GUVERNUL ROMÂNIEI
SECRETARIATUL GENERAL AL GUVERNULUI

ORDIN

pentru aprobarea Regulamentului pentru atestarea și verificarea auditorilor de securitate cibernetică

Având în vedere dispozițiile art. 32 alin. (2) lit. b) și al art. 20 lit. e) și lit. s) din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare,

în temeiul art. 7 alin. (6) din Hotărârea Guvernului nr. 137/2020 privind organizarea, funcționarea și atribuțiile unor structuri din cadrul aparatului de lucru al Guvernului,

secretarul general al Guvernului emite prezentul ordin.

Art. 1. – Se aprobă **Regulamentul pentru atestarea și verificarea auditorilor de securitate cibernetică**, prevăzut în anexa care face parte integrantă din prezentul ordin.

Art. 2. – Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

SECRETARUL GENERAL AL GUVERNULUI

Tiberiu-Horațiu GORUN

București, 22 martie 2021
Nr. 559

ANEXĂ

REGULAMENTUL

pentru atestarea și verificarea auditorilor de securitate cibernetică

CAPITOLUL I. DISPOZIȚII GENERALE

Art. 1. Aplicabilitate

(1) Prezentul regulament pentru atestarea și verificarea auditorilor de securitate cibernetică, denumit în continuare *regulament*, stabilește cadrul legal pentru atestarea auditorilor de securitate cibernetică pentru auditarea rețelelor și sistemelor informatice ce susțin servicii esențiale ori furnizează servicii digitale în condițiile Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare, denumită în continuare *Legea NIS*.

(2) În înțelesul prezentului regulament, auditorii de securitate cibernetică pot fi persoane fizice atestate cetățeni români, precum și cetățeni ai altui stat membru al Uniunii Europene ori al Spațiului Economic European, sau persoane juridice cu personal atestat, care îndeplinesc cerințele prevăzute în prezentul regulament și care doresc să desfășoare o activitate prin care se realizează o evaluare sistematică a tuturor politicilor, procedurilor și măsurilor de protecție implementate la nivelul rețelelor și sistemelor informatice, în vederea identificării disfuncțiilor și vulnerabilităților și a furnizării unor soluții de remediere a acestora; activitate pe care să o exercite în România în mod independent sau ca angajați ai unor persoane juridice.

(3) Prezentul regulament nu se aplică la nivelul instituțiilor din sistemul de apărare, ordine publică și securitate națională, din domeniul protecției infrastructurilor critice și nici la nivelul infrastructurilor cibernetice care vehiculează informații clasificate.

Art. 2. Termeni, expresii și abrevieri

(1) În cuprinsul prezentului regulament, se utilizează următoarele abrevieri:
   a) **ANSRSI** – Autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale ori furnizează serviciile digitale, denumită și Autoritatea competentă la nivel național.
   b) **CERT-RO** – Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO.
   c) **COSC** – Consiliul Operativ de Securitate Cibernetică.
   d) **CSIRT** – echipă de răspuns la incidente de securitate cibernetică.
   e) **FSD** – furnizor de servicii digitale.
   f) **OSE** – operator de servicii esențiale.

(2) În cuprinsul prezentului regulament, precum și în activitatea specifică domeniului securității rețelelor și sistemelor informatice se utilizează următoarele concepte:
   a) **Auditor de securitate cibernetică (ASC)** – persoană fizică atestată sau persoană juridică cu personal atestat care realizează activități de auditare a rețelelor și sistemelor informatice ce susțin servicii esențiale sau furnizează servicii digitale, conform reglementărilor și bunelor practici în domeniu.
   b) **Audit de securitate (ASEC)** – activitatea prin care se realizează o evaluare sistematică a tuturor politicilor, procedurilor și măsurilor de protecție implementate la nivelul rețelelor și sistemelor informatice în vederea identificării disfuncțiilor și vulnerabilităților și a furnizării unor soluții de remediere a acestora.
   c) **Atestat de auditor de securitate cibernetică (AASC)** – document emis de autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice, cu valabilitate limitată de trei ani, prin care se certifică îndeplinirea condițiilor de către persoana atestată pentru desfășurarea activităților de auditare a rețelelor și sistemelor informatice aparținând operatorilor de servicii esențiale sau furnizorilor de servicii digitale.

d) **Certificat de specializare auditor de securitate cibernetică (CSASC)** – document eliberat de către un formator sau furnizor de servicii de formare pentru auditori de securitate cibernetică autorizat de ANSRSI.

e) **Codul etic al auditorului de securitate cibernetică (CEASC)** – un ansamblu de principii și reguli de conduită care trebuie să guverneze activitatea auditorului de securitate cibernetică.

f) **Domeniul auditului** – mediul fizic, logic și organizațional în care se află rețelele și sistemele informatice sau o parte a acestora și pe care se efectuează un audit de securitate.

g) **Echipă de audit de securitate (EASEC)** – formațiune constituită din două sau mai multe persoane, condusă de un șef de echipă, ce este capabilă să efectueze auditul de securitate la nivelul unui operator de servicii esențiale sau furnizor de servicii digitale cu respectarea prezentului regulament.

h) **Evaluarea riscurilor de securitate (ERS)** – un proces de evaluare a riscurilor de securitate privind solicitantul pentru atestare ca auditor de securitate cibernetică din perspectiva Strategiei de securitate cibernetică a României și a securității naționale, precum și a obligațiilor asumate de România la nivelul Uniunii Europene. Activitatea este efectuată de ANSRSI cu sprijinul instituțiilor din COSC.

i) **Lista auditorilor de securitate cibernetică (LASC)** – cuprinde toți auditorii de securitate cibernetică valabil atestați de autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice și este publicată pe site-ul instituției.

j) **Lista standardelor și specificațiilor europene și internaționale (LSSEINIS)** – cuprinde toate standardele și specificațiile europene și internaționale utilizate în implementarea cerințelor minime de securitate și în activitatea auditorilor de securitate cibernetică.

k) **Raport de audit de securitate (RASEC)** – document sinteză întocmit de echipa de audit de securitate/ auditorul de securitate cibernetică, la sfârșitul activității de audit de securitate, prezentat operatorului economic auditat, respectiv operatorului de servicii esențiale sau furnizorului de servicii digitale, și care prezintă rezultatele auditului, și în special, vulnerabilitățile descoperite/identificate, precum și măsurile corective propuse.

l) **Registrul național al auditorilor de securitate cibernetică (RENASC)** – document constituit și administrat la nivelul autorității competente la nivel național pentru securitatea rețelelor și sistemelor informatice care cuprinde evidența cronologică a atestărilor, suspendărilor și revocărilor auditorilor de securitate cibernetică.

m) **Rețele și sisteme informatice (RSI)** – se definesc conform art. 3 lit. l) din Legea NIS; reprezintă o colecție de resurse (hardware, software, personal, date/ informații și proceduri) aparținând, după caz, operatorilor de servicii esențiale sau furnizorilor de servicii digitale și care stau la baza furnizării serviciilor esențiale și respectiv serviciilor digitale.

n) **Sistem de control industrial (ICS)** – un set de resurse umane și materiale constituit în scopul controlului instalațiilor tehnice utilizate în furnizarea unui serviciu esențial sau digital compus din senzori și dispozitive de acționare.

o) **Solicitant de atestat de auditor de securitate cibernetică (SAASC)** – o persoană care a absolvit un curs de specializare și care solicită atestarea ca auditor de securitate cibernetică, de la data solicitării și până la primirea atestatului.

p) **Testarea de penetrare** – procesul de testare a rețelelor și sistemelor informatice printr-o simulare a unui atac real asupra componentelor hardware și software, inclusiv a aplicațiilor informatice utilizate de operatorul de servicii esențiale sau furnizorul de servicii digitale auditat, după caz, efectuată cu acordul operatorului economic auditat.

q) **Vulnerabilitate** – o slăbiciune în proiectarea și implementarea rețelelor și sistemelor informatice sau a măsurilor de securitate aferente care poate fi exploatată de către o amenințare sau de un grup de amenințări.

Art. 3. Autoritatea competentă la nivel național

(1) Pentru eliberarea, revocarea sau reînnoirea atestatelor auditorilor de securitate cibernetică care pot efectua audit în cadrul rețelelor și sistemelor informatice ce susțin servicii esențiale ori furnizează servicii digitale, Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO este autoritatea competentă la nivel național în conformitate cu prevederile art. 15 alin. (1) coroborat cu art. 20 lit. p) din Legea NIS.

(2) Autoritatea competentă la nivel național organizează și gestionează procesul de atestare și verificare a auditorilor de securitate cibernetică.
(3) CERT-RO în calitate de autoritate competentă la nivel național asigură:
   a) menținerea și actualizarea permanentă a Registrului național al auditorilor de securitate cibernetică;
   b) acordarea, prelungirea, suspendarea sau retragerea atestatelor de auditori de securitate cibernetică;
   c) evaluarea riscurilor de securitate cu privire la auditorii de securitate și la activitățile de auditare a rețelelor și sistemelor informatice, împreună cu instituțiile din COSC;
   d) participarea la procesul de pregătire/specializare a auditorilor în vederea atestării ca auditori de securitate cibernetică, atât prin tematicile elaborate, cât și în comisiile de examen/evaluare;
   e) verificarea în urma sesizărilor sau din oficiu a îndeplinirii de către auditorii de securitate cibernetică atestați a obligațiilor legale ce le revin.

Art. 4. Auditorii de securitate cibernetică

(1) Auditor de securitate cibernetică poate fi orice persoană fizică sau persoană juridică ce realizează pe teritoriul României activitatea de audit de securitate a rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale ori furnizează serviciile digitale în vederea identificării disfuncțiilor și vulnerabilităților și a furnizării unor soluții de remediere a acestora.
(2) Auditorul de securitate cibernetică își desfășoară activitatea individual sau în cadrul unei echipe de audit și realizează cel puțin una dintre activitățile de audit de securitate așa cum sunt stabilite la art. 5 alin. (1).
(3) Auditorii de securitate cibernetică sunt atestați de autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice, iar evidența acestora este ținută în Registrul național al auditorilor de securitate cibernetică.
(4) Calitatea de auditor de securitate cibernetică se dovedește prin atestatul de auditor valabil eliberat de către autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice.
(5) Atestatul de auditor de securitate cibernetică este nominal, netransmisibil și are valabilitate trei ani de la data emiterii. Modelul atestatului este prevăzut în Anexa nr. 1.

Art. 5. Activități de audit de securitate

(1) Activitățile de audit de securitate tratate în prezentul regulament sunt:
   a) **Auditul arhitecturii [AS1].** Constă în verificarea conformității măsurilor de securitate legate de alegerea, poziționarea și implementarea dispozitivelor hardware/software în rețelele și sistemele informatice, cerințele minime de securitate și politicile interne ale operatorului economic. Auditul poate fi extins la interconectările cu rețele terțe, inclusiv internetul.
   b) **Auditul de configurare [AS2].** Constă în verificarea implementării măsurilor de securitate în conformitate cu stadiul tehnicii, cerințele minime de securitate și politicile de securitate în ceea ce privește configurația dispozitivelor hardware/software componente ale rețelelor și sistemelor informatice. Aceste dispozitive pot fi în special echipamente de rețea, sisteme de operare (server sau stație de lucru), aplicații sau produse de securitate.
   c) **Auditul codului sursă [AS3].** Constă în analiza totală sau parțială a codului sursă sau a condițiilor de compilare ale unei aplicații pentru a descoperi vulnerabilitățile legate de practicile de programare neadecvate sau erorile logice care ar putea avea un impact asupra securității rețelelor și sistemelor informatice.
   d) **Auditul de penetrare** sau **Testarea de penetrare [AS4]**. Constă în identificarea vulnerabilităților din rețelele și sistemele informatice și verificarea posibilităților de exploatare a acestora, precum și a impactului exploatării acestora asupra rețelei, în condițiile reale ale unui atac cibernetic asupra rețelelor și sistemelor informatice. Activitatea de audit poate fi desfășurată fie din afara rețelei (în special din internet sau din rețeaua interconectată a unei terțe părți), fie din interiorul rețelei, și reprezintă o activitate care trebuie efectuată în complementaritate cu alte activități de audit pentru a le îmbunătăți eficacitatea sau pentru a demonstra fezabilitatea exploatării vulnerabilităților descoperite.
   e) **Auditul securității organizației [AS5].** Constă în auditul organizației cu privire la securitatea logică și fizică și urmărește să se asigure că politicile și procedurile de securitate definite de operatorul economic (operatorul de servicii esențiale sau furnizorul de servicii digitale):

- ✓ sunt conforme cu nevoile de securitate ale operatorului economic auditat, nivelul tehnologic și standardele în vigoare;
- ✓ completează corect măsurile tehnice implementate;
- ✓ sunt puse efectiv în practică.

De asemenea, auditorul de securitate cibernetică trebuie să se asigure că aspectele fizice ale securității rețelelor și sistemelor informatice sunt acoperite corespunzător. Această activitate trebuie efectuată în complementaritate cu alte activități de audit pentru a le îmbunătăți eficacitatea.

f) **Auditul sistemelor de control industrial [AS6].** Constă în evaluarea nivelului de securitate al unui sistem de control industrial și a dispozitivelor de control asociate. Evaluarea de securitate presupune aplicarea activităților de audit de la lit. a) la lit. e) din prezentul articol.

(2) Activitățile de audit de securitate se împart în:
   a) activități speciale: [AS3] și [AS4].
   b) activități comune: [AS1], [AS2] și [AS5] .
   c) activități mixte: [AS6].

(3) Activitățile mixte cuprind activitățile speciale și normale/comune. În acest context, activitatea de audit a sistemelor de control industrial presupune desfășurarea tuturor activităților, respectiv speciale și comune.

(4) Corespondența între activitățile de audit și evaluarea cerințelor minime de securitate poate fi consultată în Anexa nr. 14.

(5) Pentru fiecare activitate de audit, auditorul de securitate cibernetică furnizează un raport de audit cuprinzând recomandări.

CAPITOLUL II. ATESTAREA AUDITORILOR DE SECURITATE CIBERNETICĂ

Art. 6. Noțiuni generale privind atestarea

(1) Atestarea auditorilor de securitate cibernetică se realizează de către Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO, în calitate de autoritate competentă la nivel național, în conformitate cu prevederile prezentului regulament.

(2) O persoană fizică sau juridică poate solicita atestarea ca auditor de securitate cibernetică pentru următoarele variante de atestare:
   a) **atestare tip general**: pentru toate activitățile de audit, speciale și comune, respectiv cele precizate la art. 5 alin. (1) lit. a), b), c), d) și e);
   b) **atestare tip special**: numai pentru activitățile de audit speciale, respectiv cele precizate la art. 5 alin. (1) lit. c) și d);
   c) **atestare tip comun**: numai pentru activitățile de audit comune, respectiv cele precizate la art. 5 alin. (1) lit. a), b) și e).

(3) În situația precizată la alin. (2) lit. a) din prezentul articol, auditorul de securitate cibernetică poate desfășura toate activitățile de audit, inclusiv auditul sistemelor de control industrial [AS6].

(4) În situațiile precizate la alin. (2) lit. b) și c), auditorul de securitate cibernetică poate desfășura numai activitățile de audit pentru care a fost atestat și parțial activitatea de audit a sistemelor de control industrial [AS6], respectiv activități de audit speciale sau activități de audit comune.

(5) Un auditor de securitate cibernetică poate deține și alte atestate/autorizări, inclusiv de audit, și care nu fac obiectul prezentului regulament.

Secțiunea 1. Eliberarea atestatului de auditor de securitate cibernetică

Art. 7. Documente necesare pentru atestare

(1) Atestatul de auditor de securitate cibernetică se obține în baza cererii pentru emiterea atestatului de auditor de securitate cibernetică și a dosarului pentru emiterea atestatului de auditor de securitate cibernetică. Modelele de cerere pentru persoane fizice sau juridice sunt prevăzute în Anexa nr. 2.

