Proiect

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din _____ 2025

cu privire la aprobarea resursei informaționale „Certificarea în domeniul auditului intern” formate de Sistemul informațional integrat al finanțelor publice

În temeiul art. 6 lit. h) din Legea nr. 136/2017 cu privire la Guvern (Monitorul Oficial al Republicii Moldova, 2017, nr. 252, art. 412), cu modificările ulterioare, precum și art.22 lit. c) și d) din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr.6-12, art.44), cu modificările ulterioare, Guvernul

HOTĂRĂȘTE:

1. Se creează resursa informațională „Certificarea în domeniul auditului intern” formată din Sistemul informațional integrat al finanțelor publice.

2. Se aprobă Regulamentul resursei informaționale „Certificarea în domeniul auditului intern” formate de Sistemul informațional integrat al finanțelor publice (se anexează).

PRIM-MINISTRU **Dorin RECEAN**

Contrasemnează:

Viceprim-ministru,

ministrul dezvoltării

economice și digitalizării **Dumitru ALAIBA**

Ministrul finanțelor **Victoria BELOUS**

Aprobat prin
Hotărârea Guvernului
nr._____ / 2025

REGULAMENTUL
resursei informaționale „Certificarea în domeniul auditului intern” formate de Sistemul informațional integrat al finanțelor publice

Capitolul I
DISPOZIŢII GENERALE

1. Regulamentul resursei informaționale „Certificarea în domeniul auditului intern” formate de Sistemul informațional integrat al finanțelor publice (în continuare – *Regulament*) este elaborat în vederea reglementării modului de organizare și implementare a subsistemului informațional „Certificarea în domeniul auditului intern” din cadrul Sistemului informațional integrat al finanțelor publice.

2. Regulamentul stabilește modul de organizare a resursei informaționale „Certificarea în domeniul auditului intern” formate de Sistemul informațional integrat al finanțelor publice (în continuare – *RI CAI*), componentele acestuia, procedurile și mecanismele de depunere și examinare a cererilor de înmatriculare la Programul de instruire și certificare în domeniul auditului intern în sectorul public (în continuare – *Program)*, a cererilor de eliberare, menținere, suspendare și retragere a certificatului de calificare profesională în domeniul auditului intern în sectorul public (în continuare – *Certificat de calificare profesională*), reglementează cerințele de protecție a datelor în procesul de colectare, actualizare, prelucrare, stocare și a schimbului autorizat al acestora între componentele RI CAI, precum și între RI CAI cu alte sisteme informaționale, precum și stabilește responsabilitatea și împuternicirile privind documentarea, utilizarea și furnizarea datelor stocate și gestionate prin intermediul RI CAI.

3. RI CAI constituie o platformă informațională de automatizare a procesului de gestionare a cererilor persoanelor fizice care participă la Program, având scopul facilitării procesului de instruire și certificare în domeniul auditului intern în sectorul public.

4. RI CAI creează spațiul informațional necesar pentru participanții la Program în vederea automatizării unor funcții realizate de aceștia prin implementarea tehnologiilor informaționale performante astfel încât să asigure ca procesele de înregistrare și acces să fie simple, eficiente, accesibile și transparente.

5. Noțiunile utilizate în prezentul Regulament au semnificațiile prevăzute în Legea nr. 229/2010 privind controlul financiar public intern, Legea nr.467/2003 cu privire la informatizare și la resursele informaționale de stat, Legea nr.133/2011 privind protecția datelor cu caracter personal și în Hotărârea Guvernului nr.278/2023 cu privire la aprobarea Conceptului Sistemului Informațional integrat al finanțelor publice.

Capitolul II
SUBIECŢII RAPORTURILOR JURIDICE AFERENTE CREĂRII ȘI ȚINERII RI CAI

6. Subiecții din domeniul creării, exploatării și utilizării RI CAI sunt:

6.1. proprietarul;

6.2. posesorul;

6.3. deținătorul;

6.4. administratorul tehnic;

6.5. expeditorul;

6.6. destinatarul.

