

PROGRAMA DE PREGĂTIRE

Curs: Auditor de securitate cibernetică

Durata: 30 ore

Total din care: - instruire teoretică – 18 ore

- instruire practică – 12 ore

Tip curs: Curs specializare/perfecționare

Nivel de calificare conform:

- **CNC - Cadrului Național al Calificărilor - 6**
- **ISCED - International Standard Classification of Education - 6**

Scop: Dobândirea competențelor necesare pentru exercitarea funcției de **Auditor de securitate cibernetică**.

Programul este aliniat **OUG nr. 155/2024** privind securitatea cibernetică a rețelelor și sistemelor informatice, care instituie cadrul național pentru aplicarea **Directivei (UE) 2022/2555 – NIS2**, precum și celorlalte reglementări naționale relevante în domeniu.

Competențe generale

- Înțelegerea cadrului legislativ NIS2 și OUG 155/2024
- Evaluarea riscurilor cibernetică la nivel organizațional
- Aplicarea metodologiilor de audit în domeniul securității cibernetică
- Elaborarea rapoartelor de audit conforme DNSC

Competențe specifice

- Identificarea entităților esențiale și importante
- Auditarea măsurilor tehnice și organizatorice
- Evaluarea guvernantei și managementului riscurilor
- Auditarea furnizorilor și lanțului de aprovizionare
- Verificarea capacității de răspuns la incidente
- Formularea neconformităților și recomandărilor

Obiective specifice de învățare:

- Dezvoltarea capacității de aplicare a obligațiilor legale cu privire la asigurarea auditării securității cibernetică a rețelelor și sistemelor informatice conform contextului organizațional;

- Infrastructură critică. Entități esențiale și/sau importante;
- Termeni și noțiuni privind securitatea cibernetică;
- Obligațiile de securitate a rețelelor și informațiilor;
- Standarde și specificații europene și internaționale aplicabile;
- Legislația națională aplicabilă;
- Stabilirea efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice;
- Procesul de audit – terminologie, principii, planificarea și desfășurarea auditului, raportarea;
- Tehnici și metode de audit;
- Evaluarea implementării cerințelor minime de asigurare a securității rețelelor și sistemelor informatice/cibernetice;
- Codul de etică al auditorilor de securitate cibernetică.

Rezultate ale învățării

La finalul cursului, participantul va putea:

- ✓ Interpreta corect cerințele OUG 155/2024 și NIS2
- ✓ Clasifica entitățile conform criteriilor DNSC
- ✓ Evalua riscurile cibernetice și controalele existente
- ✓ Conduce un audit complet (planificare → execuție → raportare)
- ✓ Identifica neconformități și formula recomandări
- ✓ Elabora un raport oficial de audit conform DNSC

Competențe dobândite

- Înțelegerea legislației naționale și europene în securitatea cibernetică;
- Capacitatea de a interpreta și aplica O.U.G. 155/2024 și directivele europene relevante, inclusiv NIS 2, în contextul auditului entităților esențiale și/sau importante;
- Evaluarea și clasificarea entităților auditate;
- Abilitatea de a identifica, analiza și clasifica entitățile auditate conform cerințelor legale și standardelor de securitate cibernetică;
- Analiza vulnerabilităților și a riscurilor de securitate, capacitatea de a evalua riscurile, vulnerabilitățile și impactul potențial al incidentelor asupra rețelelor și sistemelor informatice;
- Desfășurarea auditului de securitate, competența de a planifica, realiza și documenta audituri de securitate cibernetică, conform standardelor internaționale și cerințelor O.U.G. 155/2024;
- Implementarea și monitorizarea controalelor tehnice și procedurale;
- Cunoașterea și aplicarea practicilor și standardelor de securitate pentru evaluarea eficienței măsurilor tehnice și procedurale implementate de organizații;
- Elaborarea și interpretarea rapoartelor de audit, abilitatea de a întocmi rapoarte clare, coerente și relevante, care să susțină factorii decizionali și să fie conforme cerințelor legale și profesionale;

- Asigurarea conformității și supraveghere profesională Capacitatea de a monitoriza și verifica conformitatea organizațiilor auditate cu legislația națională și standardele europene, precum și cu principiile etice ale auditului;
- Comunicarea profesională cu autoritățile și factorii implicați, abilitatea de a transmite clar și eficient concluziile auditului și recomandările către management și autoritatea națională competentă.
- Aplicarea practică a cunoștințelor teoretice;
- Capacitatea de a transforma cunoștințele de audit și securitate cibernetică în soluții concrete pentru prevenirea, identificarea și remedierea vulnerabilităților.
- Dezvoltarea profesională și etica în activitatea de auditor;
- Cultivarea responsabilității, rigurozității și eticii în toate activitățile specifice auditului de securitate cibernetică, inclusiv prin colaborarea eficientă în echipe multidisciplinare.