(2) Dosarul pentru emiterea atestatului de auditor de securitate cibernetică pentru o persoană fizică trebuie să cuprindă următoarele documente:
   a) actul de identitate, în copie;

b) adeverința medicală din care să rezulte starea de sănătate fizică și psihică a solicitantului pentru exercitarea atribuțiilor de auditor de securitate cibernetică;
c) certificatul de cazier judiciar, aflate în termenul de valabilitate;
d) curriculum vitae – model europass, cu detalierea secțiunii ”experiență profesională” ce va conține justificarea privind experiența în domeniu, în conformitate cu art. 25 alin. (2), prin detalii/descrieri și anexarea de înscrisuri etc., respectiv cele care prezintă dovada a cel puțin:
   i. doi ani de experiență în domeniul administrării sau implementării rețelelor și sistemelor informatice; sau
   ii. doi ani de experiență în domeniul securității rețelelor și sistemelor informatice; sau
   iii. un an de experiență în domeniul investigațiilor, testării sau al auditului de securitate a tehnologiei informației și comunicațiilor sau a rețelelor și sistemelor informatice ori a sistemelor de control industrial.
e) certificări, în copii – în funcție de tipul de atestat solicitat:
   i. **atestare tip general** – cel puțin două dintre certificările profesionale menționate în Anexa nr. 5 (dintre care cel puțin una din activitățile de audit comune și cel puțin una dintre activitățile de audit speciale) în perioadă de valabilitate;
   ii. **atestare tip special** – cel puțin una dintre certificările profesionale pentru activitățile de audit speciale menționate în Anexa nr. 5 în perioadă de valabilitate;
   iii. **atestare tip comun** – cel puțin una dintre certificările profesionale pentru activitățile de audit comune menționate în Anexa nr. 5 în perioadă de valabilitate; sau
   iv. certificat evaluare expertiză privind securitatea cibernetică eliberat de către CERT-RO, conform art. 25 alin. (3) și (4).
f) certificatul de specializare de auditor de securitate cibernetică valabil, eliberat de un formator sau furnizor de servicii de formare autorizat de către autoritatea competentă la nivel național, conform art. 32 din Legea NIS;
g) taxa de evaluare și procesare (PF) în vederea atestării ca auditor de securitate cibernetică.

(3) Dosarul pentru emiterea atestatului de auditor de securitate cibernetică pentru o persoană juridică trebuie să cuprindă următoarele documente:
a) documentul de înființare/înregistrare al persoanei juridice, respectiv certificat de înregistrare în registrele naționale, după caz, Registrul comerțului, Registrul asociațiilor și fundațiilor, Registrul federațiilor etc.;
b) certificat constatator emis de instituția care gestionează registrul în care se ține evidența înființării persoanei juridice, cu starea la zi a persoanei juridice, nu mai vechi de 30 de zile, în original sau în copie semnată și cu mențiunea „conform cu originalul“;
c) documentele de la alin. (2) pentru fiecare auditor de securitate cibernetică persoană fizică;
d) taxa de evaluare și procesare (PJ) în vederea atestării ca auditor de securitate cibernetică.

(4) Dosarul pentru emiterea atestatului de auditor de securitate cibernetică se depune împreună cu cererea de emitere a atestatului de auditor de securitate cibernetică la CERT-RO, autoritatea competentă la nivel național, în strada Italiană nr. 22, cod poștal 020976, sector 2, București, România, sau se transmite prin poștă, cu scrisoare cu valoare declarată și confirmare de primire, sau prin email în format electronic la **nis@cert.ro**.

(5) Documentația va fi în limba română, paginată și însoțită de un opis.

(6) Autoritatea competentă la nivel național va confirma primirea documentelor/înscrisurilor.

(7) Orice modificare ulterioară a documentelor prevăzute la alin. (1) și (2) va fi transmisă la autoritatea competentă la nivel național în termen de maximum 15 de zile de la data producerea acesteia, folosind unul dintre modurile stabilite la alin. (4).

Art. 8. Inițierea procedurii de evaluare și atestare a auditorului

(1) După confirmarea primirii documentației, autoritatea competentă la nivel național procedează la inițierea procedurii de evaluare și atestare a auditorului de securitate cibernetică.

(2) Procedura de evaluare și atestare presupune parcurgerea a cinci etape procedurale, respectiv: evaluarea documentației solicitantului (EEDS); evaluarea riscurilor de securitate cu privire la solicitant (EERS);

evaluarea expertizei solicitantului (EEES); evidența auditorului de securitate cibernetică (EEAS); finalizarea procedurii de atestare (EFPA).

(3) În cazul în care autoritatea competentă la nivel național constată că pentru finalizarea procedurii de evaluare și atestare sunt necesare înscrisuri suplimentare și/sau expertize ori constată că anumite documente depuse nu îndeplinesc condițiile legale de fond sau de formă ori că lipsesc anumite documente doveditoare sau nu au fost achitate taxele legale, solicită noi informații/ documente și acordă un termen de până la 30 zile pentru furnizarea acestora.

(4) Neprezentarea completărilor în termenul precizat la alin. (3), conduce la întreruperea procedurii de evaluare și atestare, restituirea dosarului și informarea solicitantului cu privire la refuzul eliberării atestatului de auditor de securitate cibernetică.

(5) Procedura de evaluare și atestare, respectiv luarea în evidență a auditorului de securitate cibernetică sau refuzul privind înscrierea, se finalizează la nivelul autorității competente la nivel național, în termen de maximum 60 de zile de la primirea documentației complete de la solicitant.

Art. 9. Evaluarea documentației solicitantului (EEDS)

(1) Autoritatea competentă la nivel național constituie mapa auditorului de securitate cibernetică, evaluează documentele transmise de către solicitant, solicită date, informații sau înscrisuri suplimentare, dacă e cazul, și în funcție de situație dispune continuarea sau întreruperea procedurii de evaluare și atestare.

(2) Mapa auditorului de securitate cibernetică care cuprinde cererea solicitantului, dosarul pentru emiterea atestatului de auditor de securitate cibernetică, alte informații/înscrisuri suplimentare, dacă e cazul, și informații cu privire la etapele procedurale aplicate se păstrează la autoritatea competentă la nivel național, în format electronic și/sau pe suport hârtie.

(3) Autoritatea competentă la nivel național colaborează cu instituții și autorități din domeniul/sectorul învățământ, sănătate și aplicării legii în vederea evaluării înscrisurilor trimise de către solicitant.

Art. 10. Evaluarea riscului de securitate cu privire la solicitant (EERS)

(1) Întrucât rețelele și sistemele informatice care susțin serviciile esențiale sau furnizează servicii digitale fac parte din domenii cheie pentru securitatea națională, având în vedere că securitatea cibernetică este componentă a securității naționale și ținând cont de faptul că activitatea de audit de securitate presupune acces la informații critice pentru furnizarea serviciilor esențiale/digitale (de exemplu: date cu caracter sensibil sau confidențiale; date/informații ce pot fi utilizate pentru derularea de atacuri cibernetice de natură să afecteze semnificativ funcționarea serviciilor esențiale/digitale la nivel național; vulnerabilități identificate etc.), evaluarea riscurilor de securitate cu privire la solicitant inclusiv din perspectiva securității naționale este o etapă importantă în cadrul procedurii de evaluare și atestare.

(2) Autoritatea competentă la nivel național cooperează cu instituțiile din COSC și solicită efectuarea de verificări a riscurilor de securitate inclusiv din perspectiva securității naționale cu privire la solicitantul de atestat de auditor de securitate cibernetică.

(3) În urma informațiilor/datelor primite, autoritatea competentă la nivel național evaluează riscurile de securitate și în funcție de situație dispune continuarea sau întreruperea procedurii de evaluare și atestare.

Art. 11. Evaluarea expertizei solicitantului (EEES)

(1) Autoritatea competentă la nivel național analizează/evaluează valabilitatea certificărilor profesionale sau a rezultatelor obținute în etapa de examinare a expertizei solicitantului în conformitate cu documentele precizate la art. 7 alin. (2) lit. g).

(2) Autoritatea competentă la nivel național cooperează cu instituțiile din COSC, mediul academic și centre de formare și furnizare de servicii de formare pentru auditorii de securitate cibernetică în vederea evaluării expertizei solicitantului.

(3) În urma evaluării expertizei solicitantului și a rezultatelor obținute, autoritatea competentă la nivel național dispune continuarea sau întreruperea procedurii de evaluare și atestare.

Art. 12. Evidența auditorului de securitate cibernetică (EEAS)

(1) Autoritatea competentă la nivel național întocmește raportul final de evaluare prin care se propune emiterea atestatului de auditor de securitate cibernetică sau restituirea dosarului.

(2) În baza raportului final de evaluare, autoritatea competentă la nivel național emite atestatul de auditor de securitate cibernetică, ia în evidență auditorul de securitate cibernetică și actualizează lista auditorilor de securitate cibernetică.
(3) Lista auditorilor de securitate cibernetică se publică pe site-ul instituției pe pagina autorității.
(4) Evidența auditorilor de securitate cibernetică se ține de către autoritatea competentă la nivel național, în format electronic, pe baza registrului național al auditorilor de securitate cibernetică.

Art. 13. Finalizarea procedurii de atestare (EFPA)

(1) Autoritatea competentă la nivel național transmite solicitantului atestatul de auditor de securitate cibernetică.
(2) Autoritatea competentă la nivel național actualizează bazele de date specifice și trece la monitorizarea respectării aplicării Legii NIS de către auditorul de securitate cibernetică.
(3) În termen de 10 zile de la primirea atestatului de auditor de securitate cibernetică, persoana fizică sau juridică, va efectua plata taxei de auditor de securitate cibernetică, la sediul CERT-RO, autoritatea competentă la nivel național, din strada Italiană, nr. 22, sector 2, CP 020976, București sau în contul instituției.
(4) Neachitarea taxei duce la revocarea atestatului și radierea auditorului de securitate cibernetică din evidențele autorității competente la nivel național.
(5) Dosarele solicitanților care nu se încadrează în prevederile prezentului regulament, precum și dosarele incomplete ale solicitanților care nu au fost completate în termenul stabilit la art. 8 alin. (3) se restituie acestora, fiind însoțite de o adresă de informare cu privire la restituire. Taxa de evaluare și procesare în vederea atestării ca auditor de securitate cibernetică nu se restituie.

Secțiunea 2. Revocarea atestatului de auditor de securitate cibernetică

Art. 14. Revocarea atestatului

(1) CERT-RO, în calitate de autoritate competentă la nivel național, dispune revocarea atestatului de auditor de securitate cibernetică în următoarele situații:
   a) încălcarea normelor privind incompatibilitatea specificate la art. 17 alin. (1);
   b) nerespectarea în auditul de securitate a standardelor și specificațiilor europene și internaționale;
   c) nerespectarea în întocmirea tematicilor de audit de securitate a normelor tehnice în vigoare privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice ale operatorilor de servicii esențiale și ale furnizorilor de servicii digitale;
   d) nerespectarea condițiilor aplicabile activității de audit de securitate a rețelelor și sistemelor informatice stabilite în capitolul IV secțiunea 3;
   e) neachitarea taxelor de auditor de securitate cibernetică sau de reînnoire atestat;
   f) neachitarea amenzilor contravenționale stabilite de personalul de control din cadrul autorității competente la nivel național în urma controalelor impuse de sesizările primite, din oficiu sau în urma autosesizării ori încălcării de către auditorul de securitate cibernetică a obligațiilor ce îi revin în temeiul Legii NIS;
   g) nerespectarea cerințelor impuse auditorilor de securitate cibernetică stabilite în capitolul III secțiunea 2;
   h) încălcarea Codului etic al auditorului de securitate cibernetică;
   i) după a 31 zi de la primirea atestatului și nesemnării/netransmiterii declarației/angajament privind respectarea Codului etic al auditorului de securitate cibernetică;
   j) suspendarea de trei ori consecutiv a atestatului de auditor de securitate cibernetică în timpul unei perioade de valabilitate a acestuia;
   k) comiterea de infracțiuni în domeniul securității cibernetice.
(2) La cererea expresă a auditorului de securitate cibernetică privind renunțarea la atestat, autoritatea competentă la nivel național dispune revocarea atestatului și radierea auditorului de securitate cibernetică din registrul național. Modelele de cerere, persoană fizică sau juridică, sunt prezentate în Anexa nr. 3.
(3) Urmare a revocării atestatului de auditor de securitate cibernetică, autoritatea competentă la nivel național informează persoana în cauză, radiază auditorul de securitate cibernetică din evidențele autorității, respectiv Registrul național al auditorilor de securitate cibernetică și actualizează lista auditorilor de securitate cibernetică de pe site-ul instituției.

Secțiunea 3. Reînnoirea atestatului de auditor

Art. 15. Reînnoirea atestatului

(1) Cu 60 de zile înainte de expirarea termenului de valabilitate a atestatului, auditorul de securitate cibernetică va solicita CERT-RO, autoritatea competentă la nivel național, reînnoirea atestatului prin completarea și transmiterea unei cereri privind reînnoirea atestatului de auditor de securitate cibernetică însoțită de dosarul pentru reînnoirea atestatului de auditor de securitate cibernetică. Modelele de cerere, persoană fizică sau juridică, sunt prezentate în Anexa nr. 4.

(2) Dosarul pentru reînnoirea atestatului de auditor de securitate cibernetică pentru o persoană fizică va cuprinde următoarele documente:
   a) documentele stabilite la art. 7 alin. (2) lit. a), b), c), f) și g), actualizate la zi;
   b) acte doveditoare privind participarea la activități de pregătire și perfecționare;
   c) taxa de evaluare și procesare (PF) în vederea reînnoirii atestatului de auditor de securitate cibernetică;
   d) lista auditurilor de securitate desfășurate pe perioada de valabilitate a atestatului, conform modelului prezentat în Anexa nr. 12.

(3) Dosarul pentru reînnoirea atestatului de auditor de securitate cibernetică pentru o persoană juridică va cuprinde următoarele documente:
   a) documentele stabilite la art. 7 alin. (3) lit. a) și b), actualizate la zi;
   b) documentele stabilite la alin. (2) lit. a) și b), pentru fiecare auditor de securitate cibernetică persoană fizică;
   c) taxa de evaluare și procesare (PJ) în vederea reînnoirii atestatului de auditor de securitate cibernetică;
   d) lista auditurilor de securitate desfășurate pe perioada de valabilitate a atestatului, conform modelului prezentat în Anexa nr. 12.

(4) În procedura de evaluare și reînnoire a atestatului de securitate cibernetică, autoritatea competentă la nivel național aplică prevederile de la capitolul II secțiunea 1 de la art. 8 la art. 13.

(5) În termen de 10 zile de la primirea atestatului de auditor de securitate cibernetică, persoana fizică sau juridică, va efectua plata taxei de auditor de securitate cibernetică, la sediul CERT-RO, autoritatea competentă la nivel național, din strada Italiană, nr. 22, sector 2, CP 020976, București sau în contul instituției.

(6) Neachitarea taxei duce la revocarea atestatului și radierea auditorului de securitate din registrul național al auditorilor de securitate cibernetică.

Secțiunea 4. Suspendarea atestatului de auditor de securitate cibernetică

Art. 16. Suspendarea atestatului

(1) Autoritatea competentă la nivel național poate dispune suspendarea atestatului de auditor de securitate cibernetică, pentru o perioadă stabilită de autoritate, în următoarele situații:
   a) în cazul descoperirii de către autoritatea competentă la nivel național a nerespectării de către un auditor de securitate cibernetică a unei obligații prevăzute de Legea NIS sau prezentul regulament sau de un act emis de autoritatea competentă la nivel național în baza Legii NIS – până la remedierea deficiențelor constatate și conformare cu Legea NIS;
   b) în cazul procedurii de reînnoire a atestatului pentru nerespectarea termenului stabilit la art. 8 alin. (3) – de la a 31 zi de la data efectuării modificării și până la îndeplinirea cerinței stabilite, dar nu mai mult de 60 zile;
   c) în cazul nerespectării termenului stabilit la art. 20 alin. (2) – din a 11 zi de la primirea atestatului și până la transmiterea angajamentului semnat la autoritatea națională, dar nu mai mult de 30 zile.

