarea unei creșteri a nivelului de reziliență cibernetică a entităților-cheie din Republica Moldova. Aceste entități urmează fi gestionate mult mai eficient și transparent, iar incidentele cibernetice, precum și eventualele prejudicii materiale și reputaționale asociate acestora, vor fi evitate. În același timp, se urmărește implementarea unei abordări multidisciplinare, iar toate părțile interesate, inclusiv Guvernul, sectorul privat și societatea civilă, își vor asuma responsabilitatea și angajamentul comun pentru susținerea și cooperarea în asigurarea securității cibernetice.
- ***Strategia securității naționale a Republicii Moldova***[9], care evidențiază riscurile cibernetice la care este expusă Republica Moldova, subliniind în principal atacurile cinetice sau cibernetice lansate de actori statali externi asupra infrastructurii critice naționale și regionale, atacurile cibernetice lansate asupra instituțiilor publice sau private de către structuri specializate în criminalitatea cibernetică, precum și riscurile asociate evoluțiilor din domeniul tehnologiilor precum blockchain și criptomonede, inteligența artificială, învățarea automată, internetul obiectelor, tehnologia 5G, big data, tehnologiile cuantice, internetul ascuns.

La data de 16 martie 2023, Parlamentul a adoptat Legea nr. 48/2023 privind securitatea cibernetică, care a intrat în vigoare la data de 1 ianuarie 2025. Legea are ca obiectiv general să asigure legalitatea în spațiul cibernetic prin reglementarea principalelor elemente indispensabile implementării unui model de guvernanță eficient la nivel național în vederea protecției și asigurării securității rețelelor și sistemelor informatice, utilizate de către persoanele juridice, publice sau private, în procesul de prestare a serviciilor considerate a fi esențiale pentru susținerea unor activități societale și economice critice. Un

[7] https://www.legis.md/cautare/getResults?doc_id=148720&lang=ro
[8] https://www.legis.md/cautare/getResults?doc_id=139408&lang=ro
[9] https://www.legis.md/cautare/getResults?doc_id=141253&lang=ro

instrument juridic esențial asumat în procesul reglementării acestui domeniu a constituit legislația Uniunii Europene, inclusiv în contextul obținerii de către Republica Moldova a statutului de țară candidat la aderarea la Uniunea Europeană, prin Legea respectivă asigurându-se, deși doar parțial, armonizarea cadrului normativ național la prevederile Directivei NIS2[10] și, implicit, a unor elemente esențiale ale Directivei NIS1[11].

Astfel, Legea privind securitatea cibernetică cuprinde un set de reglementări care au ca scop în principal:

a) stabilirea cadrului general privind cooperarea și coordonarea strategică la nivel național și internațional, prin reglementarea expresă a constituirii unui consiliul coordonator cu rol consultativ al Guvernului, dedicat exclusiv domeniului securității cibernetice și stabilirea obligativității adoptării unei strategii naționale în acest domeniu;

b) desemnarea/instituirea de către Guvern a unei autorități competente în domeniul securității cibernetice la nivel național, care să includă în competența sa, de rând cu funcțiile de coordonare, cooperare internă, supraveghere și control de stat, și pe cele de echipă națională de răspuns la incidentele cibernetice și de punct unic de contact la nivel național;

c) reglementarea legală primară a procesului de coordonare și gestionare a crizelor în domeniul securității cibernetice și atribuirea competenței legale în această materie viitoarei autorități responsabile;

d) stabilirea cadrului legal primar în ce privește obligațiile de asigurare a securității cibernetice nu doar de către persoanele juridice de drept public, ci și de către cele de drept privat, în mod special în ceea ce privește obligațiile de implementare a măsurilor de securitate și în ceea ce privește obligațiile de notificare a incidentelor cibernetice semnificative, și împuternicirea autorității competente la nivel național în acest domeniu cu exercitarea funcțiilor de supraveghere și control de stat al modului în care persoanele vizate îndeplinesc aceste obligații;

e) determinarea cadrului normativ primar pentru identificarea persoanelor juridice ca fiind furnizori de servicii esențiale, împuternicire atribuită, de asemenea, autorității respective, ca parte componentă a funcției de supraveghere etc.

Totuși, Legea nr. 48/2023 privind securitatea cibernetică stabilește doar cadrul normativ primar în domeniul securității cibernetice, pentru punerea în aplicare a acesteia fiind necesară aprobarea unor acte normative, în mod specific, la nivelul Guvernului. O parte importantă a chestiunilor abordate în lege, reglementarea cărora a fost dată în competența Guvernului, a fost deja soluționată prin aprobarea următoarelor acte normative:

- ***Hotărârea Guvernului nr. 1028/2023*** cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică;
- ***Hotărârea Guvernului nr. 333/2024*** cu privire la instituirea, organizarea și funcționarea Consiliului coordonator în domeniul securității cibernetice;
- ***Hotărârea Guvernului nr. 860/2024*** cu privire la identificarea furnizorilor de servicii;
- ***Hotărârea Guvernului nr. 112/2025*** pentru modificarea unor hotărâri ale Guvernului (*modificarea actelor normative subsidiare în conformitate cu Legea nr.48/2023 privind securitatea cibernetică și legile conexe*)
- ***Hotărârea Guvernului nr. 562/2025*** cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice.

[10] ***Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului*** din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148;

[11] ***Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului*** din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune;

Proiectul de act normativ propus nu este generat ca urmare a identificării unei probleme noi, ci este o măsură care asigură implementarea prevederilor Legii nr. 48/2023 privind securitatea cibernetică și actele normative aprobate pentru punerea acesteia în aplicare. **Problema principală** care urmează a fi soluționată prin inițiativa propusă, astfel cum a fost identificată în analiza de impact aferentă proiectului de lege, ulterior aprobat prin Legea nr. 48/2023 privind securitatea cibernetică, constă în nivelul general insuficient de protecție împotriva incidentelor, riscurilor și amenințărilor ce vizează securitatea rețelelor și a sistemelor informatice. Această deficiență poate compromite buna funcționare a administrației publice centrale și locale, în special în ceea ce privește prestarea serviciilor publice, precum și activitatea economică a întreprinderilor din sectorul privat, afectând în consecință întreaga economie națională și, implicit, viața socială.

Categoria de subiecți interesați în intervenția propusă poate fi grupată în următoarele categorii:

1. ***Guvernul și Ministerul Dezvoltării Economice și Digitalizării, în calitatea sa de autoritate a administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice*** – din perspectiva, pe de o parte, a necesității instituirii unui mecanism instituțional și organizațional viabil de implementare a politicii de stat în domeniul securității cibernetice, în vederea asigurării rezilienței cibernetice a cercului de subiecți care cad sub incidența actului normativ, iar, pe de altă parte – necesitatea armonizării cadrului normativ național;
2. ***Persoanele juridice de drept public***, inclusiv ***autoritățile administrației publice locale*** – categorie care prin efectul legii sunt identificate ca furnizori esențiali sau importanți de servicii;
3. ***Persoanele juridice de drept privat, inclusiv întreprinderile de stat,*** care cad sub incidența prevederilor proiectului de act normativ;
4. ***Utilizatorii finali ai serviciilor*** prestate de furnizorii de servicii, esențiali sau importanți, din perspectiva interesului pe care îl au în creșterea calității serviciilor de care beneficiază, în mod special din punctul de vedere al securității și protecției datelor cu caracter personal.

Problematica descrisă mai sus are la bază o serie de cauze:

1. măsuri de securitate a rețelelor și sistemelor informatice implementate fragmentar sau chiar lipsa acestora;
2. schimbul insuficient de informații cu privire la incidente, riscuri și amenințări de securitate cibernetică în ambele sectoare, public și privat. Vulnerabilitățile și incidentele cibernetice nu sunt raportate, în principal din cauza reticenței companiilor de a dezvălui aceste informații, din temerea prejudiciilor aduse reputației sau a posibilei răspunderi.
3. cadrul instituțional, procedural și normativ-juridic incomplet.

3. Obiectivele urmărite şi soluţiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Prezentul proiect de hotărâre de Guvern va contribui la realizarea **obiectivului general al întregului cadru normativ în domeniul securității cibernetice** și anume de creștere a nivelului de reziliență cibernetică a furnizorilor de servicii, privați sau publici, asigurând un nivel ridicat de protecție a rețelelor și sistemelor informatice ale acestor furnizori utilizate în procesul de prestare de către aceștia a serviciilor esențiale.

Ca **obiective specifice** ale prezentului proiect de hotărâre de Guvern, care odată realizate vor contribui la atingerea obiectivului general enunțat mai sus, trebuie relevate următoarele:

– stabilirea unor mecanisme de evaluare a implementării cerințelor de securitate a rețelelor și sistemelor informatice pe care le dețin și le utilizează furnizorii de servicii din sectoarele critice;

– stabilirea procedurilor privind modul de exercitare de către Agenția pentru Securitate Cibernetică a funcțiilor de supraveghere și control de stat.

Proiectul de act normativ propus spre examinare are ca **obiect de reglementare** stabilirea cadrului juridic, organizatoric și procedural de exercitare de către Agenția pentru Securitate Cibernetică a

funcției de supraveghere și control de stat al modului în care furnizorii de servicii în sectoarele critice asigură conformarea cu prevederile cadrului normativ în domeniul securității cibernetice.
Domeniul de aplicare al proiectului propus spre examinare se extinde asupra tuturor furnizorilor de servicii, esențiali și importanți, care sunt sau urmează să fie identificați de Agenția pentru Securitate Cibernetică în conformitate cu prevederile Hotărârii Guvernului nr. 860/2024.
Din punct de vedere structural, proiectul include partea dispozitivă a hotărârii de Guvern și anexa.
Partea dispozitivă cuprinde decizia Guvernului de adoptare a regulamentului în speță și sarcina Ministerului Dezvoltării Economice și Digitalizării de elaborare, în comun cu Agenția pentru Securitate Cibernetică, a Metodologiei privind controlul de stat asupra activității de întreprinzător în baza analizei riscurilor aferent domeniilor de competență ale Agenției pentru Securitate Cibernetică.
Anexa cuprinde Regulamentul cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice. Acesta include patru capitole.
Capitolul I – Dispoziții generale – cuprinde prevederi care determină obiectul de reglementare al proiectului, actele legislative relevante care cuprind definițiile unor noțiuni utilizate în textul proiectului de act normativ, precum și categoria de subiecți care cad sub incidența prevederilor actului normativ. Totodată, capitolul enunță principiile specifice exercitării funcției de supraveghere și control de către Agenția pentru Securitate Cibernetică, dintre care se remarcă principiile proporționalității, eficacității și efectului de descurajare, principii expres prevăzute atât în Directiva NIS2, cât și în legislația națională în domeniul securității cibernetice.
Conform art. 25 alin. (2) lit. c) din Legea nr.98/2012 privind administrația publică centrală de specialitate, una din funcțiile de bază ale unui minister este ***funcția de supraveghere și control de stat***. Această funcție este constituită din ***două părți componente***: ***supravegherea***, definită ca fiind totalitatea acțiunilor întreprinse prin analiza continuă sau periodică a unor informații ce țin de persoanele fizice și juridice, fără a interveni în activitatea acestora, și ***controlul de stat***, definită ca verificarea respectării de către persoanele fizice și juridice a prevederilor legislației, realizate în limitele și în conformitate cu legea. Unul dintre principiile fundamentale de organizare și funcționare a administrației publice centrale de specialitate este ***delimitarea funcțiilor de elaborare și de promovare a politicilor de funcțiile de implementare a acestora,*** prevăzut la art. 4 pct. 1) lit. c) din nr.98/2012. În baza acestui principiu, pus în aplicare și prin prevederile art. 14 din Legea nr. 98/2012, funcția de supraveghere și control de stat a fost atribuită prin Legea nr. 48/2023 cu privire la securitatea cibernetică Agenției pentru Securitate Cibernetică. ***Conceptul propus în proiect*** urmează această abordare, delimitând reglementările care vizează supravegherea și controlul de stat în capitole separate. Aceasta este motivat de faptul că supravegherea este diferită de controlul de stat atât prin compoziția sa materială, cât și din punct de vedere a problematicii procedurale pe care o implică. De asemenea, supravegherea diferă de controlul de stat atât prin obiectivele pe care le urmărește și mijloacele pe care le folosește, cât și prin intensitatea și consistența intervenției autorității publice în exercitarea acestei subfuncții. Un alt aspect important al conceptului propus în proiect derivă din prevederile art. 19 alin. (5) din Legea nr. 48/2023, care deleagă Guvernului reglementarea modului de efectuare a controlului de stat de către ASC, însă separat pentru persoanele juridice de drept public și, respectiv, pentru persoanele juridice de drept privat. Această separare este determinată de domeniul de aplicare a Legii nr. 131/2012 privind controlul de stat. Potrivit art. 1 controlul se extinde doar asupra controlului de stat al activității de întreprinzător. Acțiunea legii respective poate fi extinsă și asupra controlului persoanelor care nu practică activitatea de întreprinzător doar dacă legile speciale fac referință la Legea nr. 131/2012. Potrivit prevederilor art. 19 alin. (1) din Legea nr. 48/2023, Agenția pentru Securitate Cibernetică exercită controlul de stat asupra respectării legii de către furnizorii de servicii persoane juridice de drept privat, aplicând prevederile Legii nr.131/2012 privind controlul de stat.

Prevederea punctului 5 este determinată de necesitatea asigurării complementarității dintre cadrul strategic și operațional din domeniul securității cibernetice cu cel din domeniul protecției fizice a infrastructurii critice din perspectiva exercitării funcției de supraveghere și control de stat. Cadrul strategic și operațional în domeniul protecției fizice a infrastructurii critice este reglementat prin Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale. Legea nr. 48/2023 privind securitatea cibernetică și Legea nr. 223/2025 sunt acte ce asigură armonizarea cadrului normativ național la Directiva (UE) 2022/2555 [12] și, respectiv, la Directiva (UE) 2022/2557 [13]. Complementaritatea acestor două directive și, implicit, a legilor naționale menționate mai sus, constă în necesitatea asigurării unei cooperări și unui schimb de informații între autoritățile competente în temeiul acestor cadre legislative, *„în special în ceea ce privește identificarea entităților critice, a riscurilor, a amenințărilor cibernetice și a incidentelor, precum și în legătură cu riscurile, amenințările și incidentele de altă natură decât cibernetică ce afectează entitățile critice, inclusiv măsurile în materie de securitate cibernetică și măsurile fizice adoptate de entitățile critice precum și* ***rezultatele activităților de supraveghere*** *desfășurate în legătură cu astfel de entități. În plus, pentru a raționaliza activitățile de supraveghere între autoritățile competente (n.n. – din ambele domenii de activitate) ... și pentru a reduce la minimum sarcina administrativă pentru entitățile în cauză, autoritățile competente ar trebui să depună eforturi pentru a armoniza modelele de notificare a incidentelor și* ***procesele de supraveghere****. După caz, autoritățile competente în temeiul Directivei (UE) 2022/2557 ar trebui să poată solicita autorităților competente în temeiul prezentei directive să își exercite competențele de supraveghere și de asigurare a respectării legii în legătură cu o entitate care este identificată drept o entitate critică în temeiul Directivei (UE) 2022/2557. Autoritățile competente în temeiul prezentei directive și cele competente în temeiul Directivei (UE) 2022/2557 ar trebui, atunci când este posibil în timp real, să coopereze și să facă schimb de informații în acest scop."*[14]

În **Capitolul II –** ***Supravegherea respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice*** **–** sunt reglementate aspecte privind modul de supraveghere asupra respectării cadrului normativ în domeniul securității cibernetice de către toți furnizorii de servicii în sectoarele critice: atât de către cei care sunt persoane juridice de drept public, cât și de către cei care sunt persoane juridice de drept privat. În capitol sunt enumerate măsurile de supraveghere pe care ASC urmează să le realizeze în exercitarea acestei funcții și limitele și principalele caracteristici ale acestora. Conform proiectului, măsurile de supraveghere urmează a fi aplicate în baza rezultatelor evaluării riscurilor în domeniul securității cibernetice la nivel național, intersectorial, sectorial, subsectorial, precum și atunci când este relevant, în baza evaluărilor de riscuri în alte domenii, iar scopul acestora este să asigure facilitarea conformării, consolidarea capacităților și creșterea nivelului de reziliență cibernetică a furnizorilor de servicii.

Capitolul III - ***Controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către persoanele juridice de drept privat, identificate ca furnizori de servicii în sectoarele critice*** – reglementează procedura controlului de stat în privința furnizorilor de servicii în sectoarele critice, care sunt persoane juridice de drept privat, principiile și procedura stabilită de prevederile Legii nr. 131/2012 privind controlul de stat fiind aplicate corespunzător.

[12] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555

[13] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2557

[14] Recitalul 33 din Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2).

În **Capitolul IV -** ***Controlul de stat al respectării cadrului normativ în domeniul securității cibernetice de către persoanele juridice de drept public, identificate ca furnizori de servicii în sectoarele critice*** **–** sunt reglementate aspecte privind activitatea desfășurată de către ASC în exercitarea funcției de control de stat asupra furnizorilor de servicii din sectorul public. Capitolul cuprinde prevederi privind planificarea controlului, pregătirea și realizarea controlului, etapa finalizării acestuia și monitorizarea măsurilor stabilite. Având în vedere faptul că prevederile Legii 131/2012 privind controlul de stat nu se răsfrâng asupra entităților din sectorul public, capitolul descrie o procedură separată pentru aceste entități și simplificată, într-o anumită măsură, din perspectiva faptului că entitățile din sectorul public, nepracticând activitate de întreprinzător nu pot beneficia de întregul spectru de garanții oferite de Legea respectivă mediului privat. Din contra aceste entități poartă o responsabilitate sporită dat fiind interesul public pe care îl protejează și în realizarea căruia își desfășoară activitatea administrativă. Cu toate acestea, procedura propusă păstrează garanții legate de continuitatea activității furnizorului de servicii, documentarea procesului, planificarea activității de control, etc.

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

Opțiunile alternative nu au fost luate în considerare deoarece la nivel de lege este stabilită obligația Guvernului de a aproba cerințe privind măsurile de securitate a rețelelor și sistemelor informatice ale furnizorilor de servicii.

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Proiectul de act normativ nu implică impacturi structurale și instituționale asupra sistemului administrației publice, inclusiv acțiuni de reformă structurală sau instituțională.

4.2. Impactul financiar și argumentarea costurilor estimative

Impactul financiar direct al proiectului asupra mediului de afaceri este reprezentat de costurile administrative ce urmează a fi suportate de către agenții economici. În vederea estimării costurilor administrative pe care agenții economici trebuie să le suporte pentru a se conforma obligațiilor informaționale impuse prin prezentul proiect de hotărâre de Guvern este utilizată Metodologia de estimare a costurilor administrative prin aplicarea Modelului Costului Standard aprobată prin Hotărârea Guvernului nr. 307/2016.

Astfel, în sensul Metodologiei menționate supra, obligația informațională generată pentru agenții economici de noile prevederi normative, în calitatea lor de furnizorii de servicii, este participarea la realizarea controlului de către Agenția pentru Securitate Cibernetică.

În continuare se prezintă potențialul cost administrativ care l-ar putea suporta un agent economic supus controlului, respectând formula dată de Metodologia de estimare a costurilor administrative prin aplicarea Modelului Costului Standard, aprobată prin Hotărârea Guvernului nr. 307/2016:

Acte normative	Autorități implicate	Descrierea obligației informaționale	Activități administrative	Timp, ore	Tarif, lei/oră	Preț, lei	Achiziții, lei	**Preț total, lei**	Numărul de agenți economici	Frecvența, număr pe an	**Cantitate, număr pe an**	**Costuri administrative totale, lei**
1	2	3	4	5	6	7=5x6	8	**9=7+8**	10	11		
Legea nr. 48/2023 privind securitatea cibernetică (art.4)	Agenția pentru Securitate Cibernetică	Participarea la realizarea controlului de către Agenția pentru Securitate Cibernetică	Familiarizarea cu obligația informațională	6,0	105,1	630,6	0,0	**630,6**			**630,6**	**630,6**
			Asistarea în procesul de efectuare a controlului	64,0	105,1	6726,4	0,0	**6726,4**			**6726.4**	**6726,4**
			Prezentarea informațiilor pe marginea	10,0	105,1	1051	0,0	**1051**			**1051**	**1051**

			procesului verbal de control									
			TOTAL									**8408,0**

Aceleași estimări urmează a fi aplicate și evaluării impactului financiar asupra sectorului public din perspectiva obligațiilor pe care furnizorii de servicii din acest sector urmează să le realizeze.
Totodată, evidențiem că activitatea ASC în exercitarea funcției de supraveghere și control de stat în domeniul securității cibernetice urmează a se efectua în limita mijloacelor financiare aprobate acestei autorități în bugetul de stat.

4.3. Impactul asupra sectorului privat

Sub aspectul impacturilor non-financiare asupra sectorului privat ținem să relevăm în mod special că proiectul de act normativ propus spre examinare va contribui la:
- Consolidarea rezilienței și securității cibernetice: Soluția propusă va contribui la consolidarea securității cibernetice prin detectarea și blocarea eficientă a atacurilor, protejând datele și informațiile sensibile și asigurând reacții rapide;
- Protecția informațiilor și a drepturilor utilizatorilor: Implementarea soluției va spori protecția informațiilor personale și a drepturilor utilizatorilor, prevenind accesul neautorizat și utilizarea abuzivă a datelor; Reducerea costurilor asociate incidentelor cibernetice: Soluția va reduce riscurile, impactul și costurile financiare legate de incidentele cibernetice, cum ar fi pierderile de date și daunele reputației sau perturbarea serviciilor, economisind astfel resursele necesare pentru recuperare și remediere;
- Siguranța infrastructurii critice: Soluția va proteja infrastructura critică, cum ar fi rețelele energetice, sistemul bancar și transportul, reducând riscul de întreruperi majore și asigurând continuitatea serviciilor vitale;
- Îmbunătățirea cooperării dintre autoritățile publice responsabile și furnizorii de servicii în sectorul privat în implementarea cerințelor de securitate a rețelelor și sistemelor informatice, aprobate prin Hotărârea Guvernului nr. 562/2025.

4.4. Impactul social

4.4.1. Impactul asupra datelor cu caracter personal

Din perspectiva datelor cu caracter personal, prevederile proiectului de act normativ vor avea un impact pozitiv, având în vedere că acesta are ca obiectiv ridicarea nivelului de securitate a rețelelor și sistemelor informatice ale furnizorilor de servicii esențiale.

4.4.2. Impactul asupra echității și egalității de gen

Nu este aplicabil.

4.5. Impactul asupra mediului

Nu este aplicabil.

4.6. Alte impacturi și informații relevante

Nu este aplicabil

5. Compatibilitatea proiectului actului normativ cu legislația UE

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

Nu este aplicabil.

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

Nu este aplicabil.

6. Avizarea și consultarea publică a proiectului actului normativ

În conformitate cu prevederile art. 9 din Legea nr. 239/2008 privind transparența în procesul decizional, la data de 19.05.2025 a fost publicat anunțul referitor la inițierea procesului de elaborare a proiectului

de act normativ pe pagina web oficială a Ministerului Dezvoltării Economice și Digitalizării mded.gov.md și pe platforma de consultare particip.gov.md. (https://particip.gov.md/ro/document/stages/anunt-privind-initierea-procesului-de-elaborare-a-proiectului-hotararii-de-guvern-cu-privire-la-supravegherea-si-controlul-de-stat-al-modului-in-care-furnizorii-de-servicii-respecta-prevederile-legii-nr-482023-privind-securitatea-cibernetica/14506)
Proiectul a fost plasat spre consultare publică pe pagina web oficială a Ministerului Dezvoltării Economice și Digitalizării mded.gov.md și pe platforma de consultare particip.gov.md (https://particip.gov.md/ro/document/stages/anunt-de-consultare-publica-privind-proiectul-hotararii-guvernului-cu-privire-la-supravegherea-si-co/15524).
Proiectul a fost supus avizării și consultării publice, conform prevederilor Legii nr. 100/2017 cu privire la actele normative.
Proiectul Hotărârii de Guvern a fost transmis Comisiei Europene pentru consultare la data de 11.11.2025. La data de 22.12.2025 reprezentanții DG ENEST au informat că opinia oficială urmează să fie transmisă după data de 15.01.2026 (întârziere cauzată de perioada concediilor). Totodată, s-a menționat că pentru a respecta termenul limită din Agenda de Reforme, este esențial ca Republica Moldova să aprobe proiectul Hotărîrii de Guvern în forma actuală, în timp ce ajustări suplimentare pot fi făcute ulterior în caz de necesitate, după eventualele comentarii parvenite din partea DG CNECT.

7. Concluziile expertizelor

Proiectul de act normativ a fost supus expertizei anticorupție și expertizei juridice, conform procedurii stabilite de cadrul normativ. Rezultatele examinării se regăsesc în Sinteza obiecțiilor și propunerilor.

8. Modul de încorporare a actului în cadrul normativ existent

Adoptarea și intrarea în vigoare a proiectului nu va necesita modificarea cadrului normativ existent.
Totuși, după cum este reflectat și în partea dispozitivă a hotărârii Guvernului, pentru punerea în aplicare a acestei hotărâri, Ministerul Dezvoltării Economice și Digitalizării, în comun cu Agenția pentru Securitate Cibernetică, urmează să elaboreze și să prezinte Guvernului spre examinare Metodologia privind controlul de stat asupra activității de întreprinzător în baza analizei riscurilor aferent domeniilor de competență ale Agenției pentru Securitate Cibernetică.
Perioada controlului pentru furnizorii de servicii publici și privați nu va depăși termenul prevăzut de Legea 131/2012 cu privire la controlul de stat, astfel, din momentul emiterii delegației de control, Agenția pentru Securitate Cibernetică va realiza toate acțiunile într-o perioadă de maxim 5 zile lucrătoare, cu prelungirea în caz de necesitate cu încă 5 zile lucrătoare a perioadei controlului. În acest context, vor fi respectate prevederile actului normativ superior și va fi redusă presiunea asupra furnizorilor de servicii pe parcursul efectuării acțiunilor de control.