TEMATICA
pentru formarea Auditorilor de securitate cibernetică

Nr. crt.	Tematica	Durata (ore) Din care:		Metode de formare	Mijloace de formare/ Logistică	Criterii de performanță
		Teorie	Practică			
1	Modulul 1 - Concepte și cadrul general al securității cibernetice: ▪ Introducere în securitatea cibernetică; ▪ Context general; ▪ Terminologie și concepte referitoare la securitatea rețelelor și sistemelor informatice aplicabile entităților esențiale și/sau importante și furnizorilor de servicii digitale: • <i>Active, vulnerabilități, amenințări;</i> • <i>Riscuri și impact;</i> • <i>Incidente de securitate;</i> ▪ Arhitecturi și tehnologii; • <i>Rețele și infrastructuri;</i> • <i>Cloud, IoT, OT/ICS;</i> • <i>Criptografie, IAM, monitorizare;</i> ▪ Măsuri tehnice și organizatorice: • <i>Politici de securitate;</i> • <i>Controlul accesului;</i> • <i>Protecția rețelelor;</i> • <i>Backup, logging, patching.</i>	1	-	<i>Prezentări multimedia.</i> <i>Exemplificări.</i> <i>Dezbateri.</i> <i>Brainstorming.</i>	Materiale multimedia. Laptop. Videoproiector.	• Înțelege bine conceptele utilizate în domeniul securității cibernetice. • Înțelege bine cadrul general al securității cibernetice. • Participantul poate evalua controale tehnice și organizaționale.

Nr. crt.	Tematica	Durata (ore)		Metode de formare	Mijloace de formare/ Logistică	Criterii de performanță
		Teorie	Practică			
	Prezentare glosar termeni.					
2	Modulul 2 - Cadrul de reglementare și cooperare în domeniul securității cibernetice: ☐ Cadrul european: - Directiva UE 2022/2555 (NIS2); - Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică); <i>Obligații pentru state și entități</i> <i>Relația cu alte reglementări (CER, GDPR, DORA – contextual)</i> ☐ Cadrul național: - OG 155/2024 pentru transpunerea în România a Directivei UE 2022/2555; <i>obiectul, scopul și principiile cadrului normativ, potrivit art. 1–3 din OG nr. 155/2024;</i> <i>prezentarea articolelor esențiale;</i> - Legea nr. 124/2025, aprobă Ordonanța de urgență a Guvernului nr. 155/2024; <i>prezentarea articolelor esențiale;</i> - Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative; <i>prezentarea articolelor esențiale;</i> - OG nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, cu modificările și completările ulterioare;	2	1	<i>Prezentări multimedia.</i> <i>Exemplificări.</i> <i>Dezbateri.</i> <i>Brainstorming.</i> <i>Studii de caz pe baza legislației aplicabile</i>	Materiale multimedia. Laptop. Videoproiector.	Înțelege bine legislația națională și europeană în domeniul securității cibernetice.