(2) În cazul suspendării atestatului de auditor de securitate cibernetică, persoana fizică sau juridică căreia i s-a suspendat atestarea nu va mai putea desfășura activități de audit în condițiile Legii NIS și nici să semneze rapoarte de audit de securitate până la remedierea neregulilor și intrarea în legalitate.

Secțiunea 5. Registrul național al auditorilor de securitate cibernetică

Art. 17. Constituirea, întreținerea și actualizarea registrului

(1) CERT-RO constituie, la nivelul autorității competente la nivel național, Registrul național al auditorilor de securitate cibernetică, care este întreținut și actualizat în permanență.

(2) Registrul se constituie în format electronic pe variantele de atestare prezentate la art. 6 alin. (2) și cuprinde date și informații cu privire la auditorii de securitate cibernetică supuși procesului de atestare, revocare sau suspendare a atestatului de securitate cibernetică.

(3) Pentru informarea operatorilor de servicii esențiale, furnizorilor de servicii digitale și autorităților de reglementare și administrare a sectoarelor și subsectoarelor, în baza Registrului național al auditorilor de securitate cibernetică, autoritatea competentă la nivel național elaborează, actualizează în permanență și publică pe site-ul instituției lista auditorilor de securitate cibernetică.

(4) Eliberarea, revocarea și reînnoirea atestatelor de auditor de securitate cibernetică se consemnează de către autoritatea competentă la nivel național în evidențele/bazele de date proprii.

CAPITOLUL III. CONDIȚII ȘI CERINȚE PENTRU AUDITORII DE SECURITATE CIBERNETICĂ

Secțiunea 1. Norme generale

Art. 18. Norme privind activitatea auditorilor

(1) Constituie incompatibilități următoarele activități desfășurate de către un auditor de securitate cibernetică:
   a) efectuarea auditului de securitate la un operator de servicii esențiale sau furnizor de servicii digitale pentru care auditorul atestat asigură în mod curent servicii de management, de securitate cibernetică ori de tip SOC / CSIRT sau la care este angajat printr-o altă relație contractuală ce nu este de tip audit;
   b) efectuarea auditului de securitate pentru rețelele și sistemele informatice pentru care auditorul atestat are contract de prestări servicii la momentul la care se efectuează auditul sau într-un termen mai mic de un an;
   c) efectuarea auditului de securitate, ca și cerință minimă de securitate în condițiile Legii NIS (cel puțin odată la doi ani), la un operator de servicii esențiale sau furnizor de servicii digitale de trei ori consecutiv;
   d) efectuarea auditului de securitate la un operator de servicii esențiale sau furnizor de servicii digitale în care deține o participare la capitalul social al acestuia.

(2) Auditul de securitate se realizează numai de auditori de securitate cibernetică, atestați de CERT-RO, în calitate de autoritate competentă la nivel național, potrivit standardelor și specificațiilor europene și internaționale aplicabile în domeniu, în baza unor tematici de audit stabilite în conformitate cu normele tehnice în vigoare privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale, respectiv furnizorilor de servicii digitale și după încheierea unui contract de audit.

(3) Auditul de securitate realizat în conformitate cu prevederile de la alin. (2) este un audit de securitate care se poate realiza și la solicitarea autorității competente la nivel național, și reprezintă un audit de securitate în condițiile Legii NIS.

(4) Pentru desfășurarea auditului de securitate, auditorii de securitate cibernetică se pot organiza și pot funcționa și în echipe de audit de securitate.

(5) În cazul efectuării auditului de securitate la un operator de servicii esențiale sau furnizor de servicii digitale de către un auditor care nu deține atestat sau care are atestatul suspendat/revocat, auditul este considerat ca fiind efectuat în afara condițiilor Legii NIS, iar raportul de audit de securitate nu este acceptat de către autoritate competentă la nivel național.

Secțiunea 2. Cerințe pentru auditorii de securitate cibernetică

Art. 19. Cerințe generale

(1) Pe timpul auditului de securitate, un auditor de securitate cibernetică poate desfășura una sau mai multe activități de audit menționate la art. 5 alin. (1).

(2) În desfășurarea unei activități de audit de securitate, auditorul de securitate cibernetică trebuie să:
   a) respecte legile și reglementările în vigoare pe teritoriul național;
   b) descrie și să organizeze activitatea cu operatorul economic supus auditului de securitate;
   c) își asume responsabilitatea pentru activitățile de audit de securitate pe care le desfășoară și, în special, orice daune cauzate entității auditate;

d) după caz, încheie o asigurare profesională care să acopere daunele cauzate operatorului economic, atât infrastructurii, cât și informațiilor procesate, ca parte a auditului de securitate efectuat;
e) se asigure că informațiile pe care le furnizează, inclusiv publicitatea, nu sunt false sau înșelătoare;
f) efectueze serviciul în mod imparțial, cu bună credință și cu respect pentru operatorul economic, personalul și rețelele și sistemele informatice ale acestuia;
g) dețină licențe valide pentru instrumentele (software sau hardware) utilizate pentru efectuarea activităților de audit de securitate;
h) solicite/ceară operatorului economic să îl informeze cu privire la orice cerințe legale și de reglementare specifice la care este supus și, în special, la cele legate de sectorul său de activitate;
i) informeze operatorul economic atunci când aceasta din urmă este obligat să raporteze un incident de securitate către CERT-RO și trebuie să îl susțină în acest proces, dacă aceasta din urmă solicită acest lucru;
j) realizeze auditul de securitate pe baza unui contract de furnizare servicii de audit de securitate.

Art. 20. Codul etic al auditorului de securitate cibernetică

(1) Auditorii de securitate cibernetică sunt obligați să respecte Codul etic al auditorului de securitate cibernetică prezentat în Anexa nr. 13.
(2) După obținerea atestatului de auditor de securitate cibernetică, auditorul de securitate cibernetică va lua act de codul etic și va semna, olograf sau digital, declarația/angajament privind respectarea Codul etic al auditorului de securitate cibernetică prevăzută la art. 10 din Anexa nr. 13 și o va înainta la CERT-RO, autoritate competentă la nivel național, în maximum 10 zile de la emiterea atestatului, folosind unul dintre modurile de transmitere prezentate la art. 7 alin. (4).
(3) Nesemnarea și/sau netransmiterea declarației/angajament duce, după caz, la suspendarea atestatului după a unsprezecea zi de la emiterea atestatului dar nu mai mult de 30 de zile sau la revocarea după cea de a treizeci și una zi de la emiterea atestatului.

Art. 21. Managementul resurselor și abilităților

(1) Pentru realizarea auditului de securitate, auditorul de securitate cibernetică poate să se asocieze cu alți auditori de securitate cibernetică pentru a asigura pe deplin și sub toate aspectele activitățile de audit pentru care se încheie contractul cu operatorul economic. În acest sens, pentru fiecare contract trebuie să se asigure că auditorii de securitate desemnați au calitățile și abilitățile necesare. Fiecare auditor trebuie să dețină un atestat valabil eliberat de autoritate competentă la nivel național pentru activitățile de audit pe care le efectuează.
(2) În vederea îmbunătățirii abilităților și îndeplinirii în bune condiții a activităților de audit, auditorul de securitate cibernetică trebuie să participe, periodic, la activități de pregătire și dezvoltare a capacităților profesionale prin seminarii, prezentări și exerciții tehnice, cursuri de pregătire etc.
(3) Auditorul de securitate cibernetică este responsabil pentru metodele, instrumentele (software sau hardware) și tehnicile utilizate pe timpul auditului de securitate, precum și pentru utilizarea corectă a acestora (precauții pentru utilizare, controlul configurației etc.) în efectuarea activităților de audit. În acest sens, trebuie să:
   - ✓ asigure actualizarea continuă a componentelor tehnice utilizate;
   - ✓ utilizeze componente specifice și relevante pentru fiecare tip de activitate de audit;
   - ✓ dețină licențe valide pentru instrumentele (software/hardware) utilizate pentru efectuarea activităților de audit.

Art. 22. Protecția informațiilor

(1) Auditorul de securitate cibernetică trebuie să protejeze informațiile referitoare la auditul de securitate și, în special, dovezile, constatările și rapoartele.
(2) Auditorul de securitate cibernetică trebuie să ia toate măsurile tehnice și organizatorice în vederea protejării tuturor informațiilor referitoare la activitatea de audit la nivel de procesare restricționată.
(3) Auditorul de securitate cibernetică trebuie să implementeze un Sistem de Management al Securității Informației (SMSI) în vederea protejării tuturor informațiilor privitoare la auditurile de securitate efectuate, indiferent de forma în care sunt prezentate (exemplu: verbal, pe hârtie sau în orice altă formă), inclusiv, dar fără a se limita la date, informații personale, proprietatea intelectuală, parole, informații cu privire la

operatorii economici auditați, personalul, rețelele și sistemele informatice ale acestuia, precum și informațiile care nu sunt încă publice cu privire la activitățile de audit desfășurate etc.

Secțiunea 3. Condiții pentru auditorii de securitate cibernetică

Art. 23. Abilități generale

(1) Auditorul de securitate cibernetică trebuie să cunoască legislația română în vigoare, aplicabilă auditului de securitate cibernetică.
(2) Auditorul de securitate cibernetică trebuie să aibă abilități de scriere, raportare și sinteză și să știe să se exprime oral într-un mod clar și ușor de înțeles, în limba română.
(3) Auditorul de securitate cibernetică trebuie să își îmbunătățească în mod regulat abilitățile, inclusiv prin monitorizarea activă a standardelor profesionale, metodologiilor, tehnicilor și instrumentelor utilizate în timpul activităților de audit desfășurate.

Art. 24. Abilități și cunoștințe specifice auditului de securitate

(1) Auditorul de securitate cibernetică trebuie să stăpânească cele mai bune practici și metodologii de audit în conformitate cu lista standardelor și specificațiilor europene și internaționale.
(2) Auditorul de securitate cibernetică trebuie să presteze activitatea de audit în conformitate cu cerințele stabilite în prezentul regulament.
(3) Auditorul de securitate cibernetică trebuie să aibă abilitățile/competențele cerute de tipurile de activități de audit și de funcțiile îndeplinite pe timpul unei audit de securitate, astfel cum sunt definite în Anexa nr. 6.

Art. 25. Experiență

(1) Auditorul de securitate cibernetică trebuie să dețină expertiză în domeniul auditului de securitate cibernetică, ce va fi certificată prin deținerea unei certificării profesionale conform listei din Anexa nr. 5 sau, alternativ, prin absolvirea unui examen / evaluare a expertizei privind securitatea cibernetică.
(2) Pentru desfășurarea activităților de audit de securitate, auditorul de securitate cibernetică trebuie să aibă experiență în domeniu, respectiv să îndeplinească cel puțin una din cerințele de mai jos:
   a) cel puțin doi ani de experiență în domeniul administrării sau implementării rețelelor și sistemelor informatice;
   b) cel puțin doi ani de experiență în domeniul securității rețelelor și sistemelor informatice;
   c) cel puțin un an de experiență în domeniul investigațiilor, testării sau al auditului de securitate a tehnologiei informației și comunicațiilor sau a rețelelor și sistemelor informatice sau a sistemelor de control industrial.
(3) Examinarea/evaluarea solicitantului de atestat de auditor de securitate cibernetică se realizează la sediul CERT-RO sau în centre de formare și furnizare de servicii de formare pentru auditorii de securitate cibernetică de către o comisie de evaluare desemnată de către CERT-RO, în calitate de autoritate competentă la nivel național.
(4) Modul de organizare și desfășurarea examinării / evaluării expertizei în domeniul auditului de securitate cibernetică se va aproba prin Normele referitoare la autorizarea formatorilor și furnizorilor de servicii de formare pentru auditorii de securitate cibernetică și membrilor echipelor CSIRT.

Art. 26. Angajamente

(1) Auditorul de securitate cibernetică ce va efectua un auditul de securitate trebuie să aibă semnat un contract:
   a) de muncă pe o perioadă nedeterminată valabil cu auditorul de securitate cibernetică persoană juridică contractant, în cazul în care este angajat al persoanei juridice sau
   b) de asociere cu entitatea/entitățile cu care se asociază în vederea efectuării auditului.
(2) Auditorul de securitate cibernetică care efectuează individual un audit de securitate nu se supune regulilor de la alin. (1).

CAPITOLUL IV. CONDIȚII APLICABILE ACTIVITĂȚII DE AUDIT DE SECURITATE

Secțiunea 1. Auditul de securitate

Art. 27. Desfășurarea auditului de securitate

(1) Auditul de securitate este unul dintre mijloacele disponibile oricărui operator economic pentru a testa și asigura nivelul de securitate al rețelelor și sistemelor informatice care stau la baza susținerii serviciilor esențiale sau furnizării de servicii digitale.
(2) Auditul de securitate se va desfășura în baza unui contract încheiat între operatorul economic, respectiv operatorul de servicii esențiale sau furnizorul de servicii digitale, și un auditor de securitate, valabil atestat de autoritate competentă la nivel național.
(3) Operatorul economic nu poate contracta servicii de audit de securitate cu același auditor de securitate cibernetică pentru mai mult de două audituri consecutive.
(4) În contractul de audit sunt cuprinse în mod obligatoriu clauze cu privire la faptul că auditorul de securitate cibernetică respectă cerințele impuse pentru efectuarea auditului de securitate a rețelelor și sistemelor informatice care stau la baza furnizării serviciilor esențiale sau digitale, în conformitate cu prezentul regulament și cu bunele practici în domeniu.
(5) Perioada supusă auditării reprezintă perioada cuprinsă între două audituri de securitate consecutive.
(6) Auditul de securitate se desfășoară cu respectarea standardelor și specificațiilor europene și internaționale aplicabile în domeniu. Prima listă a standardelor și specificațiilor europene și internaționale a fost aprobată prin Decizia CERT-RO nr. 88/2020 și publicată în Monitorul Oficial al României, Partea I.
(7) Tematicile de audit vor ține seama de normele tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile, după caz, operatorilor de servicii esențiale sau furnizorilor de servicii digitale.
(8) Pentru cazurile în care rețelele și sistemele informatice care stau la baza furnizării serviciilor esențiale sau digitale sunt situate în afara țării, auditarea sistemului se va face astfel:
   a) de către auditorul de securitate cibernetică – acesta va audita rețelele și sistemele informatice din străinătate; sau
   b) de către un auditor de securitate cibernetică acreditat de autoritatea competentă din acea țară – în acest caz, auditorul de securitate cibernetică contractant agreează auditarea rețelelor și sistemelor informatice din străinătate și preia responsabilitatea auditării, anexând la raportul final raportul auditorului extern tradus în limba română.
(9) Autoritatea competentă la nivel național, poate verifica derularea procesului de auditare, atât prin participarea la auditul desfășurat de către auditorul de securitate, cât și prin prisma evaluării dosarelor de emitere/reînnoire atestat de audit de securitate cibernetică.

Secțiunea 2. Documente de audit de securitate

Art. 28. Documente relevante pe timpul auditului de securitate

(1) La finalizarea auditului de securitate, auditorul de securitate cibernetică are obligația de a întocmi raportul de audit de securitate, în limba română, care va cuprinde, în anexă, rapoarte specifice pentru fiecare din activitățile de audit așa cum sunt stabilite la art. 5 alin. (1) lit. a) la f).
(2) La întocmirea raportului de audit de securitate, auditorul de securitate cibernetică va avea în vedere respectarea cerințelor și recomandărilor stabilite în Anexa nr. 7.
(3) În termen de maximum 15 zile de la solicitarea scrisă a autorității competente la nivel național, auditorul de securitate cibernetică trebuie să comunice următoarele, fără a se limita la acestea:
   a) orice raport sau document care a fost adus la cunoștința operatorului economic auditat;
   b) motivația de încetare a contractului de audit, dacă aceasta a avut loc înainte de finalizarea auditării.
(4) Auditorul de securitate cibernetică notifică atât operatorul economic auditat, cât și autoritatea competentă la nivel național, prin email (**nis@cert.ro**), în maximum 5 zile de la constatare, orice fapt sau act care, în opinia auditorului:
   a) este de natură să afecteze securitatea și utilizarea în siguranță a rețelelor și sistemelor informatice care furnizează servicii esențiale sau digitale;
   b) poate conduce la o opinie de audit cu rezerve, negativă sau imposibilitatea exprimării acesteia.