9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

Instituția principală responsabilă de asigurarea implementării proiectului de act normativ este Agenția pentru Securitate Cibernetică. Pentru a asigura punerea în aplicare a prevederilor proiectului propus spre examinare, Agenția urmează:
- să finalizeze operaționalizarea în volum deplin a subdiviziunii responsabile de supraveghere și control;
- să aprobe ghiduri și orientări metodologice privind implementarea măsurilor de securitate a rețelelor și a sistemelor informatice ale furnizorilor de servicii în sectoarele critice;
- să efectueze evaluări ale riscurilor la nivel național, sectorial, subsectorial și în baza rezultatelor acestora să planifice activitățile de supraveghere și control de stat;
- să acorde suport consultativ furnizorilor de servicii, precum și să întreprindă alte acțiuni menite să faciliteze conformarea furnizorilor de servicii în sectoarele critice cu prevederile cadrului normativ în materie de securitate cibernetică, în mod special cu cerințele de securitate a rețelelor și sistemelor informatice ale acestora;

- să evalueze nivelul de conformare a furnizorilor de servicii în sectoarele critice cu cerințele cadrului normativ în domeniul securității cibernetice.

Totodată, sub aspectul sancțiunilor care urmează a fi aplicate, va fi necesară modificarea Codului contravențional sub aspectul conferirii calității de Agent constatator pentru Agenția pentru Securitate Cibernetică și completarea părții speciale a Codului contravențional cu contravenții specifice în domeniul securității cibernetice precum neasigurarea măsurilor minime de securitate impuse prin Hotărîrea Guvernului 562/2025, neprezentarea rapoartelor de audit în termenele specificate de 12 luni și 18 luni urmare a arpobării hotărîrii anterior menționate, precum și alte contravenții fără de care nu va fi asigurată neimpuninatea față de nerespectarea cadrului normativ aferent securității cibernetice, ori dacă Agenția nu va impune sancțiuni în urma controalelor, există riscul ca reglementările naționale în domeniul securității cibernetice să nu fie respectate.

Astfel, pentru anul 2026, MDED și ASC vor elabora proiectul de lege corespunzător pentru modificarea Codului contravențional. Menționăm că sancțiunile pe care le prevede Directiva 2555/2022 (Directiva NIS2) sunt 2% din cifra de afaceri pentru furnizorii de servicii esențiali și 1.4% pentru furnizorii de servicii importanți.

Secretar de stat **Michelle ILIEV**

SINTEZA
obiecțiilor și propunerilor/recomandărilor la proiectul hotărârii Guvernului cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**Cancelaria de Stat**	**1.**	**Cu referire la Capitolul III din Regulamentul cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice:** **La punctul 12** se propune următoarea redacție: *„Planificarea controalelor se efectuează în baza analizei riscurilor conform prevederilor Legii nr. 131/2012 privind controlul de stat.”*.	**Precizare.** Pct. 12 reglementează aspectele generale de aplicare a prevederilor normative atunci când Agenția urmează a efectua controale la furnizorii de servicii. Astfel, pct. respectiv urmează a păstra redacția actuală, iar partea de planificare a controalelor în baza analizei riscurilor, de către Guvern urmează a fi aproba Metodologia privind controlul de stat asupra activității de întreprinzător în baza analizei riscurilor aferent domeniilor de competență ale Agenției pentru Securitate Cibernetică
		2.	**La punctul 13** se propune următoarea redacție: *„Agenția efectuează controale inopinate în cazul în care constată și confirmă, în urma unei investigații preliminare, fapte ce constituie încălcări ale prevederilor Legii nr. 48/2023 privind securitatea cibernetică și/sau atunci când este sesizată despre încălcări, neîndeplinirea sau îndeplinirea necorespunzătoare a obligațiilor stabilite prin această lege de către furnizorul de servicii privat. Controlul*	**Se acceptă**

			inopinat se inițiază în condițiile art. 19 din Legea nr. 131/2012 privind controlul de stat.”.	
		3.	**Punctul 14 urmează a fi comasat cu punctul 15** și redat în următoarea redacție: *„Controlul se efectuează în temeiul delegației de control de către cel puțin doi inspectori, luându-se în considerare și specializarea acestora conform domeniului de control aferent.”*.	**Nu se acceptă.** Considerăm relevant menținerea actualei redacții, reieșind din faptul că Angajați cu funcție de inspector nu pot avea competențe extinse în toate sectoarele critice. Astfel, se propune ca la necesitate inspectorii din cadrul Agenției să poată antrena și specialiști pe domeniu în efectuarea controlului, iar redacția propusă ar îngrădi cercul de subiecți, limitându-se doar la inspectori.
		4.	**La Punctul 16** se propune următoarea redacție: *„Agenția la efectuarea controalelor, va implica, în caz de necesitate, alte autorități și instituții publice ce nu se regăsesc în anexa Legii nr. 131/2012 privind controlul de stat, în măsura în care acestea sunt necesare la desfășurarea unor expertize, evaluări sau teste suplimentare ori dacă acestea au atribuții de implementare a legislației aferente domeniului de control în cauză.”*.	**Se acceptă.**
		5.	**La punctul 17** se propune următoarea redacție: *„Agenția aprobă planul controalelor pentru anul următor și îl publică pe site-ul său web oficial.”*.	**Se acceptă**
		6.	**La subpunctul 18.5** se propune următoarea redacție: *„În cadrul sau în urma controlului de stat, la depistarea încălcărilor, inspectorul Agenției poate înainta prescripții și recomandări, aplica măsuri restrictive și sancțiuni în limitele prevăzute de lege. Acțiunile și măsurile se selectează și se aplică în conformitate cu prevederile Legii nr. 131/2012 privind controlul de stat.”*.	**Se acceptă**

		7.	**La punctul 19** se propune următoarea redacție: *„Controlul se efectuează în temeiul delegației de control semnate de conducerea/persoana responsabilă din cadrul Agenției.”*.	**Se acceptă**
		8.	**La punctul 20** se propune următoarea redacție: *„În cazul controalelor planificate, delegația de control se notifică persoanei supuse controlului în conformitate cu art. 18 din Legea nr. 131/2012 privind controlul de stat și se întocmește în baza planului controalelor aprobat și înregistrat. În cazul controalelor inopinate, delegația de control va indica temeiul efectuării controlului, potrivit art. 19 din Legea nr. 131/2012. Pentru controalele inopinate, la delegația de control se anexează nota de motivare, pentru a permite persoanei supuse controlului să ia cunoștință de aceasta.”*.	**Se acceptă**
		9.	**Punctul 24 și 25** necesită a fi comasate într-un singur punct și redat următoarea redacție: *„**24.** În cazul în care în timpul desfășurării controlului, inspectorii constată încălcări ce conțin semne ale unei infracțiuni, aceștia consemnează în procesul-verbal de control și sesizează organele de urmărire penală cu privire la încălcările constatate, respectând procedura stabilită de Legea nr. 131/2012 privind controlul de stat.”*.	**Se acceptă**
		10.	**Punctele 29, 30, 31 și 32** urmează a fi comasate într-un singur punct și redat în următoarea redacție: *„**29.** Procedura de control se încheie prin întocmirea de către inspectori a unui proces-verbal de control în conformitate cu art. 28 din Legea nr. 131/2012 privind controlul de stat.”*.	**Se acceptă**
		11.	**Punctul 36** urmează a fi exclus pe motiv că se repetă conținutul punctului 24 din proiect.	**Se acceptă** Redacția propusă la punctele menționate supra a fost ajustată în contextul în care Agenția pentru Securitate Cibernetică a devenit organ de control și a fost inclusă în

				anexa Legii nr. 131/2012 privind controlul de stat, fiindu-i atribuite domeniile aferente controlului *„Supravegherea și controlul de stat al respectării de către furnizorii de servicii a obligațiilor privind asigurarea securității cibernetice prevăzute de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative de punere în aplicare a legii respective”*.
		12.	**Capitolul IV** urmează a fi comasat cu **Capitolul III** pentru a asigura uniformitatea terminologiei utilizate. Totodată, se propune utilizarea normelor din Legea nr. 131/2012 privind controlul de stat pentru controalele efectuate la persoanele de drept public sau privat. Or, conform art. 1 alin. (1) din Legea nr.131/2012 privind controlul de stat, *în măsura în care prevederile legilor de specialitate fac referință la prezenta lege, dispozițiile prezentei legi se aplică activității organelor de control în privința persoanelor care nu practică activitatea de întreprinzător și/sau a obiectelor utilizate de aceste persoane sau aflate în proprietatea acestora.* Legea nr. 131/2012 are caracter preponderent procedural, stabilind mecanismele și procedurile de organizare, coordonare și exercitare a controalelor de stat, aplicabile atât organelor de control, cât și persoanelor supuse controlului. Prin urmare, acest act normativ stabilește reguli clare pentru organele de control asupra planificării, inițierii, organizării și desfășurării controlului de stat.	**Nu se acceptă** Comasarea prevederilor într-un singur capitol contravine prevederilor art. 19 alin (5) din Legea nr. 48/2023 cu privire securitatea cibernetică. Astfel, Lege menționează expres că Guvernul, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice, stabilește, separat pentru furnizorii de servicii persoane juridice de drept privat și separat pentru furnizorii de servicii persoane juridice de drept public, procedurile detaliate privind modul de efectuare a controlului de stat de către autoritatea competentă asupra respectării obligațiilor ce le revin acestora conform prezentei legi.
2.	**Ministerul Apărării** *(nr. 11/1353 din 19.11.2025)*	**13.**	Lipsa obiecțiilor și propunerilor.	

3.	**Ministerul Culturii** *(nr. 05/1-09/3275 din 24.11.2025)*	**14.**	Lipsa obiecțiilor și propunerilor.	
4.	**Agenția Națională pentru Reglementare în Energetică** *(nr. 12/6541 din 24.11.2025)*	**15.**	Agenția constată că proiectul Hotărârii și Regulamentul anexat constituie un instrument necesar pentru aplicarea Legii nr. 48/2023 privind securitatea cibernetică, însă unele prevederi necesită clarificări pentru a asigura compatibilitatea intervențiilor prevăzute cu regimul de supraveghere sectorială aplicabil tuturor domeniilor reglementate de ANRE, inclusiv energie electrică, gaze naturale, energie termică, apă și canalizare, produse petroliere și alte servicii esențiale cu obligații de serviciu public.	**Se acceptă.**
		16.	Analiza proiectului relevă că Regulamentul conferă Agenției pentru Securitate Cibernetică atribuția de a dispune măsuri de restricționare a utilizării sau accesului la sistemele informatice ale furnizorilor de servicii esențiale, conform pct. 27 din Regulament. În lipsa unui mecanism de consultare prealabilă cu ANRE, aplicarea unor astfel de măsuri poate afecta continuitatea funcționării serviciilor publice în oricare dintre domeniile supuse reglementării, fie că este vorba despre rețele energetice, sistemele publice de alimentare cu apă sau procesele tehnologice aferente altor sectoare esențiale. Pentru prevenirea unor consecințe operaționale nedorite, se consideră necesară instituirea unei obligații explicite de consultare a ANRE înaintea aplicării unor măsuri excepționale în raport cu operatorii din sectoarele reglementate.	**Precizare.** Pct. 27 prevede necesitatea îndeplinirii unor condiții cumulative pentru a restricționa utilizarea unuia sau mai multe sisteme informatice sau accesul la acesta/acestea. Tot în această ordine de idei, se menționează că Agenția e obligată ca prin măsurile dispuse să nu cauzeze un prejudiciu disproporționat persoanelor afectate în procesul de contracarare a amenințării sau de eliminare a perturbării generate de incidentul cibernetic.
		17.	Totodată, proiectul stabilește un regim detaliat de supraveghere, incluzând controale planificate, conform pct. 29–31, și controale inopinate, conform pct. 32–33 din Regulament. În prezent, operatorii supuși reglementării ANRE se află deja sub incidența unui cadru extins de raportare, monitorizare și control, aplicat în funcție de	**Se acceptă.** La pct. respective le-a fost oferită o redacție nouă.

			particularitățile fiecărui sector. Lipsa unei prevederi care să asigure coordonarea controalelor ASC cu cele ale ANRE poate conduce la suprapuneri, sarcini administrative suplimentare și eventuale interferențe în procesele tehnice de operare. Considerăm necesară stabilirea unui mecanism instituțional clar de cooperare, astfel încât acțiunile de control să fie complementare.	
		18. .	În ceea ce privește planurile de remediere ce urmează a fi impuse furnizorilor, conform pct. 59 65, acestea pot genera costuri investiționale sau operaționale substanțiale pentru operatorii reglementați. Întrucât toate aceste sectoare sunt supuse reglementării tarifare sau aprobării planurilor de investiții de către ANRE, este indispensabil ca Regulamentul să prevadă obligativitatea informării ANRE ori de câte ori operatorilor din sectoarele reglementate le sunt impuse măsuri care pot influența nivelul tarifelor sau necesarul de investiții.	**Precizare.** Notificarea respectivă urmează a fi făcută de fiecare furnizor în parte, nu de către Agenție, or scopul Agenției este de a implementa politica de stat în domeniul securității cibernetice și respectiv de a supraveghea implementarea măsurilor de securitate de către furnizorii de servicii în sectoarele critice.
		19.	Referitor la regimul informațiilor sensibile, proiectul stabilește obligații de protecție, conform pct. 39–41, precum și secretizarea actelor, conform pct. 73. Având în vedere natura infrastructurilor și serviciilor reglementate de ANRE, precum și obligațiile instituției în materia supravegherii și a securității operaționale, este necesar ca Regulamentul să prevadă expres că ANRE este destinatar autorizat al informațiilor relevante referitoare la vulnerabilități, riscuri și arhitectura sistemelor, cu respectarea regimului de confidențialitate aplicabil.	**Nu se acceptă** Ca instituție de reglementare, ANRE poate solicita independent de la furnizorul de servicii informații periodice privind implementarea măsurilor de securitate. Astfel, considerăm inoportun modificarea proiectului în sensul menționat de Dvs.
		20.	De asemenea, prevederea conform căreia furnizorii de servicii public pot solicita suspendarea sau amânarea controlului atunci când acesta poate afecta continuitatea activității, conform pct. 61 lit. e), este esențială pentru toate domeniile reglementate. Pentru a asigura aplicarea uniformă și predictibilă a acestei dispoziții, ar fi oportună clarificarea procedurii de examinare a acestor solicitări.	**Nu se acceptă.** Suspendarea sau amânarea controlului nu poate fi esențială pentru toate domeniile de reglementare. Mai mult, pct. 61 se regăsește în capitul IV care reglementează procedura de control doar în sectorul public.

		21.	În ceea ce privește obligația ASC de a sesiza organele de urmărire penală în cazurile ce prezintă elementele unei infracțiuni, conform pct. 25, se consideră necesar ca Regulamentul să prevadă obligația informării ANRE atunci când un astfel de demers vizează operatori supuși reglementării, astfel încât instituția să poată evalua impactul potențial asupra obligațiilor de licență și asupra continuității serviciilor.	**Nu se acceptă.** Nu poate fi acceptată asemenea propunere, reieșind din faptul că pct. 25 face trimitere expresă cadru primar, Legea 131/2012.
		22.	În concluzie, ANRE susține adoptarea proiectului Hotărârii Guvernului, cu recomandarea de a introduce ajustările necesare consolidării coordonării interinstituționale, de a clarifica procedurile aplicabile în raport cu operatorii tuturor sectoarelor reglementate de ANRE, de a integra mecanisme adecvate de consultare privind măsurile cu impact investițional sau tarifar, precum și de a asigura accesul instituțional corespunzător la informațiile sensibile. Considerăm că aceste ajustări sunt indispensabile pentru evitarea conflictelor de competențe și pentru asigurarea unui cadru coerent de implementare a măsurilor de securitate cibernetică în toate sectoarele esențiale aflate sub reglementarea ANRE.	**Se acceptă.**
5.	**Serviciul Tehnologia Informației și Securitate Cibernetică** *(nr. 1.4/1824/25 din 24.11.2025)*	**23.**	STISC comunică următoarele obiecții la proiectul Regulamentului cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice (în continuare Regulament): 1. La pct. 1, textul „de către furnizorii de servicii în sectoarele critice a cadrului normativ în domeniul securității cibernetice” se va substitui cu textul „cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice”, în vederea adaptării la denumirea regulamentului.	**Se acceptă.**
		24.	La pct. 3, după textul *„Legii nr. 131/2012 privind controlul de stat” se va completa cu textul „în partea*	**Nu se acceptă.**

			furnizorilor de servicii persoane juridice de drept privat”. De subliniat că, potrivit art. 1 alin. (1) din Legea nr. 131/2012 privind controlul de stat, „... În măsura în care prevederile legilor de specialitate fac referință la prezenta lege, dispozițiile prezentei legi se aplică activității organelor de control în privința persoanelor care nu practică activitatea de întreprinzător și/sau a obiectelor utilizate de aceste persoane sau aflate în proprietatea acestora.”. Or, prin art. 9 alin. (1) din Legea nr. 48/2023 privind securitatea cibernetică, s-a indicat expres că „Autoritatea competentă exercită controlul de stat asupra respectării prezentei legi de către furnizorii de servicii persoane juridice de drept privat, aplicând prevederile Legii nr.131/2012 privind controlul de stat.”.	Pct.3 se referă la aspectele generale privind efectuarea controlului de stat de către Agenție. Ulterior în cuprinsul Regulamentului se detaliază procedura în parte pentru fiecare tip de furnizor de servicii. Astfel, includerea propunerii Dvs. ar crea doar confuzie în interpretare și nu o claritate la prevederile normative.
		25.	În cuprinsul pct. 4, considerăm oportun a se face trimitere inclusiv la Hotărârea Guvernului 860/2024 cu privire la identificarea furnizorilor de servicii.	**Nu se acceptă.** Hotărârea menționată este aplicabilă la identificarea furnizorilor de servicii în sectoarele critice, iar norma menționată face referire la controlul de stat asupra persoanelor identificate deja de către Agenție.
		26.	La pct. 5, autorul va specifica cine sunt 5*„autoritățile de supraveghere și control a gestionarilor de infrastructură critică națională”* sau va face trimitere la actul normativ care le instituie, întrucât redacția actuală este incertă și produce confuzii.	**Nu se acceptă.** Pct. respectiv se regăsește în dispoziții generale, iar textul normativ propus oferă o claritate suficientă, indicând expres subiecții cui se referă. Introducerea nominală a unor autorități ar crea confuzie și o posibilă omitere normativă a unei autorități de supraveghere, ceea ce ar duce la un vid legislativ.
		27.	La pct. 8, se va exclude virgula de după sintagma „competenței sale”.	**Se acceptă.**
		28.	Se va exclude pct. 18.5.	**Precizare.**

			Reieșind din prevederile Legii nr. 48/2023 și Regulamentul cu privire la organizarea și funcționarea Agenției pentru Securitate Cibernetică, aprobat prin Anexa nr. 1 la Hotărârea Guvernului nr.1028/2023, Agenția nu este învestită cu competența de constatare a contravențiilor, respectiv aplicare a sancțiunilor. În contextul acestei obiecții, se va ajusta tot cuprinsul proiectului.	Pct. respectiv i-a fost oferită o redacție nouă.
		29.	Pct. 24 se va exclude întrucât nu este clar în ce măsură sau prin prisma cărei competențe inspectorii sunt în drept să desfășoare acțiuni de conservare, solicitări de precizări și explicații de la persoanele aflate la fața locului. Or, cercetarea la fața locului se efectuează de către organul de urmărire penală în conformitatea cu prevederile Secțiunii a 3-a a Codului de procedură penală. Mai mult decât atât, legislația penală nu prevede infracțiuni aferente nerespectării cadrului normativ în domeniul securității cibernetice. Suplimentar, nici în legislația contravențională nu se regăsesc contravenții aferente nerespectării cadrului normativ în domeniul securității cibernetice.	**Se acceptă.** Pct. 24 i-a fost oferită o redacție nouă.
		30.	Pct. 27 se va expune în redacție nouă după cum urmează: *„27. Pentru a contracara o amenințare cibernetică semnificativă imediate asupra securității rețelelor și sistemelor informatice sau a atenua consecințele unui incident cibernetic cu impact semnificativ, Agenția poate restricționa utilizarea ori accesul la una sau mai multe rețele sau sisteme informatice, dacă sunt îndeplinite condițiile stabilite la art. 15 alin. (2) din Legea nr. 48/2023.”.*	**Se acceptă.**
		31.	Pentru a uniformiza terminologia utilizată, Secțiunea a 3-a a Capitolului III, după caz întreg cuprinsul proiectului, se va revizui în totalitate prin prisma articolelor corespunzătoare din Legea nr. 131/2012, întrucât în cuprinsul acesteia se operează cu noțiuni/denumiri de	**Precizare.** Conținutul proiectului de act normativ corespunde rigorilor normative, inclusiv terminologiei pentru efectuarea controlului de stat.

			documente, proceduri și termeni, nespecifice și nealiniate cu cadrul normativ în domeniul efectuării controlului de stat.	
		32.	La pct. 43, sintagma *„pagina oficială în Internet a”* se va substitui cu sintagma „site-ul web oficial al”, în vederea adaptării la terminologia utilizată de Hotărârea Guvernului nr. 728/2023 cu privire la site-urile web oficiale ale autorităților și instituțiilor publice și cerințele minime privind profilurile de socializare ale acestora.	**Se acceptă**
		33.	Cu referire la sbp. 44.3, subliniem că prin Hotărârea Guvernului nr. 562/2025 s a aprobat Regulamentul cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice, Regulament aplicabil inclusiv furnizorilor de servicii persoane juridice de drept privat. În acest context, autorul va revizui sbp. 44.3 și va completa Capitolul III cu o prevedere similară.	**Nu se acceptă.** Considerăm judicios ca prevederea respectivă să se regăsească doar pentru sectorul public.
		34.	Cu referire la „Controlul inopinat” care se regăsește doar în cuprinsul Capitolului IV, urmând a se realiza doar în cazul furnizorilor de servicii persoane juridice de drept public. Prin prisma principiului proporționalității și al principiului proporționalității controlului și oportunității la inițierea lui, cu regret se remarcă o disproporționalitate față de furnizorii de servicii persoane juridice de drept public. În acest context, autorul fie va exclude acest tip de control și prevederile aferente lui din cuprinsul Capitolului IV, fie îl va stabili și în cazul furnizorilor de servicii persoane juridice de drept privat.	**Se acceptă.** În conformitate cu prevederile Legii nr. 131/2012 pot fi efectuate atât controale planificate, cât și inopinate. Respectiv, prevederile actului normativ menționat se aplică direct la efectuarea controlului de către Agenție. În concluzie, la toți furnizorii de servicii urmează a fi efectuate controale planificate și la necesitate și inopinate în conformitate cu prevederile cadrului normativ aplicabil.
		35.	La pct. 47.5., pentru a nu admite anumite incertitudini și abuzuri, autorul va specifica cine este *„organul ierarhic superior”* și *„autoritatea publică care exercită supravegherea administrativă și controlul administrativ al furnizorului de servicii public”*, precum și cazurile	**Nu se acceptă.** Este imposibil a fi indicat nominal organul ierarhic superior, or identificarea acestuia urmează a fi

			exprese în care acestea pot solicita efectuarea controlului inopinat.	făcută individual pentru fiecare autoritate publică.
		36.	Autorul va indica în proiect termenii în *„zile”* sau *„zile lucrătoare”*. Or, conform Codului civil, prin „zile” se are în vedere „zile calendaristice”.	**Se acceptă.** Proiectul urmează a fi ajustat corespunzător.
		37.	La pct. 55, autorul va indica expres în proiectul supus avizării „modul de documentare al activității de control” sau „cadrul normativ” la care se referă. Or, potrivit alin. (5) al art. 19 al Legii nr. 48/2023, „Guvernul, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice, **stabilește,** separat pentru furnizorii de servicii persoane juridice de drept privat și **separat pentru furnizorii de servicii persoane juridice de drept public, procedurile detaliate privind modul de efectuare a controlului de stat de către autoritatea competentă asupra respectării obligațiilor ce le revin acestora conform prezentei legi”.**	**Se acceptă** Pct. respectiv se exclude din proiect.
		38.	Cu referire la punctele 59-62, se constată că autorul stabilește alte drepturi și obligații în procesului efectuării controlului la furnizorii de servicii persoane juridice de drept public, decât cele din procesul efectuării controlului la furnizorii de servicii persoane juridice de drept privat. Astfel, în spiritul principiului obiectivității și imparțialității la planificarea și desfășurarea controlului de stat, la întocmirea documentelor aferente controlului și dispunerea de măsuri, pentru a nu interpreta aceste reglementări intenționat stabilite în defavoarea furnizorilor de servicii persoane juridice de drept public, autorul va stabili aceleași drepturi și obligații pentru echipa de control și furnizorii de servicii persoane juridice de drept public și de drept privat în cadrul procesului de efectuare a controlului.	**Precizare.** Considerăm că drepturile și obligațiile sunt similare, însă unele diferențe pot apărea reieșind din specificul activității acestora.