Nr. crt.	Tematica	Durata (ore) Din care:		Metode de formare	Mijloace de formare/ Logistică	Criterii de performanță
		Teorie	Practică			
	• <i>prezentarea articolelor esențiale;</i> ▪ Ordinul Directorului DNSC nr. 2/2025 pentru aprobarea Criteriilor și pragurilor de determinare a gradului de perturbare a unui serviciu și a Metodologiei privind evaluarea nivelului de risc al entităților;					
3	Modulul 3 - Standarde și specificații europene și internaționale aplicabile entităților esențiale și/sau importante, furnizorilor de servicii digitale și auditorilor de securitate cibernetică: ▪ ISO/IEC 27001:2022- Sistem de management al securității informației (ISMS) ▪ ISO/IEC 27701: Extensie de confidențialitate pentru ISO/IEC 27001 – alinierea cu GDPR ▪ ISO/IEC 27002:2022- Cod de bune practici pentru controale de securitate ▪ ISO/IEC 27005: Managementul riscului de securitate a informației ▪ ISO/IEC 27035: Managementul incidentelor de securitate ▪ ISO 22301: Continuitatea afacerii ▪ IEC 62443 – securitate pentru ICS/OT ▪ NIST CSF 2.0-Cadru de bune practici (Identify–Protect–Detect–Respond–Recover) ▪ NIST SP 800-53 / 800-171: controale detaliate, mai ales în medii cu cerințe ridicate. ▪ ISO/IEC 20000-1: Managementul serviciilor IT – important pentru DSP (cloud, marketplace, motoare de căutare). ▪ Standarde tehnice și sectoriale (CEN/CENELEC, ETSI, IEC etc.) ▪ Standarde și referințe pentru	2	-	<i>Prezentări multimedia.</i> <i>Exemplificări.</i> <i>Dezbateri.</i> <i>Brainstorming.</i> <i>Studii de caz pe baza legislației aplicabile</i>	Materiale multimedia. Laptop. Videoproiector.	• Cunoașterea standardelor din domeniul securității cibernetice. • Cunoașterea specificațiilor europene și internaționale din domeniul securității cibernetice. • Cunoașterea standardelor din domeniul securității cibernetice aplicabile auditorilor pentru acest domeniu.

Nr. crt.	Tematica	Durata (ore)		Metode de formare	Mijloace de formare/ Logistică	Criterii de performanță
		Teorie	Practică			
	auditori de securitate cibernetică: • <i>ISO 19011: Ghid pentru auditarea sistemelor de management</i> • <i>ISO/IEC 17021-1: Cerințe pentru organisme care certifică sisteme de management</i> • <i>ISO/IEC 17065 / 17020: Pentru organisme de certificare de produse/servicii sau de inspecție</i> • <i>Standardele ISAE (IFAC) – ISAE 3000, ISAE 3402: Pentru rapoarte de asigurare asupra controalelor</i> • <i>Cadrul ENISA și ghidurile naționale NIS: Folosite ca referință de audit pentru verificarea cerințelor minime de securitate și raportare a incidentelor.</i> ▪ NIS2 – Directiva privind securitatea rețelelor și sistemelor informatice ▪ DORA – Digital Operational Resilience Act ▪ Cyber Resilience Act (CRA) – securitate pentru produse digitale ▪ CER Directive – Critical Entities Resilience ▪ CyberFundamentals (CyFun) ▪ Bune practici în domeniul auditului sistemelor informatice ▪ ITAF – Information Technology Assurance Framework ▪ Legătura între reglementări (pe scurt) • <i>NIS2 / DORA / CRA / CER îți spun „CE trebuie să faci” (obligații legale).</i> • <i>ISO 27001 / 27002 / 22301 / IEC 62443 / NIST CSF îți spun „CUM poți demonstra” că</i>					

Nr. crt.	Tematica	Durata (ore) Din care:		Metode de formare	Mijloace de formare/ Logistică	Criterii de performanță
		Teorie	Practică			
	<i>faci ce trebuie.</i> - Directivă (UE) 2022/2555 (NIS2) stabilesc cerințe minime de securitate și raportare a incidentelor pentru entitățile esențiale și furnizori de servicii digitale; - Regulamentul (UE) 2018/679-GDPR.					
4	Modulul 4 - Condiții și cerințe pentru auditorii de securitate cibernetică (Norme privind activitatea auditorilor; Cerințe pentru auditorii de securitate cibernetică; Codul etic al auditorului de securitate cibernetică): - Cadrul legislativ și normativ - Tipuri de audit în securitate cibernetică - Principiile auditului de securitate cibernetică - Documente obligatorii în activitatea auditorului - Cerințe pentru auditorii de securitate cibernetică (competențe, certificări, abilități și responsabilități) - Codul etic al auditorului de securitate cibernetică - Principiile morale și profesionale care guvernează activitatea auditorului (Integritate; Independență și obiectivitate; Confidențialitate; Profesionalism; Imparțialitate; Diligență profesională; Responsabilitate socială.)	1	1	<i>Prezentări multimedia. Exemplificări. Dezbateri. Brainstorming. Studii de caz pe baza legislației aplicabile</i>	Materiale multimedia. Materiale tipărite. Fișe de lucru. Laptop. Videoproiector.	- Cunoașterea principiilor auditului de securitate cibernetică. - Cunoașterea cerințelor pentru auditorii de securitate cibernetică. - Cunoașterea prevederilor Codului etic al auditorului de securitate cibernetică.
5	Modulul 5 - Auditul de securitate cibernetică, potrivit art. 57–59 din OUG nr. 155/2024. - Desfășurarea auditului de securitate. - Ce este auditul de securitate - Tipuri de audit: conformitate, tehnic, operațional, integrat IT/OT	3	2	<i>Prezentări multimedia. Exemplificări. Dezbateri. Brainstorming. Studii de caz și exerciții pe</i>	Materiale multimedia. Materiale tipărite. Fișe de lucru. Laptop. Videoproiector.	- Cunoașterea tipurilor de audit de securitate cibernetică. - Cunoașterea etapelor auditului de securitate