Secțiunea 3. Cerințe referitoare la desfășurarea unui audit de securitate

Art. 29. Cerințe generale privind auditul de securitate

(1) Definirea auditului de securitate și descrierea activităților de audit de securitate solicitate se formulează în cererea de oferte.
(2) Cerințe specifice și recomandări cu privire la furnizarea serviciilor de audit de securitate și la desfășurarea auditului, precum și tipurile de audit care urmează a fi efectuate în funcție de sfera auditului sunt prezentate în Anexa nr. 8.
(3) Auditorul de securitate cibernetică solicită și se asigură că operatorul economic îi oferă un mediu de lucru adecvat misiunilor sale.
(4) Auditorul de securitate cibernetică verifică dacă operatorul economic a identificat corect rețelele și sistemele informatice de auditat, precum și inter-dependențele externe ale rețelelor și sistemelor informatice.
(5) Auditorul de securitate cibernetică se asigură că auditul de securitate furnizat este adaptat la context și la obiectivele dorite de operatorul economic. În caz contrar, auditorul de securitate cibernetică informează operatorul economic înainte de furnizarea auditului de securitate.
(6) Furnizarea și desfășurarea unui audit de securitate presupune atingerea următoarelor etape:
   - ✓ Contractul de audit de securitate.
   - ✓ Pregătirea auditului de securitate.
   - ✓ Executarea auditului de securitate.
   - ✓ Finalizarea auditului de securitate.
   - ✓ Închiderea auditului de securitate.

Art. 30. Contractul de audit de securitate

(1) Auditul de securitate a rețelelor și sistemelor informatice se desfășoară de auditorul de securitate cibernetică în baza unui contract de audit de securitate, încheiat cu operatorul economic înaintea începerii auditului.
(2) Contractul de audit de securitate trebuie semnat de reprezentantul legal al operatorului economic și de auditorul de securitate cibernetică contractant.
(3) Termenii serviciului. Contractul de audit:
   a) descrie domeniul de aplicare al auditului, abordarea generală a auditului de securitate a rețelelor și sistemelor informatice, activitățile de audit și termenii auditului (obiective, locuri și criterii ale auditului, etape, livrabile așteptate ca input, condiții prealabile etc.);
   b) specifică dacă serviciul de audit este calificat sau nu;
   c) specifică rezultatele așteptate la finalizarea auditului, ședințele de deschidere și de închidere, publicul țintă, nivelul de confidențialitate și metodele asociate;
   d) descrie mijloacele tehnice (echipamente și instrumente) și organizaționale implementate de auditorul de securitate cibernetică ca parte a auditului;
   e) descrie metodele de comunicare care vor fi utilizate în timpul auditului între auditorul de securitate cibernetică și operatorul economic;
   f) prevede ce mijloace logistice vor fi puse la dispoziția auditorului de securitate cibernetică de către operatorul economic (resurse materiale, umane, tehnice etc.);
   g) definește regulile de proprietate asupra elementelor protejate de proprietatea intelectuală, cum ar fi instrumentele dezvoltate special de auditorul de securitate cibernetică ca parte a auditului, indicatorii de compromis sau raportul de audit;
   h) specifică acțiunile care nu pot fi efectuate asupra rețelelor și sistemelor informatice și/sau informațiilor colectate fără autorizarea expresă a operatorului economic și, eventual, acordul sau prezența personalului operatorului economic, precum și modalitățile asociate (implementare, persoane prezente, durată, interval program, planificări, descrierea datelor sensibile și a acțiunilor autorizate etc.);
   i) definește mijloacele care asigură trasabilitatea între operatorul economic și auditorul de securitate a informațiilor și suporturilor materiale prezentate pentru analiză.
(4) Organizare. Contractul de audit trebuie să:
   a) specifice numele responsabilului de legătură din partea operatorului economic cu auditorul de securitate cibernetică, precum și pentru punerea în legătură a auditorului de securitate cu diferite persoane/furnizori implicați;

b) specifice numele, rolurile, responsabilitățile, precum și drepturile și nevoile de cunoaștere a persoanelor cheie desemnate de auditorul de securitate cibernetică și de operatorul economic;
c) stipuleze că auditorul de securitate cibernetică trebuie, acolo unde este cazul, să colaboreze cu furnizori de servicii terți care lucrează în numele operatorului economic și care au fost desemnați în mod specific de către operatorul economic și să distingă clar responsabilitățile furnizorului de servicii terț. Această cerință trebuie să permită în special auditorului de securitate cibernetică să colaboreze cu un furnizor de servicii de detectare a incidentelor de securitate;
d) stipuleze că auditorul de securitate cibernetică nu implică alți auditori care nu au nicio relație contractuală cu acesta, care nu au semnat Codul etic al auditorului de securitate cibernetică, care nu au un atestat de auditor de securitate cibernetică valabil eliberat de ANSRSI sau care sunt sub efectul unor sancțiuni, respectiv suspendare sau retragere atestat.

(5) Responsabilități. Contractul de audit:
a) stipulează că auditorul de securitate cibernetică va efectua auditul numai după o autorizare formală (scrisă) din partea operatorului economic;
b) stipulează că auditorul de securitate cibernetică informează operatorul economic în cazul încălcării contractului/acordului;
c) stipulează că auditorul de securitate cibernetică se angajează ca acțiunile întreprinse ca parte a auditului de securitate să rămână strict conforme cu obiectivele auditului;
d) stipulează că operatorul economic garantează că are toate drepturile de proprietate și accesul la domeniul de aplicare al auditului (rețele și sisteme informatice, suporturi materiale etc.) sau că a obținut acordul oricărui terț; și în special a furnizorilor sau partenerilor săi de servicii, ale căror rețele și sisteme informatice ar intra în sfera de aplicare;
e) stipulează că operatorul economic și auditorul de securitate cibernetică îndeplinesc toate obligațiile legale și de reglementare necesare desfășurării auditului;
f) stipulează că operatorul economic autorizează temporar auditorul de securitate cibernetică, cu scopul unic de a efectua auditul, să acceseze și să efectueze prelucrarea datelor accesate, indiferent de natura acestor date;
g) stipulează că operatorul economic autorizează temporar auditorul de securitate cibernetică să reproducă, să colecteze și să analizeze, în scopul efectuării auditului, date aparținând rețelelor și sistemelor informatice auditate;
h) definește responsabilitățile și măsurile de precauție obișnuite care trebuie respectate de către toate părțile cu privire la riscurile potențiale asociate auditului, în ceea ce privește confidențialitatea informațiilor colectate și analizate, precum și în ceea ce privește disponibilitatea (de exemplu, refuzul de serviciu în timpul testări de penetrare, scanarea vulnerabilităților privind un sistem informatic sau a unui server) și integritatea rețelelor și sistemelor informatice vizate;
i) stabilește dacă auditorul de securitate cibernetică are nevoie de o asigurare de practică profesională care acoperă daunele cauzate în timpul desfășurării auditului și, dacă este cazul, specifică acoperirea acestora și include certificatul de asigurare.

(6) Confidențialitate. Contractul de audit:
a) prevede regimul de distribuție al raportului de audit (e.g. public, confidențial, etc.);
b) prevede o clauză explicită prin care raportul de audit poate fi transmis către ANSRSI, pe baza autorizației scrise din partea operatorului economic;
c) stipulează că auditorul de securitate cibernetică poate, cu excepția unui refuz formal și scris din partea operatorului economic, să păstreze anumite tipuri de informații legate de audit odată ce acesta a fost finalizat. Auditorul de securitate cibernetică trebuie să identifice aceste tipuri de informații în contract (de exemplu: livrabile, informații, documente etc.);
d) stipulează că auditorul de securitate cibernetică anonimizează și decontextualizează (ștergerea oricăror informații care identifică operatorul economic, orice informații cu caracter personal etc.) toate informațiile pe care operatorul economic le autorizează să le păstreze;
e) stipulează că auditorul de securitate cibernetică distruge toate informațiile referitoare la operatorul economic, cu excepția celor pentru care a primit o autorizație de păstrare / stocare de la operatorul economic;

f) specifică metodele (conținutul, forma, domeniul de aplicare etc.) pentru elaborarea recomandărilor;
g) prevede o procedură pentru obținerea consimțământului personalului operatorului economic auditat și al oricărui partener terț pentru efectuarea auditului de securitate.

(7) Reglementări. Contractul de audit:
a) scris în limba română;
b) stipulează că legea aplicabilă este legea română;
c) prevede cerințele care trebuie îndeplinite de auditorul de securitate cibernetică în contextul unui caz judiciar, civil sau de arbitraj;
d) definește perioada de păstrare a informațiilor legate de audit și, în special, a evenimentelor colectate și a incidentelor de securitate detectate. Dacă este necesar, se poate face o distincție privind perioada de păstrare în funcție de tipurile de informații. Perioada minimă de păstrare este de șase luni, sub rezerva legislației și reglementărilor române actuale.

(8) Subcontractare. Contractul trebuie să specifice că auditorul de securitate cibernetică contractant nu poate subcontracta o parte/sau în întregime activitatea de audit de securitate cibernetică executată în baza acestui regulament și a Legii NIS.

(9) Participare experți. Contractul trebuie să specifice că auditorul de securitate cibernetică contractant poate implica alți experți în activitățile de audit de securitate executate în baza acestui regulament și a Legii NIS, cu condiția ca implicarea experților să nu depășească 10% din volumul total activității de audit executate.

(10) Livrabile. Contractul trebuie să precizeze că toate livrabilele produse de auditorul de securitate cibernetică contractant sunt furnizate / emise în limba română, cu excepția cazului în care operatorul economic auditat solicită utilizarea unei alte limbi. În cazul în care livrabilele produse de auditorul de securitate cibernetică sunt produse atât în română cât și în alte limbi, versiunea în limba română prevalează.

(11) Conformitate. Contractul de audit:
a) Indică faptul că auditul de securitate furnizat este:
- ✓ un serviciu de audit executat în condițiile Legii NIS. În acest caz, auditorul de securitate cibernetică informează operatorul economic despre faptul că atât el, cât și orice subcontractant dețin atestate de auditor de securitate cibernetică valabile eliberate de autoritatea competentă la nivel național;
- ✓ un serviciu de audit executat în afara condițiilor Legii NIS. În acest caz, auditorul de securitate cibernetică trebuie să informeze operatorul economic cu privire la riscurile ce decurg din furnizarea unui astfel de serviciu.

b) Indică faptul că auditorii de securitate cibernetică dețin un atestat de auditor de securitate cibernetică individual pentru fiecare din activitățile de audit pentru care se efectuează misiunea de audit, inclusiv aceste atestate.

Art. 31. Pregătirea auditului de securitate

(1) În cazul în care auditul de securitate este efectuat de doi sau mai mulți auditori se constituie în echipă de audit pentru care trebuie să fie numit / desemnat formal un șef al echipei de audit.

(2) Șeful echipei de audit va constitui și conduce echipa de auditori, ce trebuie să aibă – în ansamblul său – cunoștințele, experiența și abilitățile necesare pentru executarea auditului.

(3) Șeful echipei de audit / auditorul de securitate cibernetică [acolo unde nu există constituită o echipă de audit] trebuie, de la începutul pregătirii auditului, să stabilească contactul cu operatorul economic și propria conducere managerială. Acest contact, formal sau informal, are ca scop în special stabilirea canalelor de comunicare și de luare a deciziilor și specificarea termenilor și condițiilor pentru prestarea misiunii de audit. Șeful echipei de audit/auditorul de securitate cibernetică [acolo unde nu există constituită o echipă de audit] trebuie să obțină, de asemenea, de la operatorul economic lista punctelor de contact necesare pentru efectuarea auditului.

(4) Șeful echipei de audit / auditorul de securitate cibernetică [acolo unde nu există constituită o echipă de audit] se asigură, împreună cu operatorul economic, că reprezentanții legali ai entităților afectate de audit au fost anunțați în prealabil și că și-au dat acordul.

(5) Șeful echipei de audit / auditorul de securitate cibernetică [acolo unde nu există constituită o echipă de audit] elaborează un plan de audit. Planul de audit acoperă în special următoarele puncte: obiectivele, domeniile și criteriile auditului, componenta tehnică și organizatorică a serviciului de audit, datele și locurile în care vor fi desfășurate activitățile de audit și, în special, cele posibile auditate, informații generale despre ședințele de

începere și de închidere a misiunii de audit, auditorii de securitate care alcătuiesc echipa de audit, confidențialitatea datelor colectate și anonimizarea constatărilor și rezultatelor.

(6) Tematica de audit va ține seama de cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale, respectiv furnizorilor de servicii digitale.

(7) Obiectivele, criteriile și programul auditului, precum și activitățile de audit aplicate, trebuie definite între auditorul de securitate cibernetică contractant și operatorul economic, ținând seama de constrângerile de funcționare ale rețelelor și sistemelor informatice. Aceste elemente trebuie incluse în planul de audit.

(8) În funcție de activitatea de audit, echipa de audit/auditorul trebuie să obțină mai întâi toată documentația existentă de la operatorul economic (exemple: politica de securitate, analiza riscurilor, proceduri de securitate etc.), referitoare la rețelele și sistemele informatice auditate în scopul evaluării și revizuirii acesteia.

(9) Auditul de securitate va începe numai după o ședință oficială în timpul căreia șeful echipei de audit / auditorul de securitate cibernetică [acolo unde nu există constituită o echipă de audit] și reprezentanții autorizați ai operatorului economic își confirmă contractul cu privire la toți termenii serviciului de audit furnizat. Această întâlnire poate fi și video on-line sau telefonică, dar trebuie, în acest caz, să facă obiectul unei confirmări scrise.

(10) Înainte de începerea auditului, auditorul de securitate cibernetică trebuie să conștientizeze operatorul economic despre valoarea backup-ului și păstrării datelor, aplicațiilor și sistemelor de operare din rețelele și sistemele informatice auditate.

(11) În prealabil și în cazul specific al testării de penetrare, trebuie semnat un formular de autorizare de către operatorul economic, entitățile auditate și orice terți. În formularul de autorizare vor fi specificate, în special:
- ✓ lista infrastructurilor auditate (adrese IP, nume de domenii etc.);
- ✓ lista adreselor IP din care provin testele;
- ✓ data și orele exclusive ale testelor;
- ✓ durata autorizației.

Art. 32. Executarea auditului de securitate

(1) Șeful echipei de audit / auditorul de securitate cibernetică [acolo unde nu există constituită o echipă de audit] va informa, permanent, operatorul economic despre vulnerabilitățile critice descoperite pe timpul auditului. Șeful echipei de audit / auditorul de securitate cibernetică [acolo unde nu există constituită o echipă de audit] trebuie să raporteze operatorului economic orice element găsit care prezintă un risc imediat și semnificativ și, în măsura posibilului, să propună măsuri pentru eliminarea acestui risc.

(2) Auditul de securitate trebuie efectuat cu respect pentru activitatea, reputația, personalul, precum și pentru rețelele și sistemele informatice ale operatorului economic.

(3) Constatările și observațiile făcute de auditorul de securitate cibernetică trebuie să fie reale / faptice / obiective și să se bazeze pe dovezi, date și informații analizate de auditor în timpul auditului.