		39.	În cuprinsul proiectului, autorul va înlătura greșelile ortografice și reduplicările accidentale, inclusiv din denumirea Capitolului II și pct. 13. De asemenea va substitui sintagma *„servicii public”* cu sintagma *„servicii publici”*.	**Se acceptă.**
6.	**Agenția Servicii Publice** *(Nr. 01/13416 din 24.11.2025)*	**40.**	Lipsa obiecțiilor și propunerilor.	
7.	**Ministerul Sănătății** *(Nr. 27/3652 din 21.11.2025)*	**41.**	Lipsa obiecțiilor și propunerilor.	
8.	**Ministerul Educației și Cercetării** *(nr. 15/17/25 din 21.11.2025)*	**42.**	Lipsa obiecțiilor și propunerilor.	
9.	**Ministerul Mediului** *(nr. 13-05/3159 din 25.11.2025)*	**43.**	Lipsa obiecțiilor și propunerilor.	
10	**Ministerul Agriculturii și Industriei Alimentare** *(nr. 21-03/3222 din 26.11.2025)*	**44.**	În opinia Ministerului, denumirea actului normativ, precum și a obiectului Regulamentului, specificat la pct. 1, nu corelează cu prevederile art. 7 alin. (3) lit. e), art. 18 alin. (3) și art. 19 alin. (5) din Legea nr. 48/2023 privind securitatea cibernetică conform cărora: autoritatea competentă (Agenția pentru Securitate Cibernetică) exercită supravegherea şi controlul respectării de către furnizorii de servicii a obligaţiilor ce le revin ***conform prezentei legi***, iar Guvernul stabilește ***măsurile de supraveghere şi modul de aplicare a acestora***, precum și ***procedurile detaliate privind modul de efectuare a controlului de stat*** asupra respectării obligaţiilor ce le revin acestora conform prezentei legi. Recomandăm să fie revizuite prevederile menționate, iar drept alternativă considerăm mai corectă următoarea formulă: a) denumirea hotărârii și a regulamentului: *„cu privire la măsurile de supraveghere și procedurile de control al*	**Precizare.** În conformitate cu prevederile art. 42 din Legea 100/2017, denumirea actului normativ trebuie să fie laconică și să exprime cu claritate obiectul de reglementare. Astfel, reieșind din temeiurile de adoptare a prezentului act normativ i-a fost oferită denumirea dată și reglementat obiectul de reglementare a-l acesteia.

			respectării obligațiilor furnizorilor de servicii, conform Legii nr. 48/2023 privind securitatea cibernetică”; b) obiectul regulamentului: *„Prezentul Regulament stabileşte măsurile de supraveghere, modul de aplicare a acestora și procedurile detaliate de control al respectării obligațiilor ce revin furnizorilor de servicii, în conformitate cu prevederile Legii nr. 48/2023 privind securitatea cibernetică”*. Această formulare este concisă, tehnică și respectă cerințele de corelare a actului normativ secundar față de legea cadru.	
		45.	În anexă: la pct. 4 în care este stipulat că: *„La solicitarea unei autorități de supraveghere și control a gestionarilor* de infrastructură critică națională, Agenția efectuează un *control inopinat al furnizorului de servicii în cauză* și *informează autoritatea de supraveghere și control de stat* în sectorul corespunzător despre încălcările constatate într-un termen care nu depășește 5 zile calendaristice de la data finalizării controlului.”, se observă că, în Legea nr. 48/2023 se utilizează noțiunile de *„operator al infrastructurii critice”* – art. 3 alin. (2) lit. h), *„operatori care au în gestiune obiective ale infrastructurii critice”* – art. 4 alin. (3), care pot fi și furnizori de servicii. Totodată, potrivit art. 19 alin. (1) și (21) din Legea nr. 131/2012 privind controlul de stat, controalele inopinate pot fi efectuate, în baza evaluării riscurilor, din oficiu de către organul de control sau să fie inițiate în temeiul unor petiții, sesizări sau solicitări ale organelor de drept sau ale altor organe de stat. În contextul prevederilor legale menționate, se va completa textul pct. 4 sau nota de fundamentare cu precizări relevante pentru conformarea la cadrul legal.	**Se acceptă.** A fost completată nota de fundamentare corespunzător.

		46.	la pct. 9, textul propus: *„În cazul în care pe parcursul desfășurării activității de supraveghere se constată săvârșirea unor fapte care întrunesc elemente constitutive ale unor contravenții sau infracțiuni, Agenția implică la necesitate, autoritățile competente.”*, vă atragem atenția că Agenția nu are atribuții de constatare a faptelor ce întrunesc elementele constitutive ale contravențiilor sau infracțiunilor, această competență revenind exclusiv organelor abilitate prin lege. De asemenea, organele competente nu pot fi *„implicate”* la discreția Agenției, ci doar sesizate, urmând ca acestea să decidă asupra măsurilor legale. În consecință, pentru conformitate cu cadrul normativ, se recomandă reformularea astfel: *„În cazul în care pe parcursul desfășurării activității de supraveghere se constată săvârșirea unor fapte care pot întruni elemente constitutive ale unor contravenții sau infracțiuni, Agenția sesizează autoritățile competente.”*.	**Se acceptă**
		47.	la subpct. 18.5, textul *„dispune, după caz, de aplicarea de sancțiuni prevăzute de cadrul normativ în vigoare.”* se va redacta pentru a nu genera aparență de contradicție cu prevederile art. 7 din Legea nr. 48/2023 și pct. 6-9 Regulamentul cu privire la organizarea şi funcţionarea Agenţiei pentru Securitate Cibernetică, aprobat prin Hotărârea Guvernului 1028/2023, care reglementează funcțiile, atribuțiile și drepturile Agenției, precum și cu prevederile Codul contravențional în care Agenția nu se regăsește ca agent constatator. Având în vedere că în virtutea calității de autoritate publică, Agenția emite acte administrative, sunt relevante prevederile art. 11 alin. (1) lit. a) din Codul administrativ: *„actele administrative individuale defavorabile sunt actele* care impun destinatarilor lor obligaţii, sancţiuni, sarcini sau afectează drepturile/interesele legitime ale persoanelor ori care resping, în tot sau în parte, acordarea	**Se acceptă.** Pct. respectiv urmează a avea o redacție nouă.

			avantajului solicitat.”. În același timp, în conformitate cu art. 179 din Codul administrativ, o obligaţie bazată pe un act administrativ individual (…) îndreptată spre predarea unui bun, spre realizarea unei alte acţiuni, spre tolerare sau inacţiune, poate fi realizată prin următoarele măsuri coercitive: realizarea prin substituire, *amenda de constrîngere* şi exercitarea nemijlocită a constrîngerii (constrîngerea directă). Subpct. 18.5 ar putea fi formulat astfel: *„18.5. dispune, după caz, de aplicarea măsurilor coercitive în conformitate cu Codul administrativ.”*	
11	**Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informație** *(nr. 01-DRA din 24.11.2025)*	**48.**	La pct. 27 din proiectul hotărârii de Guvern, prevede: "Restricționarea accesului la sistemele informatice (intervenție la incident cibernetic)", respectiv, aceste prevederi introduce în proiectul de Regulament introduce drepturi foarte intruzive (restricționare în utilizarea unuia sau mai multe sisteme informatice sau accesul la acesta/acestea), aceste drepturi care nu sunt prevăzute clar în Legea nr. 131/2012, dar care ipotetic ar putea ridica probleme de legalitate și protecție a drepturilor (*ex.: dreptul la proprietate, continuitatea afacerii, protecţia datelor, etc*);	**Precizare** Pct. 27 prevede necesitatea îndeplinirii unor condiții cumulative pentru a restricționa utilizarea unuia sau mai multe sisteme informatice sau accesul la acesta/acestea. Tot în această ordine de idei, se menționează că Agenția e obligată ca prin măsurile dispuse să nu cauzeze un prejudiciu disproporționat persoanelor afectate în procesul de contracarare a amenințării sau de eliminare a perturbării generate de incidentul cibernetic.
		49.	La pct, 43 din proiectul hotărîrii de Guvern, textul se completează cu următorul conținut după cum urmează: *"...și se înregistrează în Registrul de stat al controalelor în termenul stabilit"*;	**Se acceptă**
		50.	La pct. 48 din proiectul hotărîrii de Guvem, textul se modifică cu următorul conținut după cum urmează: *"Controlul inopinat se motivează. Nota de motivare se anexează la delegația de control și se înregistrează în Registrul de stat al controalelor în modul stabilit"*;	**Se acceptă**

		51.	La pct. 52 din proiectul hotărîrii de Guvem, textul: *„5 zile înaintea începerii acestuia”* se substituie cu textul: *„5 zile lucrătoare înaintea începerii acestuia”*;	**Se acceptă**
		52.	La pct. 67 din proiectul hotărîrii de Guvern, se completează cu un subpunct nou cu următorul conținut după cum urmează: *"Procesul-verbal de control include obligatoriu explicații și/sau obiecțiile furnizorului în privința măsurilor restrictive prescrise, anexate integral la proces"*;	**Se acceptă.** Urmează a fi completat cu un subpunct nou în următoarea redacție. *„Procesul-verbal de control include explicații și/sau obiecțiile furnizorului de servicii”*
		53.	Se propune în proiectul hotărîrii de Guvern de a reglementa aspectele privind activitatea desfășurată de către Agenția pentru Securitate Cibemetică (ASC) în exercitarea funcției de control de stat asupra *furnizorilor* de servicii din *sectorul public*;	**Se acceptă.** Capitolul IV reglementează procedura de control în asupra furnizorilor de servicii din sectorul public, inclusiv și drepturile și obligațiile Agenției în procesul desfășurării controlului.
		54.	În proiectul hotărîrii de Guvern autorul afirmă că prevederile Legii nr. 131/2012 privind controlul de stat *nu se răsfrînge* asupra entităților din sectorul public;	**Se acceptă.**
		55.	În proiectul hotărîrii de Guvern, autorul proiectului propune o procedură *separată* (distinctă) pentru aceste entități și *simplificată;* prin *motivarea* acestui fapt din considerentul că entitățile din sectorul public, nepracticînd activitate de întreprinzător *nu pot beneficia* de întregul spectru de *garanții* oferite de Legea nr. 131/2012 (din mediului privat). Considerăm că o astfel de abordare *contravine* Legii nr. 131/2012, în redactarea Legii nr. 95/*2024*, prin care s-a decis că Legea nr. 131/2012 se aplică *tuturor* entităților controlate (în acest scop s-a modificat titlul legii, precum și s-a revizuit semnificația noțiunii *persoană supusă controlului (persoană controlată)*;	**Precizare.** Legea 48/2023 prevede expres că Guvernul, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice, **stabilește, separat** pentru furnizorii de servicii persoane juridice de drept privat și separat pentru furnizorii de servicii persoane juridice de drept public, procedurile detaliate privind modul de efectuare a controlului de stat de către autoritatea competentă asupra respectării obligațiilor ce le revin acestora conform prezentei legi

		56.	ASC nu este prevăzută în pct. 2 din anexa (Lista) din Legea nr. 131/2012 a autorităților publice care sunt abilitate să deroge, prin legi sectoriale, de la prevederilor legale privind activitatea de control și supraveghere a acestor autorități;	**Precizare.** Legea 48/2023 a oferit temei legal Guvernului de a reglementa procedura de control atât pentru sectorul public, cât și pentru cel privat. Legea 131/2012 este legea generală care reglementează procedura de control, și nu specială în coraport cu prevederile stabilite de Legea 48/2023.
		57.	În proiectul hotărîrii de Guvern la pct. 24, autorul proiectului propune ca: *în cazul în care în timpul desfășurării controlului, inspectorii constată încălcări ce conțin semne ale unei infracțiuni, aceștia sunt obligați să ia măsuri de conservare a locului săvîrșirii infracțiunii și de conservare a mijloacelor materiale de probă*, respectiv, instrumentul vizat *(conservarea probelor)* este admis de legislație - a se vedea art. 4 alin. (2) lit. b) și art. 4 lit. lit. b) în corelare cu art. 10 din Legea nr. 20/2009; **10.1.** *Însă*, aceast5a se dispune de organe cu *competențe în urmărire penală*. La rîndul său, furnizorii au obligația de a realiza conservarea datelor - art. 7 alin. (1) lit. c) și g) din Legea nr.20/2009; **10.2.** În cazul ASC, fiind organ de control, acesta trebuie să exercite obligațiile ce sunt prevăzute în art. 19 alin. (2^2) și art. 28 alin. (3) din Legea nr. 131/2012, care admit astfel de abordări. Totodată, comunicăm că deciziile ASC sunt pasibile de contestare (inclusiv ce țin cu suspendarea deciziei de,,conservare"), respectiv, un eventual abuz este sub control judiciar.	**Se acceptă.** Pct. 24 i-a fost oferită o redacție nouă.

		58.	În concluzie, se propune ca textul din proiectul hotărîrii de Guvern, Capitolul IV, să fie ajustat în condițiile stabilite de Legea nr. 131/2012.	**Precizare.** Capitolul IV stabilește procedura de control pentru autoritățile publice, care nu se supune reglementărilor Legii nr. 131/2012. .
12	**Agenția Proprietății Publice** *(nr. 05-04-8943 din 25.11.2025)*	**59.**	Lipsa obiecțiilor și propunerilor.	
13	**Agenția Națională pentru Siguranța Alimentelor** *(nr. 18-6358 din 24.11.2025)*	**60.**	Lipsa obiecțiilor și propunerilor.	
14	**Agenția Medicamentului și Dispozitivelor Medicale** *(nr. Rg02-005739 din 26.11.2025)*	**61.**	Lipsa obiecțiilor și propunerilor.	
15	**Agenția Națională pentru Cercetare și Dezvoltare** *(nr. 309 din 21.11.2025)*	**62.**	Lipsa obiecțiilor și propunerilor.	
16	**Agenția Mediului** *(nr. 08/2132/2025 din 20.11.2025)*	**63.**	Lipsa obiecțiilor și propunerilor.	
17	**Biroul Naţional De Statistică** *(nr. 24-01/19 din 25.11.2025)*	**64.**	Lipsa obiecțiilor și propunerilor.	
18	**Serviciul de Informații și Securitate** *(nr. IE/12479 din 27.11.2025)*	**65.**	La punctul 4, după cuvîntul „baza” se propune completare cu textul „rapoartelor de evaluare a conformității (audit) și” deoarece conform art. 19, alin. (4) din Legea nr. 48/2023 privind securitatea cibernetică, autoritatea competentă efectuează controale dacă a depistat și confirmat fapte de încălcare a prevederilor	**Precizare.** Considerăm oportună remarca Dvs., însă menționăm că temei pentru realizarea unui control poate servi doar prevederile menționate în Legea 131/2012. Introducerea de temeiuri noi ar contravine cu cadrul normativ

			legii sau a fost sesizată cu privire la încălcări, neîndeplinire necorespunzătoare a obligațiilor. Respectiv, Serviciul consideră că și rezultatele rapoartelor de evaluare prezinta temei pentru realizarea controlului de stat asupra respectarii cadrului normativ în domeniul securității cibernetice.	primar ce reglementează controlul de stat.
		66.	La punctul 5, după sintagma „critică națională” se propune completare cu textul „sau în baza constatărilor rapoartelor de evaluare a conformității (audit)" or, conform art. 19 alin. (2) din Legea nr. 131/2012 privind controlul de stat, controlul inopinat poate fi realizat si în cazul deținerii informațiilor/indiciilor, susținute prin probe aflate în posesia organelor de control, despre existent situațiilor de avarie, incident sau încălcare grava a regulilor de securitate ori siguranță care prezintă un pericol iminent și imediat pentru mediu, viață, sănătatea si proprietatea persoanelor.	**Se acceptă.**
		67.	La subpunctul 18.1, Serviciul propune înlocuirea sintagmei „realizează verificarea sistematică” cu cuvîntul „monitorizează”, or, verificările sunt necesar de a fi efectuate de companiile specializate, iar Agenția pentru Securitate Cibernetică (în continuare - Agenția) urmează să intervină doar atunci cand sunt neconformități.	**Nu se acceptă.** In timpul controlului, Agenția într-adevăr urmează să verifice respectarea măsurilor de securitate impuse de cadrul normativ de către furnizorii de servicii, or acesta și este scopul principal al controlului efectuat de către Agenție. Monitorizarea furnizorilor se va efectua în cadrul procedurii de supraveghere a acestora.
		68.	Considerăm necesar de a revizui punctul 23 și 63, or, realizarea controlului în lipsa personalului furnizorului privat nu oferă garanții procedurale (dreptul la apărare, participare, prezentarea explicațiilor) și poate genera litigii.	**Nu se acceptă.** Considerăm oportun a păstra redacția actuală pentru a evita anumite eschivări de la efectuarea controlului. Mai mult, la un control planificat furnizorul este notificat un prealabil despre efectuarea controlului, fapt ce

			Mai mult ca atat, în lipsa personalului responsabil (IT sau cyber) din cadrul furnizorului, efectuarea controlului va fi destul de dificil. Astfel, Serviciul propune adăugarea condiției ca realizarea controlului în lipsă, să se facă doar după o notificare rezonabila eșuată sau în caz de refuz nejustificat de participare si doar în cazuri strict motivate (ex: risc iminent), respectînd principiile contradictorialității.	ar presupune posibilitatea acestuia de a fi prezent în cadrul desfășurării controlului.
		69.	La punctul 41 sintagma „În baza evaluarii rapoartelor" urmează a fi înlocuită cu sintagma „În baza rapoartelor de evaluare", or, este important ca în Regulament să fie pastrată utilizarea sintagmei „rapoarte de evaluare" pentru coerență. Sintagma respectivă este utilizată în tot textul Regulamentului cu excepția pct. 41, unde a fost reformulat în „evaluarea rapoartelor transmise" fapt care creează o confuzie.	**Se acceptă.**
		70.	La subpunctul 59.1, pătrunderea în „orice încăpere" trebuie să fie strict limitată la cele relevante pentru obiectul controlului (echipamente IT/servere/birouri administrative) și să respecte regimul sediilor diplomatice/militare (dacă e cazul). Astfel, Serviciul propune adăugarea următoarei precizări: „...să pătrundă în orice încăpere utilizată de furnizorul de servicii în activitatea sa, care găzduiește rețele și sisteme informatice sau date relevante obiectului controlului, în măsura în care aceasta este parte a obiectului controlului."	**Se acceptă.**
		71.	La subpunctul 59.3, Serviciul solicită completarea cu sintagma „cu excepția celor atribuite la secret de stat", or, pentru informațiile atribuite la secretul de stat, este procedura separată de accesare și realizare a copiilor și înregistrarea acestora.	**Precizare.** Este evident faptul că informațiile obținute urmează a fi prelucrate în forma în care acestea sunt deținute de către furnizorii de servicii. Nu poate un angajat al Agenției care nu are acces la secret de stat să

			Mai mult ca atît, pentru prelucrarea informațiilor atribuite la secret de stat, persoanele implicate trebuie să dețină dreptul de acces la secret de stat. Suplimentar, atragem atenția că, deși în proiect se menționează privind posibilitatea de secretizare a actelor aferente procesului de control, Agenția încă nu și-a instituit regimul secret în cadrul instituției. Anterior Serviciul a solicitat faptul dat prin scrisoarea nr. IE/2499 din 18.03.2025.	prelucreze informații care sunt atribuite unui asemenea regim.
19	**Autoritatea Aeronautică Civilă** *(nr. 3200 din 27.11.2025)*	**72.**	Lipsa de obiecții și propuneri.	
20.	**Agenția de Guvernare Electronică** *(nr. 3007 – 233 din 27.11.2025)*	**73.**	Pct. 3 din proiectul Regulamentului cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice care indică temeiurile legale sub care operează ASC în activitatea de supraveghere si control, urmează a fi completat cu o trimitere la **Regulamentul privind ținerea Registrului de stat al controalelor, aprobat prin Hotărârea Guvernului nr. 464/2018**. Totodată, proiectul Regulamentului se va completa cu norme referitoare la utilizare Registrului respectiv în calitate de soluție informațională care permite comunicarea prin intermediul mijloacelor electronice, precum și transmiterea, încărcarea și semnarea documentelor aferente controlului.	**Precizare.** Legea 131/2012 face trimitere expresă la folosirea Registrului de stat al controloarelor. Astfel, nu considerăm relevant oferirea de trimiteri la Regulamentul Registrului respectiv, atunci când legea menționează expres modul de lucru cu registrul respectiv.
		74.	Proiectul hotărârii operează cu sintagma vagă de *aplică sancțiuni prevăzute de cadrul normativ în vigoare*. Proiectul evită însă să enumere sancțiunile care pot fi aplicate de către ASC. Doar **pct. 34** enumeră o serie de decizii care pot fi emise de către ASC în urma exercitării controlului, lăsându-se să se înțeleagă că pot exista și **alte sancțiuni aplicate în temeiul procesului-verbal de control**. În scopul oferirii previzibilității prevederilor	**Nu se acceptă.** Sancțiunile aplicate de către Agenție, nu pot fi reglementate la nivel de Hotărâre, or măsurile respective trebuie să fie reglementate în cadrul normativ primar. Astfel, Hotărârea urmează a menționa general că urmează a se aplica anumite

			normative, considerăm necesară enumerarea expresă a tipurilor de sancțiuni (ex: *avertisment, amendă, suspendarea activității sau altele după caz*).	sancțiuni, însă acestea trebuie să fie prevăzute de cadrul normativ (lege, adoptată de către Parlament).
		75.	Potrivit **pct. 9 din proiect**, *în cazul în care pe parcursul desfășurării activității de supraveghere se constată săvârșirea unor fapte care întrunesc elemente constitutive ale unor contravenții sau infracțiuni, Agenția implică la necesitate, autoritățile competente*. La acest aspect, sugerăm substituirea termenului *implică autoritățile competente* cu termenul *sesizează autoritățile competente*. Reieșind din prerogativele ASC descrise în proiect, considerăm că sesizarea autorităților competente ar fi o atribuție potrivită pentru a descrie acțiunea de atragere a altor autorități conexe pentru examinarea încălcărilor din domeniul securității cibernetice.	**Se acceptă.**
		76.	Conținutul proiectului necesită a fi completat cu prevederi referitoare la modalitatea și termenele de contestare a proceselor-verbale întocmite, autoritatea sau instanța competentă cu examinarea contestațiilor.	**Se acceptă** Proiectul de hotărâre urmează a fi completat corespunzător.
21.	**Agenția Națională Transport Auto** *(Nr. 02/1-1- 6326 din 28.11.2025)*	**77.**	În proiectul hotărârii Capitolul II, la pct. 10, subpct. 10.6. textul *„înaintarea recomandărilor corespunzătoare”* se propune a fi modificată cu următoarea formulare: *„înaintarea recomandărilor cu caracter obligatoriu”*. - De asemenea se propune completarea acestui subpct. după textul *„prevederilor normative”* cu textul *„și stabilește termenul în care aceștia trebuie să se conformeze.”* **Motivare:** redacția propusă are drept scop alinierea textului la prevederile Legii nr. 48/2023 privind securitatea cibernetică și stabilirea în mod expres obligația furnizorilor de servicii de a se conforma și asigura aplicarea măsurilor prevăzute, iar stabilirea unui termen concret de conformare este esențială, deoarece permite destinatarilor să cunoască	**Nu se acceptă.** Redacția propusă nu poate fi acceptată, reieșind din faptul că o recomandare nu poate fi obligatorie. Este evident faptul că Agenția urmează să vină cu unele recomandări privind implementarea măsurilor de securitate, însă responsabilitatea implementării acestora revine furnizorilor de servicii, care pot utiliza și măsuri mai stricte, reieșind din propriile posibilități.

			intervalul în care trebuie să întreprindă acțiunile necesare și facilitează monitorizarea eficientă a îndeplinirii obligațiilor.”	
		78.	La Capitolul II, la pct. 10, se propune completarea cu subpct. 10.9. cu următorul conținut: „Asigură interacțiunea în domeniul securității cibernetice cu autoritățile de control și cu furnizorii de servicii.” **Motivare:** completarea propusă are drept scop alinierea textului la prevederile Legii nr. 48/2023 privind securitatea cibernetică, precum și contribuie la asigurarea unui flux de informații eficient, la implementarea coerentă a măsurilor de protecție și la consolidarea securității cibernetice la nivel național.	**Nu se acceptă** Această propunere de completare deja se regăsește în cadrul normativ general aplicabil Agenției și furnizorilor de servicii. O asemenea prevedere la pct. respectiv nu este oportună.
		79.	Referitor la Capitolul III, secțiunea 2, se propune a fi completat cu un punct nou, care va avea următorul cuprins: *„toate cheltuielile ce țin de efectuarea controalelor sunt suportate de Agenție, cu excepția cazurilor prevăzute expres de lege.”* **Motivare:** completarea propusă are drept scop alinierea textului la prevederile Legii nr. 131/2012 privind controlul de stat și la delimitarea situațiilor în care costurile pot fi transferate persoanelor supuse controlului.	**Nu se acceptă** Legea 131/2012 prevede expres de către cine sunt suportate cheltuielile în cadrul unui control de stat.
		80.	Se înaintează propunerea de completare a Capitolului III, secțiunea 1, cu două puncte noi, după pct. 14, cu următorul conținut: - *„Controlul poate fi exercitat doar de inspectorii specificați expres în delegația de control și doar în timpul programului de activitate al furnizorului de servicii controlate;”* - *„În situația în care se impune înlocuirea inspectorului desemnat inițial pentru efectuarea controlului sau desemnarea unor inspectori suplimentari, Agenția va elibera o nouă delegație de control.”*	**Se acceptă parțial.** Reglementările din proiect nu contravin prevederilor Legii 131/2012. Mai mult, pct. 14 în redacția actuală menționează expres că controlul se efectuează în temeiul delegației de control de către cel puțin 2 inspectori.