7. Proprietarul RI CAI este statul, care își realizează dreptul de proprietate, de gestionare și de utilizare a datelor din RI CAI. Resursele financiare pentru dezvoltarea, mentenanța și exploatarea RI CAI sunt asigurate din bugetul de stat și alte mijloace financiare, conform legislației.

8. Ministerul Finanțelor este posesorul RI CAI și asigură condițiile juridice, financiare și organizatorice pentru crearea și dezvoltarea acestuia, în limitele reglementate de proprietar.

9. Posesorul RI CAI are următoarele atribuții:

9.1. asigură condițiile juridice, organizatorice și financiare pentru crearea și funcționarea RI CAI;

9.2. stabilește scopurile și sarcinile funcționale ale RI CAI;

9.3. asigură funcționarea, administrarea și dezvoltarea continuă a RI CAI, inclusiv prin identificarea și integrarea noilor tipuri de funcționalități, în conformitate cu nivelul agreat de servicii și în limitele bugetului alocat;

9.4. autorizează, suspendă și revocă dreptul de acces la RI CAI;

9.5. asigură înregistrarea, modificarea, completarea și radierea datelor în cadrul RI CAI;

9.6. exercită alte atribuții necesare asigurării bunei funcționări a RI CAI.

10. Deținătorul RI CAI este I.P. „Centrul de Tehnologii Informaționale în Finanțe", care are următoarele atribuții:

10.1. asigură dezvoltarea, administrarea, mentenanța și securitatea RI CAI, în baza contractului încheiat cu posesorul acestuia;

10.2. acordă suport metodologic în procesul de integrare cu sistemele informaționale ale expeditorilor și destinatarul RI CAI;

10.3. monitorizează procesul de înregistrare și prelucrare a datelor în cadrul RI CAI;

10.4. asigură securitatea, integritatea și protecția datelor din RI CAI, inclusiv protecția datelor cu caracter personal;

10.5. asigură modificările, rectificările și dezvoltările solicitate de către posesorul RI CAI;

10.6. exercită alte atribuții necesare asigurării bunei funcționalități a RI CAI.

11. Administratorul tehnic al RI CAI este I.P. „Centrul de Tehnologii Informaționale în Finanțe" care își realizează atribuțiile în conformitate cu cadrul normativ privind administrarea tehnică și menținerea sistemelor informaționale de stat, în baza unui acord semnat în acest sens cu posesorul RI CAI.

12. Expeditorul este persoana fizică, care are calitatea de candidat sau participant la Program, sau este deținător al certificatului de calificare profesională.

13. Expeditorul are obligația să utilizeze RI CAI pentru a depune cererile de înmatriculare la Program la nivelul de bază / intermediar / avansat, precum și cererile de eliberare, inclusiv de eliberare a duplicatului, de menținere și de suspendare a certificatului de calificare profesională.

14. Expeditorul are următoarele atribuții:

14.1. utilizează RI CAI pentru depunerea în format electronic a cererilor;

14.2. asigură conformitatea și veridicitatea conținutului cererilor depuse și actelor confirmative anexate, cu cadrul legal;

14.3. se conformează regulilor de utilizare a RI CAI stabilite de posesor.

15. Destinatarul RI CAI este Ministerul Finanțelor, care recepționează și prelucrează cererile depuse prin intermediul RI CAI și este responsabil de procesul de certificare a persoanelor fizice în domeniul auditului intern în sectorul public.

Capitolul III
DREPTURILE ŞI OBLIGAŢIILE SUBIECŢILOR RI CAI
Secțiunea 1
Drepturile și obligațiile posesorului

16. Posesorul RI CAI are dreptul:

16.1. să utilizeze informația disponibilă în cadrul RI CAI, în scopul executării atribuțiilor sale;

16.2. să solicite deținătorului îmbunătățirea funcționalităților RI CAI, în bază de contract;

16.3. să inițieze procedura de suspendare a drepturilor de acces la RI CAI pentru utilizatorii care nu respectă regulile stabilite;

16.4. să identifice și să propună integrarea noilor tipuri de cereri și funcționalități în cadrul RI CAI;

16.5. să verifice autenticitatea și veridicitatea datelor transmise de către utilizatorii RI CAI, după caz.