Nr. crt.	Tematica	Durata (ore)		Metode de formare	Mijloace de formare/ Logistică	Criterii de performanță
		Teorie	Practică			
	• <i>Diferențe între audit, evaluare și testare tehnică</i> • <i>Etapele auditului de securitate cibernetică (Planificarea auditului; Desfășurarea auditului (on-site / remote); Colectarea și validarea evidențelor; Analiza constatărilor; Raportarea auditului.)</i> • <i>Rollurile în audit</i> • <i>Reguli de desfășurare</i> ▪ Documente de audit de securitate - documentele obligatorii și modul în care sunt utilizate. • <i>Documente pregătitoare</i> • <i>Documente generate în timpul auditului</i> • <i>Documente finale</i> • <i>Caracteristicile unui document de audit</i> ▪ Cerințe referitoare la desfășurarea unui audit de securitate - reguli, standarde și bune practici pe care auditorii trebuie să le respecte. • <i>Cerințe normative</i> • <i>Cerințe operaționale</i> • <i>Cerințe tehnice</i> • <i>Cerințe privind comunicarea</i> • <i>Cerințe privind etica și profesionalismul</i>			<i>baza legislației aplicabile</i> <i>Scenarii și studii de caz privind gestionarea alertelor și răspunsul la incidente.</i>		cibernetică.
6	Modulul 6 - Evaluarea implementării cerințelor minime de asigurare a securității rețelelor și sistemelor informatice: ▪ Cadrul legislativ și normativ (UE + România) - Fundamentul oricărei evaluări de conformitate ▪ Cerințele minime de securitate – structură și domenii- <i>Ce trebuie implementat înainte de orice evaluare</i>	2	3	<i>Prezentări multimedia.</i> <i>Exemplificări.</i> <i>Dezbateri.</i> <i>Brainstorming.</i> <i>Studii de caz pe baza legislației aplicabile</i>	Materiale multimedia. Materiale tipărite. Fișe de lucru. Laptop. Videoproiector.	• Dovedirea abilității aplicarea practicilor și standardelor de securitate pentru evaluarea eficienței măsurilor tehnice și procedurale implementate de organizații.

Nr. crt.	Tematica	Durata (ore) Din care:		Metode de formare	Mijloace de formare/ Logistică	Criterii de performanță
		Teorie	Practică			
	▪ Solicitarea, furnizarea și utilizarea datelor și informațiilor necesare pentru prevenirea și contracararea amenințărilor cibernetice, potrivit art. 25 și art. 26 din Legea nr. 58/2023; ▪ Metodologia de evaluare a implementării cerințelor minime - <i>Cum se face evaluarea în practică</i> ▪ Evidențe obligatorii pentru evaluare - <i>Ce trebuie să poți demonstra</i> ▪ Evaluarea riscurilor – cerință centrală în NIS2 - <i>Fără evaluare de risc, nu există conformitate</i> ▪ Măsurile de gestionare a riscurilor de securitate cibernetică și obligațiile de raportare, potrivit art. 10-11 din OUG nr. 155/2024; ▪ Determinarea impactului generat de perturbarea serviciilor furnizate, potrivit art. 10 din OUG nr. 155/2024; • Criteriile și pragurile de determinare a gradului de perturbare a serviciilor și metodologia de evaluare a nivelului de risc, potrivit Ordinului Directorului DNSC nr. 2/2025; ▪ Evaluarea controalelor tehnice (IT + OT) - Partea practică a evaluării ▪ Evaluarea Incident Response (IR) ▪ Cerință critică în NIS2 și Normele tehnice ▪ Evaluarea maturității organizației ▪ Cum se măsoară nivelul de implementare ▪ Gap Assessment – identificarea neconformităților ▪ Pregătirea planului de remediere ▪ Planul de remediere 30–60–90 zile ▪ Cum se încheie evaluarea ▪ Dashboard de conformitate (KPIs + risc + maturitate)					• Dovedirea abilității de a identifica, analiza și clasifica entitățile auditate conform cerințelor legale și standardelor de securitate cibernetică. • Poate analiza și verifica implementarea corectă cerințelor minime de securitate cibernetică. • Poate evalua împreună cu specialiști IT eficacitatea măsurilor de securitate cibernetică, conform nivelului de securitate al organizației. • Capacitatea de a evalua riscurile, vulnerabilitățile și impactul potențial al incidentelor asupra rețelelor și sistemelor informatice.