(4) Auditorul de securitate cibernetică trebuie să notifice imediat, direct sau prin șeful de echipă [când este constituită echipa de audit], conducerea managerială proprie și operatorul economic, în conformitate cu clauzele de confidențialitate stabilite în contractul de audit, cu privire la concluziile activității de audit.

(5) Orice modificare adusă rețelelor și sistemelor informatice auditate, în timpul auditului, trebuie urmărită, iar la sfârșitul auditului, rețelele și sistemele informatice, în cauză, trebuie să revină într-un stadiu a cărui securitate nu este degradată în comparație cu starea inițială.

(6) Constatările auditului de securitate trebuie să fie bine documentate, iar informațiile primite de către auditor trebuie păstrate pe toată durata misiunii de audit.

(7) Auditorul de securitate cibernetică trebuie să ia toate măsurile de precauție necesare pentru a păstra confidențialitatea documentelor și informațiilor referitoare la operatorul economic.

(8) Operatorul economic va urmări log-urile acțiunilor și rezultatele auditorilor de securitate cu privire la rețelele și sistemele informatice auditate, precum și datele de finalizare a acestora. Aceste log-uri pot fi utilizate pentru a stabili cauzele unui posibil incident tehnic care a avut loc în timpul auditului.

(9) Detalierea cerințelor impuse auditorului de securitate și operatorului economic pe timpul executării auditului de securitate sunt specificate în Anexa nr. 9.

Art. 33. Finalizarea auditului de securitate.

(1) La finalizarea auditului și fără a aștepta finalizarea raportului de audit, șeful echipei de audit / auditorul de securitate cibernetică [acolo unde nu există constituită o echipă de audit] trebuie să informeze operatorul economic cu privire la constatările și concluziile inițiale ale auditului.

(2) Acolo unde este cazul, auditorul de securitate cibernetică prezintă vulnerabilitățile majore și critice care ar necesita o acțiune rapidă și descrie recomandările asociate.

(3) Pentru orice audit de securitate, auditorul de securitate cibernetică trebuie să pregătească un raport formal de audit care va cuprinde fiecare dintre activitățile de audit stabilite la art. 5 alin. (1), în funcție de serviciile de audit contractate și să îl trimită operatorului economic, în format electronic sau hârtie.

(4) Raportul de audit trebuie să conțină în special:
- ✓ o mențiune privind destinatarul raportului de audit și regimul de distribuție al acestui raport (exemplu public, confidențial, clasificat etc.);
- ✓ o mențiune privind standardele profesionale, metodologiei sau cadrului utilizat pentru executarea auditului de securitate cibernetică;
- ✓ un rezumat întocmit într-un limbaj accesibil și persoanelor non-tehnice, care specifică:
  - contextul și domeniul de aplicare al serviciului de audit de securitate furnizat;
  - vulnerabilități critice, tehnice sau organizaționale și măsurile corective propuse;
  - evaluarea nivelului de securitate al rețelelor și sistemelor informatice auditate în comparație cu stadiul tehnicii și ținând cont de domeniul de aplicare al auditului.
- ✓ un tabel rezumat al rezultatelor auditului, care specifică:
  - un rezumat al vulnerabilităților identificate, clasificat în funcție de o scară valorică;
  - rezumatul măsurilor corective propuse, clasificat după nivelul critic și după complexitate sau costul estimat al corecției;
- ✓ la efectuare unei testări de penetrare, o descriere a cursului liniar al testelor de penetrare și a metodologiei utilizate pentru a detecta vulnerabilitățile și, dacă este cazul, a le exploata;
- ✓ o concluzie / opinie generală a auditorului privind securitatea rețelelor și sistemelor informatice auditate, care prezintă rezultatele diferitelor activități de audit desfășurate.

(5) Raportul de audit trebuie adaptat în funcție de activitatea de audit desfășurată de auditorul de securitate cibernetică.

(6) Vulnerabilitățile, de origine tehnică sau organizațională, trebuie clasificate în funcție de impactul lor asupra securității rețelelor și sistemelor informatice și de dificultatea lor de exploatare. Se va utiliza scala stabilită de CERT-RO, în calitate de autoritate competentă la nivel național, în Anexa nr. 10.

(7) Fiecare vulnerabilitate trebuie să fie asociată cu una sau mai multe recomandări adaptate rețelelor și sistemelor informatice ale operatorului economic. Recomandările descriu soluții pentru rezolvarea temporară sau permanentă a vulnerabilității și îmbunătățirea nivelului de securitate.

(8) Raportul de audit poate prezenta, de asemenea, recomandări generale care nu au legătură cu vulnerabilitățile și sunt destinate să consilieze operatorul economic cu privire la acțiunile pe care le poate întreprinde acesta pentru asigurarea unui nivel sporit al securității rețelelor și sistemelor informatice proprii.

(9) Raportul de audit trebuie să menționeze rezervele legate de exhaustivitatea rezultatelor auditului (referitoare la termenele alocate, disponibilitatea informațiilor solicitate, colaborarea operatorului economic etc.) sau relevanța rețelelor și sistemelor informatice auditate.

(10) Raportul de audit trebuie să includă numele și detaliile de contact ale auditorilor, șefului echipei de audit, dacă este cazul, și conducerii manageriale a auditorului de securitate contractat.

(11) Raportul de audit trebuie să precizeze dacă serviciul de audit realizat a fost executat în baza legii NIS și să specifice activitățile de audit asociate.

Art. 34. Închiderea auditului de securitate.

(1) Pentru închiderea auditului și finalizarea contractului de audit, auditorul de securitate cibernetică va organiza, împreună cu operatorul economic, o ședință (fizic sau online) de închidere a auditului de securitate la predarea raportului de audit. În timpul întâlnirii se va prezenta rezumatul raportului de audit, concluziile auditului, recomandările auditorului și se va răspunde întrebărilor ridicate de reprezentanții operatorului

economic. De asemenea, este o oportunitate a auditorului de securitate cibernetică de a explica recomandări complexe și, eventual, de a sugera alte soluții mai ușor de implementat.

(2) Toate datele, înregistrările, informațiile sau documentele referitoare la rețelele și sistemele informatice auditate obținute de auditorul de securitate cibernetică trebuie returnate operatorului economic sau, la cererea acestuia, distruse în conformitate cu contractul de audit. După caz, șeful echipei de audit / auditorul de securitate cibernetică [acolo unde nu există constituită o echipă de audit] întocmește un raport privind distrugerea datelor pe care îl transmite operatorului economic și în care specifică datele distruse și modul în care acestea au fost distruse.

(3) Contractul de audit este considerat finalizat atunci când au fost efectuate toate activitățile planificate și operatorul economic a confirmat în mod formal primirea raportului de audit emis de auditor.

(4) Auditorul de securitate cibernetică poate oferi/propune operatorului economic efectuarea unui audit de validare la o dată ulterioară, pentru a verifica dacă măsurile corective propuse în timpul misiunii de audit au fost implementate corect.

CAPITOLUL V. VERIFICAREA ACTIVITĂȚII AUDITORILOR DE SECURITATE CIBERNETICĂ

Art. 35. Verificarea activității auditorilor de securitate cibernetică

(1) CERT-RO, în calitate de autoritate competentă la nivel național, verifică modul de îndeplinire a activității de către auditorii de securitate cibernetică, în baza planului de control anual, a sesizărilor primite sau a activității de monitorizare a aplicării prevederilor Legii NIS la nivelul României.

(2) În cazul în care, în urma verificărilor, se constată nerespectarea prevederilor prezentului regulament sau a Legii NIS, autoritatea competentă la nivel național poate dispune suspendarea pe o perioadă de timp stabilită în vederea remedierii sau revocarea atestatului de auditor de securitate cibernetică.

(3) CERT-RO, în calitate de autoritate competentă la nivel național, verifică, în urma sesizărilor sau din oficiu, în conformitate cu prevederile art. 35 – 42 din Legea NIS, îndeplinirea de către auditorii de securitate cibernetică a obligațiilor legale ce le revin și dispune, după caz, măsuri de remediere, suspendarea activității pe o perioadă specificată sau revocarea atestatului de auditor de securitate cibernetică.

(4) Anual, în primul trimestru, auditorii de securitate cibernetică vor transmite la CERT-RO, autoritatea competentă la nivel național, în format electronic, la adresa de email **nis@cert.ro** – o situație a auditurilor de securitate desfășurate în anul calendaristic precedent, respectiv numărul, beneficiarii, perioadele, neregulile grave constatate și vulnerabilitățile constatate. Modelul de situație se regăsește în Anexa nr. 11.

CAPITOLUL VI. DISPOZIȚII FINALE

Art. 36. Termene tranzitorii

(1) În procesul de eliberare a atestatului de auditor de securitate cibernetică, lipsa certificatului de specializare auditor de securitate cibernetică, prevăzut la art. 7 alin. (2) lit. f), va fi acceptată până la data publicării listei formatorilor și furnizorilor de servicii de formare pentru auditorii de securitate cibernetică pe site-ul instituției, la secțiunea/ pagina autorității competente la nivel național.

(2) După această dată, auditorul de securitate cibernetică are la dispoziție șase luni pentru finalizarea cursului de specializare auditor și transmiterea la autoritatea competentă la nivel național a copiei certificatului de specializare auditor prin una dintre modalitățile specificate la art. 7 alin. (4).

(3) Dacă după termenul stabilit la art. 35 alin. (2) auditorul de securitate cibernetică nu transmite la autoritatea competentă la nivel național copia certificatului de specializare auditor de securitate cibernetică, atestatul de auditor de securitate cibernetică este revocat de drept, auditorul de securitate cibernetică este radiat din evidențele autorității naționale și lista auditorilor de securitate cibernetică este actualizată.

Art. 37. Anexe

Anexele nr. 1 la 14 fac parte integrantă din prezentul regulament.

ANEXA Nr. 1 la Regulament

CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ – CERT-RO
AUTORITATEA COMPETENTĂ LA NIVEL NAȚIONAL PENTRU SECURITATEA REȚELELOR ȘI SISTEMELOR INFORMATICE

Simplitatea este o complexitate rezolvată

ATESTAT

AUDITOR DE SECURITATE CIBERNETICĂ

(S/N) ..../..... din ...../...../20....

În aplicarea dispozițiilor art. 20 lit. p) din *Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*, cu modificările și completările ulterioare,

în temeiul prevederilor art. 11 din *Regulamentul pentru atestarea și verificarea auditorilor de securitate cibernetică*, aprobat prin Ordinul secretarului general al Guvernului nr. ..... /20...,

în baza *Raportului final de evaluare* nr. ..... din ..../.../20..., întocmit de Autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice,

II SRL / Ion IONESCU

cu sediul/domiciliul în localitatea ....., județul ....., CUI/CNP ....., seria/nr. înregistrare RC / CI ....., este atestat ca:

AUDITOR DE SECURITATE CIBERNETICĂ

Înscris în **Registrul național al auditorilor de securitate cibernetică** / IDASC ..... .

Perioada de valabilitate: ...../...../20.... – ...../..../20.... .

TIP ATEST: ☐ General / ☐ Special / ☐ Comun

Restricții privind desfășurarea activităților de audit speciale: ☐ Nu / ☐ Da

Activități de audit speciale calificate: Audit cod sursă [AS3] ☐ Nu / ☐ Da | Audit de penetrare [AS4] ☐ Nu / ☐ Da

---

DIRECTOR GENERAL, CERT-RO
(Prenume NUME, Semnătura și ștampilă)

DIRECTOR, CERT-RO/ANSRSI
(Prenume NUME, Semnătura)

ROC/120E21

ANEXA Nr. 2 la Regulament

CERERE

pentru emiterea atestatului de auditor de securitate cibernetică

Tip persoană: ☐ [fizică]

A. Date generale (identificare solicitant)

SOLICITANT .....
(nume, prenume)

DOMICILIU

Adresa .....
(strada nr., bl./clădire, et., ap., cod poștal)

Localitatea ..... / Județul/Municipiul ..... / Sectorul .....

DATE DE IDENTIFICARE

CNP ..... / BI/CI ..... Seria ..... /Număr .....

DATE DE CONTACT

Telefon ...../ Fax ...../

Email ...../ Web .....

ADRESĂ CORESPONDENȚĂ[1]

Adresa .....
(strada nr., bl./clădire, et., ap., cod poștal)

Localitatea ..... / Județul/Municipiul ..... / Sectorul .....

B. Solicitare

În temeiul *Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*, solicit:

☐ emiterea atestatului de auditor de securitate cibernetică.
Solicit următorul tip de atest[2]: ☐ General / ☐ Special / ☐ Comun.

C. Acord prelucrare date[3]

Îmi exprim acordul cu privire la prelucrarea datelor cu caracter personal și procesarea electronică a datelor de către ANSRSI în procesul de implementare și monitorizare a Legii NIS. ☐ Da

D. Conformitatea cu originalul a documentelor furnizate

Confirm că toate documentele furnizate, în copie, sunt „conform cu originalul" . ☐ Da / ☐ Nu

Nume și prenume: .....

Data: .....

Semnătura: .....

[1] Se va completa numai dacă diferă de sediu/domiciliu solicitantului (specificat mai sus).
[2] Se va marca cu "X" tipul de atestat solicitat: General – pentru toate activitățile de audit ([AS1] ÷ [AS5]) și implicit [AS6]; Special – numai pentru activitățile speciale ([AS3] și [AS4]) și parțial [AS6]; Comun – pentru activitățile comune ([AS1], [AS2] și [AS5]) și parțial [AS6].
[3] În procesele interne, ANSRSI protejează interesele de securitate și comerciale ale solicitanților/ auditorilor de securitate cibernetică, precum și confidențialitatea informațiilor furnizate de către aceștia.
Informațiile prelucrate în sensul îndeplinirii obligațiilor de la art. 32 din Legea NIS nu fac parte din categoria informațiilor de interes public așa cum acestea sunt reglementate în *Legea nr. 544/2001 privind liberul acces la informațiile de interes public,* cu modificările și completările ulterioare.

CERERE

pentru emiterea atestatului de auditor de securitate cibernetică

Tip persoană: ☐ [juridică]

A. Date generale (identificare solicitant)

SOLICITANT .....
(denumire persoană juridică)

SEDIUL
Adresa .....
(strada nr., bl./clădire, et., ap., cod poștal)

Localitatea ..... / Județul/Municipiul ..... / Sectorul .....

DATE DE IDENTIFICARE
CUI ..... / Nr. înregistrare RN[1].....

DATE DE CONTACT
Telefon ...../ Fax ...../

Email ...../ Web .....

ADRESĂ CORESPONDENȚĂ[2]
Adresa .....
(strada nr., bl./clădire, et., ap., cod poștal)

Localitatea ..... / Județul/Municipiul ..... / Sectorul .....

B. Date privind personalul pentru care se solicită atestarea

#1. Nume/prenume ..... CNP ..... CI (S/N) .....
....
#n. Nume/prenume ..... CNP ..... CI (S/N) .....

C. Solicitare

În temeiul *Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*, solicit:

☐ emiterea atestatului de auditor de securitate cibernetică.

Solicit următorul tip de atest[3]: ☐ General / ☐ Special / ☐ Comun.

Solicitări privind personalul pentru care se solicită atestatul:

#1. ... / tip atestat solicitat: ☐ General / ☐ Special / ☐ Comun;
....
#n. ... / tip atestat solicitat: ☐ General / ☐ Special / ☐ Comun.

D. Acord prelucrare date[4]

Îmi exprim acordul cu privire la prelucrarea datelor cu caracter personal și procesarea electronică a datelor de către ANSRSI în procesul de implementare și monitorizare a Legii NIS. ☐ Da

E. Conformitatea cu originalul a documentelor furnizate

Confirm că toate documentele furnizate, în copie, sunt „conform cu originalul" . ☐ Da / ☐ Nu

Nume și prenume: .....

Data: .....

Semnătura: .....

[1] Registrul comerțului; Registrul asociațiilor și fundațiilor; Registrul federațiilor etc.