17. Posesorul RI CAI este obligat:

17.1. să asigure condițiile juridice, organizatorice și financiare pentru crearea și funcționarea RI CAI;

17.2. să asigure elaborarea cadrului normativ cu privire la RI CAI;

17.3. să asigure planificarea mijloacelor financiare pentru asigurarea mentenanței anuale și a dezvoltărilor suplimentare necesare pentru RI CAI.

Secțiunea a 2-a

Drepturile și obligațiile deținătorului și administratorului tehnic

18. Deținătorul și administratorul tehnic are dreptul:

18.1. să asigure modificările, rectificările și dezvoltările solicitate de către posesorul RI CAI;

18.2. să stabilească condițiile tehnice de funcționare a RI CAI;

18.3. să propună soluții de perfecționare și eficientizare a funcționalităților RI CAI, precum și să le pună în aplicare;

18.4. să acorde suport consultativ pentru expeditorii și destinatarul RI CAI;

18.5. să supravegheze respectarea cerințelor de securitate a datelor de către participanții la RI CAI, să fixeze cazurile și tentativele de încălcare a acestora;

18.6. să autorizeze suspendarea activității RI CAI în cazul unei situații excepționale, stabilită în conformitate cu actele normative în domeniu, în cazul unor incidente sau în cazul existenței riscurilor semnificative de securitate pentru resursele informaționale de importanță publică.

19. Deținătorul și administratorul tehnic este obligat:

19.1. să asigure administrarea, mentenanța și securitatea informațională a RI CAI;

19.2. să asigure atribuirea rolurilor și a drepturilor de acces la RI CAI;

19.3. să monitorizeze procesul de înregistrare și prelucrare a datelor în cadrul RI CAI;

19.4. să supravegheze respectarea cerințelor de securitate a informației de către subiecții RI CAI și să fixeze cazurile și tentativele de încălcare ale acestora;

19.5. să stabilească condițiile tehnice de funcționare a acestuia;

19.6. să întreprindă măsurile organizatorice și tehnice necesare pentru contracararea tentativelor nesancționate de distrugere, modificare, blocare, copiere, răspândire, precum și împotriva altor acțiuni ilicite, măsuri menite să asigure un nivel de securitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor prelucrate;

19.7. să asigure implementarea măsurilor organizatorice și tehnice necesare pentru

asigurarea regimului de confidențialitate și securitate a datelor cu caracter personal în conformitate cu cadrul normativ;

19.8. să informeze participanții la RI CAI despre modificările condițiilor tehnice de funcționare a acestuia;

19.9. să asigure suportul metodologic și practic, prin elaborarea de proceduri, reguli și instrucțiuni în ceea ce privește înregistrarea, acumularea, păstrarea, completarea, corectarea, sistematizarea și utilizarea datelor;

19.10.să acorde suportul necesar persoanelor autorizate care au acces la RI CAI privind utilizarea complexului de mijloace software aferente acestuia;

19.11.să dețină auditul accesărilor care conține evidența operațiunilor ce au fost efectuate de către utilizatorii portalului și, la solicitare, în conformitate cu actele normative, să ofere informații despre auditul cu privire la accesări;

19.12.să asigure accesul securizat la informația conținută în RI CAI și să respecte condițiile de securitate și regulile de exploatare a acestuia.

Secțiunea a 3-a
Drepturile și obligațiile expeditorului

20. Expeditorul are dreptul:

20.1. să utilizeze funcționalitățile RI CAI;

20.2. să solicite de la deținător suport consultativ pentru utilizarea RI CAI;

20.3. să solicite de la destinatar suport consultativ la completarea corectă, din punct de vedere metodologic reglementat, a cererilor disponibile în cadrul RI CAI.