			Motivare: Completarea propusă urmărește ajustarea textului la prevederile Legii nr. 131/2012 privind controlul de stat și stabilește clar că numai inspectorii desemnați în delegație pot exercita controlul, asumându-și întreaga responsabilitate pentru legalitatea și corectitudinea verificărilor efectuate.	
		81.	Se propune completarea Capitolului III, secțiunea 2, cu un punct nou, după pct. 23, cu următorul conținut: *„Orice fapt constatat de inspector în cadrul efectuării controlului, care ulterior nu poate fi probat sau care împiedică desfășurarea acestuia (cum ar fi absența personalului furnizorului de servicii de la adresa indicată), se consemnează în procesul-verbal de control. Procesul-verbal se semnează de inspector și de cel puțin un martor, cu indicarea datelor sale de identificare”* **Motivare:** Prevederea are drept scop alinierea textului la prevederile Legii nr. 131/2012 privind controlul de stat și asigură documentarea corectă a situațiilor care împiedică controlul și garantează credibilitatea procesului-verbal prin semnătura unui martor identificat.	**Nu se acceptă** În capitolul I se menționează expres că prevederile Legii 131/2012 se aplică direct în desfășurarea controlului efectuat de către Agenție. Astfel, toate normele primare ce se regăsesc în actul normativ menționat urmează a se aplica direct atât de către autoritatea ce efectuează controlul, cât și de cea asupra căruia este efectuat acesta.
		82.	La Capitolul IV, Secțiunea 1, la pct. 43 textul: *„pagina oficială în Interne”* să fie reformulată în felul următor: *„pagina web oficială”* **Motivare:** Modificarea propusă are drept scop alinierea textului la prevederile Legii nr. 100/2017 cu privire la actele normative, prin utilizarea termenului corect și unitar „pagina web oficială”.	**Se acceptă.** A fost ajustat textul corespunzător.
		83.	La Capitolul IV, secțiunea 1, se înaintează propunerea de completare cu un punct nou, care va avea următorul cuprins: *„La efectuarea controlului planificat, dacă în anul curent deja a fost efectuat un control inopinat la aceeași persoană, organul de control va ajusta/restrânge durata controlului și aria aspectelor necesare de a fi verificate în corespundere cu controlul inopinat deja efectuat.”*	**Nu se acceptă.** Durata controlului, cât și aria aspectelor necesare de a fi verificate de către angajații Agenției urmează a fi analizat în fiecare caz particular, inclusiv prin prisma materialelor de care dispun angajații Agenției și de

			Motivare: Completarea propusă este în conformitate cu prevederile Legii 131/2012 privind controlul de stat și are drept scop evitarea suprapunerii inutile a activităților de control și asigurarea unui tratament proporțional față de subiectul controlului.	infrastructura deținută de către furnizorul de servicii.
		84.	Referitor la Capitolul IV, Secțiunea 2, după pct. 53 din proiectul prezentat, se propune completarea cu două puncte noi având următorul conținut: - *„Delegația de control își pierde valabilitatea la expirarea termenului de 5 zile lucrătoare de la data începerii controlului, indiferent de temeiul efectuării acestuia și de tipul controlului;”* - *„Conducerea organului de control poate prelungi termenul prevăzut la pct. anterior cu încă 5 zile lucrătoare, în baza unei decizii motivate, care poate fi contestată de către persoana supusă controlului.”* **Motivare:** Prevederea urmărește asigurarea unei durate determinate a activităților de control, prevenind extinderea nejustificată a perioadei de verificare. Limitarea valabilității delegației la 5 zile lucrătoare contribuie la respectarea și la protejarea operatorilor de eventuale abuzuri sau tergiversări ale procesului de control, iar posibilitatea prelungirii termenului prin decizie motivată permite adaptarea controlului în situații excepționale.	**Se acceptă** Proiectul a fost completat corespunzător.
		85.	La Capitolul IV, secțiunea 3, se propune expunerea punctului 72 în următoarea formă: *„La procesul-verbal se anexează un plan de măsuri pentru remedierea deficiențelor și îmbunătățirea activității furnizorului de servicii publici, care include în mod obligatoriu termene-limită pentru realizare, corelate cu procedurile legale de achiziții publice și cu mijloacele financiare alocate în acest sens. Pentru măsurile care necesită resurse financiare suplimentare, neprevăzute în bugetul aprobat,*	**Nu se acceptă.** În conformitate cu prevederile Hotărârii Guvernului nr. 562/2025 Furnizorii de servicii efectuează audituri privind securitatea informațiilor, în vederea determinării nivelului de conformitate cu cerințele privind măsurile de securitate a rețelelor și a sistemelor informatice,

			termenul de realizare începe să curgă de la data alocării fondurilor necesare .” **Motivare:** În situația în care furnizorul de servicii publice prezintă dovezi că a solicitat Ministerului Finanțelor bugetarea măsurilor necesare, însă alocarea mijloacelor financiare nu a fost aprobată, Agenția nu poate sancționa furnizorul și nici nu îi poate imputa nerealizarea acestor măsuri. În acest context menționăm că, Agenția Națională Transport Auto susține proiectul hotărârii de Guvern cu includerea propunerilor menționate.	prevăzute în anexă, cel puțin o dată la trei ani sau ori de câte ori este necesar în conformitate cu cerințele stabilite în anexă. Astfel, fiecare furnizor în parte urmează să își evalueze propria infrastructură, inclusiv să își aloce resurse necesare pentru protejarea infrastructurii proprii. Rolul Agenției în principal este de a verifica implementarea măsurilor de securitate și nu aplicarea de sancțiuni pecuniare furnizorilor de servicii.
22.	**Ministerul Infrastructurii și Dezvoltării Regionale** *(Nr. 05 – 6213 din 26.11.2025)*	**86.**	Comunică despre lipsa de obiecții. Totodată, pentru îmbunătățirea procedurii de control, propunem completarea proiectului cu prevederi cu privire la contestarea delegației de control și a procesului verbal de control.	**Precizare.** Propunerile Dvs. se regăsesc în cadrul normativ primar.
23.	**Ministerul Afacerilor Interne** *(Nr. 38/4232 din 01.12.2025)*	**87**	Potrivit proiectului, în exercitarea funcției de control, Agenția pentru Securitate Cibernetică constată abateri de la obligațiile privind respectarea măsurilor de securitate impuse de cadrul normativ (subpct. 18.2.) precum și dispune, după caz, de aplicarea de sancțiuni prevăzute de cadrul normativ în vigoare (subpct. 18.5.). Considerăm aceste prevederi ca fiind în afara cadrului normativ existent la moment, or, potrivit prevederilor Hotărârii Guvernului nr. 1028/2023 cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică, în domeniul realizării funcției de supraveghere și control de stat al respectării de către furnizorii de servicii a prevederilor cadrului normativ în domeniul securității cibernetice, instituția nu este investită cu atribuții de constatare a încălcărilor privind securitatea cibernetică. Mai mult, potrivit Capitolului III al Cărții a doua din Codul contravențional nr. 218/2008, Agenția pentru	**Precizare.** Pct. respectiv i-a fost oferită o redacție nouă.

			Securitate Cibernetică nu este desemnată ca autoritate competentă să soluţioneze cauze contravenţionale. Astfel, rămâne neclară situația privind modalitatea și procedura de sancționare a eventualelor încălcări depistate în domeniul securității cibernetice.	
		87.	În aceeași ordine de idei, se recomandă ca la pct. 34, subpct. 1 să fie exclus, în contextul în care, potrivit alin. (5) al art. 32 din Codul contravențional, sancţiunile contravenţionale aplicabile persoanei juridice sunt: a) amenda; b) privarea de dreptul de a desfăşura o anumită activitate. Totodată, „avertismentul”, potrivit art. 32 alin. (1) lit. a) din Codul contravențional, reprezintă o sancțiune contravenţională aplicabilă doar persoanei fizice. Potrivit prevederilor art. 5¹ alin. (4) din Legea nr. 131/2012 privind controlul de stat, în cazul încălcărilor minore pot fi emise doar prescripții în baza cărora se indică ce încălcări trebuie înlăturate și se recomandă modalități de înlăturare a încălcărilor, însă nu pot fi aplicate sancțiuni prevăzute de legea contravențională sau altă lege și nu pot fi aplicate măsuri restrictive. Astfel, recomandăm ca, la subpct. 2 din pct. 34 al proiectului, cuvântul „instrucțiuni” să fie înlocuit cu cuvântul „prescripții”.	**Precizare.** Pct. 34 menționează expres că pe lângă prescripții și sancțiuni aplicate în baza procesului-verbal, Agenția emite și actele menționate în pct. dat în raport cu persoana juridică la care a efectuat controlul. Astfel, urmează a se face diferențiere între sancțiunile impuse în baza Codului contravențional și a celor incluse în pct. din Regulament.
		88.	Cu toate că, potrivit proiectului înaintat spre avizare, printre principiile specifice supravegherii și controlului de stat asupra respectării cadrului normativ în domeniul securității cibernetice se regăsesc principiul proporționalității și cel al protecției drepturilor fundamentale, proiectul nu prevede careva căi de atac sau de contestare a acțiunilor angajaților Agenției pentru Securitate Cibernetică, urmare a controalelor de stat efectuate la furnizorii de servicii pe domeniul de referință.	**Se acceptă parțial.** Reglementările menționate de Dvs. se regăsesc în cadrul normativ primar care reglementează aspectele date. Totodată, menționăm că proiectul a fost ajustat pentru a îndeplini rigorile impuse de Legea nr. 100/2017.

			Subsidiar, se recomandă autorilor proiectului a se conforma cerințelor art. 54 din Legea nr. 100/2017 cu privire la actele normative și a expune conținutul proiectului într-un limbaj simplu, clar și concis, pentru a exclude orice echivoc, cu respectarea regulilor gramaticale, de ortografie și de punctuație.	
24.	**Ministerul Afacerilor Externe** *(Nr. DI/3/041- 12188 din 25 noiembrie 2025)*	**89.**	Lipsa obiecțiilor și propunerilor.	
25.	**Centrul Național pentru Protecția Datelor cu Caracter Personal** *(Nr. 04-01/4241 din 01.12.2025)*	**90.**	Lipsa obiecțiilor și propunerilor.	
26.	**Ministerul Afacerilor Interne (Inspectoratul de Management Operațional)** *(nr. 27/17646 din 02.12.2025)*	**100.**	**De ordin conceptual:** Deși proiectul supus examinării reglementează supravegherea și controlul furnizorilor de servicii din sectoarele critice, se constată că Regulamentul nu conține nici o referință la Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale, deși subiecții vizați de proiect coincid în mod direct cu categoria gestionarilor de infrastructuri critice naționale. În vederea asigurării coerenței cadrului de reglementare aplicabil și evitării eventualelor suprapuneri de competență, se propune completarea pct. 1 al Regulamentului, după cum urmează: „Prezentul Regulament se aplică în concordanță cu prevederile Legii nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale, în special în ceea ce privește obligațiile gestionarilor de infrastructuri critice naționale și mecanismele de protecție și informare aferente acestora.”	**Nu se acceptă** Proiectul de hotărâre propus are drept temei legal prevederile art. 19 din Legea 48/2023. Controlul pe care urmează să îl efectueze furnizorii de servicii se referă la implementarea măsurilor de securitate cibernetică, iar legea pe care ați menționate, are în general alt obiect de reglementare, fiind tangențial diferit de obiectul proiectului supus discuției.

		101.	În conformitate cu prevederile art. 8 din Legea nr. 223/2025, la nivelul Ministerului Afacerilor Interne, prin intermediul CNCPIC, poate fi instituit și administrat un mecanism național securizat de comunicare și avertizare timpurie, destinat gestionării integrate a informațiilor privind incidentele, amenințările, punctele vulnerabile și riscurile aferente infrastructurilor critice naționale. Totodată, proiectul Regulamentului stabilește, la pct. 10, pct. 27 si pct. 33, un set distinct de instrumente de colectare, transmitere și schimb de informații privind incidentele cibernetice, precum și mecanisme proprii de avertizare și intervenție. Dat fiind faptul, că funcțiile reglementate prin proiect se suprapun parțial cu atribuțiile MeCAT stabilite prin Legea nr. 223/2025, se impune evitarea paralelismelor instituționale și asigurarea unei arhitecturi unitare de gestionare a riscurilor și evenimentelor ce afectează infrastructurile critice naționale. Asadar, dupa pct. 10.8 se recomandă introducerea pct. 10.9, cu următorul cuprins: „10.9. Măsurile de supraveghere și instrumentele de colectare și schimb de informații prevăzute la pct. 10 se realizează în interoperabilitate și coordonare cu mecanismul de comunicare și avertizare timpurie instituit în cadrul Ministerului Afacerilor Interne, prin intermediul CNCPIC, potrivit art. 8 din Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale."	**Nu se acceptă** Proiectul de act normativ nu are ca obiect de reglementare stabilirea anumitor mecanisme de cooperare la nivel național în ce privește mecanismele securizate de comunicare și avertizare timpurie, destinate gestionării integrate a informațiilor privind incidentele, amenințările, punctele vulnerabile și riscurile aferente infrastructurilor critice naționale, ci reglementarea modului de exercitare de către ASC a funcției de supraveghere și control.
		102.	Este de menționat, că deși în Nota de fundamentare a proiectului se subliniaza complementaritatea dintre Legea nr. 48/2023 si Legea nr. 223/2025, precum și necesitatea unei cooperări și schimb de informații în timp real între autoritățile competente în domeniul securității cibernetice și cele în domeniul infrastructurilor critice naționale, includerea referințelor la Legea nr. 223/2025 și la mecanismul MeCAT este în deplină concordanță cu	**Nu se acceptă.** Cooperări și schimbul de informații între autoritățile competente în domeniul securității cibernetice și cele în domeniul infrastructurilor critice naționale va face obiectul de reglementare a altui act normativ.

			raționea proiectului și cu obligațiile prevăzute de cadrul european (Directiva (UE) 2022/2555 și Directiva (UE) 2022/2557).	
		103.	Proiectul instituie la pct. 26-28 măsuri de intervenție urgentă, restricționare a utilizării unor sisteme informatice și acțiuni imediate în situații de risc major, care se suprapun cu etapele și regimul juridic al managementului situațiilor de criză, reglementat prin Legea nr. 248/2025 privind managementul situațiilor de criză. În vederea asigurării unității cadrului procedural de criză, se recomandă completarea secțiunii relevante cu o trimitere la legea menționată, astfel: „Gestionarea incidentelor de securitate cibernetică cu impact semnificativ se realizează în concordanță cu prevederile Legii nr. 248/2025 privind managementul situațiilor de criză." Această mențiune este necesară pentru evitarea conflictelor de competență și pentru integrarea corectă a proceselor de răspuns la incidente cibernetice în arhitectura națională de coordonare a crizelor.	**Nu se acceptă** Managementul crizelor și controlul de stat sunt două instituții diferite. Astfel, dacă se va face referire la Legea 248/2025, atunci prevederile din proiect care fac referire la condițiile care trebuie să fie întrunite în cazul restricționării sistemelor informatice devin neaplicabile. Considerăm că în proiectul de hotărâre sunt descrise toate condițiile necesare pentru a aplica prevederile legale enunțate.
		104.	**De ordin normativ:** Subsidiar, învederăm că autorul proiectului urmează a se conforma prevederilor art. 54 din Legea nr. 100/2017 cu privire la actele normative, cu modificările ulterioare și a expune conținutul proiectului într-un limbaj simplu, clar și concis, pentru a exclude orice echivoc, cu respectarea regulilor gramaticale, de ortografie și de punctuație.	**Se acceptă.**
		105.	În atare circumstanțe, Inspectoratul de Management Operațional susține conceptual promovarea proiectului de hotărîre, în condițiile în care vor fi operate ajustările expuse supra, în vederea asigurării coerenței normative, a corelării cu legislația națională aplicabilă, precum și a integrării corecte a domeniului infrastructurilor critice în	**Se acceptă.** Proiectul a fost completat cu prevederi noi.

			arhitectura națională de securitate cibernetică și management al crizelor.	
27.	**Aparatul Președintelui Republicii Moldova** *(nr. 2/2-06-1721 din 03.12.2025)*	**106.**	Lipsa obiecțiilor și propunerilor.	
28.	**Ministerul Finanțelor** *(nr. 09/2-03/585/1671 din 03.12.2025)*	**107.**	Lipsa obiecțiilor.	
		108.	Totodată, proiectul hotărârii urmează a fi redactat pentru a elimina greșelile gramaticale, de ortografie și de punctuație, întru respectarea prevederilor art. 54 alin. (1) din Legea nr. 100/2017 cu privire la actele normative, precum și pentru a corela terminologia utilizată cu cea din cadrul normativ existent.	**Se acceptă.**
29.	**Ministerul Afacerilor Externe** *(Nr. DI/3/041- 12188 din 25 noiembrie 2025)*	**109.**	Lipsa obiecțiilor și propunerilor.	
30.	**Ministerul Muncii și Protecției Sociale** *(nr.22/5614 din 01.12.2025)*	**110.**	Lipsa obiecțiilor și propunerilor.	
31.	**Banca Națională a Moldovei** *(Nr. 31-002/151/6250 din 05.12.2025)*	**111.**	Cu referire la competențele Agenției de Securitate Cibernetică (în continuare - ASC) de supraveghere și control a respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii din sectorul bancar, semnalăm că unele competențe de supraveghere și control ale ASC (prevăzute în proiectul de regulament), în raport cu băncile, se suprapun cu competențele BNM de supraveghere și control a acestora (art. 5 din Legea nr. 202/2017 privind activitatea băncilor; art. 5 alin. (1) lit. d), f) din Legea nr. 548/1995 cu privire la Banca Națională a Moldovei). Mai mult, opinăm că o astfel de suprapunere de competențe va crea riscuri și impedimente procesului de supraveghere efectuat atât de BNM, cât și de către ASC.	**Nu se acceptă.** ASC nu exclude că unele competențe în materie de control s-ar putea suprapune cu BNM, însă controlul ce urmează a fi efectuat de către Agenție se referă strict la respectarea măsurilor de securitate care sunt impuse de Legea 48/2023 și actele normative de punere în aplicare a acesteia. Totodată, menționăm că conform Legii 48/2023 și Hotărârii Guvernului 1028/2023 ASC este desemnată autoritate competentă la nivel național în domeniul securității cibernetice și

			Menționăm în acest context că BNM evaluează, inclusiv în cadrul controalelor desfășurate la bancă, cadrul intern aferent TIC în fiecare bancă, în raport cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate de bancă și cu profilul/apetitul de risc și poate aplica măsuri de supraveghere și sancțiuni în cazul identificării riscurilor sau încălcărilor în acest domeniu. Atenționăm că BNM a instituit deja un sistem funcțional de raportare a incidentelor pentru entitățile supravegheate, inclusiv pentru incidentele operaționale, de securitate a informației și TIC, cu termene, canale și responsabilități clar definite și integrate în procesele de supraveghere prudențială și operațională. Opinăm în acest sens, că introducerea unor fluxuri paralele de raportare de către sectorul bancar direct ASC, fără o interfață clară cu BNM, riscă să creeze dublări de rapoarte, să fragmenteze informația și să îngreuneze analiza de ansamblu a impactului semnificativ al unui incident cibernetic în sectorul bancar. În continuare, prezentăm câteva riscuri semnificative de suprapunere și necorelare identificate, care pot afecta atât procesul de supraveghere și control efectuat de către BNM, cât și cel efectuat de către ASC: 1) Competența ASC de supraveghere în mod sistematic și continuu a furnizorilor de servicii în sectorul bancar (prin solicitări de informații, exerciții și simulări în materie de securitate cibernetică, teste la stres, teste de penetrare și scanări ale rețelelor și sistemelor informatice, etc.), se suprapune direct misiunii de supraveghere tematică TIC desfășurată de BNM, prin intermediul căreia, la fel, se solicită rapoarte cu privire la risc, proceduri de audit și teste de reziliență, și se impun măsuri de remediere a deficiențelor constatate. Astfel, există un risc evident de dublare a controalelor	autoritate responsabilă de gestionarea crizelor în domeniul securității cibernetice la nivel național. În acest context, ASC nu poate fi subrogat cu BNM deoarece pct. 3 al proiectului prevede că „Supravegherea și controlul de stat asupra respectării de către furnizorii de servicii în sectoarele critice a prevederilor cadrului normativ în domeniul securității cibernetice se realizează de către Agenția pentru Securitate Cibernetică (în continuare - *Agenția*) în conformitate cu prevederile Legii nr. 48/2023 privind securitatea cibernetică, Legii nr. 131/2012 privind controlul de stat și a prezentului Regulament.” Totodată, opțiunea controlului comun conform Legii 131/2012 ar putea fi aplicată, dacă autoritățile vor întruni condițiile din art. 4 alin. (7).

			efectuate sectorului bancar, precum și a măsurilor de remediere prescrise sau a sancțiunilor aplicate urmare constatării unor deficiențe sau neregularități privind securitatea cibernetică. 2) Împuternicirile care sunt atribuite ASC prin proiectul de regulament (verificarea modului de îndeplinire a obligațiilor privind respectarea măsurilor de securitate cibernetică; constatarea abaterilor; emiterea unor dispoziții cu caracter obligatoriu în vederea conformării și remedierii deficiențelor constatate; stabilirea termenelor de conformitate cu măsurile de securitate impuse; solicitarea de declanșare imediată a măsurilor de remediere a anumitor deficiențe; dispunerea aplicării de sancțiuni), în măsura în care se referă la exercitarea funcției de control a sectorului bancar, sunt inerente BNM ca autoritate de reglementare și supraveghere a sectorului bancar. 3) Competența ASC de restricționare a utilizării unuia sau a mai multor sisteme informatice sau accesul la acestea, în condițiile prevăzute de proiectul de regulament, poate avea un impact negativ semnificativ asupra entităților supravegheate de BNM, spre exemplu, poate afecta continuitatea serviciilor de plată și decontare, accesul nerestricționat a clienților la conturile sale. 4) Controalele efectuate de ASC vor genera planuri de măsuri de remediere obligatorii pentru furnizorii de servicii din sectorul bancar, cu termene de implementare și obligații de raportare către ASC. În acest context, menționăm că pentru entitățile din sectorul bancar, BNM, la fel, stabilește planuri de măsuri de remediere și termene de remediere în urma misiunilor de supraveghere și control. În lipsa unei coordonări între BNM și ASC, înțelegem că aceeași entitate poate primi, pentru aceleași deficiențe de securitate cibernetică sau	**3. Precizare** restricționarea utilizării unui sistem informatic sau a accesului la acesta are prevăzute condițiile exprese care trebuie întrunite pentru ca ASC să aplice astfel de măsuri restrictive. **4 Se acceptă parțial** Aceste coordonări ar putea fi reglementate printr-un Acord sau Memorandum de Înțelegere încheiat între ASC și BNM.

			incidente cibernetice constatate, măsuri de remediere și termene de îndeplinire diferite de la ASC și BNM, ceea ce poate rezulta în îndeplinirea neuniformă, defectuoasă a măsurilor de remediere, prioritizare dificilă și utilizare ineficientă de către entitate a resurselor de conformare. Observația este valabilă și în cazul aplicării sancțiunilor față de entități pentru aceeași încălcare de către ASC și BNM. 5) Conform proiectului de regulament, ASC va planifica controalele în sectorul bancar în baza evaluărilor de risc la nivel național, sectorial și subsectorial, inclusiv în funcție de rezultatele auditului de securitate cibernetică efectuat în conformitate cu hotărârea Guvernului privind cerințele de securitate pentru rețele și sisteme informatice ale furnizorilor din sectoarele critice. În acest context, menționăm, că în sectorul bancar, BNM realizează deja în mod continuu evaluări de risc TIC și operațional la nivel de bancă și la nivel de sistem, pe baza raportărilor periodice, a incidentelor notificate și a rezultatelor misiunilor de supraveghere. Lipsa unei obligații de a valorifica evaluările efectuate de BNM, de a coordona planificarea controalelor ASC cu BNM, face analiza de risc a ASC redundantă în partea ce ține de sectorul bancar și poate conduce la o imagine necorelată a profilului de risc al băncii. Adițional, observăm că potrivit pct. 12 din proiectul de regulament, controlul în privința furnizorilor de servicii persoane juridice de drept privat se efectuează în baza Legii nr. 131/2012 privind controlul de stat. În acest context, atenționăm asupra prevederilor art. 1 alin. (4) lit. c) din Legea nr. 131/2012, conform cărora dispozițiile legii nu se aplică controalelor efectuate în domeniul financiar (bancar și nebancar). O prevedere similară este stabilită la art. 5 alin. (6) din Legea nr. 548/1995 cu privire la Banca Națională a Moldovei.	**5 Precizare** ASC va analiza toate actele care îi vor fi transmise de către furnizorii de servicii, inclusiv actele care au fost prezentate către BNM de furnizorii menționați.

			În continuare, remarcăm că art. 3 alin. (5) din Legea nr. 48/2023 privind securitatea cibernetică stabilește caracterul special al prevederilor Legii nr. 202/2017 privind activitatea băncilor (care la art. 382 reglementează cerințe speciale privind gestionarea riscurilor aferente tehnologiei informației și comunicațiilor, securității informației și continuității activității), inclusiv a prevederii care stipulează rolul BNM de autoritate de supraveghere a sectorului bancar (art. 5 din aceeași lege). Având în vedere cele menționate supra, semnalăm că pentru sectorul bancar este esențială asigurarea unei delimitări clare între atribuțiile de supraveghere și control ale ASC și aceleași atribuții ale BNM, astfel încât să fie evitate dublări de competențe și sarcini suplimentare pentru entitățile supravegheate. În acest sens, propunem completarea proiectului de regulament cu o prevedere adițională care să menționeze că supravegherea furnizorilor de servicii critice din sectorul bancar se efectuează de către BNM în conformitate cu Legea nr. 202/2017, Legea nr. 548/1995 și actele normative subordonate acestora. Subsidiar, în măsura în care ASC consideră stringentă asumarea unor competențe de supraveghere a sectorului bancar, înaintăm următoarele propuneri: - reglementarea cerinței de informare și coordonare prealabilă cu BNM a controalelor planificate la bănci. Aceasta ar include obligația ASC de a informa BNM în prealabil asupra controalelor planificate în sectorul bancar, obligația de a lua în considerare constatările și planurile de măsuri de remediere deja stabilite de BNM și, acolo unde este posibil, organizarea de controale coordonate sau comune pentru a reduce sarcina asupra băncilor. De asemenea, în cazul controalelor inopinate la bănci, urmează a fi prevăzută informarea prealabilă a	

			BNM într-un termen scurt, nu doar comunicarea constatărilor la sfârșitul controlului; - completarea proiectului de regulament cu o prevedere care să stabilească că orice măsură dispusă de ASC care poate afecta în mod semnificativ funcționarea sistemelor informatice ale băncilor (în special măsurile de restricționare a utilizării sau a accesului la sisteme) trebuie adoptată numai după o consultare prealabilă cu BNM și cu evaluarea comună a impactului asupra stabilității financiare și a continuității serviciilor esențiale de plăți și decontare. În situațiile în care este necesară o intervenție de urgență, trebuie prevăzută obligația de informare imediată a BNM cu privire la măsurile dispuse, pentru a permite BNM să adopte măsuri corelative din perspectiva mandatului său; - completarea proiectului de regulament (eventual și a proiectului Metodologiei privind controlul de stat, elaborată de către ASC și MDED), cu o prevedere care să stabilească mecanisme de recunoaștere și valorificare a raportărilor și evaluărilor realizate în cadrul supravegherii efectuate de către BNM (din perspectiva sistemului existent de raportare a incidentelor și a cadrului normativ sectorial TIC al BNM). Aceasta ar trebui să includă: utilizarea de către ASC a datelor și analizelor furnizate de BNM cu privire la incidentele operaționale și TIC raportate de bănci, evitarea instituirii unor canale paralele de raportare pentru aceleași categorii de incidente, precum și recunoașterea auditului și testelor de reziliență efectuate în baza cerințelor BNM, pentru a nu obliga băncile să repete aceleași exerciții la solicitarea ASC. Totodată, semnalăm că responsabilitățile ASC privind asigurarea securității cibernetice de către sectorului bancar urmează a fi corelate cu angajamentele Republicii Moldova în domeniul securității cibernetice	

			din Programul Național de Aderare a Republicii Moldova la UE 2025-2029, care actualmente, sunt puse în sarcina BNM și CNPF.	
		112.	Cu referire la competențele ASC de supraveghere și control a respectării cadrului normativ în domeniul securității cibernetice de către persoanele juridice de drept public, comunicăm următoarele. Reiterăm susținerea pentru eforturile consolidate ale autorităților publice în fortificarea cadrului privind securitatea cibernetică și de creștere a nivelului de reziliență cibernetică în toate sectoarele relevante. În același timp, semnalăm că mecanismele statale instituite în vederea consolidării rezilienței cibernetice la nivel național urmează să țină cont de mandatul și statutul băncii centrale – fapt consemnat și în opiniile Băncii Centrale Europene (în continuare – BCE) emise cu referire la proiectul Directivei (UE) 2022/2555 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune1 și cu referire la proiectele de lege privind sistemul național de securitate cibernetică ale statelor-membre ale UE, detaliate infra. Astfel, BCE a semnalat că orice prevederi ale legislației naționale care transpun Directiva (UE) 2022/2555 trebuie să fie interpretate și aplicate în mod consistent cu competențele Sistemului European al Băncilor Centrale și să respecte principiile aplicabile băncilor centrale consacrate în articolul 130 din Tratatul privind funcționarea Uniunii Europene. Mai mult, remarcăm că în opiniile aferente proiectelor de lege privind sistemul național de securitate cibernetică (a se vedea spre ex. pct. 2.2 din Opinia CON/2025/22; CON/2024/243; CON/2024/144), BCE semnalează că măsurile legislative naționale nu trebuie să afecteze exercitarea sarcinilor și responsabilităților băncii centrale.	**Se acceptă parțial.** Proiectul a fost completat cu unele prevederi în acest sens. Totodată, menționăm că ASC este deschisă în vederea încheierii unor acorduri de colaborare interinstituționale inclusiv pentru efectuarea controlului.