[2] Se va completa numai dacă diferă de sediu/domiciliu solicitantului (specificat mai sus).

[3] Se va marca cu "X" tipul de atestat solicitat: General – pentru toate activitățile de audit ([AS1] ÷ [AS5]) și implicit [AS6]; Special – numai pentru activitățile speciale ([AS3] și [AS4]) și parțial [AS6]; Comun – pentru activitățile comune ([AS1], [AS2] și [AS5]) și parțial [AS6].

[4] În procesele interne, ANSRSI protejează interesele de securitate și comerciale ale solicitanților/ auditorilor de securitate cibernetică, precum și confidențialitatea informațiilor furnizate de către aceștia.

Informațiile prelucrate în sensul îndeplinirii obligațiilor de la art. 32 din Legea NIS nu fac parte din categoria informațiilor de interes public așa cum acestea sunt reglementate în *Legea nr. 544/2001 privind liberul acces la informațiile de interes public,* cu modificările și completările ulterioare.

ANEXA Nr. 3 la Regulament

CERERE

pentru renunțarea la atestatul de auditor de securitate cibernetică

Tip persoană: ☐ [fizică]

A. Date generale (identificare auditor)

SOLICITANT

Nume/prenume .....
(nume, prenume)

IDASC[1] .....

ADRESĂ CORESPONDENȚĂ

Adresa .....
(strada nr., bl./clădire, et., ap., cod poștal)

Localitatea ..... / Județul/Municipiul ..... / Sectorul .....

Email .....

B. Solicitare

În temeiul *Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*, solicit:

☐ renunțarea la atestatul de auditor de securitate cibernetică.

Solicit renunțarea la următorul tip de atest[2]: ☐ General / ☐ Special / ☐ Comun.

C. Acord prelucrare date[3]

Îmi exprim acordul cu privire la prelucrarea datelor cu caracter personal și procesarea electronică a datelor de către ANSRSI în procesul de implementare și monitorizare a Legii NIS. ☐ Da

Nume și prenume: .....

Data: .....

Semnătura: .....

[1] IDASC – Codul unic de identificare a auditorului de securitate cibernetică.

[2] Se va marca cu ”X” tipul de atestat solicitat: General – pentru toate activitățile de audit ([AS1] ÷ [AS5]) și implicit [AS6]; Special – numai pentru activitățile speciale ([AS3] și [AS4]) și parțial [AS6]; Comun – pentru activitățile comune ([AS1], [AS2] și [AS5]) și parțial [AS6].

[3] În procesele interne, ANSRSI protejează interesele de securitate și comerciale ale auditorilor de securitate cibernetică, precum și confidențialitatea informațiilor furnizate de către aceștia.

Informațiile prelucrate în sensul îndeplinirii obligațiilor de la art. 32 din Legea NIS nu fac parte din categoria informațiilor de interes public așa cum acestea sunt reglementate în *Legea nr. 544/2001 privind liberul acces la informațiile de interes public,* cu modificările și completările ulterioare.

CERERE

pentru renunțarea la atestatul de auditor de securitate cibernetică

Tip persoană: ☐ [juridică]

A. Date generale (identificare auditor)

SOLICITANT

Denumire .....
(denumire persoană juridică)

IDASC[1] .....

ADRESĂ CORESPONDENȚĂ

Adresa .....
(strada nr., bl./clădire, et., ap., cod poștal)

Localitatea ..... / Județul/Municipiul ..... / Sectorul .....

Email .....

B. Date privind personalul pentru care se solicită renunțarea la atestat (dacă este cazul)

#1. Nume/prenume ..... CNP ..... CI (S/N) ..... IDASC .....

....

#n. Nume/prenume ..... CNP ..... CI (S/N) ..... IDASC .....

C. Solicitare

În temeiul *Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*, solicit:

☐ renunțarea la atestatul de auditor de securitate cibernetică.

Solicit renunțarea la următorul tip de atest[2]: ☐ General / ☐ Special / ☐ Comun.

Solicitări privind personalul pentru care se solicită renunțarea atestat:

#1. ... / tip atestat la care se renunță: ☐ General / ☐ Special / ☐ Comun;

....

#n. ... / tip atestat la care se renunță: ☐ General / ☐ Special / ☐ Comun.

D. Acord prelucrare date[3]

Îmi exprim acordul cu privire la prelucrarea datelor cu caracter personal și procesarea electronică a datelor de către ANSRSI în procesul de implementare și monitorizare a Legii NIS. ☐ Da

Nume și prenume: .....

Data: .....

Semnătura: .....

[1] IDASC – Codul unic de identificare a auditorului de securitate cibernetică.

[2] Se va marca cu ”X” tipul de atestat solicitat: General – pentru toate activitățile de audit ([AS1] ÷ [AS5]) și implicit [AS6]; Special – numai pentru activitățile speciale ([AS3] și [AS4]) și parțial [AS6]; Comun – pentru activitățile comune ([AS1], [AS2] și [AS5]) și parțial [AS6].

[3] În procesele interne, ANSRSI protejează interesele de securitate și comerciale ale auditorilor de securitate cibernetică, precum și confidențialitatea informațiilor furnizate de către aceștia.

Informațiile prelucrate în sensul îndeplinirii obligațiilor de la art. 32 din Legea NIS nu fac parte din categoria informațiilor de interes public așa cum acestea sunt reglementate în *Legea nr. 544/2001 privind liberul acces la informațiile de interes public,* cu modificările și completările ulterioare.

ANEXA Nr. 4 la Regulament

CERERE

pentru reînnoirea atestatului de auditor de securitate cibernetică

Tip persoană: ☐ [fizică]

A. Date generale (identificare auditor)

SOLICITANT

Nume/prenume .....
(nume, prenume)

IDASC[1] .....

ADRESĂ CORESPONDENȚĂ

Adresa .....
(strada nr., bl./clădire, et., ap., cod poștal)

Localitatea ..... / Județul/Municipiul ..... / Sectorul .....

Email .....

B. Solicitare

În temeiul *Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*, solicit:

☐ reînnoirea atestatului de auditor de securitate cibernetică.

Solicit reînnoirea următorului tip de atest[2]: ☐ General / ☐ Special / ☐ Comun.

C. Acord prelucrare date[3]

Îmi exprim acordul cu privire la prelucrarea datelor cu caracter personal și procesarea electronică a datelor de către ANSRSI în procesul de implementare și monitorizare a Legii NIS. ☐ Da

D. Conformitatea cu originalul a documentelor furnizate

Confirm că toate documentele furnizate, în copie, sunt „conform cu originalul" . ☐ Da / ☐ Nu

Nume și prenume: .....

Data: .....

Semnătura: .....

[1] IDASC – Codul unic de identificare a auditorului de securitate cibernetică.

[2] Se va marca cu "X" tipul de atestat solicitat: General – pentru toate activitățile de audit ([AS1] ÷ [AS5]) și implicit [AS6]; Special – numai pentru activitățile speciale ([AS3] și [AS4]) și parțial [AS6]; Comun – pentru activitățile comune ([AS1], [AS2] și [AS5]) și parțial [AS6].

[3] În procesele interne, ANSRSI protejează interesele de securitate și comerciale ale auditorului de securitate cibernetică, precum și confidențialitatea informațiilor furnizate de către aceștia.

Informațiile prelucrate în sensul îndeplinirii obligațiilor de la art. 32 din Legea NIS nu fac parte din categoria informațiilor de interes public așa cum acestea sunt reglementate în *Legea nr. 544/2001 privind liberul acces la informațiile de interes public,* cu modificările și completările ulterioare.

CERERE

pentru reînnoirea atestatului de auditor de securitate cibernetică

Tip persoană: ☐ [juridică]

A. Date generale (identificare entitate solicitantă)

SOLICITANT

Denumire .....
(denumire persoană juridică)

IDASC[1] .....

ADRESĂ CORESPONDENȚĂ

Adresa .....
(strada nr., bl./clădire, et., ap., cod poștal)

Localitatea ..... / Județul/Municipiul ..... / Sectorul .....

Email .....

B. Date privind personalul pentru care se solicită reînnoirea atestatului (dacă este cazul)

#1. Nume/prenume ..... CNP ..... CI (S/N) ..... IDASC .....

....

#n. Nume/prenume ..... CNP ..... CI (S/N) ..... IDASC .....

C. Solicitare

În temeiul *Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*, solicit:

☐ reînnoirea atestatului de auditor de securitate cibernetică.

Solicit reînnoirea următorului tip de atest[2]: ☐ General / ☐ Special / ☐ Comun.

Solicitări privind personalul pentru care se solicită reînnoirea atestatului (dacă este cazul):

#1. ... / tip atestat de reînnoit: ☐ General / ☐ Special / ☐ Comun;

....

#n. ... / tip atestat de reînnoit: ☐ General / ☐ Special / ☐ Comun.

D. Acord prelucrare date[3]

Îmi exprim acordul cu privire la prelucrarea datelor cu caracter personal și procesarea electronică a datelor de către ANSRSI în procesul de implementare și monitorizare a Legii NIS. ☐ Da

E. Conformitatea cu originalul a documentelor furnizate

Confirm că toate documentele furnizate, în copie, sunt „conform cu originalul" . ☐ Da / ☐ Nu

Nume și prenume: .....

Data: .....

Semnătura: .....

[1] IDASC – Codul unic de identificare a auditorului de securitate cibernetică.

[2] Se va marca cu "X" tipul de atestat solicitat: General – pentru toate activitățile de audit ([AS1] ÷ [AS5]) și implicit [AS6]; Special – numai pentru activitățile speciale ([AS3] și [AS4]) și parțial [AS6]; Comun – pentru activitățile comune ([AS1], [AS2] și [AS5]) și parțial [AS6].

[3] În procesele interne, ANSRSI protejează interesele de securitate și comerciale ale auditorului de securitate cibernetică, precum și confidențialitatea informațiilor furnizate de către aceștia.

Informațiile prelucrate în sensul îndeplinirii obligațiilor de la art. 32 din Legea NIS nu fac parte din categoria informațiilor de interes public așa cum acestea sunt reglementate în *Legea nr. 544/2001 privind liberul acces la informațiile de interes public,* cu modificările și completările ulterioare.

ANEXA Nr. 5 la Regulament

LISTA CERTIFICĂRILOR PROFESIONALE[1]

#	Certificare			Activități audit	
				Comune	Speciale
1.	C)PEH	-	Certified Professional Ethical Hacker		x
2.	C)PTC	-	Certified Penetration Testing Consultant		x
3.	C)PTE	-	Certified Penetration Testing Engineer		x
4.	CASP +	-	CompTIA Advanced Security Practitioner	x	
5.	CEH	-	EC-Council Certified Ethical Hacker		x
6.	CEPT	-	IACRB Certified Expert Penetration Tester		x
7.	CGEIT	-	Certified in the Governance of Enterprise IT	x	
8.	CHA	-	Certified Hacker Analyst	x	
9.	CHAT	-	Certified Hacker Analyst Trainer	x	
10.	CISA	-	Certified Information Systems Auditor	x	
11.	CISM	-	Certified Information Security Manager	x	
12.	CISSP	-	Certified Information Systems Security Professional	x	
13.	CMWAPT	-	IACRB Certified Mobile and Web Application Penetration Tester		x
14.	COBIT5	-	COBIT 5 Certification	x	
15.	CPT	-	IACRB Certified Penetration Tester		x
16.	CRISC	-	Certified in Risk and Information Systems Control	x	
17.	CTA	-	OSSTMM Certified Trust Analyst	x	
18.	CySA +	-	CompTIA Cybersecurity Analyst	x	
19.	ECSA	-	EC-Council / Certified Security Analyst	x	
20.	GCIP	-	GIAC Critical Infrastructure Protection	x	
21.	GIAC	-	GSNA Systems and Network Auditors	x	
22.	GIAC	-	GCCC Critical Controls Certification	x	
23.	GICSP	-	GIAC Global Industrial Cyber Security Professional	x	
24.	GPEN	-	GIAC Certified Penetration Tester		x
25.	GRID	-	GIAC Response and Industrial Defense	x	
26.	GWAPT	-	GIAC Web Application		x
27.	GXPN	-	GIAC Exploit Researcher and Advanced Penetration Tester		x
28.	LPT	-	EC-Council / Licensed Penetration Tester		x
29.	OPSA	-	OSSTMM Professional Security Analyst		x
30.	OPSE	-	OSSTMM Professional Security Expert	x	
31.	OPST	-	OSSTMM Professional Security Tester Accredited Certification		x
32.	OSCE	-	Offensive Security Certified Expert		x
33.	OSCP	-	Offensive Security Certified Professional		x
34.	OSWE	-	Offensive Security Web Expert		x
35.	OSWP	-	Offensive Security Wireless Professional		x
36.	OWSE	-	OSSTMM Wireless Security Expert		x
37.	PenTest+	-	CompTIA PenTest+		x

[1] Notă. Lista certificărilor profesionale va fi completată/actualizată, permanent, în baza evaluării realizate de CERT-RO, în calitate de autoritate competentă la nivel național și vor fi publicate pe site-ul instituției la secțiunea ANSRSI.

ANEXA Nr. 6 la Regulament

ABILITĂȚI, APTITUDINI ȘI ACȚIUNI

Specifice auditorilor de securitate cibernetică

I. Abilități

1. Comportament profesional

(1) Auditorul de securitate cibernetică trebuie să posede abilități necesare pentru a-i permite să acționeze în conformitate cu principiile auditului.

(2) Auditorul de securitate cibernetică trebuie să prezinte un comportament profesional adecvat în timpul desfășurării activităților de audit, iar în acest sens trebuie să fie:

a) etic – corect, veridic, sincer, cinstit și discret;

b) rațional – dispus să ia în considerare idei sau puncte de vedere alternative;

c) diplomatic – tacticos în relațiile cu indivizii;

d) observator – observarea activă a mediului fizic și a activităților;

e) perceptiv – conștient și capabil să înțeleagă situațiile;

f) versatil – capabil să se adapteze cu ușurință la diferite situații;

g) tenace – persistent și axat pe atingerea obiectivelor;

h) decisiv – capabil să ajungă la concluzii în timp util pe baza raționamentului și analizei logice;

i) autonom – capabil să acționeze și să funcționeze independent în timp ce interacționează eficient cu ceilalți;

j) ferm – capabil să acționeze responsabil și etic, chiar dacă aceste acțiuni nu pot fi întotdeauna populare și pot duce uneori la dezacord sau confruntare;

k) responsabil – dispus să învețe din situații;

l) sensibil – observator și respectuos față de cultura organizațională a operatorului economic auditat;

m) cooperant – interacționează eficient cu alții, inclusiv cu membrii echipei de audit și personalul operatorului economic auditat.

2. Cunoștințe și abilități

(1) Auditorul de securitate cibernetică trebuie să aibă cunoștințe și abilități în domeniile:

a) <u>Principii, procese și metode de audit.</u>

Cunoștințele și abilitățile din acest domeniu permit auditorului de securitate cibernetică să se asigure că activitățile de audit sunt efectuate într-un mod consecvent și sistematic, iar în acest sens trebuie să:

- ✓ înțeleagă tipurile de riscuri și oportunități asociate activității de audit, precum și principiile abordării auditului bazate pe managementul riscurilor;
- ✓ planifice și organizeze munca eficient;
- ✓ efectueze activitatea de audit în termenele convenite prin contractul de audit;
- ✓ acorde prioritate și să se concentreze pe chestiuni importante;
- ✓ comunice eficient, oral și în scris (fie personal sau prin utilizarea interpreților);
- ✓ colecteze informații prin interviuri eficiente, ascultare, observare și revizuire a informațiilor documentate, inclusiv înregistrări și date;
- ✓ înțeleagă și să ia în considerare opiniile experților tehnici;

- ✓ auditeze un proces de la început până la sfârșit, inclusiv interacțiunile cu alte procese și diferite funcții, după caz;
- ✓ verifice relevanța și acuratețea informațiilor colectate;
- ✓ confirme suficiența și adecvarea dovezilor pentru a susține constatările, concluziile și recomandările pe timpul și după misiunea de audit;
- ✓ evalueze factorii care pot afecta fiabilitatea constatărilor, recomandărilor și concluziilor auditului;
- ✓ documenteze activitățile de audit, constatările pe timpul misiunii de audit și raportul de audit;
- ✓ păstreze confidențialitatea și securitatea informațiilor.

b) Standarde și specificații.