Nr. crt.	Tematica	Durata (ore)		Metode de formare	Mijloace de formare/ Logistică	Criterii de performanță
		Teorie	Practică			
	- Cum se prezintă rezultatele evaluării - Studiu de caz – Evaluarea unei infrastructuri IT/OT.					
7	Modulul 7 - Formulare/rapoarte utilizate în activitatea de audit de securitate. Modele și moduri de completare: - Documentele utilizate în auditul de securitate - Context, rol și importanță - Formulare utilizate în etapa de planificare a auditului - Planul de audit - Agenda auditului - Declarația de independență și confidențialitate - Lista documentelor solicitate (Document Request List – DRL) - Formulare utilizate în etapa de desfășurare a auditului - - Documente folosite pentru colectarea și validarea evidențelor - Formulare utilizate în etapa de analiză și raportare - Raportul de audit de securitate – structura și modul de completare - Documentul final, obligatoriu pentru auditul NIS2 și ISO 27001	1	3	Prezentări multimedia. Exemplificări. Dezbateri. Brainstorming. Studii de caz pe baza legislației aplicabile Scenarii.	Materiale multimedia. Materiale tipărite. Fișe de lucru. Laptop. Videoproiector.	- Cunoașterea tipurilor de formulare utilizate în auditul de securitate cibernetică. - Cunoașterea modului de completare a formularelor utilizate în auditul de securitate cibernetică. - Cunoașterea modului de realizare a rapoartelor de audit de securitate cibernetică.
8	Modulul 8 - Cerințe și recomandări privind întocmirea raportului de audit de securitate. Elaborare și completare raport de audit de securitate: - Ce trebuie să conțină raportul, cum se redactează și ce standarde trebuie respectate - Rolul raportului de audit în procesul de evaluare - Cerințe normative aplicabile raportului	2	2	Prezentări multimedia. Exemplificări. Dezbateri. Brainstorming. Studii de caz pe baza legislației aplicabile Scenarii. Simulări	Materiale multimedia. Materiale tipărite. Fișe de lucru. Laptop. Videoproiector.	Cunoașterea modului de întocmire a raportului de audit de securitate.

Nr. crt.	Tematica	Durata (ore)		Metode de formare	Mijloace de formare/ Logistică	Criterii de performanță
		Teorie	Practică			
	• Structura obligatorie a raportului de audit • Principii de redactare • Bune practici în redactarea raportului ▪ Procesul efectiv de redactare, de la colectarea evidențelor la formularea concluziilor • Colectarea și organizarea evidențelor • Analiza constatărilor • Formularea recomandărilor • Redactarea concluziilor • Validarea internă a raportului ▪ Completarea raportului de audit de securitate - finalizarea raportul și prezentarea rezultatelor ▪ Completarea anexelor ▪ Prezentarea raportului către conducere ▪ Predarea raportului către autorități (DNSC) ▪ Închiderea auditului ▪ Erori frecvente în completarea raportului. ▪ Regimul sancționator și mecanismele de constatare și aplicare a sancțiunilor conform dispozițiilor relevante din capitolul X din Legea nr. 58/2023 și art. 60–62 din OUG nr. 155/2024;					
9	Modulul 9 - Verificarea activității auditorilor de securitate cibernetică: ▪ Scopul verificării activității auditorilor de securitate cibernetică; ▪ Componentele activității de verificare a auditorilor de securitate cibernetică; ▪ Procesele principale ale activității de verificare a auditorilor de securitate cibernetică;	0,5	-	Prezentări multimedia. Exemplificări. Dezbateri. Brainstorming. Studii de caz pe baza legislației aplicabile	Materiale multimedia. Laptop. Videoproiector.	• Cunoașterea etapelor verificării activității auditorilor de securitate cibernetică. • Cunoașterea principiilor eticii activității specifice auditului de securitate