			În acest sens, BCE menționează că *„exercitarea puterilor autorităților responsabile de securitatea cibernetică este supusă unor reguli, garanții și limitări specifice, în timp ce scopul pentru care pot fi folosite este clar definit. BCE salută excluderea dispozițiilor referitoare la retragerea produselor, serviciilor și proceselor TIC în legătură cu o bancă centrală națională [...]”*. Astfel, în opinia BCE, aplicarea unui regim legislativ special pentru băncile centrale „susține autonomia operațională a băncii centrale naționale în cadrul național de securitate cibernetică și reflectă importanța menținerii garanțiilor specifice aplicabile independenței și integrității operaționale a băncilor centrale”. În același sens, BCE atrage atenția că evaluarea securității sistemului informațional al băncii centrale naționale trebuie să fie realizat doar după obținerea consimțământului băncii centrale. Suplimentar, cu referire la cooperarea între autoritățile responsabile de implementarea măsurilor de securitate cibernetică și banca centrală, BCE remarcă în opiniile sale (a se vedea spre ex. pct. 3.4 din Opinia CON/2025/2; pct. 3.6 din CON/2024/24 și CON/2024/14) că „BCE ar saluta înființarea, în cadrul proiectului de lege, a unor aranjamente suplimentare de cooperare între organismele responsabile cu implementarea măsurilor de securitate cibernetică și banca națională. BCE sugerează ca, în contextul acestei cooperări, să fie puse în aplicare mecanisme eficiente de schimb de informații și de consultare pentru a preveni situațiile care ar putea submina capacitatea băncii naționale de a-și îndeplini sarcinile [...]”. În special, conform opiniei BCE, banca națională ar trebui să fie informată despre incidentele cibernetice actuale și potențiale, precum și despre măsurile planificate sau adoptate care ar afecta	

			capacitatea băncii naționale să-și îndeplinească obligațiile. Astfel de aranjamente de cooperare ar asigura, de asemenea, ca organismele responsabile cu implementarea securității cibernetice și banca națională să schimbe informații și să se consulte cu privire la incidentele sau amenințările cibernetice actuale și potențiale din sistemele sectorului financiar și din infrastructurile financiare, precum și despre măsurile planificate și adoptate. BCE remarcă că un astfel de schimb de informații trebuie să fie efectuat într-un mod eficient și în timp util, fără a se recurge la măsuri de aplicare unilaterală. În acest context, remarcăm modelul de cooperare dintre autoritățile din Franța, unde Autoritatea de Control Prudential și de Rezoluție (parte a Băncii Naționale a Franței) și Agenția Națională pentru Securitatea Sistemelor Informatice au semnat în 2018 un memorandum de cooperare în domeniul securității sistemelor informatice. Memorandumul prevede un schimb regulat de informații privind incidentele cibernetice care afectează securitatea sistemelor informatice și o cooperare consolidată în gestionarea crizelor și a securității digitale. Un alt model de cooperare este cel al Băncii Centrale a Lituaniei și Centrul Național de Securitate Cibernetică. Remarcăm că aceste autorități au formalizat o nouă fază a cooperării interinstituționale în domeniul securității cibernetice, astfel, în cadrul acordului, Banca Lituaniei se alătură platformei naționale de gestionare a incidentelor cibernetice, coordonată de Centrul Național de Securitate Cibernetică (aceasta facilitează schimbul de informații în timp real despre amenințările și incidentele cibernetice, sprijină răspunsurile coordonate și îmbunătățește gestionarea generală a riscurilor cibernetice).	

			Totodată, atragem atenția asupra faptului, că în privința informațiilor gestionate de BNM se aplică regimul de confidențialitate reglementat de art. 36 din Legea nr. 548/1995, care la alin. (4) stabilește exhaustiv cazurile în care BNM poate divulga sau furniza informații ce constituie secret profesional. De asemenea, protecția informațiilor confidențiale dobândite de BNM în calitate de autoritate de supraveghere este reglementată și de legile care reglementează activitatea entităților supravegheate de BNM. Consecvent, orice solicitare de informații (inclusiv din partea ASC în cadrul controalelor efectuate, conform pct. 59 sau 62 din proiectul de regulament) poate fi satisfăcută doar în măsura în care aceasta corespunde normelor legale privind protecția secretului profesional, respectarea cărora ar putea fi asigurată prin determinarea de comun acord cu BNM a informațiilor care pot fi furnizate. În concluzie, opinăm că procedurile de control prevăzute în proiectul de regulament nu pot fi aplicate în raport cu BNM, având în vedere principiile aplicabile activității și statutului unei bănci centrale, iar cooperarea și schimbul de informații dintre BNM și ASC, în vederea implementării cerințelor privind asigurarea securității cibernetice care rezultă din Legea nr. 48/2023 precum și din actele normative subordonate acestei legi, urmează a fi realizate în baza unui acord de cooperare între BNM și ASC, cu modificarea corespunzătoare a Legii nr. 48/2023 și includerea în legislație a aspectelor menționate supra, conform opiniilor BCE și practicilor aplicate în statele-membre ale UE.	
		113.	Cu referire la conținutul proiectului de regulament, înaintăm următoarele propuneri. La pct. 6.5, norma urmează a fi revizuită astfel încât aceasta să reglementeze că ASC în exercitarea atribuțiilor asigură confidențialitatea datelor ce	**Precizare** A se vedea pct. 71 din Regulament.

			constituie secret profesional, nu doar a datelor ce reprezintă secret comercial.	
		114.	La pct. 16, urmează a se preciza în normă sau în nota de fundamentare a proiectului de regulament cine sunt „alte autorități sau instituții publice cu competențe în domeniul securității cibernetice” al căror suport poate fi solicitat de ASC în procesul de efectuare a controlului (inclusiv pot participa la efectuarea controlului) furnizorilor de servicii critice. Observația este valabilă și pentru pct. 54 din proiectul de regulament.	**Nu se acceptă** O listă exhaustivă de autorități nu poate fi oferită, reieșind din faptul că în dependență de specificul fiecărui furnizor de servicii urmează, în caz de necesitate, să fie atrasă și altă autoritate publică, inclusiv posibil să fie solicitat și ajutorul BNM pe anumite segmente.
		115.	La pct. 30, opinăm că nu este clar formulată ipoteza în care survine excepția de neprezentare a procesului verbal pentru observațiile furnizorului de servicii în sectoare critice. Propunem revizuirea prevederii în vederea explicitării cazului în care se admite omiterea acestei garanții procedurale a furnizorului de servicii.	**Se acceptă.** Proiectul a fost ajustat corespunzător.
		116.	La pct. 34: - nu este clar la ce se referă termenul de „prescripții emise”, or, potrivit pct. 29 din proiectul de regulament, procesul verbal conține constatările efectuate pe timpul verificărilor, concluziile și măsurile de remediere propuse; - recomandăm a se revedea textul „sancțiuni aplicate în temeiul procesului verbal” având în vedere că pct. 33 reglementează că în caz de depistare a unor neconformități privind implementarea măsurilor de securitate, la procesul-verbal de control se anexează un plan de măsuri pentru remedierea deficiențelor și îmbunătățirea activităților furnizorului de servicii, respectiv, pct. 33 nu prevede și stabilirea sancțiunilor așa cum reglementează pct. 34; - la subpct. 6), urmează a se preciza cel puțin în nota de fundamentare aferentă proiectului de regulament cine sunt acele „autoritățile publice competente cărora ASC le solicită aplicarea, în conformitate cu cadrul normativ,	**Se acceptă parțial.** Termenul de prescripții urmează a fi înțeles în sensul Regulamentului exact cum este descris în Legea 131/2012. Totodată, menționăm cu unele din prevederile enunțate au fost ajustate conform proiectului, iar la obiecția referitoare la subpct. 6) a fost oferită o explicație mai sus, la fel la obiecția BNM.

			a unei sancțiuni proporționale încălcării și impactului produs”.	
		117.	La pct. 47. 5, urmează a se preciza în normă sau în nota de fundamentare a proiectului de regulament cine este „organului ierarhic superior sau autoritatea publică care exercită supravegherea administrativă și controlul administrativ al furnizorului de servicii publice care poate solicita efectuarea controlului inopinat al furnizorului public de servicii în sectoarele critice”.	**Precizare.** Este imposibil a fi indicat nominal organul ierarhic superior, or identificarea acestuia urmează a fi făcută individual pentru fiecare autoritate publică.
		118.	La pct. 65, recomandăm completarea normei cu termenul exact de extindere a controlului în cazul în care obiectivele stabilite la planificarea activității de control nu au fost atinse sau au apărut circumstanțe noi pentru a căror clarificare sunt necesare acțiuni suplimentare. Pe final, solicităm respectuos reevaluarea proiectului de regulament din perspectiva propunerilor enunțate în prezentul aviz și comunicăm disponibilitatea pentru a discuta în comun potențialele soluții de ordin legislativ și practic.	**Precizare.** Prelungirea controlului urmează a fi efectuată în termenele stabilite de cadrul normativ primar.

Ședința Grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**GL al Comisiei de stat pentru reglementarea activității de întreprinzător**	**1.**	Cu toate că proiectul propus derivă din Legea nr.131/2012 privind controlul de stat (și Legea nr. 48/2023) totuși pe parcursul proiectului atestăm o serie de norme care depășesc limitele de reglementare prevăzute de legile în cauză, ceea ce ar fi încălcarea art.14 din Legea nr.235/2006 dar și al principiului supremației legii, precum și o serie de norme care sunt în contradicție cu reglementări similare din Legea nr.131/2012. În special ne referim la următoarele: - La pct.5 se prevede dreptul Agenției de a iniția controale inopinate, avînd ca temei o simplă solicitare (indiferent de conținutul acesteia) de la alte organe de control, ceea ce este contrar prevederilor din art.19 din Legea nr.131/2012, care prevede o listă exhaustivă a temeiurilor pentru inițierea unui control inopinat;	**Se acceptă.**
		2.	La pct.10.3 în rîndul măsurilor de „supraveghere” (care în proiect nu sunt calificate ca și acțiuni de control de stat) se listează „solicitarea informațiilor necesare pentru determinarea gradului de conformitate cu cadrul normativ”. Atenționăm că în conformitate cu art.4 din Legea nr.131/2012 solicitarea informațiilor de la agenți economici reprezintă control de stat și necesită să se efectueze în temeiul delegației, respectînd procedura de control (chiar dacă inspectorul nu face o vizită la fața locului). Poate fi solicitată în afara controlului doar informația pe care agentul economic este obligat să o raporteze conform legii (tipul informației trebuie să fie clar specificat în lege), la care organul de control nu are acces, și informațiile care sunt indispensabile pentru planificarea controalelor în baza criteriilor de risc, conform metodologiei aferente domeniului de control și aceste informații agentul economic este obligat să le acorde în termen rezonabil. Din altă perspectivă, în	**Se acceptă.**

			procedura administrativă generală, autoritatea poate solicita oricare tip de informații necesare, însă agentul economic nu este obligat să o acorde;	
		3.	La pct.23 se admite ca controlul să fie realizat în lipsa reprezentantului agentului economic, ceea ce este contrar cu prevederile art.24 alin.(2) din Legea nr.131/2012, la care se prevede expres că în procesul efectuării controlului, inspectorul nu este în drept să efectueze, în cazul controlului inopinat, controale în lipsa reprezentanţilor persoanei supuse controlului, dacă există temeiuri de a considera că absenţa acestora este justificată. Totodată art.26 prevede că persoana controlată este obligată să asigure prezența conducătorului sau reprezentantului, cu atît mai mult că procesul-verbal de control urmează să fie semnat și de persoana controlată;	**Se acceptă.**
		4.	La pct.29 se prevede că procesul-verbal de control se semnează doar de inspectori, deși Legea nr.131/2012 prevede obligația semnării acestuia și de către persoana controlată. În același timp, la pct.30 se prevede că acest proces-verbal este remis persoanei controlate, care în 5 zile poate veni cu obiecții (și nu se prevede că trebuie să fie semnat de aceasta). Ceea ce la fel este contrar cu Legea nr.131/2012 care prevede că „persoana supusă controlului are dreptul, în termen de 10 zile lucrătoare de la semnarea procesului-verbal de control, să prezinte dezacordul cu actul în cauză, aducînd probe suplimentare ce confirmă poziţia sa”, după care, inspectorul examinează dezacordul și dacă este cazul emite un proces-verbal suplimentar în care reflectă modificările operate, comparativ cu procesul-verbal inițial. Aceste proceduri de semnare și analiză a procesului-verbal sunt expuse diferit în proiect, atenționăm că divergențele de norme între o Hotărîre de Guvern și o lege, întotdeauna se soluționează în favoarea legii;	**Se acceptă.**
		5.	- Contrar cu prevederile Legii nr.131/2012 care prevede că prescripțiile, recomandările și dispunerea de măsuri	**Nu se acceptă.**

			restrictive se indică direct în procesul-verbal de control (la compartimentul corespunzător), în proiect la pct.33 se prevede că „planul de măsuri pentru remediere” se întocmește ca un act distinct de procesul-verbal. Atenționăm că Legea nr.131/2012 în mod intenționat a comasat mai multe documente de procedură într-un singur proces-verbal, cu scopul de a exclude posibilitatea de a distorsiona în timp informația despre cele depistate în cadrul controlului și a elimina elemente de corupție și abuz;	Considerăm judicios posibilitatea de a anexa la procesul-verbal de control anumite măsuri la necesitate pentru remedierea deficienților reieșind din domeniul specific de control efectuat de către Agenție în coraport cu activitatea desfășurată de către furnizorul de servicii.
		6.	La pct.34 conceptual se diferențiază prescripțiile de o listă de alte măsuri pe care le poate impune inspectorul – „instrucțiuni obligatorii de remediere”, „dispune să înceteze conduita”, dispune obligatoriu să pună în aplicare recomandările auditului ș.a. Această abordare creează confuzii și poate duce la încălcarea principiului proporționalității intervenției prin control, odată ce favorizează aplicarea mai multor tipuri de măsuri restrictive și prescriptive în mod simultan. Astfel de abordare este contrară conceptual cu Legea nr.131/2012 care operează doar cu 3 categorii – prescripții (care conține indicații obligatorii pentru remedierea încălcărilor, care urmează ulterior să fie verificate), recomandări (care expun în mod facultativ cum persoana să evite încălcări pe viitor, îndeplinirea cărora nu este verificată de inspector), măsuri restrictive (sunt limitări care se dispun de inspector pentru a diminua prejudiciul sau riscul prejudiciului în timpul cît se remediază încălcările). Astfel, acordarea mai multor instrumente inspectorului, decît cele prevăzute de Legea nr.131/2012, nu reprezintă doar depășirea limitelor legii dar și poate crea situații de intervenții disproporționate sau chiar abuz din partea inspectorului.	**Precizare.** Considerăm că acțiunile enunțate la pct. 34 nu depășesc conceptual cele 3 principii cu care operează Legea 131/2012. Pct.34 doar oferă o dezvoltare a celor 3 principii enunțate, însă finalitatea acestora este identică cu ce este stipulat în Legea 131/2012.
		7.	**IV. Concluzie** Proiectul conține prevederi contradictorii cu principiile de reglementare ale activității de întreprinzător și divergențe cu cadrul legislativ superior.	**Se acceptă.** Proiectul și nota de fundamentare a fost ajustată corespunzător.

			Nota de fundamentare conține suficiente informații pentru a stabili de principiu oportunitatea intervenției, însă nu se argumentează necesitatea unor soluții și nu este analizat și expus suficient de desfășurat impactul asupra mediului privat, astfel corespunde parțial cu cerințele metodologice prevăzute de Legea nr.100/2017.	

Expertizare și notificare

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**Ministerul Justiției** *(nr. 04/2-12503 din 17.12.2025)*	**1.**	Sub aspectul intenției de reglementare, proiectul are drept temei juridic art. 18 alin. (3) și art. 19 alin. (5) din Legea nr. 48/2023 privind securitatea cibernetică (în continuare – Legea nr. 48/2023), care prevede competența Guvernului de a stabili măsurile de supraveghere a respectării legislației privind securitatea cibernetică, modul de aplicare a acestora, precum și de a stabili procedurile detaliate privind modul de efectuare a controlului de stat de către autoritatea competentă asupra respectării obligațiilor ce le revin furnizorilor de servicii în sectoarele critice. Totodată, potrivit notei de fundamentare, se atestă că proiectul de hotărâre urmărește realizarea obiectivului general al întregului cadru normativ în domeniul securității cibernetice și anume de creștere a nivelului de reziliență cibernetică a furnizorilor de servicii, privați sau publici, asigurând un nivel ridicat de protecție a rețelelor și sistemelor informatice ale acestor furnizori utilizate în procesul de prestare de către aceștia a serviciilor esențiale.	**Se acceptă.**
		2.	Aferent redacției proiectului se expun următoarele observații și propuneri de îmbunătățire a calității acestuia. ***La proiectul hotărârii:*** Denumirea proiectului de hotărâre se propune a fi revăzută, ținând cont că, potrivit pct. 1, proiectul are ca obiect	**Se acceptă.** Proiectul a fost completat corespunzător.

			principal aprobarea *Regulamentului cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice*.	
		3.	În clauza de adoptare a proiectului de hotărâre, referința la sursa publicării *Legii nr. 48/2023,* se va completa cu textul „ , art. 225”.	**Se acceptă.**
		4.	***La anexa proiectului*** - *Regulamentul cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice* (în continuare – *Regulament*): În parafa de aprobare, textul „nr. ___ din ____” sugerăm a fi substituit cu textul „nr. ___/2025”, în vederea respectării regulilor de tehnică legislativă și uzanțelor de redactare a actelor normative”.	**Se acceptă.**
		5.	Pentru a nu se dubla dispozițiile pct. 3, cuvintele „Agenția pentru Securitate Cibernetică” din pct. 1 se propun a fi substituite cu cuvintele „autoritatea competentă”. În pct. 3, se propune a se face referire și la *Regulamentul cu privire la organizarea și funcționarea Agenției pentru Securitate Cibernetică, aprobat prin Hotărârea Guvernului nr. 1028/2023*.	**Nu se acceptă.** Nu considerăm relevant trimiterea la Hotărârea de Guvern ce reglementează modul de organizare a Agenției. Obiectul de reglementare este al proiectului este diferit de cel propus.
		6.	Potrivit pct. 4, „Agenția exercită controlul de stat asupra respectării de către furnizorii de servicii a cadrului normativ în domeniul securității cibernetice în baza rezultatelor evaluării riscurilor de securitate cibernetică la nivel național, sectorial/subsectorial, intersectorial sau pe tipuri de furnizori de servicii în conformitate cu cadrul metodologic aprobat în conformitate cu art. 16 alin. (2) din Legea nr. 131/2012 privind controlul de stat.”. În context, se va asigura indicarea denumirii concrete a metodologiei la care se face referire. Subsecvent, nu este clar dacă cadrul metodologic la care se face referire în acest punct are tangență cu „Metodologia	**Precizare.** Pct. respectiv face trimitere expresă la metodologia care urmează a fi elaborată în baza art. 16 alin. (2) din Legea 131/2012.

			privind controlul de stat asupra activității de întreprinzător în baza analizei riscurilor aferent domeniilor de competență ale Agenției pentru Securitate Cibernetică” care, potrivit pct. 2 din proiectul hotărârii, Ministerul Dezvoltării Economice și Digitalizării, în comun cu Agenția pentru Securitate Cibernetică, au sarcina de a o elabora și prezenta Guvernului pentru aprobare, în termen de 12 luni de la data intrării în vigoare a respectivei hotărâri. În altă ordine de idei, în măsura în care aceasta se va elabora și aproba în termen de 12 luni de la data intrării în vigoare a respectivei hotărâri, nu este clar cum se va asigura realizarea sarcinilor Agenției pentru Securitate Cibernetică, prevăzute la pct. 4 din proiectul *Regulamentului*, până la aprobarea acestei metodologii de către Guvern.	
		7.	Complementar celor indicate mai sus, se va atrage atenție sporită la dispozițiile finale și cele tranzitorii ale proiectului, astfel încât să fie asigurată punerea în aplicare a dispozițiilor actului normativ prin rezervarea unui termen suficient de lung pentru aducerea în concordanță a actelor normative conexe. Totodată, recomandăm ca la elaborarea actelor normative să fie pregătit întreg pachetul de acte normative care necesită a fi aprobate/amendate, astfel încât ulterior să nu apară dificultăți privind punerea în aplicare a noilor soluții juridice și să se asigure coerența, stabilitatea și predictibilitatea normelor juridice.	**Precizare.** Hotărârea a fost completată cu un punct nou ce prevede intrarea în vigoare a prezentului proiect de Hotărâre la data publicării, reieșind din necesitatea de a respecta termenii stabiliți în Agenda de reforme.
		8.	La pct. 5, se vor revedea cuvintele „autorități de supraveghere și control a gestionarilor de infrastructură critică națională” și cuvintele „autoritatea de supraveghere și control de stat”, în vederea utilizării unei terminologii uniforme și constante în tot textul proiectului, precum și a unei terminologii juridice adecvate compatibile cu cea prevăzută în *Legea nr. 48/2023* și în *Legea nr. 131/2012 privind controlul de stat* (în continuare – *Legea nr. 131/2012*). De asemenea, se atestă că în textul *Regulamentului* se operează atât cu termenul de „furnizori	**Se acceptă parțial.** Proiectul a fost completat cu norme corespunzătoare.

			de servicii în 2 sectoarele critice”, cât și cu termenul „furnizori de servicii”. Termenul „furnizori de servicii” este utilizat și în cazul referinței la „furnizorii de servicii publice”(a se vedea, de ex. pct. 68, 71, ș.a.), motiv pentru care se consideră necesară uniformizarea terminologiei și în acest caz (observațiile sunt valabile în tot textul proiectului).	
		9.	La subpct. 6.5, cuvintele „Agenția pentru Securitate Cibernetică” se vor substitui cu cuvântul „Agenția”, având în vedere prescurtarea stabilită în pct. 3.	**Se acceptă.**
		10.	La pct. 8, pentru claritatea și previzibilitatea normei, se va analiza oportunitatea includerii tipurilor de măsuri care nu au caracter coercitiv, care vor fi aplicate de către Agenție în activitatea de supraveghere a furnizorilor de servicii în sectoarele critice. În măsura în care aceste tipuri de măsuri sunt reglementate în pct. 10, atunci în pct. 8 se va face trimitere la pct. 10.	**Precizare.** Pct. 8 este unul general ce menționează expres ca în procesul de monitorizare de către Agenție pot fi aplicate anumite măsuri, care sunt diferite de cele ce urmează a fi aplicate în cadrul controlului de stat.
		11.	Începând cu pct. 10, dispozițiile necesită a fi renumerotate, or, pct. 9 a fost omis.	**Se acceptă.**
		12.	Dispozițiile subpct. 10.2, 10.3 și 10.5 se propun a fi reformulate, în vederea stabilirii clarității normei. Astfel: - la subpct. 10.2, este oportun de indicat concret obiectul de reglementare a ghidurilor, orientărilor metodologice, etc; - la subpct. 10.3 este necesar de identificat de la cine se solicită informațiile; - la subpct. 10.5, norma se propune a fi completată cu cuvintele „aferente securității cibernetice” (observație similară valabilă și pentru subpct. 18.1).	**Se acceptă parțial.** La pct. 10.2 se menționează obiectul de reglementare – referitor la acordarea asistenței consultative furnizorilor de servicii în asigurarea conformității cu prevederile cadrului normativ în domeniul securității cibernetice.
		13.	Dispozițiile subpct. 10.9 se vor integra într-un punct distinct, având în vedere obiectul de reglementare al acestora, care diferă de dispozițiile subpct. 10.1-10.8.	**Se acceptă.**
		14.	La pct. 11 și 14, cuvântul „control” sugerăm a fi succedat de cuvintele „de stat”, întru asigurarea uniformității terminologice (observație valabilă și pentru alte puncte din proiect).	**Se acceptă.**

		15.	Pct. 12 se consideră a fi inutil, deoarece dublează, în parte, dispozițiile pct. 3, motiv pentru care se propune a fi exclus. Totodată, referința la „furnizorii de servicii persoane juridice de drept privat (în continuare - furnizori de servicii private)” se propune a fi substituită cu referința la „persoanele juridice de drept privat, identificate ca furnizori de servicii în sectoarele critice (în continuare - furnizori de servicii private)” (observație similară și pentru pct. 38, aferent referinței la termenul „furnizori de servicii publici”).	**Nu se acceptă.** Redacția respectivă a fost propusă pentru claritatea și accesibilitatea normei.
		16.	La pct. 14 și 46, se va indica procedura de selectare a inspectorilor Agenției care vor efectua controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii privați/publici. Astfel, considerăm relevant a face trimitere la art. 20 alin. (4) al Legii nr. 131/2012. Potrivit acestuia, inspectorii specificați în delegație sunt selectați în mod aleatoriu, luându-se în considerare și specializarea acestora conform domeniului de control aferent.	**Precizare.** Nu considerăm oportun completarea pct. respective, dat fiind faptul că Legea 131/2012 se aplică direct în cadrul controlului de stat. Respectiv art. 20 din lege urmează a fi aplicat corespunzător.
		17.	Referitor la dispozițiile prevăzute în pct. 16, 17 și 39, se va analiza suplimentar necesitatea acestora, ținând cont că reglementări generale se regăsesc în art. 4 alin. (111) și art. 15 alin. (3) al Legii nr. 131/2012, iar potrivit pct. 3 din proiectul Regulamentului, controlul de stat asupra respectării de către furnizorii de servicii în sectoarele critice a prevederilor cadrului normativ în domeniul securității cibernetice se realizează de către Agenție, în conformitate cu prevederile Legii nr. 131/2012.	**Precizare.** Considerăm oportun păstrarea acestora pentru claritatea și previzibilitatea actului normativ avizat.
		18.	Dispozițiile subpct. 18.5 se recomandă a fi expuse într-un punct distinct. Totodată, în partea ce vizează dispoziția „În cadrul sau în urma controlului de stat, la depistarea încălcărilor, inspectorul Agenției poate înainta prescripții și recomandări, aplica măsuri restrictive și sancțiuni în limitele prevăzute de lege. Acțiunile și măsurile se selectează și se aplică în conformitate cu prevederile Legii nr. 131/2012 privind controlul de stat.”, se va analiza	**Se acceptă.** Totodată, menționăm că de către Guvern urmează a se veni cu un proiect de modificare a Codului contravențional pentru stabilirea de sancțiuni în sensul menționat.

			necesitatea includerii inițiale în Codul contravențional a unor contravenții aferente securității cibernetice. Or, deși în art. 24 alin. (2) lit. g) al Legii nr. 131/2012 este prevăzut că în procesul efectuării controlului, inspectorul nu este în drept să aplice măsuri restrictive și/sau sancțiuni contravenționale pentru încălcările depistate în cadrul controlului cu încălcarea limitelor stabilite de respectiva lege, în Codul contravențional nu sunt stabilite anumite contravenții aferente încălcării reglementărilor privind securitatea cibernetică. Totodată, menționăm că potrivit art. 28 alin. (10) al Legii nr. 131/2012, „În cazul în care în procesul-verbal de control se constată o contravenție, acesta substituie procesul-verbal cu privire la contravenție, având regim juridic și forță juridică similare. Constatarea contravențiilor identificate în timpul efectuării controlului și aplicarea sancțiunilor, conform competenței, se vor efectua în limitele stabilite de prezenta lege și cu aplicarea cerințelor stabilite de Codul contravențional.”. Astfel, pentru aplicarea sancțiunilor de către Agenție este necesară intervenția inițială în Codul contravențional de a determina faptele care constituie contravenție în domeniul securității cibernetice și, respectiv, determinarea sancțiunilor aferente acestora. De asemenea, potrivit art. 385 din Codul contravențional persoana împuternicită cu atribuții de constatare a contravenției și/sau de sancționare este agentul constatator. Prin urmare, pentru aplicarea de către Agenție a unor sancțiuni, se va revedea necesitatea determinării în Codul contravențional a rolului de agent constatator funcționarului Agenției. În altă ordine de idei, dispoziția subpct. 18.5 este contrară subpct. 31.6 din proiect, care prevede că Agenția poate solicita autorităților publice competente aplicarea, în conformitate cu cadrul normativ, a unei sancțiuni proporționale încălcării și impactului produs. În acest sens, nu este clar cui i se atribuie calitatea de agent constatator al	Referitor la pct. 18.5 și 31.6 menționăm că prevederile de la pct. 31.6 se referă în caz de necesitate de implicare a altor autorități competente urmare a controlului. Nu se referă la competența Agenției de a aplica sancțiuni în baza Legii 131/2012.