Cunoștințele și abilitățile din acest domeniu permit auditorului de securitate cibernetică să înțeleagă sfera auditului de securitate, să aplice criteriile de audit și să acopere următoarele:

- ✓ standardele sistemului de management sau alte documente normative sau de orientare / susținere utilizate pentru stabilirea criteriilor sau metodelor de audit;
- ✓ standardele și specificațiile europene și internaționale utilizate în implementarea cerințelor minime de securitate și în activitatea auditorilor de securitate.
- ✓ aplicarea standardelor și specificațiile europene și internaționale de către operatorul economic, respectiv operatorul de servicii esențiale sau furnizorul de servicii digitale;
- ✓ relațiile și interacțiunile la nivelul rețelelor și sistemelor informatice care stau la baza furnizării serviciilor esențiale sau digitale;
- ✓ înțelegerea importanței și priorității multiplelor standarde sau referințe;
- ✓ aplicarea standardelor sau referințelor la diferite situații de audit.

c) Organizația și contextul acesteia.

Cunoștințele și abilitățile din acest domeniu permit auditorului de securitate cibernetică să înțeleagă structura, scopul și practicile de management ale operatorului economic și, în acest sens, trebuie să acopere următoarele:

- ✓ nevoile și așteptările părților interesate relevante care au impact asupra sistemului de management;
- ✓ tipul de organizație, guvernanța, dimensiunea, structura, funcțiile și relațiile operatorului economic;
- ✓ concepte generale de afaceri și management, procese și terminologii conexe (inclusiv planificarea, bugetarea și gestionarea resurselor umane) care stau la baza furnizării serviciilor esențiale/digitale;
- ✓ aspectele culturale și sociale ale operatorului economic.

d) Legalitate și reglementare aplicabile.

Cunoștințele și abilitățile din acest domeniu permit auditorului de securitate cibernetică să fie conștient de cerințele organizației și modul de organizare a activităților de lucru în cadrul acesteia. Cunoștințele și abilitățile specifice jurisdicției sau activităților, proceselor, produselor și serviciilor auditate trebuie să acopere următoarele:

- ✓ cerințele statutare, de reglementare și guvernanța acestora;
- ✓ terminologia juridică de bază;
- ✓ contracte și răspunderi.

II. Aptitudini și acțiunii specifice rolurilor echipei de audit

1. ȘEFUL ECHIPEI DE AUDIT[1]

1.1. Acțiuni/sarcini

1.1.1. Acțiuni:

- ✓ Constituirea și structurarea echipei de audit adaptată obiectivelor serviciului de audit furnizat în baza unui contract de audit.
- ✓ Gestionarea misiunii de audit, prin/inclusiv:

[1] Rolul de șef echipă de audit de securitate este preluat de auditorul de securitate cibernetică [acolo unde nu există o echipă de audit, dar auditorul de securitate cibernetică este atestat pentru toate activitățile de audit conform art. 6 alin.(2) lit.a) din Regulament].

- identificarea, stabilirea și gestionarea priorităților pentru fiecare membru al echipei de audit;
- utilizarea eficientă a resurselor;
- gestionarea incertitudinii de atingere a obiectivelor auditului;
- protejarea sănătății și siguranței membrilor echipei de audit în timpul misiunii de audit, inclusiv asigurarea conformității auditorilor cu dispozițiile relevante privind sănătatea și securitatea în muncă;
- coordonarea și controlul membrilor echipei de audit;
- prevenirea și rezolvarea conflictelor și problemelor care pot apărea în timpul auditului, inclusiv a celor din cadrul echipei de audit, după caz;
- dezvoltarea și menținerea unei relații de colaborare între membrii echipei de audit.

✓ Sprijinirea operatorului economic în evaluarea impactului asupra rețelelor și sistemelor informatice a amenințărilor care ar putea exploata potențialele vulnerabilități descoperite în timpul serviciului de audit furnizat, în special în ceea ce privește confidențialitatea, integritatea și disponibilitatea serviciului esențial sau digital furnizat de către OE.;

✓ Formularea de recomandări adecvate pentru remedierea riscurilor care decurg din vulnerabilitățile descoperite.

✓ Controlul calității produselor și livrabilelor destinate informării operatorului economic, inclusiv pregătirea și completarea raportului de audit de securitate.

1.2. Aptitudini

1.2.1. Competențe.

✓ Aprofundate în majoritatea domeniilor necesare auditorilor pe care îi supraveghează.

1.2.2. Calități.

✓ Gestionarea unei echipe de auditori de securitate cibernetică.

✓ Managementul priorităților.

✓ Sintetizarea și prezentarea informațiilor utile pentru personalul tehnic și non-tehnic.

✓ Scrierea unei documentații adaptate unor niveluri diferite de interlocutori (structuri tehnice, organisme de conducere, management instituțional etc.).

1.3. Abilități necesare pentru auditul sistemelor de control industrial

1.3.1. Competențe.

✓ Arhitecturi funcționale bazate pe automate de comandă și reglare programabile, respectiv sisteme de control industrial (ICS), sisteme pentru monitorizare, control și achiziție de date (SCADA) și sisteme de control distribuite (DCS); controlere logice programabile (PLC).

✓ Rețele industriale și protocoale:

- topologia rețelelor industriale;
- partiționarea rețelelor industriale față de alte rețele și sisteme informatice;
- protocoale de transmisie și comunicație utilizate de controlere logice programabile și echipamente industriale (Modbus, S7, EtherNetIP, Profibus, Profinet, IEC 61850, OPC – clasic și UA – etc.);
- tehnologii radio și wireless din mediul industrial (inclusiv protocoale bazate pe stratul 802.15.4, respectiv Modelul OSI: nivelul 1 – Fizic și nivelul 2 – Legături de date).

✓ Funcționalitatea diferitelor echipamente din sistemele de control industrial.

2. Auditorul pentru AUDITUL ARHITECTURII

2.1. Acțiuni/sarcini

2.1.1. Acțiuni:

✓ Adoptarea unei viziuni globale a rețelelor și sistemelor informatice pentru a identifica:

- vulnerabilitățile și orice cale de atac asociată;
- elementele/componentele relevante care urmează a fi auditate.

- ✓ Identificarea și colectarea elementelor de arhitectură și echipamentelor de rețea care urmează să fie auditate.
- ✓ Auditarea configurației echipamentelor de rețea alese anterior.
- ✓ Dezvoltarea de instrumente adaptate țintelor auditului, dacă este cazul.
- ✓ Realizarea de interviuri cu administratorii de rețea.
- ✓ Identificarea vulnerabilităților prezente în arhitectură și în configurația echipamentului auditat.
- ✓ Formularea de recomandări adecvate pentru remedierea riscurilor care decurg din vulnerabilitățile descoperite.
- ✓ Valorificarea cunoștințelor dobândite, oferirea de feedback și răspunsuri către OE, precum și elaborarea și prezentarea unui raport de audit.

2.2. Aptitudini

2.2.1. Competențe.

- ✓ Rețele și protocoale:
  - ➢ protocoale și infrastructuri de rețea;
  - ➢ servicii de infrastructură;
  - ➢ configurarea și securizarea principalelor echipamente de rețea de pe piață;
  - ➢ rețele de telecomunicații;
  - ➢ tehnologie wireless;
  - ➢ telefonie.
- ✓ Echipamente și software de securitate:
  - ➢ firewall (”ziduri de protecție”);
  - ➢ sisteme de backup (”rezervă”);
  - ➢ sisteme de stocare partajate;
  - ➢ dispozitive de criptare a comunicațiilor;
  - ➢ servere de autentificare;
  - ➢ servere proxy inversate;
  - ➢ soluții de gestionare a exploatării/utilizării rețelelor și sistemelor informatice;
  - ➢ sisteme/soluții de detecție și prevenirea intruziunilor.

2.2.2. Calități.

- ✓ Sintetizarea și prezentarea informațiilor utile pentru personalul tehnic și non-tehnic.
- ✓ Scrierea unei documentații adaptate unor niveluri diferite de interlocutori (structuri tehnice, organisme de conducere, management instituțional etc.).
- ✓ Lucrul în echipă (schimb de cunoștințe, colaborare tehnică și ajutor reciproc).

2.3. Abilități necesare pentru auditul sistemelor de control industrial

2.3.1. Competențe.

- ✓ Arhitecturi funcționale bazate pe automate de comandă și reglare programabile, respectiv sisteme de control industrial (ICS), sisteme pentru monitorizare, control și achiziție de date (SCADA) și sisteme de control distribuite (DCS); controlere logice programabile (PLC).
- ✓ Rețele industriale și protocoale:
  - ➢ topologia rețelelor industriale;
  - ➢ partiționarea rețelelor industriale față de alte rețele și sisteme informatice;
  - ➢ protocoale de transmisie și comunicație utilizate de controlere logice programabile și echipamente industriale (Modbus, S7, EtherNetIP, Profibus, Profinet, IEC 61850, OPC – clasic și UA – etc.);
  - ➢ tehnologii radio și wireless din mediul industrial (inclusiv protocoale bazate pe stratul 802.15.4, respectiv Modelul OSI: nivelul 1 – Fizic și nivelul 2 – Legături de date).
- ✓ Funcționalitatea diferitelor echipamente din sistemele de control industrial.

3. Auditorul pentru AUDITUL DE CONFIGURARE

3.1. Acțiuni/sarcini

3.1.1. Acțiuni:

- ✓ Adoptarea unei viziuni globale a rețelelor și sistemelor informatice pentru a:
  - ➢ înțelege rolul infrastructurii care urmează să fie auditată,
  - ➢ identifica elementele/componentele relevante care urmează să fie auditate.
- ✓ Identificarea și colectarea elementelor de configurare ale echipamentelor de rețea care urmează să fie auditate.
- ✓ Auditarea configurației echipamentelor de rețea alese anterior.
- ✓ Dezvoltarea de instrumente adaptate țintelor auditului, dacă este cazul.
- ✓ Realizarea de interviuri cu administratorii de sistem și/sau de aplicații.
- ✓ Identificarea vulnerabilităților prezente în configurația elementelor auditate.
- ✓ Formularea de recomandări adecvate pentru remedierea riscurilor care decurg din vulnerabilitățile descoperite.
- ✓ Valorificarea cunoștințelor dobândite, oferirea de feedback și răspunsuri către OE, precum și elaborarea și prezentarea unui raport de audit.

3.2. Aptitudini

3.2.1. Competențe.

- ✓ Rețele și protocoale:
  - ➢ protocoale și infrastructuri de rețea;
  - ➢ servicii de infrastructură;
  - ➢ configurarea și securizarea principalelor echipamente de rețea de pe piață;
  - ➢ rețele de telecomunicații;
  - ➢ tehnologie wireless;
  - ➢ telefonie.
- ✓ Echipamente și software de securitate:
  - ➢ firewall (”ziduri de protecție”);
  - ➢ sisteme de backup (”rezervă”);
  - ➢ sisteme de stocare partajat;
  - ➢ dispozitive de criptare a comunicațiilor;
  - ➢ servere de autentificare;
  - ➢ servere proxy inversate;
  - ➢ soluții de gestionare a exploatării/utilizării rețelelor și sistemelor informatice;
  - ➢ sisteme/soluții de detecție și prevenirea intruziunilor;
  - ➢ software/soluții de securitate client/server etc.
- ✓ Sisteme de operare (mediu și avansat):
  - ➢ sisteme Microsoft;
  - ➢ sisteme UNIX / Linux;
  - ➢ sisteme centralizate (de exemplu, bazate pe OS/400 sau z/OS);
  - ➢ soluții de virtualizare.
- ✓ Aplicații (Model OSI: nivelul 7 – Aplicație):
  - ➢ aplicații de tip client / server;
  - ➢ limbaje de programare utilizate pentru configurare (de ex. scripturi, filtre WMI etc.);
  - ➢ mecanisme criptografice;
  - ➢ baze de date și aplicații:
    - servere web;
    - servere de aplicații;
    - sisteme de gestionare a bazelor de date;
    - pachete software.
- ✓ Tehnici de intruziune.

3.2.2. Calități.

- ✓ Sintetizarea și prezentarea informațiilor utile pentru personalul tehnic și non-tehnic.
- ✓ Scrierea unei documentații adaptate unor niveluri diferite de interlocutori (structuri tehnice, organisme de conducere, management instituțional etc.).
- ✓ Lucrul în echipă (schimb de cunoștințe, colaborare tehnică și ajutor reciproc).

3.3. Abilități necesare pentru auditul sistemelor de control industrial

3.3.1. Competențe.

- ✓ Rețele industriale și protocoale:
  - ➢ protocoale de transmisie și comunicație utilizate de controlere logice programabile și echipamente industriale (Modbus, S7, EtherNetIP, Profibus, Profinet, IEC 61850, OPC – clasic și UA – etc.);
  - ➢ tehnologii radio și wireless din mediul industrial (inclusiv protocoale bazate pe stratul 802.15.4, respectiv Modelul OSI: nivelul 1 – Fizic și nivelul 2 – Legături de date).
- ✓ Echipamente:
  - ➢ configurarea și securizarea principalelor controlere logice programabile (PLC) și echipamente de control industriale de pe piață.

4. Auditorul pentru AUDITUL CODULUI SURSĂ

4.1. Acțiuni/sarcini

4.1.1. Acțiuni:

- ✓ Adoptarea unei viziuni globale a rețelelor și sistemelor informatice pentru a înțelege rolul aplicației care urmează a fi auditată.
- ✓ Identificarea în cadrul aplicației a elementelor relevante care urmează a fi auditate în cadrul codului sursă.
- ✓ Auditarea codului sursă.
- ✓ Dezvoltarea de instrumente adaptate țintelor auditului, dacă este cazul.
- ✓ Realizarea de interviuri cu dezvoltatorii de aplicații.
- ✓ Utilizarea de tehnici de inginerie inversă, dacă e cazul.
- ✓ Identificarea vulnerabilităților prezente în codul sursă auditat.
- ✓ Formularea de recomandări adecvate pentru remedierea riscurilor care decurg din vulnerabilitățile descoperite.
- ✓ Valorificarea cunoștințelor dobândite, oferirea de feedback și răspunsuri către OE, precum și elaborarea și prezentarea unui raport de audit.

4.2. Aptitudini

4.2.1. Competențe.

- ✓ Aplicații (Model OSI: nivelul 7 – Aplicație):
  - ➢ ghiduri și principii de dezvoltare a securității/siguranței aplicației;
  - ➢ arhitecturi de aplicații (client / server, multi-nivel (”n-tier”) etc.);
  - ➢ limbaje de programare;
  - ➢ mecanisme criptografice;
  - ➢ mecanisme de comunicare (interne sistemului și prin rețea) și protocoale asociate;
  - ➢ baze de date/aplicații:
    - servere web;
    - servere de aplicații;
    - sisteme de gestionare a bazelor de date;
    - pachete software.
- ✓ Atacuri cibernetice:
  - ➢ principiile și metodele de intruziune în aplicații;
  - ➢ eludarea măsurilor de securitate software;
  - ➢ exploatarea vulnerabilităților și eliminarea tehnicilor de privilegii.

4.2.2. Calități.

- ✓ Sintetizarea și prezentarea informațiilor utile pentru personalul tehnic și non-tehnic.
- ✓ Scrierea unei documentații adaptate unor niveluri diferite de interlocutori (structuri tehnice, organisme de conducere, management instituțional etc.).
- ✓ Lucrul în echipă (schimb de cunoștințe, colaborare tehnică și ajutor reciproc).