21. Expeditorul este obligat:

21.1. să respecte regulile de utilizare a RI CAI;

21.2. să colaboreze cu deținătorul RI CAI pentru asigurarea securității accesului la servicii și să informeze despre orice acțiune suspicioasă de care are cunoștință și care ar putea să reprezinte un atentat la serviciile respective;

21.3. să nu publice, transmită sau distribuie informații care pot fi dăunătoare, obscene, defăimătoare sau ilegale;

21.4. să nu utilizeze RI CAI într-un mod care poate duce la încălcarea drepturilor altor sisteme informaționale;

21.5. să nu folosească nicio aplicație software și niciun dispozitiv care să bruieze RI CAI și nici să încarce sau să pună la dispoziție fișiere conținând date eronate sau viruși, prin niciun fel de metodă;

21.6. să nu obțină sau să nu încerce să obțină acces neautorizat la informații, indiferent de metodă;

21.7. să nu utilizeze RI CAI în scop publicitar sau pentru orice fel de cerere / ofertă cu caracter comercial.

Secțiunea a 4-a
Drepturile și obligațiile destinatarului

22. Destinatarul RI CAI are dreptul:

22.1. să solicite și să primească de la deținător asistență la utilizarea RI CAI;

22.2. să înainteze propuneri privind modificarea actelor normative care reglementează funcționarea RI CAI.

23. Destinatarul RI CAI este obligat:

23.1. să întreprindă măsuri pentru evitarea accesului neautorizat al persoanelor terțe;

23.2. să utilizeze funcționalitățile RI CAI în exclusivitate conform destinației acestora și în strictă conformitate cu legislația.

Capitolul IV
ȚINEREA ȘI FUNCȚIONAREA RI CAI

24. Funcția principală a RI CAI constituie depunerea în format electronic a cererilor de înregistrare în calitate de candidat la Program la nivelul de bază / intermediar / avansat, precum și depunerea cererilor de eliberare, inclusiv de eliberare a duplicatului, de menținere și de suspendare a certificatului de calificare profesională, de către persoanele fizice. La fel, RI CAI permite ținerea electronică a Registrelor certificatelor de evaluare a cunoștințelor corespunzător fiecărui nivel al Programului, precum și Registrului certificatelor de calificare profesională.

25. RI CAI se accesează prin intermediul paginii-web https://certificare-ai.mf.gov.md (cu acces prin rețeaua internet). Pentru a accesa sistemul, utilizatorii (persoane fizice) vor folosi serviciul electronic guvernamental de autentificare și control

al accesului (MPass);

26. RI CAI oferă următoarele funcționalități de bază:

26.1. înregistrarea și autentificarea utilizatorilor de sistem;

26.2. completarea dosarului / actualizarea profilului;

26.3. crearea cererilor de înmatriculare la Program la nivelul de bază / intermediar / avansat, cu încărcarea actelor confirmative, înregistrarea, validarea, stocarea și expedierea acestora în mod electronic către posesor;

26.4. crearea cererilor de eliberare, inclusiv de eliberare a duplicatului, de menținere și de suspendare a certificatului de calificare profesională, cu încărcarea actelor confirmative, înregistrarea, validarea, stocarea și expedierea acestora în mod electronic către posesor;

26.5. recepționarea, înregistrarea și prelucrarea cererilor;

26.6. înregistrarea certificatelor de evaluare a cunoștințelor corespunzător fiecărui nivel al Programului, precum și a certificatelor de calificare profesională, eliberate în conformitate cu deciziile Comisiei de certificare în domeniul auditului intern în sectorul public;

26.7. vizualizarea și gestionarea Registrului certificatelor de calificare profesională în domeniul auditului intern în sectorul public și Registrelor certificatelor de evaluare a cunoștințelor corespunzător fiecărui nivel al Programului;

26.8. expedierea și recepționarea notificărilor în baza cererilor depuse de către utilizatori.

Capitolul V
ÎNREGISTRAREA, MODIFICAREA, COMPLETAREA ŞI RADIEREA DATELOR ÎN RI CAI

27. Înregistrarea, modificarea şi/sau completarea, precum și radierea datelor din cadrul RI CAI se efectuează de către posesorul acestuia.