			încălcării contravenționale comise în domeniul securității cibernetice și, respectiv, rolul de aplicare a sancțiunii contravenționale.	
		19.	Dispozițiile pct. 19 se recomandă a fi comasate la dispozițiile pct. 14.	**Se acceptă.**
		20.	La pct. 23, textul „Legea 131/2012” se va substitui cu textul „Legea nr. 131/2012 privind controlul de stat”, iar la pct. 26, textul „Legea nr. 48/2023” se va completa cu cuvintele „privind securitatea cibernetică”. Totodată, în scopul includerii unor prescurtări a actelor normative menționate, la prima utilizare în text a acestora se va indica „(în continuare - Legea nr. 131/2012)” și „(în continuare – Legea nr. 48/2023)”.	**Se acceptă.**
		21.	La pct. 27, textul „la pct. 27” se va substitui cu textul „la pct. 26”. Suplimentar dispoziției propuse la pct. 27, atragem atenția că potrivit art. 15 alin. (3) al *Legii nr. 48/2023*, autoritatea competentă notifică, fără întârzieri nejustificate și nu mai târziu de 24 de ore, cu privire la aplicarea măsurilor prevăzute la alin. (2), utilizatorii și, în cazul furnizorului de servicii, autoritatea publică care realizează politica de stat în domeniul respectiv și, după caz, autoritatea cu funcții regulatorii pe piața din domeniul în care se prestează serviciul respectiv.	**Se acceptă.**
		22.	Pct. 28 prevede că „Constatările efectuate pe timpul verificărilor, concluziile și măsurile propuse se reflectă în procesul-verbal de control, care se semnează de toate persoanele cooptate pentru efectuarea controlului.”. În acest sens, se vor revedea cuvintele „toate persoanele cooptate pentru efectuarea controlului”, or, nu este clar dacă prin aceste cuvinte se face referire și la persoana supusă controlului. În acest sens, atragem atenția că potrivit art. 28 alin. (3) al Legii nr. 131/2012, procesul-verbal de control se întocmește în format electronic și se semnează cu semnătură electronică calificată de către toți inspectorii și de către	**Se acceptă.**

			persoana supusă controlului/persoana împuternicită cu funcții de răspundere (observație valabilă și pentru pct. 62).	
		23.	La pct. 31: - potrivit subpct. 6, pe lângă prescripțiile emise și sancțiuni aplicate în temeiul procesului-verbal de control, Agenția poate solicita autorităților publice competente aplicarea, în conformitate cu cadrul normativ, a unei sancțiuni proporționale încălcării și impactului produs. Este de menționat că, norma citată este ambiguă și imprevizibilă. Astfel, nu este clar cine va aplica sancțiunile în temeiul procesului-verbal. Totodată, Agenția nu poate poate avea competența de a solicita altor autorități publice de a aplica sancțiuni, or, în cazul depistării unor încălcări care ține de competența unor altor autorități publice, cum ar fi, de exemplu, sesizării unor infracțiuni, organul de control transmite materialele către organul de urmărire penală, iar acesta decide existența sau inexistența caracterului infracțional al faptei și necesitatea aplicării unor sancțiuni. Totodată, la definitivarea normelor, în special a cuvintelor „pe lângă prescripțiile emise și sancțiuni aplicate în temeiul procesului-verbal de control” în coraport cu cuvintele „Agenția poate solicita autorităților publice competente aplicarea, în conformitate cu cadrul normativ, a unei sancțiuni proporționale încălcării și impactului produs” se va ține cont că pentru una și aceiași faptă, o persoană nu poate fi sancționată de mai multe ori (a se vedea art. 380 alin. (1) din *Codul contravențional*); - subdiviziunile cuprinse în acest punct se vor numerota în conformitate cu art. 52 alin. (3) al *Legii nr. 100/2017 cu privire la actele normative* (în continuare – *Legea nr. 100/2017*). Potrivit acestuia, pentru interpretare corectă și aplicare comodă, punctele pot fi divizate în subpuncte care se numerotează prin adăugarea consecutivă a cifrelor arabe, până la gradul de detaliere necesar.	**Se acceptă parțial.** Pct. respectiv a fost renumerotat corespunzător. Totodată menționăm că urmează a se vedea comentariu de la pct. 18.

		24.	Pct. 33 se recomandă a fi exclus, deoarece reglementări similare sunt prevăzute în pct. 24 din proiect.	**Precizare.** Considerăm relevant menținerea ambelor puncte pentru claritatea proiectului.
		25.	La pct. 35 și 73, considerăm necesar a fi stabilit un termen maxim pe care poate să-l solicite furnizorul de servicii privat/publici, pentru remedierea deficiențelor sesizate de către Agenție, ținând cont de reglementările și termenii prevăzuți în acest sens în *Legea nr. 131/2012*.	**Precizare.** Este greu de a stabili un termen exact pentru implementarea măsurilor de securitate. Astfel, acest termen urmează a fi coordonat cu Agenția pentru a putea realiza măsurile respective.
		26.	În subpct. 40.3, textul „Cerințele privind măsurile de securitate a rețelelor și a sistemelor informatice ale furnizorilor de servicii în sectoarele critice, aprobate prin Hotărârea Guvernului nr. 562/2025” se va substitui cu textul „anexa la Regulamentul cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice, aprobat prin Hotărârea Guvernului nr. 562/2025”.	**Se acceptă.**
		27.	Pct. 45 nu corespunde întocmai prevederilor art. 20 alin. (2) al Legii nr. 131/2012. Mai mult, se consideră inutile dispozițiile care prevăd ce trebuie să conțină delegația de control, având în vedere că aceste aspecte sunt reglementate exhaustiv în art. 20 alin. (2) al *Legii nr. 131/2012*.	**Precizare.** Pentru claritatea și previzibilitatea actului normativ, considerăm relevant menținerea textului respectiv. Totodată, menționăn că controlul în privința furnizorilor publici nu este guvernat de prevederile Legii nr. 131/2012.
		28.	La pct. 46, se atestă că angajații Agenției care vor efectua controlul se identifică, în continuare prin „echipa de control”, pe când la pct. 14 din proiect, angajații Agenției care vor efectua controlul se identifică ca inspectori ai Agenției. În context, se constată lipsa de uniformizare terminologică în textul proiectului. Astfel, relevante sunt dispozițiile art. 54 alin. (1) lit. c) al *Legii nr. 100/2017*, care prevede că terminologia utilizată în actul normativ trebuie	**Precizare.** Sunt 2 tipuri de controale diferite, respectiv și normele urmează a fi reglementate diferit, inclusiv și în baza temeiului de adoptare a proiectului supus consultării.

			să fie constantă, uniformă și să corespundă celei utilizate în alte acte normative.	
		29.	Aferent dispozițiilor pct. 47, se va revedea necesitatea acestora, întrucât în art. 18 alin. (1) al *Legii nr. 131/2012* este prevăzut deja că, organul de control va expedia persoanei supuse controlului un exemplar al delegației de control astfel încât între momentul primirii efective a exemplarului şi momentul începerii controlului să treacă cel puțin 5 zile lucrătoare, dar nu mai mult de 15 zile lucrătoare.	**Nu se acceptă.** Prevederile Legii 131/2012 urmează a se aplica asupra furnizorilor de servicii privați, pe când pentru cei din sectorul public a fost reglementat Capitolul IV. Această reglementare derivă inclusiv din temeiul de adoptare, unde e stipulat expres în Legea 48/2023 că de către Guvern urmează a fi reglementare proceduri diferite pentru sectorul public și cel privat.
		30.	La pct. 50, se va indica concret la ce cadrul normativ se face referire.	**Precizare.** Nu poate fi menționat exact un act normativ, fiindcă urmează a se aplica corespunzător diferite acte normative.
		31.	Al doilea enunț al pct. 53 și 54 se propune a fi exclus, deoarece dublează dispozițiile art. 22 alin. (1) și (2) din *Legea nr. 131/2012*. Subsecvent, din punct de vedere redacțional și al regulilor de tehnică legislativă, din pct. 54 textul „la pct. anterior” necesită a fi substituit cu textul „pct. 53”.	**Precizare.** Urmează a se vedea comentariul de la pct. 29.
		32.	În partea ce vizează drepturile și obligațiile persoanelor care efectuează controlul de stat, prevăzute la pct. 55 și 56, menționăm că acestea nu sunt întocmai conforme cu art. 23 și 24 din *Legea nr. 131/2012*. Or, în aceste articole sunt prevăzute mai multe drepturi și obligații ale inspectorilor, care de altfel sunt expuse exhaustiv. Mai mult, întru respectarea regulilor de tehnică legislativă se recomandă evitarea dublajului normativ.	**Precizare.** Urmează a se vedea comentariul de la pct. 29.
		33.	De asemenea, se va analiza suplimentar necesitatea pct. 57 și 58, aferente drepturilor și obligațiilor furnizorului de serviciu public, în calitate de persoană supusă controlului, ținând cont că aceste drepturi și obligații sunt prevăzute	**Precizare.** Urmează a se vedea comentariul de la pct. 29.

			exhaustiv în art. 6 25 și 26 ale Legii nr. 131/2012. Complementar, se va revizui conformitatea drepturilor și obligațiilor prevăzute la pct. 57 și 58 cu dispozițiile articolelor citate.	
		34.	La pct. 59, sugerăm a se completa cu textul „conform art. 24 și 26 ale Legii nr. 131/2012 privind controlul de stat”.	**Precizare.** Urmează a se vedea comentariul de la pct. 29.
		35.	Dispozițiile pct. 60 se vor comasa la dispozițiile pct. 70, având în vedere că au același obiect de reglementare.	**Nu se acceptă.** Considerăm oportun menținerea ambelor puncte pentru claritate.
		36.	La pct. 63, menționăm că părțile componente ale procesului-verbal nu sunt conforme cu art. 28 alin. (2) al Legii nr. 131/2012. Or, în articolul citat sunt indicate mai multe elemente constitutive ale procesului -verbal.	**Precizare.** Urmează a se vedea comentariul de la pct. 29.
		37.	Pct. 66 prevede că „Proiectul procesului-verbal se prezintă furnizorului de servicii, oferind un termen de 10 zile lucrătoare pentru prezentarea observațiilor, cu excepția cazurilor justificate în mod corespunzător, când sunt în desfășurare acțiuni imediate pentru a preveni sau răspunde la un incident.”. Astfel, norma citată se va revizui prin prisma art. 28 alin. (6) al *Legii nr. 131/2012*, care prevede că „Persoana supusă controlului are dreptul, în termen de 10 zile lucrătoare de la semnarea procesului-verbal de control, să prezinte dezacordul cu actul în cauză, aducând probe suplimentare ce confirmă poziția sa. Inspectorul examinează materialele prezentate şi, după caz, întocmește un proces-verbal de control adițional, fără a opera rectificări în actul de bază. În procesul-verbal de control adițional se indică procesul-verbal de bază, iar în partea constatatoare se reflectă pozițiile modificate, cu respectarea procedurii de întocmire a procesului-verbal de control, inclusiv a celei de anexare a documentelor. Dreptul de a prezenta dezacordul nu afectează şi nici nu limitează posibilitatea contestării procesului-verbal de control în modul stabilit de lege.”. În context, conform dispozițiilor legale citate se constată că	**Precizare.** Urmează a se vedea comentariul de la pct. 29.

			persoana supusă controlului are dreptul în termen de 10 zile lucrătoare de la ***semnarea procesului-verbal de control*** și nu de la ***prezentarea proiectului procesului-verbal*** să prezinte dezacordul cu actul în cauză. Subsecvent, în partea ce vizează excepția prevăzută în pct. 66 - „cu excepția cazurilor justificate în mod corespunzător, când sunt în desfășurare acțiuni imediate pentru a preveni sau răspunde la un incident”, menționăm că *Legea nr. 131/2012*, inclusiv art. 28 alin. (6) al acesteia, nu prevede o asemenea excepție.	
		38.	Suplimentar la proiect, se atestă existența unui dezechilibru între reglementările aferente controlului de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către persoanele juridice de drept privat, identificate ca furnizori de servicii în sectoarele critice (capitolul III) și controlul de stat al respectării cadrului normativ în domeniul securității cibernetice de către persoanele juridice de drept public, identificate ca furnizori de servicii în sectoarele critice (capitolul IV). Astfel, informația nu este sistematizată după aceleași principii/obiect de reglementare. Spre exemplu, în capitolul IV, aferent controlului de stat al respectării cadrului normativ în domeniul securității cibernetice de către persoanele juridice de drept public, identificate ca furnizori de servicii în sectoarele critice, este indicat ce trebuie să conțină delegația de control (pct. 45), însă în capitolul III, aferent controlului de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către persoanele juridice de drept privat, identificate ca furnizori de servicii în sectoarele critice, aceste reglementări nu există. De asemenea, în capitolul IV sunt indicate situațiile concrete în care poate fi efectuat controlul inopinat (pct. 43), pe când în capitolul III, situațiile sunt prezentate sub formă generalizată (pct. 13). În partea ce vizează procedura de desfășurare a controlului privind respectarea cadrului normativ în domeniul securității cibernetice de către	**Precizare.** Urmează a se vedea comentariul de la pct. 29.

			persoanele juridice de drept public, identificate ca furnizori de servicii în sectoarele critice, menționăm că aceasta, la fel, este mult mai detaliată decât cea prevăzută în capitolul III. Astfel, atragem atenția că potrivit art. 3 alin. (1) lit. c) al *Legii nr. 100/2017*, la elaborarea unui act normativ se respectă ***principiul echilibrului între reglementările concurente***. Mai mult, la definitivarea proiectului se va evita pe cât posibil dublarea dispozițiilor prevăzute de Legea nr. 131/2012 sau, alternativ, se va face trimitere la articolul concret din legea citată, fără a reproduce norma. Totodată, dispozițiile vor fi expuse clar și previzibil, astfel încât la aplicarea acestora să nu existe interpretări diferite sau eronate. Concomitent, în proiect se impune o clarificare legată de aplicarea reglementărilor raportând la domeniile exceptate de la prevederile Legii nr. 131/2012. Astfel, cu toate că proiectul este elaborat în temeiul Legii nr. 48/2023, art. 19 alin. (1) din aceeași lege prevede că „Autoritatea competentă exercită controlul de stat asupra respectării prezentei legi de către furnizorii de servicii persoane juridice de drept privat, aplicând prevederile Legii nr. 131/2012 privind controlul de stat”. Astfel, proiectul de Regulament trebuie să stabilească în mod explicit modul în care excepțiile stabilite în Legea nr. 131/2012 se aplică în contextul controlului de stat asupra securității cibernetice, asigurându-se astfel o aplicare coerentă și corectă a reglementărilor. Este esențial, din perspectiva unei reglementări clare și eficiente, ca proiectul de Regulament să precizeze explicit în ce măsură ASC va interveni în domeniile exceptate și cum se va face distincția între controalele de securitate cibernetică și cele care sunt efectuate de alte autorități.	

2.	**Cancelaria de Stat**	**39.**	În scopul conformării la prevederile Legii nr. 131/2012 privind controlul de stat și la prevederile art. 19 alin (5) din Legea nr. 48/2023 cu privire securitatea cibernetică. Pct. 38 și 39 din proiect urmează a fi redat în următoarea redacție: „Controlul respectării de către furnizorii de servicii în sectoarele critice care sunt persoane juridice de drept public (în continuare - furnizorii de servicii publici) se efectuează de Agenție în conformitate cu prevederile Legii nr. 131/2012 privind controlul de stat. Pct. 39 Planul anual al controlului respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii publici (în continuare - Planul) se aprobă de către Directorul Agenției și se publică pe site-ul web oficial al acesteia nu mai târziu de data de 15 a lunii care precedă perioada de gestiune.”	**Precizare.** Urmează a se vedea comentariul de la pct. 29.
3.	**Ministerul Afacerilor Interne** *(Nr. 38/4442 din 17.12.2025)*	**40.**	Astfel, se relevă că, recomandarea formulată la pct. 1, nu a fost acceptată de autor, cu argumentarea faptului precum că, elaborarea proiectului are drept temei legal art. 19 din Legea nr. 48/2023 privind securitatea cibernetică, în timp ce Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale, ar avea un obiect de reglementare diferit. Pe această cale, se reiterează că propunerea de includerea referinței la Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale, nu urmărește modificarea sau extinderea temeiului legal al proiectului, stabilit în mod expres la art. 19 din Legea nr. 48/2023 privind securitatea cibernetică, întrucât observația vizează exclusiv asigurarea coerenței și corelării cadrului normativ aplicabil, având în vedere că subiecții supuși supravegherii și controlului în temeiul proiectului de act normativ, coincid, în mod obiectiv, cu categoria gestionarilor de infrastructuri critice naționale, reglementată de Legea nr. 223/2025.	**Nu se acceptă** Proiectul de hotărâre propus are drept temei legal prevederile art. 19 din Legea 48/2023. Controlul pe care urmează să îl efectueze furnizorii de servicii se referă la implementarea măsurilor de securitate cibernetică, iar legea pe care ați menționat-o, are în general alt obiect de reglementare, fiind tangențial diferit de obiectul proiectului supus discuției. Astfel, menționăm repetat că Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale, nu poate fi inclusă în proiect, dat fiind faptul că nu se referă la control, ci la identificarea și desemnarea

			În acest sens, referința propusă la Legea nr. 223/2025 are caracter complementar și sistemic, fiind destinată evitării interpretărilor divergente și a eventualelor suprapuneri sau lacune de reglementare, fără a afecta obiectul sau mecanismele de control instituite prin Legea nr. 48/2023. În vederea realizării acestui obiectiv, se menține propunerea de completare a pct. 1 al Regulamentului, după cum urmează: „Prezentul Regulament se aplică în concordanță cu prevederile Legii nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale, în special în ceea ce privește obligațiile gestionarilor de infrastructuri critice naționale și mecanismele de protecție și informare aferente acestora.”. În rest, se comunică despre susținerea de principiu a proiectului de act normativ în redacția actuală, cu recomandarea către autor de a face claritate la pct. 27 din Regulamentul cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice, la care condiții îndeplinite cumulativ se face referire.	infrastructurilor critice naționale și evaluarea necesității de a îmbunătăți protecția acestora în scopul creșterii capacității de asigurare a stabilității, securității și siguranței sistemelor economice, sociale și a protecției persoanelor.
4.	**Banca Națională a Moldovei** *(Nr. 31-002/160/6567 din 18.12.2025)*	**41.**	BNM constată că, deși proiectul de hotărâre a preluat unele propuneri procedurale în urma procesului de avizare, obiecțiile de fond semnalate în avizul nr. 31-002/151/6250 din 05.12.2025 privind suprapunerea atribuțiilor de supraveghere și control ale BNM și Agenția pentru Securitatea Cibernetică (în continuare – ASC) asupra furnizorilor de servicii în sectorul bancar, regimul măsurilor restrictive, procedurile de control aplicabile în raport cu BNM, regimul secretului profesional aplicabil în cadrul BNM și în sectorul bancar nu au fost acceptate și rămân insuficient clarificate. Reținem că, în sinteză, autorul acceptă parțial ideea coordonării cu BNM a mecanismului de control a	**Nu se acceptă.** Considerăm că argumentele expuse anterior urmează a fi luate în considerare și la actuala observație. Totodată, menționăm că proiectul a fost completat cu suficiente prevederi și eventuale mecanisme de cooperare între Agenție și Banca Națională. Deja la nivel de implementare urmează cele 2 instituții să stabilească cea mai optimă platformă de cooperare pentru realizarea controlului de stat în vederea respectării de către furnizorii

			furnizorilor de servicii din sectorul bancar și indică posibilitatea reglementării acesteia printr-un acord sau memorandum de înțelegere între ASC și BNM, precum și deschiderea ASC pentru acorduri interinstituționale în ceea ce privește dimensiunea de bancă centrală. Cu toate acestea, din perspectiva riscurilor, un memorandum de înțelegere este necesar, dar nu este suficient, în absența consacrării în proiect a garanțiilor esențiale cu referire la aspectele invocate. Memorandumul urmează a fi conceput ca un instrument de implementare, vizând canalele de schimb de informații, coordonarea controalelor, gestionarea situațiilor de criză, precum și clasificarea și protecția informațiilor, în timp ce proiectul de hotărâre urmează să conțină cadrul minim obligatoriu care să prevadă coordonarea ASC și BNM în supravegherea furnizorilor de servicii din sectorul bancar, precum și aspectul privind reglementarea prin acord (memorandum) a mecanismului de evaluare a securității sistemului informațional al BNM. Acest model este pe deplin aliniat exemplelor europene invocate în avizul BNM, respectiv Memorandumul din 2018 privind securitatea cibernetică în sectorul financiar încheiat între autoritățile publice franceze ACPR (Autorité de Contrôle Prudentiel et de Résolution) și ANSSI (Agence nationale de la sécurité des systèmes d'information) și cooperarea dintre Banca Lituaniei și Centrul Național de Securitate Cibernetică. În contextul dat, BNM menține obiecțiile expuse în avizul BNM nr. 31- 002/151/6250 din 05.12.2025 și reiterează necesitatea completării proiectului cu prevederi privind acțiunile de coordonare între BNM și ASC în sectorul bancar, inclusiv coordonarea prealabilă a controalelor planificate, a măsurilor cu potențial impact operațional semnificativ; inaplicabilitatea cadrului general de control în raport cu sectorul bancar; procedurile de control aplicabile în raport cu BNM, având în vedere principiile aplicabile activității și statutului unei bănci centrale; garanții explicite	de servicii din sectorul bancar a măsurilor de securitate cibernetică.

			privind protecția datelor ce reprezintă secret profesional, secret bancar ș.a. BNM își exprimă disponibilitatea în vederea identificării celor mai adecvate soluții normative, în scopul atingerii obiectivului comun de consolidare a rezilienței cibernetice pentru componenta aferentă sectorului financiar.	
5.	**Serviciul Tehnologia Informației și Securitate Cibernetică** *(nr. 1.4/1998/25 din 19.12.2025)*	**42.**	La pct. 3, după textul „Legii nr. 131/2012 privind controlul de stat” se va completa cu textul „în partea furnizorilor de servicii persoane juridice de drept privat”. Argumentul din Sinteza obiecțiilor și propunerilor/ recomandărilor la proiectul hotărârii, precum că „Pct. 3 se referă la aspecte generale privind efectuarea controlului de stat de către Agenție” nu este unul plauzibil, întrucât Regulamentul stabilește cadrul juridic, organizatoric și procedural de exercitare de către Agenția pentru Securitate Cibernetică (în continuare Agenție) a funcției de supraveghere și control de stat al modului în care furnizorii de servicii în sectoarele critice, adică furnizorii de servicii persoane juridice de drept public și furnizorii de servicii persoane juridice de drept privat, asigură conformitatea cu prevederile cadrului normativ în domeniul securității cibernetice. Or, potrivit art. 9 alin. (1) din Legea nr. 48/2023 privind securitatea cibernetică, ținând cont inclusiv de art. 1 alin. (1) din Legea nr. 131/2012 privind controlul de stat, prevederile Legii nr.131/2012 se aplică doar în raport cu exercitarea controlului de stat față de furnizorii de servicii persoane juridice de drept privat.	**Precizare.** Pct. 3 este unul general care menționează general ce acte normative urmează a fi aplicate de către Agenție în cadrul efectuării supravegherii și controlului de stat. Este evident faptul că Legea 131/2012 urmează a se aplica doar către furnizorii persoane juridice de drept privat, reieșind din obiectul de reglementare al actului respectiv.
		43.	La pct. 18.5., deși autorul a expus cuprinsul acestuia în redacție nou, va exclude sintagma „și sancțiuni”. Reieșind din prevederile Legii nr. 48/2023 și Regulamentul cu privire la organizarea și funcționarea Agenției pentru Securitate Cibernetică, aprobat prin Anexa nr. 1 la Hotărârea Guvernului nr.1028/2023, Agenția nu este învestită cu competența de constatare a contravențiilor, respectiv aplicare a sancțiunilor.	**Nu se acceptă.** Agenția urmează să fie investită de Parlament cu competențe în acest sens.