Nr. crt.	Tematica	Durata (ore) Din care:		Metode de formare	Mijloace de formare/ Logistică	Criterii de performanță
		Teorie	Practică			
	- Rolurile implicate în activitatea de verificare a auditorilor de securitate cibernetică; - Indicatori de performanță (KPI) în activitatea de verificare a auditorilor de securitate cibernetică; - Riscuri de gestionat în activitatea de verificare a auditorilor de securitate cibernetică; - Provocări în implementare activității de verificare a auditorilor de securitate cibernetică; - Bune practici în activitatea de verificare a auditorilor de securitate cibernetică.					cibernetică.
10	Modulul 10 - Autorități, roluri și responsabilități în baza OUG nr. 155/2024 privitor la: - Arhitectura națională de securitate cibernetică în 2026; - Coordonarea strategică în domeniul securității cibernetică; - Autoritățile competente conform NIS2; - Autoritatea competentă la nivel național – DNSC; - Rolul și atribuțiile conform art. 2-7 și art. 16-20 din OUG nr. 104/2021; - Registrul entităților, potrivit art. 18 din OUG nr. 155/2024; - Atribuțiile autorităților și instituțiilor cu responsabilități în domeniul securității și apărării cibernetică, mecanismele de cooperare instituțională, potrivit art. 10 din Legea nr. 58/2023 și art. 24-27 din OUG nr. 155/2024; - Desemnarea punctului unic de contact la nivel național și a echipei	1,5	-	<i>Prezentări multimedia.</i> <i>Exemplificări.</i> <i>Dezbateri.</i> <i>Brainstorming</i> <i>Studii de caz.</i>	Materiale multimedia. Laptop. Videoproiector.	- Cunoașterea autorităților din domeniul securității cibernetică la nivel național și european, a rolului acestora. - Cunoașterea relaționării dintre autorități. - Cunoașterea bună a modului de colaborare între entități și autoritățile de supraveghere și control din domeniul securității cibernetică - Interacționează eficient cu autoritățile de supraveghere și control din domeniul securității

Nr. crt.	Tematica	Durata (ore) Din care:		Metode de formare	Mijloace de formare/ Logistică	Criterii de performanță
		Teorie	Practică			
	naționale de răspuns la incidente de securitate cibernetică; ▪ Mecanisme de supraveghere, verificare și control potrivit art. 46–50 din OUG nr. 155/2024; ▪ Mecanismele de coordonare la nivel național, potrivit art. 21–23 din OUG nr. 155/2024; ▪ Cadrul național de gestionare a crizelor cibernetică, potrivit art. 28–29 din OUG nr. 155/2024; ▪ Cadrul de cooperare instituțională, mecanismele de coordonare și măsurile de asigurare a rezilienței în spațiul cibernetic, potrivit dispozițiilor relevante din capitolul V din Legea nr. 58/2023; ▪ Identificarea categoriei în care se încadrează organizația; • <i>clasificarea entităților și domeniul de aplicare, inclusiv criteriile de identificare a entităților esențiale și importante, conform art. 5–9 și anexelor nr. 1 și 2;</i> ▪ Rolurile și responsabilitățile entităților esențiale (EE) și importante (EI)-art. 5–9+anexe nr. 1 și 2; • Responsabilitățile organelor de conducere în domeniul securității cibernetică, potrivit art. 14 din OUG nr. 155/2024; • Raportarea incidentelor și gestionarea incidentelor, inclusiv utilizarea mecanismelor de notificare (PNRISC), potrivit art. 15 din OUG nr. 155/2024; • Organizarea și funcționarea echipelor de răspuns la incidente de securitate cibernetică (CSIRT), potrivit art. 30–36 din OUG nr. 155/2024; • Dispozițiile privind CSIRT-urile,					cibernetice. • Înțelege bine utilizarea legislației naționale și europene din domeniul securității cibernetică pentru identificarea categoriei în care se încadrează o anumită organizație.

Nr. crt.	Tematica	Durata (ore) Din care:		Metode de formare	Mijloace de formare/ Logistică	Criterii de performanță
		Teorie	Practică			
	auditorii și furnizorii de servicii de formare, potrivit art. 53–56 din OUG nr. 155/2024.					
11	TOTAL 30 ore din care:	18 Teorie	12 Practică			

**VOCHITOIU
HARALAMBIE**

Digitally signed by
VOCHITOIU HARALAMBIE
Date: 2026.04.07 13:42:08
+03'00'