28. RI CAI asigură posibilitatea de a accesa şi de a vizualiza informaţia la orice etapă de înregistrare, de modificare şi/sau de completare, de radiere a datelor, precum şi evidenţa tuturor modificărilor şi completărilor. Toate modificările operate în RI CAI se păstrează în ordine cronologică.

Capitolul VI

INTERACŢIUNEA CU FURNIZORII DE DATE

29. Furnizori de date ai RI CAI sunt expeditorii, persoane fizice care au calitatea de candidat sau participant la Program, sau sunt deținători ai certificatelor de calificare profesională.

30. Pentru asigurarea securității conținutului informațional al RI CAI și, în special, a datelor cu caracter personal ale expeditorilor, este efectuată interacțiunea RI CAI cu alte sisteme informaționale/servicii electronice guvernamentale pentru autorizarea subiecților cu acces la RI CAI.

31. RI CAI va interacționa cu serviciul electronic guvernamental de autentificare și control al accesului (MPass) pentru autentificarea și controlul accesului în cadrul sistemului.

Capitolul VII

ASIGURAREA SECURITĂŢII RI CAI

32. Datele din RI CAI fac parte din categoria datelor care necesită a fi protejate. Asigurarea securității, confidențialității și a integrității datelor prelucrate în cadrul RI CAI se efectuează de către subiecții cu drepturi de acces la sistem cu respectarea strictă a cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora.

33. Măsurile de protecție și securitate a datelor din RI CAI reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a RI CAI și se actualizează de către toți subiecții RI CAI.

34. Schimbul informațional se efectuează cu utilizarea mijloacelor software și hardware, doar prin canale securizate, asigurând integritatea și securitatea datelor.

35. Prelucrarea datelor cu caracter personal în cadrul RI CAI se efectuează în conformitate cu prevederile Legii nr. 133/2011 privind protecția datelor cu caracter personal. În condițiile prezentului Regulament, datele cu caracter personal se prelucrează exclusiv în măsura în care sunt necesare scopului și obiectivelor stabilite, conform competențelor atribuite subiecților raporturilor juridice aferente creării și ținerii RI CAI, asigurându-se la nivel de securitate și confidențialitate corespunzător în ceea ce

privește riscurile prezentate de prelucrare și caracterul datelor prelucrate, conform principiilor stabilite de legislația privind protecția datelor cu caracter personal.

36. Obiecte ale asigurării protecției și securității informației din cadrul RI CAI se consideră tot complexul de mijloace software și hardware care asigură realizarea proceselor informaționale:

36.1. bazele de date, suporturile materiale care conțin informații privind date cu caracter personal;

36.2. sistemele informaționale, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații care asigură activitatea RI CAI;

36.3. sistemele de comunicații electronice, rețelele, serverele, calculatoarele și alte echipamente și mijloace tehnice de captare și prelucrare a informației.

37. Protecția datelor se efectuează prin următoarele metode:

37.1. asigurarea măsurilor de protecție a datelor prin folosirea metodelor criptografice de transmitere a informației prin rețelele de transport de date guvernamentale;

37.2. excluderea accesului neautorizat la date din RI CAI, prin utilizarea funcționalităților de autentificare ale serviciului guvernamental de autentificare și control al accesului (MPass);

37.3. prevenirea acțiunilor intenționate și/sau neintenționate ale utilizatorilor care pot duce la distrugerea sau denaturarea datelor;

37.4. utilizarea obligatorie a produselor de program licențiate aprobate;

37.5. coordonarea solicitării de instalare a unui produs de program cu posesorul/deținătorul;

37.6. monitorizarea procesului de exploatare al RI CAI prin intermediul mecanismului de jurnalizare.