			În contextul acestei obiecții, se va ajusta tot cuprinsul proiectului, inclusiv pct. 31.	
		44.	Cu referire la sbp. 40.3 reiterăm. Prin Hotărârea Guvernului nr. 562/2025 s-a aprobat Regulamentul cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice, aplicabil inclusiv furnizorilor de servicii persoane juridice de drept privat. Din acest considerent, autorul va completa Capitolul III cu o prevedere similară.	**Nu se acceptă.** Nu considerăm necesar introducerea textului respectiv și în Capitolul III. A fost propus exclusiv pentru Capitolul IV pentru planificarea controalelor la furnizorii de servicii, persoane juridice de drept public.
		45.	Alineatul al doilea de la pct. 43.5 se va expune întru-un punct nou.	**Se acceptă.**
		46.	La pct. 50, autorul va indica expres în proiectul supus avizării „modul de documentare al activității de control” sau „cadrul normativ” la care se referă.	**Nu se acceptă.** Textul punctului respectiv este unul generic și urmează a fi aplicat corespunzător.
		47.	Cu referire la punctele 55-58, reiterăm necesitatea revizuiri acestora în vederea uniformizării drepturilor și obligațiilor echipelor de control și a furnizorilor de servicii în sectoarele critice în procesul de efectuare a controlului. Evitând crearea unui cadru restrictiv sau defavorabil pentru persoanele juridice de drept public, autorul va stabili un regim juridic identic pentru furnizorii de servicii persoane juridice de drept public și de drept privat, cu alinierea după caz a normelor din Capitolul IV la rigorile Legii nr. 131/2012.	**Nu se acceptă.** Nu poate fi stabilit un regim juridic identic, reieșind din faptul că temeiul legal de adoptare prezentului act normativ menționează expres că urmează a fi stabilitate separat pentru persoanele juridice de drept și de drept privat proceduri privind efectuarea controlului de stat.
		48.	În această ordine de idei, prin prisma prevederilor art. 19 alin. (5) din Legea nr. 48/2023, este imperativ ca autorul să asigure o redactare clară și neechivocă a proiectului supus avizării repetate, reglementând explicit procedurile de control exercitate de Agenția pentru Securitate Cibernetică. O astfel de abordare este esențială pentru a garanta furnizorilor de servicii în sectoarele critice, în special celor de drept public, predictibilitatea necesară în îndeplinirea obligațiilor legale și pentru a facilita o aplicare uniformă a	**Se acceptă parțial.** Textul proiectului a fost completat cu unele norme suplimentare.

			Regulamentului în raport cu cadrul normativ conex. Or, în redacția actuală, proiectul nu stabilește proceduri detaliate și echivalente pentru furnizorii de servicii persoane juridice de drept public în raport cu cei de drept privat. În timp ce sectorul privat beneficiază de protecția normativă a Legii nr. 131/2012, Capitolul IV lasă loc multor decizii arbitrare. În consecință, se impune revizuirea mecanismelor de control pentru furnizorii de servicii persoane juridice de drept public, astfel încât acestea să beneficieze de aceleași rigori procedurale și protecții juridice ca și furnizorii de servicii persoane juridice de drept privat.	
6.	**Centrul Național Anticorupție**	**49.**	**I. Analiza riscurilor de corupere a procesului de promovare a proiectului** **I.1. Pertinența autorului, categoriei propuse a actului și a procedurii de promovare a proiectului** Autor al proiectului de act normativ este Guvernul, iar autor nemijlocit este Ministerul Dezvoltării Economice și Digitalizării, ceea ce corespunde art.102 din Constituție, art.14 din Legea nr.100/2017 cu privire la actele normative. Categoria actului normativ propus este Hotărâre a Guvernului, ceea ce corespunde art.102 din Constituție, art.6 și art.14 din Legea nr.100/2017 cu privire la actele normative.	**S-a luat act**
		50.	**I.2. Respectarea rigorilor de transparenţă în procesul decizional la promovarea proiectului** Potrivit art.8 al Legii nr.239/2008 privind transparenţa în procesul decizional *„etapele asigurării transparenţei procesului de elaborare a deciziilor sunt:* *a) informarea publicului referitor la iniţierea elaborării deciziei;* *b) punerea la dispoziţia părţilor interesate a proiectului de decizie şi a materialelor aferente acestuia;* *c) consultarea cetăţenilor, asociaţiilor constituite în corespundere cu legea, altor părţi interesate;*	**S-a luat act**

			d) examinarea recomandărilor cetăţenilor, asociaţiilor constituite în corespundere cu legea, altor părţi interesate în procesul de elaborare a proiectelor de decizii; *e) informarea publicului referitor la deciziile adoptate".* Totodată, art.10 din Legea nr.239/2008 stabileşte expres că: *„(1) Autoritatea publică asigură accesul la proiectele de decizii şi la materialele aferente acestora prin publicarea obligatorie a lor pe pagina web oficială a autorităţii publice, prin asigurarea accesului la sediul autorităţii, precum şi prin expediere prin poştă sau prin alte mijloace disponibile, la solicitarea persoanei interesate.* *(2) Proiectul de decizie şi materialele aferente acestuia se plasează pe pagina web oficială a autorităţii publice responsabile cel puţin pentru perioada recepţionării şi examinării recomandărilor".* Proiectul, însoțit de nota informativă și anunțurile inițierea elaborării proiectului și consultarea publică a acestuia, se regăsesc pe pagina web oficială a autorului și portalul particip.gov.md, după cum urmează: https://particip.gov.md/ro/document/stages/anunt-de-consultare-publica-privindproiectul-hotararii-guvernului-cu-privire-la-supravegherea-si-co/15524 Astfel, în procesul de promovare a proiectului, au fost respectate rigorile de asigurare a transparenţei decizionale statuate de prevederile art.8 lit.a)-d) al Legii nr.239-XVI din 13 noiembrie 2008 privind transparenţa în procesul decizional.	
		51.	**I.3. Scopul anunțat și scopul real al proiectului** Potrivit notei de fundamentare, proiectul are drept scop creștere a nivelului de reziliență cibernetică a furnizorilor de servicii, privați sau publici, asigurând un nivel ridicat de protecție a rețelelor și sistemelor informatice ale acestor furnizori utilizate în procesul de prestare de către aceștia a serviciilor esențiale.	**S-a luat act**

		52.	**I.4. Interesul public şi interesele private promovate prin proiect** Implementarea prevederilor propuse, poate contribui la realizarea interesului public vizat de proiect, fapt care nu este detrimentul interesului public general (în sensul prevăzut de prevederile Legii integrităţii nr.82 din 25 mai 2017) în condițiile revizuirii proiectului potrivit recomandărilor vizate de compartimentul III al prezentului raport.	**S-a luat act**
		53.	**I.5. Justificarea soluțiilor proiectului** **I.5.1. Suficienţa argumentării din nota informativă.** În conformitate cu art.30 al Legii nr.100/2017 cu privire la actele normative, proiectele de acte normative sunt însoțite de *„nota de fundamentare care cuprinde:* *a) denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ;* *b) condițiile ce au impus elaborarea proiectului actului normativ;* *c) obiectivele urmărite și soluțiile propuse;* *d) analiza impactului de reglementare;* *e) compatibilitatea proiectului actului normativ cu legislația UE;* *f) avizarea și consultarea publică a proiectului actului normativ;* *h) modul de încorporare a actului în cadrul normativ existent;* *i) măsurile necesare pentru implementarea prevederilor proiectului actului normativ."* Nota informativă a proiectului a fost structurată potrivit exigențelor de tehnică legislativă statuate de prevederile art.30 lit.a)-f) al Legii cu privire la actele normative nr.100 din 22 decembrie 2017. **I.5.2. Argumentarea economică-financiară.** Conform art.30 lit.d) al Legii nr.100/2017 cu privire la actele normative, nota de fundamentare trebuie să conțină	**S-a luat act**

			„d) analiza impactului de reglementare". Potrivit notei informative a proiectului *Impactul financiar direct al proiectului asupra mediului de afaceri este reprezentat de costurile administrative ce urmează a fi suportate de către agenții economici.*	
		54.	**II. Analiza generală a factorilor de risc ale proiectului** **II.1. Limbajul proiectului** Potrivit art.54 al Legii nr.100/2017 cu privire la actele normative *„textul proiectului actului normativ se elaborează [...] cu respectarea următoarelor reguli: [...]* *a) se expune într-un limbaj simplu, clar şi concis [...]* *c) terminologia utilizată este constantă, uniformă şi corespunde celei utilizate în alte acte normative, în legislația Uniunii Europene și în alte instrumente internaționale la care Republica Moldova este parte, cu respectarea prevederilor prezentei legi; [...]* *e) se interzice folosirea neologismelor dacă există sinonime de largă răspândire, [...]* *f) se evită folosirea [...] a cuvintelor și expresiilor [...] care nu sînt utilizate sau cu sens ambiguu;* *g) se evită tautologiile juridice;* *h) se utilizează, pe cât este posibil, noțiuni monosemantice, [...]".* Redacția propusă necesită o reconsiderare prin prisma normelor de tehnică legislativă citate supra, or operează cu *o terminologie neuniformă în abordarea aspectelor reglementate(”autoritățile competente”, ”organele de urmărire penală”, ”organului de urmărire penală sau procurorului”; ” constată”/”a depistat şi,”.) și expresii ambigue (”după caz,”, ”În limitele admisibile”, ”obiectivele stabilite la planificarea activității de control nu au fost atinse”, ”necesare pentru realizarea controlului”)*, care periclitează certitudinea reglementării și poate condiționa multiple riscuri de corupție la etapa implementării.	**S-a luat act**

		55.	**II.2. Coerența legislativă a proiectului** Prevederile proiectului necesită o reconsiderare prin prisma Legii privind securitatea cibernetică nr. 48/2023 și Legii privind controlul de stat nr.131/2012 sub aspectul reglementării temeiurilor inițierii controlului de stat și aspectelor procedurale aferente desfășurării acestuia.	**S-a luat act**
		56.	**II.3. Activitatea agenţilor publici şi a entităților publice reglementată în proiect** Prevederile proiectului reglementează preponderent activitatea desfășurată de către Agenția pentru Securitate Cibernetică. Analiza prevederilor propuse, denotă unele deficiențe ce pot condiționa disfuncționalități ale proceselor administrative reglementate și multiple riscuri de corupție aferente - *inițierii* controlului inopinat al furnizorului de servicii la *solicitarea* organului ierarhic superior, sau a autoritatea publică care exercită supravegherea administrativă și controlul administrativ al furnizorului de servicii public; - *insuficienței reglementării aspectelor procedurale aferente planificării controlului de stat* (omiterea reglementării termenului-limită de aprobare și publicare a planului controalelor) și *nemijlocit desfășurării controlului de stat* (reglementarea ambiguă a limitelor inadmisibile în activitatea organului de control și nemijlocit inspectorului; extinderea termenului de realizare a măsurilor prevăzute în anexa la procesul-verbal de control/anexa; prelungirea perioadei de desfășurare a controlului; reglementării ambigue a spectrului de atribuții exercitate de către echipa de control; utilizării formulei permisive „poate" de determinare a competenţelor organului de control/inspectorului; etc.) Aspectele date, sunt examinate suplimentar în compartimentul III al prezentului raport de expertiză anticorupție.	**S-a luat act**

		57.	**II.4. Atingeri ale drepturilor omului care pot fi cauzate la aplicarea proiectului** Prevederile proiectului nu aduc atingere drepturilor fundamentale ale omului consacrate de Constituţia Republicii Moldova, Declaraţia Universală a Drepturilor Omului și Convenţia Europeană a Drepturilor Omului.	**S-a luat act**
			III. Analiza detaliată a factorilor de risc și a riscurilor de corupție ale proiectului	
		58.	**Pct.5, Pct.43.5** 5. La solicitarea unei autorități de supraveghere și control a gestionarilor de infrastructură critică națională sau în baza constatărilor rapoartelor de evaluare a conformității (audit), Agenția efectuează un control inopinat al furnizorului de servicii în cauză și informează autoritatea de supraveghere și control de stat în sectorul corespunzător despre încălcările constatate într-un termen care nu depășește 5 zile lucrătoare de la data finalizării controlului. 43. Controlul inopinat al furnizorului de servicii public poate fi efectuat în următoarele cazuri: 43.5. solicitarea din partea organului ierarhic superior sau a autorității publice care exercită supravegherea administrativă și controlul administrativ al furnizorului de servicii public. **Obiecții:** Prevederile proiectului citate supra, instituie un temei de inițiere a controlului inopinat ce excede limitele vizate de art.19 al Legii privind securitatea cibernetică nr.48/2023 și art.19 al Legii privind controlul de stat nr.131/2012, după cum urmează: *Articolul 19. Controlul de stat (1) Autoritatea competentă exercită controlul de stat asupra respectării prezentei legi de către furnizorii de servicii persoane juridice de drept privat, aplicând prevederile Legii nr. 131/2012 privind controlul de stat.*	**Nu se acceptă.** *temeiul* solicitării de către organul ierarhic superior sau a autoritatea publică care exercită supravegherea administrativă și controlul administrativ al furnizorului de servicii public **este un temei special** doar pentru furnizorii de servicii persoane juridice de drept public. Totodată, analizând prevederile art. 19 alin (4) din Legea 48/2023 observăm că drept temei pentru efectuarea controlului este sesizarea cu privire la incălcări, neîndeplinirea sau îndeplinirea necorespunzătoare a obligaţiilor prevăzute de prezenta lege de către furnizorul de servicii. Astfel, considerăm oportun și reglementat de prevederile normative posibilitatea solicitării din partea organului ierarhic superior sau a autorității publice care exercită supravegherea administrativă și controlul administrativ al furnizorului de servicii public efectuarea unui control inopinat de către Agenție.

			(2) Autoritatea competentă realizează controlul de stat exclusiv în baza unui act motivat, emis în acest scop, în baza evaluării riscurilor pentru securitatea reţelelor şi sistemelor informaţionale ale furnizorilor de servicii, precum şi cu înştiinţarea prealabilă a furnizorului de servicii despre controlul preconizat. *(3) În vederea efectuării controlului de stat, autoritatea competentă este în drept să beneficieze de acces la informaţiile, bunurile şi încăperile deţinute de furnizorul de servicii supus controlului, care sunt necesare realizării obiectivelor controlului.* *(4) Autoritatea competentă efectuează controale dacă:* *a) a depistat şi, în urma unei investigaţii preliminare, a confirmat fapte de încălcare a prevederilor prezentei legi; şi/sau* *b) a fost sesizată cu privire la încălcări, neîndeplinirea sau îndeplinirea necorespunzătoare a obligaţiilor prevăzute de prezenta lege de către furnizorul de servicii.* *(5) Guvernul, la propunerea autorităţii administraţiei publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securităţii cibernetice, stabileşte, separat pentru furnizorii de servicii persoane juridice de drept privat şi separat pentru furnizorii de servicii persoane juridice de drept public, procedurile detaliate privind modul de efectuare a controlului de stat de către autoritatea competentă asupra respectării obligaţiilor ce le revin acestora conform prezentei legi.* *Articolul 19. Temeiurile şi condiţiile efectuării controalelor inopinate (1) Organul de control poate decide efectuarea controalelor inopinate asupra unei persoane, în baza evaluării riscurilor, precum şi poate emite inspectorului delegaţie de control, doar în cazul:* *2) deţinerii informaţiilor/indiciilor, susţinute prin probe aflate în posesia organelor de control, inclusiv ca urmare a*	Totodată, referitor la observația de a fi ajustat textul la prevederile Legii 131/2012, nu este relevantă, dat fiind faptul că Legea 48/2023 cât și obiectul de reglementare al legii menționate prevede expres că se aplică doar către persoanele juridice de drept privat.

			autosesizării, despre existenţa situaţiilor de avarie, incident sau încălcare gravă a regulilor de securitate ori siguranţă, precum şi de încălcare gravă a drepturilor şi libertăţilor fundamentale care fac obiectivul prezentei legi, situaţii care prezintă un pericol iminent şi imediat pentru mediu, viaţa, sănătatea şi proprietatea persoanelor, sau care lezează drepturile şi libertăţile fundamentale care fac obiectivul prezentei legi, dacă sînt întrunite următoarele condiţii: *a) necesitatea iniţierii controlului este motivată în prealabil;* *b) poate fi rezonabil stabilit, din informaţia deţinută pînă la iniţierea controlului şi din nota de motivare, cădoar intervenţia inopinată prin control va preveni şi/sau stopa încălcările care în mod iminent provoacă prejudicii sau că astfel ar putea fi diminuate substanţial prejudiciile deja cauzate;* *3) verificării informaţiei, care, conform legii, este raportată în mod obligatoriu, dacă sînt întrunite următoarele condiţii:* *a) această informaţie nu a fost prezentată în termenul stabilit de lege sau de un act normativ;* *b) organul abilitat cu funcţii de control sau organul responsabil de recepţionarea informaţiei corespunzătoare nu a primit notificare justificativă din partea persoanei obligate să raporteze informaţia în termen şi/sau această persoană nu a răspuns în termen rezonabil la înştiinţarea din partea organului responsabil;* *4) verificării informaţiei obţinute în cadrul altui control la întreprinzătorul cu care persoana controlată a avut anterior relaţii economice, dacă sînt întrunite următoarele condiţii:* *a) întreprinzătorul refuză să prezinte informaţiile în cauză;* *b) nu există altă modalitate de obţinere a informaţiei în cauză;*	

			c) informaţia dată este decisivă şi indispensabilă pentru atingerea scopului controlului iniţiat anterior; *5) solicitării directe din partea persoanei care urmează a fi supusă controlului privind iniţierea controlului sau al solicitării directe din partea autorităţii emitente a actului permisiv şi/sau licenţei, inclusiv în condiţiile art.111 din Legea nr.160/2011 privind reglementarea prin autorizare a activităţii de întreprinzător;* *7) deţinerii informaţiilor/indiciilor privind utilizarea muncii nedeclarate, achitarea salariului sau a altor plăţi fără reflectarea acestora în evidenţa contabilă, privind traficul de fiinţe umane sau exploatarea în muncă la angajator;* *8) eschivării vădite a persoanei ce urma să fie controlată de la controlul planificat, adică, fără coordonarea prealabilă cu organul de control, în perioada de la notificare şi până la iniţierea controlului, a creării intenţionate a unor circumstanţe ce fac imposibilă desfăşurarea controlului, inclusiv suspendarea propriei activităţi ori sistarea lucrărilor la obiectul ce urma a fi controlat;* *9) în care persoana sau obiectul trebuie să fie controlate conform Planului de gestionare a situaţiei de criză, aprobat conform art.31 şi publicat pe portalul controale.gov.md;* *10) notificării pentru produsele ce prezintă un risc grav în sistemul de schimb rapid de informaţii privind produsele periculoase.* Se remarcă faptul că prevederile proiectului nu reglementează aspecte procedurale ce țin de *temeiul* solicitării de către organul ierarhic superior sau a autoritatea publică care exercită supravegherea administrativă și controlul administrativ al furnizorului de servicii public. Carența în speță, denotă întrunirea parțială a exigențelor de tehnică legislativă vizate de art.3, art.29 alin.(2), art.54	

			alin.(1) lit.a) al Legii nr. 100/2017, art.32 Cod administrativ și poate condiționa multiple riscuri de corupție aferente inițierii tendențioase a controlului. **Recomandări:** Reconsiderarea prevederilor prenotate și adaptarea la exigențele art.19 al Legii privind securitatea cibernetică nr.48/2023 și art.19 al Legii privind controlul de stat nr.131/2012. **Factori de risc:** ● Atribuții excesive, improprii sau contrare statutului entității publice ● Atribuții care admit derogări și interpretări abuzive ● Temeiuri neexhaustive/ambigui/subiective pentru refuzul sau inacțiunea entității publice ● Lipsa/ambiguitatea procedurilor administrative ● Lipsa responsabilității clare pentru încălcări ● Concurența normelor de drept ● Lipsa/insuficiența transparenței funcționării entităților publice **Riscuri de corupție:** ● Generale ● Legalizarea actelor de: - trafic de influență - abuz de serviciu - depășire a atribuțiilor de serviciu - conflict de interese și/sau favoritism - influențare necorespunzătoare	
		59.	**Pct.10** 10. În cazul în care pe parcursul desfășurării activității de supraveghere se constată săvârșirea unor fapte care pot întruni elemente constitutive ale unor contravenții sau infracțiuni, Agenția sesizează autoritățile competente. 24. În cazul în care în timpul desfășurării controlului, inspectorii constată încălcări ce conțin semne ale unei infracțiuni, aceștia consemnează în procesul-verbal de	**Se acceptă.** Proiectul a fost completat cu norme privind uniformizarea textului, precum și excluderea factorilor de corupție semnalați.

			control și sesizează organele de urmărire penală cu privire la încălcările constatate, respectând procedura stabilită de Legea nr. 131/2012 privind controlul de stat. 33. Procesul-verbal de control și anexele acestuia se comunică, după caz, organului de urmărire penală sau procurorului atunci când există indici cu privire la săvârșirea unei posibile infracțiuni, respectând prevederile legale în domeniu. 60. Agenția sesizează organele de urmărire penală sau procurorul cu privire la încălcări constatate ce conțin semne ale unei infracțiuni, respectând procedura stabilită de actele normative relevante. 70. Procesul-verbal și anexele acestuia se comunică, după caz, organului de urmărire penală sau procurorului atunci când există indicii cu privire la săvârșirea unei infracțiuni, respectând prevederile legale în domeniu. **Obiecții:** *Primo*, apreciind prin prisma exigențelor de tehnică legislativă vizate de art.54 alin.(1) lit.c), d), h) alin.(5) al Legii nr.100/2017, se remarcă utillizarea unor noțiuni diferite întru reglementarea unor aspecte comune *(" autoritățile competente", "organele de urmărire penală ", "organului de urmărire penală sau procurorului.")*. Subsecvent, utilizarea cuvintelor *"după caz, "* poate amplifica caracterul ambiguu al normei atribuind incertitudine cazurilor cînd procesul-verbal de control se comunică organului de urmărire penală și facilitează decizii arbitrare. *Secundo*, se remarcă omiterea reglementării termenului de sesizare a organelor de urmărire penală/procurorului. Reglementarea lacunară sau confuză a termenelor administrative întotdeauna lasă loc pentru interpretări abuzive din partea agenților publici, or determină discreția excesivă a agentului public de a aprecia şi stabili în fiecare caz separat termene care îi sunt convenabile, atât pentru	

			propriile acţiuni, cât şi pentru acţiunile altor subiecţi de drept cărora aceste termene le sunt aplicabile. **Recomandări:** Uniformizarea terminologiei utilizate și excluderea cuvintelor *”după caz, ”* Reglementarea *termenului* de sesizare a organelor de urmărire penală/procurorului. **Factori de risc:** ● Formulare ambiguă care admite interpretări abuzive ● Atribuții care admit derogări și interpretări abuzive ● Utilizarea neuniformă a termenilor ● Nedeterminarea entității publice responsabile/subiectului la care se referă prevederea ● Lipsa unor termene concrete/termenene justificate/prelungirea nejustificată a termenilor **Riscuri de corupţie:** ● Generale ● Încurajarea sau facilitarea actelor de: - corupere activă - corupere pasivă - trafic de influență - abuz de serviciu - depășire a atribuțiilor de serviciu - conflict de interese și/sau favoritism - îmbogăţire ilicită - influențare necorespunzătoare - nerespectare a regimului cadourilor ● Legalizarea actelor de: - abuz de serviciu - depășire a atribuțiilor de serviciu - conflict de interese și/sau favoritism	
		60.	**Pct.13** 13. Agenția efectuează controale inopinate în cazul în care constată și confirmă, în urma unei investigații preliminare,	**Se acceptă.** Proiectul a fost ajustat corespunzător.

			fapte ce constituie încălcări ale prevederilor Legii nr. 48/2023 privind securitatea cibernetică și/sau atunci când este sesizată despre încălcări, neîndeplinirea sau îndeplinirea necorespunzătoare a obligațiilor stabilite prin această lege de către furnizorul de servicii privat. Controlul inopinat se inițiază în condițiile art. 19 din Legea nr. 131/2012 privind controlul de stat. **Obiecții:** În materie contravențională, verbul „a constata” are o utilizare consacrată și un sens tehnic bine definit, fapt care a determinat asocierea acestuia cu legislația contravențională. Agentul constatator constată săvârșirea unei contravenții, această constatare reprezentând actul inițial prin care se stabilește existența faptei contravenționale și a împrejurărilor în care aceasta a fost săvârșită. Constatarea precedă aplicarea sancțiunii și se materializează, de regulă, într-un proces-verbal de constatare a contravenției. În acest context, termenul „a constata” exprimă un demers de stabilire obiectivă a unei situații de fapt, pe baza percepției directe sau a probelor administrate, fără a se confunda cu actul de sancționare propriu-zis. Apreciind prin prisma exigențelor de tehnică legislativă vizate de art.54 alin.(1) lit.c), d), h) alin.(5) al Legii nr. 100/2017, se remarcă faptul că utilizarea la pct.13 citat supra, a cuvîntului ”constată” nu este potrivită terminologiei, or procesul de control, generic vizează totalitatea acţiunilor de verificare a respectării de către persoanele supuse controlului a prevederilor legislaţiei, realizate de un organ abilitat cu funcţii de control, în rezultatul căruia este întocmit un proces-verbal de control în care se înregistrează constatările/rezultatele controlului, după caz se prescriu modalităţi de înlăturare a încălcărilor şi/sau măsuri restrictive şi, după caz, se constată contravenţii.	