38. Deținătorul RI CAI elaborează și implementează politica de securitate informațională pentru asigurarea respectării regulilor, standardelor și normelor acceptate în domeniul securității informaționale, incluzând:

38.1. identitatea persoanei responsabile de politica de securitate;

38.2. principalele măsuri tehnico-organizatorice necesare pentru asigurarea

funcționării RI CAI;

38.3. procedurile interne care exclud cazurile de modificare nesancționată a mijloacelor software și/sau a informației în cadrul RI CAI;

38.4. responsabilitățile personalului privind asigurarea securității informaționale;

38.5. procedurile de control intern al subiecților implicați în operarea RI CAI privind respectarea condițiilor de securitate informațională.

39. Politica de securitate se aduce la cunoștința fiecărui utilizator care trebuie să cunoască obligațiile de serviciu în materie de respectare a securității informaționale și totalitatea procedurilor formale pe care trebuie să le respecte în strictă concordanță cu politica de securitate.

40. Prelucrarea datelor cu caracter personal se efectuează în conformitate cu cadrul normativ privind protecția datelor cu caracter personal. În cadrul RI CAI se prelucrează datele cu caracter personal strict necesare, neexcesive scopului prestabilit de acesta, asigurându-se un nivel de securitate și confidențialitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor.

Capitolul VIII
CONTROLUL ȘI RĂSPUNDEREA

41. Crearea, organizarea și funcționarea RI CAI este supusă controlului intern. Controlul intern privind organizarea și funcționarea RI CAI se efectuează de către posesor.

42. Responsabilitatea pentru organizarea funcționării RI CAI aparține posesorului acestuia.

43. Utilizatorii în atribuțiile cărora intră administrarea RI CAI, introducerea datelor, furnizarea / recepționarea informațiilor și asigurarea funcționării RI CAI, poartă răspundere personală în conformitate cu legislația în vigoare, pentru completitudinea, autenticitatea, veridicitatea, integritatea informației, precum și pentru păstrarea și utilizarea ei.

44. Toți subiecții RI CAI poartă răspundere conform legislației în vigoare pentru prelucrarea, divulgarea și transmiterea informației din sistem ce conține date cu caracter personal, persoanelor terțe, contrar prevederilor legislative.

45. Pentru asigurarea funcționalității și eficienței RI CAI, deținătorul poate întrerupe funcționalitatea RI CAI pentru efectuarea operațiunilor de întreținere. Prin urmare, nu se garantează disponibilitatea permanentă sau faptul că va putea fi accesat întotdeauna cu o anumită viteză sau cu o anumită funcționalitate.

46. Posesorul și deținătorul nu își asumă nicio răspundere în cazul în care anumite informații sunt furnizate cu întârziere, sunt pierdute, șterse sau nu pot fi stocate pe serverele RI CAI din orice motive care au survenit fără vina lor și nu sunt responsabili pentru folosirea incorectă de către utilizator a funcționalităților acestuia.

47. Posesorul și deținătorul nu poartă răspundere pentru datele transmise în RI CAI, pentru erorile, lacunele, ștergerea datelor, schimbarea funcțiilor, reținerile și defectele ce au loc în timpul transmiterii datelor, care au survenit fără vina lor.

48. Posesorul, deținătorul și destinatarul nu poartă răspundere pentru daunele indirecte cauzate deținătorului, inclusiv venitul ratat, economii ratate, oportunități ratate, netransmiterea sau transmiterea cu întârziere a informației, alterarea sau pierderea informației.

49. Funcționarea RI CAI se suspendă de către deținător, după coordonarea prealabilă cu posesorul, în caz de apariție a uneia dintre următoarele situații:

49.1. în timpul efectuării lucrărilor profilactice ale complexului de mijloace software și hardware al RI CAI;

49.2. la apariția impedimentelor justificatoare;

49.3. la încălcarea cerințelor sistemului securității informației, dacă aceasta prezintă pericol pentru funcționarea RI CAI;

49.4. în cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware al RI CAI;

49.5. la solicitarea oficială a posesorului.

50. În cazul apariției impedimentelor justificatoare și a dificultăților tehnice în funcționarea complexului de mijloace software și hardware al RI CAI din vina terților persoane, este posibilă suspendarea funcționării RI CAI, cu informarea subiecților prin mijloace tehnice disponibile.