			În aceeași ordine de idei, se remarcă corespunderea parțială a redacției pct.13 cu prevederile art.19 alin.(4) al Legii nr.48/2023 privind securitatea cibernetică, potrivit cărora: *Articolul 19. Controlul de stat [...] (4) Autoritatea competentă efectuează controale dacă: a) a depistat şi, în urma unei investigaţii preliminare, a confirmat fapte de încălcare a prevederilor prezentei legi; şi/sau b) a fost sesizată cu privire la încălcări, neîndeplinirea sau îndeplinirea necorespunzătoare a obligaţiilor prevăzute de prezenta lege de către furnizorul de servicii.* În context se remarcă exigențele de tehnică legislativă vizate de art.3 alin.(1) lit.d), f) alin.(4) al Legii nr. 100/2017, după cum urmează: *Articolul 3. Principiile activităţii de legiferare (1) La elaborarea unui act normativ se respectă următoarele principii: [...] d) oportunitatea, coerenţa, consecutivitatea, stabilitatea şi predictibilitatea normelor juridice; [..] f) respectarea ierarhiei actelor normative.* *(4) Actul normativ trebuie să se integreze organic în cadrul normativ în vigoare, scop în care:* *a) proiectul actului normativ trebuie corelat cu prevederile actelor normative de nivel superior sau de acelaşinivel cu care se află în conexiune;* *b) proiectul actului normativ întocmit în temeiul unui act normativ de nivel superior nu poate depăşi limitele competenţei instituite prin actul de nivel superior şi nici nu poate contraveni scopului, principiilor şi dispoziţiilor acestuia.* *Articolul 7. Corelaţia actelor normative (1) Forţa juridică a actelor normative se stabileşte în funcţie de competenţa şi statutul autorităţii publice emitente, precum şi de categoria actului. Limitele de competenţă privind adoptarea, aprobarea sau emiterea actelor normative sînt stabilite de Constituţia Republicii Moldova, de Legea nr.136/2017 cu privire la Guvern şi de alte acte normative.*	

			(2) Actul normativ cu forţă juridică superioară poate modifica sau abroga un act normativ cu forţă juridică inferioară al aceluiaşi emitent. În cazul modificării exprese a actului inferior, modificarea are aceeaşi forţă juridică ca şi actul modificat. **Recomandări:** Substituirea cuvîntului *"constată"* cu cuvintele *"a depistat şi,"*. **Factori de risc:** ● Atribuții excesive, improprii sau contrare statutului entității publice ● Utilizarea neuniformă a termenilor ● Concurenţa normelor de drept **Riscuri de corupţie:** ● Generale ● Încurajarea sau facilitarea actelor de: - corupere pasivă - trafic de influență - abuz de serviciu - depășire a atribuțiilor de serviciu - conflict de interese și/sau favoritism - influențare necorespunzătoare - nerespectare a regimului cadourilor ● Legalizarea actelor de: - abuz de serviciu - depășire a atribuțiilor de serviciu - conflict de interese și/sau favoritism	
		61.	**Pct.17** 17. Agenția aprobă planul controalelor pentru anul următor și îl publică pe site-ul său web oficial. **Obiecții:** Prevederile proiectului citate supra, nu reglementează termenul-limită de aprobare și publicare a planului controalelor, fapt care denotă întrunirea parțială a	**Precizare.** Pct. 17 din proiectul de Regulament urmează a se aplica în concordanță cu prevederile similare din Legea 131/2012. Astfel, partea planul controalelor este reglementată detaliat în art. 15-16 din Legea menționată.

			exigențelor de tehnică legislativă vizate de art.29 alin.(2) al Legii nr.100/2017, art.32 Cod administrativ. Reglementarea lacunară sau confuză a termenelor administrative întotdeauna lasă loc pentru interpretări abuzive din partea agenților publici. Astfel, apare discreția excesivă a agentului public de a aprecia şi stabili în fiecare caz separat termene care îi sunt convenabile, atât pentru propriile acţiuni, cât şi pentru acţiunile altor subiecţi de drept cărora aceste termene le sunt aplicabile. **Recomandări:** Completarea normei cu referinței la termenul administrativ aplicabil. **Factori de risc:** ● Lacună de drept ● Lipsa/ambiguitatea procedurilor administrative Lipsa responsabilității clare pentru încălcări ● Lipsa unor termene concrete/termene nejustificate/prelungirea nejustificată a termenilor **Riscuri de corupţie:** ● Generale ● Încurajarea sau facilitarea actelor de: - corupere activă - corupere pasivă - trafic de influență - abuz de serviciu - depășire a atribuțiilor de serviciu - conflict de interese și/sau favoritism - îmbogăţire ilicită - influențare necorespunzătoare - nerespectare a regimului cadourilor ● Legalizarea actelor de: - abuz de serviciu - depășire a atribuțiilor de serviciu	

			- conflict de interese și/sau favoritism	
		62.	**Pct.18.5, Pct.25-26, Pct.43** 18.5. În cadrul sau în urma controlului de stat, la depistarea încălcărilor, inspectorul Agenției poate înainta prescripții și recomandări, aplica măsuri restrictive și sancțiuni în limitele prevăzute de lege. Acțiunile și măsurile se selectează și se aplică în conformitate cu prevederile Legii nr. 131/2012 privind controlul de stat. 25. Agenția poate solicita declanșarea imediată a măsurilor de remediere a anumitor deficiențe în situații de risc major sau care impun măsuri urgente. 26. Pentru a contracara o amenințare cibernetică semnificativă imediate asupra securității rețelelor și sistemelor informatice sau a atenua consecințele unui incident cibernetic cu impact semnificativ, Agenția poate restricționa utilizarea ori accesul la una sau mai multe rețele sau sisteme informatice, dacă sunt îndeplinite condițiile stabilite la art. 15 alin. (2) din Legea nr.48/2023. 43. Controlul inopinat al furnizorului de servicii public poate fi efectuat în următoarele cazuri: **Obiecții:** Determinarea competenţei după formulă „este în drept", „poate" este o modalitate coruptibilă de determinare a competenţelor entităţilor şi agenților publici. Coruptibilitatea acestui element rezidă în discreţia agenților publici care apare în cazul utilizării unor asemenea determinări permisive ale competenţelor lor, care urmau a fi stabilite de o manieră imperativă. Această discreţie poate fi folosită în mod abuziv de către agentul public pentru a nu-şi executa obligaţiile sale legale tocmai în virtutea caracterului permisiv al formulării competenţelor sale. Riscul de coruptibilitate a acestor norme creşte în cazul în care lipsesc criterii pentru a stabili în ce cazuri agentul public „este în drept" sau „poate" şi în ce cazuri este în drept şi poate să nu-şi realizeze competenţele.	**Se acceptă.**

			Recomandări: Excluderea formulei permisive ”poate”. **Factori de risc:** ● Stabilirea unui drept al entității publice în loc de o obligație **Riscuri de corupţie:** ● Generale ● Încurajarea sau facilitarea actelor de: - corupere pasivă - trafic de influență - abuz de serviciu - depășire a atribuțiilor de serviciu - conflict de interese și/sau favoritism - îmbogăţire ilicită - influențare necorespunzătoare - nerespectare a regimului cadourilor - corupere activă ● Legalizarea actelor de: - abuz de serviciu - depășire a atribuțiilor de serviciu - conflict de interese și/sau favoritism	
		63.	Pct.21 21. <u>În limitele admisibile</u>, controlul se efectuează fără a influența desfășurarea activităților curente a furnizorului de servicii privat supus controlului. **Obiecții:** Expresia *”În limitele admisibile”* este ambiguă și nu permite delimitarea clară și fără echivoc a limitelor inadmisibile în activitatea organului de control și nemijlocit inspectorului, fapt care denotă întrunirea parțială a exigențelor de tehnică legislativă vizate de art.3, art.54 alin.(1) lit.a) al Legii nr.100/2017.	**Se acceptă.**

			În context, se remarcă exigențele vizate de art.3 alin.(1) lit.b), l), art.27 al Legii nr.131/2012 privind controlul de stat, după cum urmează: *Articolul 3. Principiile fundamentale ale controlului. (1) Principiile fundamentale ale controlului sînt:* *b) obiectivitate şi imparţialitate la planificarea şi desfăşurarea controlului de stat, la întocmirea documentelor aferente controlului şi dispunerea de măsuri şi sancţiuni. Desfăşurarea controlului de stat nu poate fi influenţată de niciun grup prin promovarea intereselor acestuia;* *l) neadmiterea afectării şi/sau suspendării activităţii persoanei supuse controlului;* *Articolul 27. Neadmiterea afectării şi/sau suspendării activităţii persoanei supuse controlului (1) Organelor de control şi colaboratorilor acestora li se interzice, în procesul realizării funcţiilor de control, să afecteze funcţionarea normală a persoanei supuse controlului şi/sau să întreprindă măsuri ce vor conduce la suspendarea completă sau temporară a activităţii acesteia, cu excepţia cazurilor de încălcări foarte grave, în sensul prezentei legi, care necesită aplicarea măsurilor restrictive corespunzătoare.* *(2) Orice daune cauzate persoanei supuse controlului prin încălcarea prevederilor alin.(1) de către organele de control şi colaboratorii acestora în procesul realizării funcţiilor de control, prin prescripţiile şi deciziile luate în urma efectuării controlului, vor fi reparate din contul organului de control şi/sau din contul colaboratorilor acestuia. În cazul nerezolvării pe cale amiabilă a conflictului, persoana prejudiciată poate acţiona în instanţa de judecată organul de control şi/sau colaboratorii acestuia.*	

			(3) Faptul cauzării de daune şi cuantumul despăgubirilor în cazurile specificate la alin.(2) sînt stabilite de instanţa de judecată, la cererea persoanei interesate. **Recomandări:** Reconsiderarea utilizării expresiei ”În limitele admisibile”. **Factori de risc:** ● Formulare ambiguă care admite interpretări abuzive ● Atribuții care admit derogări și interpretări abuzive ● Lipsa/ambiguitatea procedurilor administrative ● Lipsa responsabilității clare pentru încălcări ● Lipsa/insuficiența mecanismelor de supraveghere și control (ierarhic, intern, public) **Riscuri de corupţie:** ● Generale ● Încurajarea sau facilitarea actelor de: - nerespectare a regimului cadourilor - corupere activă - corupere pasivă - abuz de serviciu - depășire a atribuțiilor de serviciu - conflict de interese și/sau favoritism - îmbogăţire ilicită - influențare necorespunzătoare ● Legalizarea actelor de: - abuz de serviciu - depășire a atribuțiilor de serviciu - conflict de interese și/sau favoritism ● Generale ● Încurajarea sau facilitarea actelor de: - nerespectare a regimului cadourilor - corupere activă - corupere pasivă - abuz de serviciu - depășire a atribuțiilor de serviciu - conflict de interese și/sau favoritism	

			- îmbogăţire ilicită - influențare necorespunzătoare ● Legalizarea actelor de: - abuz de serviciu - depășire a atribuțiilor de serviciu - conflict de interese și/sau favoritism	
		64.	**Pct.35-36; Pct.73-74** 35. În cazul în care anumite măsuri prevăzute în anexa la procesul-verbal de control nu pot fi realizate în termen, furnizorul de servicii privat poate solicita Agenției extinderea termenului de realizare. 36. Decizia cu privire la extinderea termenului de realizare a măsurilor prevăzute în anexa la procesul-verbal de control se aprobă de Directorul Agenției. 73. În cazul în care anumite măsuri prevăzute în anexa la procesul-verbal nu pot fi realizate în termen, furnizorul de servicii solicită Agenției extinderea termenului de realizare. 74. Decizia cu privire la extinderea termenului de realizare a măsurilor prevăzute în anexa la procesul-verbal se aprobă de Directorul Agenției. **Obiecții:** Prevederile proiectului citate supra nu reglementează aspecte procedurale ce vizează examinarea cererii prenotate de către agentul public, fapt care denotă întrunirea parțială a exigențelor de tehnică legislativă vizate de art.29 alin.(2) al Legii nr.100/2017 art.32 Cod administrativ (termen de examinare, temei de refuz). Insuficiența reglementării procedurilor administrative ale organului de control poate creea premise favorabile exercitării discreționare a prerogativelor de putere publică, periclitînd transparența și predictibilitatea actului de control. Deficiența în cauză, obstrucționează documentarea și trasabilitatea deciziilor, fapt care	**Precizare.** Proiectul se completează inclusiv cu termenii administrativi prevăzuți de Codul administrativ. Astfel, considerăm oportun ca redacția la pct. respective să conțină redacția expusă pentru realizarea optimă a procedurii de control realizată de către Agenție.

			îngreunează identificarea abaterilor și reduc eficiența mecanismelor de răspundere disciplinară sau penală. **Recomandări:** Reglementarea aspectelor ce țin de termenul de examinare a solicitării și temeiurilor de refuz. **Factori de risc:** ● Lacună de drept ● Atribuții care admit derogări și interpretări abuzive ● Temeiuri neexhaustive/ambigui/subiective pentru refuzul sau inacțiunea entității publice ● Lipsa/ambiguitatea procedurilor administrative ● Lipsa responsabilității clare pentru încălcări ● Lipsa unor termene concrete/termene nejustificate/prelungirea nejustificată a termenilor **Riscuri de corupţie:** ● Generale ● Încurajarea sau facilitarea actelor de: - îmbogăţire ilicită - influențare necorespunzătoare - nerespectare a regimului cadourilor - corupere pasivă - trafic de influență - abuz de serviciu - depășire a atribuțiilor de serviciu - conflict de interese și/sau favoritism - corupere activă ● Legalizarea actelor de: - abuz de serviciu - depășire a atribuțiilor de serviciu - conflict de interese și/sau favoritism	
		65.	**Pct.61** 61. În cazul în care <u>obiectivele stabilite la planificarea activității de control nu au fost atinse</u> sau au apărut circumstanțe noi pentru a căror clarificare sunt necesare acțiuni suplimentare, perioada de desfășurare a controlului	**Se acceptă.** Textul a fost reformulat conform obiecției.

			se poate prelungi până la realizarea acestora, cu aprobarea Directorului Agenției. **Obiecții:** Conform art.20 al Legii nr.131/2012, controlul (atît planificat cît și inopinat) se efectuează *în temeiul delegației* care evidențiază expres, inter alia, *obiectul/obiectele care urmează a fi supuse controlului şi aspectele ce urmează a fi verificate, trimitere expresă la lista de verificare aplicabilă şi actul normativ prin care aceasta este aprobată.* În context se remarcă faptul că, utilizarea expresiilor *"obiectivele stabilite la planificarea activității de control", "până la realizarea acestora,",* atribuie caracter ambiguu normei, fapt care denotă întrunirea parțială a exigențelor de reglementare vizate de art.3, art.54 alin.(1) lit.a) al Legii nr.100/2017. Deficiența în cauză poate determina interpretarea subiectivă a normei și prelungirea tendențioasă a activității de control fapt care amplifică riscurile specifice corupției regulatorii. **Recomandări:** Reconsiderarea expresiilor "obiectivele stabilite la planificarea activității de control", "până la realizarea acestora," (i) substituirea expresiei "obiectivele stabilite la planificarea activității de control" cu o expresiei ce face referință la posibilitatea prelungirii perioadei de desfășurare a controlului în cazul în care nu a fost verificate toate aspectele vizate de delegația de control, și ii) excluderea expresiei "până la realizarea acestora,"). **Factori de risc:** ● Formulare ambiguă care admite interpretări abuzive ● Atribuții care admit derogări și interpretări abuzive ● Temeiuri neexhaustive/ambigui/subiective pentru refuzul sau inacțiunea entității publice ● Lipsa/ambiguitatea procedurilor administrative	

			● Stabilirea unui drept al entității publice în loc de o obligație ● Lipsa unor termene concrete/termene nejustificate/prelungirea nejustificată a termenilor **Riscuri de corupţie:** ● Generale ● Încurajarea sau facilitarea actelor de: - corupere activă - corupere pasivă - trafic de influență - abuz de serviciu - depășire a atribuțiilor de serviciu - conflict de interese și/sau favoritism - îmbogăţire ilicită - influențare necorespunzătoare - nerespectare a regimului cadourilor ● Legalizarea actelor de: - abuz de serviciu - depășire a atribuțiilor de serviciu - conflict de interese și/sau favoritism	
		66.	**Pct.55** 55. În procesul efectuării controlului, echipa de control are următoarele drepturi: 55.1. să pătrundă în orice încăpere utilizată de furnizorul de servicii în activitatea sa, care găzduiește rețele și sisteme informatice sau date relevante obiectului controlului, în măsura în care aceasta este parte a obiectului controlului. 55.2. să solicite și să obțină orice informații, documente sau alte tipuri de date necesare pentru realizarea controlului; 55.3. să facă copii, înregistrări foto sau video ale documentelor sau ale altor obiecte purtătoare de informații. **Obiecții:** Aspectele citate supra urmează a fi examinate prin prisma art.23 al Legii nr.131/2012 privind controlul de stat:	**Se acceptă.**

			Articolul 23. Drepturile inspectorului. (1) În procesul efectuării controlului, inspectorul are dreptul: *a) să pătrundă în orice încăpere utilizată de întreprinzător în activitatea sa, în măsura în care aceasta este parte a obiectului controlului, cu excepţia domiciliului, în cazul cînd lipseşte permisiunea posesorului legal. În caz de necesitate, inspectorul va putea intra în domiciliu sau în încăperea asimilată domiciliului doar cu asistenţa poliţiei, în condiţiile legii;* *b) să ceară informaţii, certificate, licenţe, autorizaţii şi alte documente obligatorii, cu respectarea prevederilor art.5 alin.(2), relevante obiectului controlului;* *c) să facă copii, înregistrări foto sau video ale documentelor sau ale altor obiecte purtătoare de informaţii, inclusiv înregistrări foto sau video ale faptelor constatate în limitele controlului efectuat; [...]* *e) să inspecteze mijloacele de transport doar în cazul cînd deţine informaţii că în ele se află bunuri care constituie obiectul controlului sau dacă mijloacele de transport sînt obiect al controlului în corespundere cu domeniul de control;* *f) să achiziţioneze produse pentru prelevarea de mostre şi efectuarea încercărilor de laborator în domeniul supravegherii pieţei, cu includerea informaţiei privind prelevarea mostrelor în procesul-verbal de control.* Utilizarea la pct.55.2. expresiei *”necesare pentru realizarea controlului;”*, atribuie caracter ambiguu normei și nemijlocit obiectului supus controlului, fapt care denotă neîntrunirea exigențelor de tehnică legislativă vizate de prevederile art.54 alin.(1) lit.a) al Legii nr.100/2017. Subsecvent, la pct.55.3. se remarcă omiterea reglementării relevanței pentru obiectul controlului a	

			documentelor sau ale altor obiecte purtătoare de informații de pe care este în drept sa facă copii echipa de control. Carențele prenotate, pot condiționa incertitudine la etapa implementării normelor și interpretarea extensivă a acestora sub aspectul lărgii arbitrare a obiectului supus controlului. **Recomandări:** La 55.2. - substituirea expresiei *"necesare pentru realizarea controlului;"* cu expresia "relevante obiectului controlului". Completarea 55.3. la sfîrșit cu expresia "relevante obiectului controlului". **Factori de risc:** ● Atribuții excesive, improprii sau contrare statutului entității publice ● Formulare ambiguă care admite interpretări abuzive **Riscuri de corupţie:** ● Generale ● Încurajarea sau facilitarea actelor de: - corupere activă - corupere pasivă - trafic de influență - abuz de serviciu - depășire a atribuțiilor de serviciu - conflict de interese și/sau favoritism - îmbogăţire ilicită - influențare necorespunzătoare - nerespectare a regimului cadourilor ● Legalizarea actelor de: - abuz de serviciu - depășire a atribuțiilor de serviciu - conflict de interese și/sau favoritism	
		67.	**Pct.63** 63. Procesul-verbal cuprinde:	**Nu se acceptă.**

			63.1. principalele realizări; 63.2. deficiențele, disfuncțiile, neregulile și măsurile de ordin organizatoric și administrativ; 63.3. concluziile echipei de supraveghere; 63.4. alte aspecte care pot contribui la creșterea eficacității și eficienței activităților evaluate. 63.5. Procesul-verbal de control include obligatoriu explicații și/sau obiecțiile furnizorului în privința măsurilor restrictive prescrise, anexate integral la proces; **Obiecții:** Prevederile pct.63 urmează a fi raportate la prevederile art.28 al Legii nr.131/2012 privind controlul de stat, potrivit cărora: *Articolul 28. Încheierea procedurii de control. (1) Procedura de control se încheie prin întocmirea de către inspectori a unui proces-verbal de control, care se completează şi se semnează de toţi inspectorii indicaţi în delegaţia de control, la locul efectuării controlului.* *(11) Conducerea organului de control dispune, printr-o decizie motivată, încetarea imediată a controlului, cu menţiunea corespunzătoare în procesul-verbal de control, în cazul în care constată că iniţierea şi/sau desfăşurarea controlului se efectuează cu încălcarea, din partea organului de control, a normelor procedurale stabilite de prezenta lege.* *(2) Procesul-verbal de control este documentul prin care se confirmă faptul desfăşurării controlului şi în care se conţine toată informaţia cu privire la controlul desfăşurat, la procedurile aplicate şi constatările în urma acestuia, prescripţiile şi recomandările înaintate în baza constatărilor, măsurile restrictive aplicate şi sancţiunile stabilite în urma controlului. Procesul-verbal de control este alcătuit din partea constatatoare, partea prescriptivă şi partea sancţionatorie şi conţine în mod obligatoriu:*	Observația referitor la ajustarea la Legea 131/2012 a capitolului IV din proiectul de regulament nu este oportună, dat fiind faptul că actul normativ menționat urmează a fi aplicat doar către furnizorii de servicii persoane juridice de drept privat.

			a) denumirea completă a organului de control, numele complet şi funcţia persoanelor care au efectuat controlul; *b) date cu privire la delegaţia de control şi temeiul efectuării controlului;* *c) denumirea completă/numele persoanei supuse controlului şi identificarea obiectului de control;* *d) tipul controlului;* *e) lista de verificare aplicată;* *f) date privind toate aspectele, documentele, bunurile, încăperile, produsele, utilajele şi obiectele de altă natură care au fost supuse controlului, relevante în scopul controlului;* *g) constatările şi rezultatele controlului;* *h) referinţa expresă la prevederile actelor legislative şi normative pe care le-a încălcat persoana supusă controlului;* *i) copiile documentelor examinate care confirmă încălcarea legii, ale altor documente întocmite în cadrul controlului;* *j) date privind durata controlului;* *k) explicaţiile în scris ale persoanei supuse controlului şi/sau ale angajaţilor acesteia;* *l) recomandările şi indicaţiile pentru înlăturarea încălcărilor stabilite în partea prescriptivă, după caz;* *m) prescripţia de aplicare a măsurilor restrictive, după caz;* *n) constatarea contravenţiilor sau altor tipuri de încălcări prevăzute de lege, cu indicarea sancţiunii prevăzute de lege, după caz;* *o) descrierea semnelor componenţei de infracţiune constatate în cadrul procedurii de control şi referinţa expresă la normele de drept penal vizate;* *p) informaţia privind calea de atac a procesului-verbal de control.* **Recomandări:**	

			Apreciind prin prisma exigențelor de tehnică legislativă vizate de art.3,7 al Legii nr.100/2017, se recomandă corelarea textelor regulatorii și ajustarea conținutului procesului-verbal la exigențele art.28 al Legii nr. 131/2012 citate supra. **Factori de risc:** ● Concurenţa normelor de drept **Riscuri de corupţie:** ● Generale	
		68.	**IV. Concluzia expertizei** Potrivit notei de fundamentare, proiectul are drept scop creștere a nivelului de reziliență cibernetică a furnizorilor de servicii, privați sau publici, asigurând un nivel ridicat de protecție a rețelelor și sistemelor informatice ale acestor furnizori utilizate în procesul de prestare de către aceștia a serviciilor esențiale. Autorul a prezentat *Sinteza* avizelor parvenite în cadrul procesului de consultare publică a proiectului de către autoritățile responsabile de implementarea prevederilor conţinute în proiect/instituţiilor interesate, fapt ce denotă aspectul *definitivat* al acestuia și întrunirea condițiilor stabilite de prevederile art.28 al Legii nr.82/2017 - pentru efectuarea *expertizei* anticorupție. În procesul de promovare a proiectului, au fost respectate rigorile de asigurare a transparenţei decizionale statuate de prevederile art.8 lit.a)-d) al Legii nr. 239-XVI din 13 noiembrie 2008 privind transparenţa în procesul decizional. Nota informativă a proiectului a fost structurată potrivit exigențelor de tehnică legislativă statuate de prevederile art.30 lit.a)-f) al Legii cu privire la actele normative nr.100 din 22 decembrie 2017.	**Se acceptă.** Proiectul în general a fost ajustat la obiecțiile avute de către Centrul Național Anticorupție pentru e exclude eventuale riscuri de corupție semnalate în aviz.

			Analiza prevederilor propuse, denotă unele deficiențe ce pot condiționa disfuncționalități ale proceselor administrative reglementate și multiple riscuri de corupție aferente - *inițierii* controlui inopinat al furnizorului de servicii la solicitarea organului ierarhic superior, sau a autoritatea publică care exercită supravegherea administrativă și controlul administrativ al furnizorului de servicii public; - *insuficienței reglementării aspectelor procedurale aferente planificării controlului de stat* (omiterea reglementării termenului-limită de aprobare și publicare a planului controalelor) *și nemijlocit desfășurării controlului de stat* (reglementarea ambiguă a limitelor inadmisibile în activitatea organului de control și nemijlocit inspectorului; extinderea termenului de realizare a măsurilor prevăzute în anexa la procesul-verbal de control/anexa; prelungirea perioadei de desfășurare a controlului; reglementării ambigue a spectrului de atribuții exercitate de către echipa de control; utilizării formulei permisive „poate" de determinare a competenţelor organului de control/inspectorului; etc.) Implementarea prevederilor propuse, poate contribui la realizarea interesului public vizat de proiect, fapt care nu este detrimentul interesului public general (în sensul prevăzut de prevederile Legii integrităţii nr.82 din 25 mai 2017) în condițiile revizuirii proiectului potrivit recomandărilor vizate de compartimentul III al prezentului raport.	

Secretar de stat **Michelle ILIEV**