4.3. Abilități necesare pentru auditul sistemelor de control industrial

4.3.1. Competențe.

- ✓ Arhitecturi funcționale bazate pe controlere logice programabile (PLC).
- ✓ Arhitecturi de aplicații SCADA (bazate sau nu pe un pachet software).
- ✓ Arhitecturi de aplicații ale programelor de utilizator prezente în controlere programabile industriale.
- ✓ Rețele industriale și protocoale:
  - ➢ protocoale de transmisie și comunicație utilizate de controlere logice programabile și echipamente industriale (Modbus, S7, EtherNetIP, Profibus, Profinet, IEC 61850, OPC – clasic și UA – etc.).

5. Auditorul pentru AUDITUL DE PENETRARE

5.1. Acțiuni/sarcini

5.1.1. Acțiuni:

- ✓ Adoptarea unei viziuni globale a sistemului informațional pentru a identifica:
  - ➢ țintele relevante de atacat (de exemplu, documente comerciale, date sensibile, servere sensibile etc.),
  - ➢ scenariile de atac adecvate.
- ✓ Identificarea în cadrul infrastructurii a elementelor/componentelor care pot fi atacate permițând executarea scenariilor de atac alese.
- ✓ Efectuarea de atacuri relevante asupra infrastructurii țintă.
- ✓ Dezvoltarea de instrumente adaptate țintelor atacate, dacă este necesar.
- ✓ Utilizarea de tehnici de inginerie inversă, după caz.
- ✓ Identificarea vulnerabilităților prezente în orice element al infrastructurii care permite efectuarea atacurilor.
- ✓ Formularea de recomandări adecvate pentru remedierea riscurilor care decurg din vulnerabilitățile descoperite.
- ✓ Valorificarea cunoștințelor dobândite, oferirea de feedback și răspunsuri către OE, precum și elaborarea și prezentarea unui raport de audit.

5.2. Aptitudini

5.2.1. Competențe.

- ✓ Rețele și protocoale:
  - ➢ protocoale și infrastructuri de rețea;
  - ➢ servicii de infrastructură;
  - ➢ configurarea și securizarea principalelor echipamente de rețea de pe piață;
  - ➢ rețele de telecomunicații;
  - ➢ tehnologie wireless;
  - ➢ telefonie.
- ✓ Echipamente și software de securitate:
  - ➢ firewall (”ziduri de protecție”);
  - ➢ sisteme de backup (”rezervă”);
  - ➢ sisteme de stocare partajate;
  - ➢ dispozitive de criptare a comunicațiilor;
  - ➢ servere de autentificare;
  - ➢ servere proxy inversate;

- soluții de gestionare a exploatării/utilizării rețelelor și sistemelor informatice;
- sisteme/soluții de detecție și prevenirea intruziunilor;
- software/soluții de securitate client/server etc.

✓ Sisteme de operare :
- sisteme Microsoft;
- sisteme UNIX / Linux;
- sisteme centralizate (de exemplu, bazate pe OS/400 sau z/OS);
- soluții de virtualizare.

✓ Aplicații (Model OSI: nivelul 7 – Aplicație):
- ghiduri și principii de dezvoltare a securității/siguranței;
- aplicații de tip client / server;
- limbaje de programare pentru auditurile de cod;
- mecanisme criptografice;
- mecanisme de comunicare (interne sistemului și prin rețea) și protocoale asociate;
- baze de date și aplicații:
  - servere web;
  - servere de aplicații;
  - sisteme de gestionare a bazelor de date;
  - pachete software.

✓ Atacuri cibernetice:
- principiile și metodele de intruziune în aplicații;
- eludarea măsurilor de securitate software;
- exploatarea vulnerabilităților și eliminarea tehnicilor de privilegii.

5.2.2. Calități.

✓ Sintetizarea și prezentarea informațiilor utile pentru personalul tehnic și non-tehnic.

✓ Scrierea unei documentații adaptate unor niveluri diferite de interlocutori (structuri tehnice, organisme de conducere, management instituțional etc.).

✓ Lucrul în echipă (schimb de cunoștințe, colaborare tehnică și ajutor reciproc).

5.3. Abilități necesare pentru auditul sistemelor de control industrial

5.3.1. Competențe.

✓ Arhitecturi funcționale bazate pe controlere logice programabile (PLC).

✓ Rețele industriale și protocoale:
- topologia rețelelor industriale;
- partiționarea rețelelor industriale față de alte rețele și sisteme informatice;
- protocoale de transmisie și comunicație utilizate de controlere logice programabile și echipamente industriale (Modbus, S7, EtherNetIP, Profibus, Profinet, IEC 61850, OPC – clasic și UA – etc.);
- tehnologii radio și wireless din lumea industrială (inclusiv protocoale bazate pe stratul 802.15.4, respectiv Modelul OSI: nivelul 1 – Fizic și nivelul 2 – Legături de date).

✓ Echipamente:
- configurarea și securizarea principalelor controlere logice programabile (PLC) și echipamente de control industriale de pe piață.

6. Auditorul pentru AUDITUL SECURITĂȚII ORGANIZAȚIEI

6.1. Acțiuni/sarcini

6.1.1. Acțiuni:

✓ Adoptarea unei viziuni globale a organizației pentru a identifica:
- politicile și procesele relevante care urmează să fie auditate,
- locurile relevante care urmează să fie auditate,
- vulnerabilitățile și orice cale de atac fizică asociată.

✓ Colectarea documentelor asociate proceselor care urmează să fie auditate.

- ✓ Auditarea proceselor și locațiilor alese anterior.
- ✓ Desfășurarea de interviuri cu managerii de proces și responsabilii cu securitate, inclusiv responsabilii NIS.
- ✓ Identificarea vulnerabilităților prezente în procesele și arhitectura fizică a locurilor auditate.
- ✓ Formularea de recomandări adecvate pentru remedierea riscurilor care decurg din vulnerabilitățile descoperite.
- ✓ Valorificarea cunoștințelor dobândite, oferirea de feedback și răspunsuri către OE, precum și elaborarea și prezentarea unui raport de audit.

6.2. Aptitudini

6.2.1. Competențe.

- ✓ Cunoașterea și stăpânirea standardelor tehnice.
- ✓ Cunoașterea și stăpânirea cadrului normativ:
  - ➢ lista standardelor și specificațiilor europene și internaționale (LSSEINIS);
  - ➢ actele de reglementare referitoare la securitatea rețelelor și sistemelor informatice, la activitatea de audit de securitate cibernetică, precum și cele conexe[1].
- ✓ Cunoașterea și stăpânirea domeniilor legate de organizarea securității rețelelor și sistemelor informatice:
  - ➢ analiza riscurilor;
  - ➢ politica de securitate a rețelelor și sistemelor informatice;
  - ➢ lanțuri de responsabilitate pentru asigurarea securității rețelelor și sistemelor informatice;
  - ➢ securitatea resursei umane;
  - ➢ gestionarea funcționării și administrării rețelelor și sistemelor informatice;
  - ➢ control logic al accesului la rețelele și sistemele informatice;
  - ➢ dezvoltarea și întreținerea aplicațiilor informatice;
  - ➢ gestionarea incidentelor de securitate a informației;
  - ➢ gestionarea planului de continuitate a activității organizației;
  - ➢ securitate fizică.
- ✓ Cunoașterea și stăpânirea practicilor legate de audit:
  - ➢ întreținere;
  - ➢ vizită la fața locului;
  - ➢ analiză documentară.

6.2.2. Calități.

- ✓ Sintetizarea și prezentarea informațiilor utile pentru personalul tehnic și non-tehnic.
- ✓ Scrierea unei documentații adaptate unor niveluri diferite de interlocutori (structuri tehnice, organisme de conducere, management instituțional etc.).
- ✓ Lucrul în echipă (schimb de cunoștințe, colaborare tehnică și ajutor reciproc).

6.3. Abilități necesare pentru auditul sistemelor de control industrial

6.3.1. Competențe.

- ✓ Să fie familiarizat cu următoarele subiecte:
  - ➢ standarde de siguranță/securitate funcțională pentru sistemele de control industrial;
  - ➢ arhitecturi funcționale bazate pe controlere logice programabile (PLC);
  - ➢ rolurile și utilizarea protocoalelor industriale;
  - ➢ cunoașterea rolului funcțional al diferitelor echipamente.

[1] În special normele referitoare la protecția datele cu caracter personal, la secretul profesional, la protecția corespondenței, la atacurile asupra intereselor fundamentale ale națiunii, la terorism și atacurile asupra siguranței publice, la proprietatea intelectuală privind utilizarea mijloacelor de criptografie, patrimoniul științific și tehnic național.

ANEXA Nr. 7 la Regulament

CERINȚE ȘI RECOMANDĂRI

privind întocmirea raportului de audit de securitate

I. Cerințe privind conținutul raportului de audit de securitate

#	CERINȚE	OBSERVAȚII
1.	Titlul raportului.	Raport de audit de securitate (RASEC) ....
2.	Beneficiarii/destinatarii raportului, restricții privind conținutul și circulația raportului.	Se vor preciza datele cu privire la contractul de furnizare servicii de audit, destinatarul(ii) RASEC și modul de circulație a acestuia.
3.	Identificarea operatorului economic.	Identificarea operatorului economic (OSE sau FSD) supus misiunii de audit (*denumire/ CUI/ număr înregistrare la Oficiul Național al Registrului Comerțului/ adresă etc.*). Identificarea serviciilor esențiale și digitale furnizate pe baza rețelelor și sistemelor informatice auditate. Includerea afirmației că rețelele și sistemele informatice au fost auditate ca urmare a obligației legale impuse de ”*Legea NIS,* de *Normele tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale, respectiv furnizorilor de servicii digitale* și de *Regulamentul pentru atestarea și verificarea auditorilor de securitate cibernetică pentru auditarea rețelelor și sistemelor informatice aparținând operatorilor de servicii esențiale sau furnizorilor de servicii digitale și pentru stabilirea condițiilor de valabilitate pentru atestatele acordate”*.
4.	Tipul serviciului de audit furnizat/efectuat.	Se va preciza tipul de serviciul de audit efectuat, respectiv **în condițiile Legii NIS** sau **în afara condițiilor Legii NIS**. Așa cum a fost stipulat în contractul de audit, auditorul de securitate cibernetică va insera în paragrafele de început că serviciul de audit furnizat este unul calificat sau nu.
5.	Asumarea responsabilității conducerii operatorului economic.	Se va preciza faptul că managementul operatorului economic (reprezentanții legali) își asumă responsabilitățile cu privire la implementarea recomandărilor stabilite prin auditul efectuat asupra rețelelor și sistemelor informatice și reducerea riscurilor de securitate.
6.	Responsabilitatea auditorilor de securitate cibernetică.	RASEC va include cel puțin afirmațiile că: - *„este responsabilitatea auditorului de securitate cibernetică să exprime o opinie cu privire la conformitatea rețelelor și sistemelor informatice cu prevederile Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale, respectiv furnizorilor de servicii digitale și a prezentului regulament ...*; - *„raportul de audit de securitate a fost elaborat în conformitate cu standardul de audit utilizat, respectiv ..... (menționarea acestuia)*“.
7.	Identificare auditori de securitate cibernetică.	Datele de identificare ale șefului echipei de audit, precum și a membrilor echipei: - Numele, prenumele, telefon, fax, adresa de e-mail și adresa unde își desfășoară activitatea etc.
8.	Semnături.	Semnătura șefului echipei de audit și a auditorilor pentru fiecare activitate de audit de securitate desfășurată
9.	Obiectivele auditului de securitate.	Obiectivele generale și individualizate pe fiecare activitate de audit ([AS1] ÷ [AS6])

#	CERINȚE	OBSERVAȚII
10.	Perioada desfășurării auditului de securitate.	Se va preciza perioada în care s-a realizat auditul.
11.	Data elaborării și prezentării raportului de audit de securitate.	Se va preciza data întocmirii RASEC, precum și data ședinței de închidere și prezentare a acestuia.
12.	Locații de desfășurare a auditul de securitate.	Se vor specifica locațiile, pe fiecare activitate de audit, unde s-a desfășurat misiunea de audit; adresa sediu central/ sucursală/ filială etc.
13.	Descrierea domeniului/sferei de audit.	Identificarea rețelelor și sistemelor informatice utilizate de către operatorul economic pentru furnizarea serviciilor esențiale sau digitale ……. (*menționarea denumirii SE/SD*). Pentru rețelele și sistemele informatice supuse auditului de securitate se vor menționa următoarele: - măsurile organizatorice: politicile aplicabile și procedurile implementate; - un sumar conținând analiza riscurilor aferente furnizării de SE/SD, a posibilelor deficiențe ale rețelelor și sistemelor auditate și a măsurilor de reducere a riscurilor asociate, în baza cerințelor minime de securitate implementate conform prevederilor Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale, respectiv furnizorilor de servicii digitale.
14.	Implementarea planului de măsuri asumat de operatorul economic la ultimul audit de securitate.	Referiri cu privire la implementarea planului de măsuri/ acțiune asumat de operatorul economic rezultat în urma activității de audit de securitate anterioare, dacă este cazul. Se va verifica modul de implementare a măsurilor și respectarea termenelor asumate prin RASEC anterior.
15.	Evaluarea anuală a riscurilor operaționale.	Referiri cu privire la modul de efectuare de către operatorul economic a evaluării anuale a riscurilor operaționale generate de utilizarea rețelelor și sistemelor informatice importante. Se va verifica și opina cu privire la plauzibilitatea metodologiei/ tehnicilor utilizate, precum și asupra măsurilor de control implementate în vederea gestionării riscurilor operaționale identificate.
16.	Testarea de penetrare.	Se vor menționa/prezenta date cu privire la rezultatul obținut în urma efectuării testării de penetrare. Conform raportului de securitate a testării și evaluarea securității rețelelor și sistemelor informatice – auditul de penetrare se consemnează în RASEC următoarele elemente: - nr. de înregistrare/dată raportul privind testarea de penetrare: - perioada în care s-au desfășurat testării de penetrare; - descrierea metodologiei/tehnicilor utilizate; - menționarea rezultatelor obținute în urma testării; - concluziile raportului; - recomandările transmise operatorului economic și răspunsul managementului acestuia.
17.	Opinia auditorului de securitate cibernetică.	Afirmația de conformitate, reflectată prin opinia auditorului de securitate cibernetică, respectiv opinie pozitivă, opinie cu rezerve/calificată, opinie negativă, după caz.
18.	Anexe la raportul de audit de securitate.	Câte o anexă pentru fiecare activitate de audit desfășurată. Alte anexe.

II. Recomandări privind întocmirea raportului de audit de securitate.

1. Sumarul observațiilor.

La elaborarea RASEC, auditorul de securitate cibernetică va avea în vedere, fără a se limita la acestea:

a) descrierea neconformității/constatării;

b) importanța neconformității/constatării;

c) riscurile asociate;

d) probabilitatea ca aceste constatări să aibă un impact semnificativ; recomandările pentru acțiuni corective și răspunsul conducerii operatorului economic supus misiunii de audit pentru fiecare constatare din raport (inclusiv în urma testului de penetrare);

e) planul de acțiune asumat de către operatorul economic auditat, care conține măsurile propuse, termenul de implementare și persoanele responsabile de implementare.

2. Analiza și managementul riscurilor.

În ceea ce privește, analiza internă și riscurile asociate, auditorul de securitate cibernetică va avea în vedere cuprinderea în RASEC, fără a se limita la acestea:

a) descrierea politicii/metodologiei utilizate de către operatorul economic;

b) rezultatele revizuirii riscurilor generate de utilizarea rețelelor și sistemelor informatice;

c) rezultatele evaluării de către auditorul de securitate cibernetică a măsurilor de control implementate în vederea gestionării riscurilor identificate (pentru riscuri semnificative).

3. Furnizarea serviciilor de tehnologia informației și comunicațiilor externalizate pentru rețelele și sistemele informatice auditate.

Serviciile furnizate de terți pentru funcționarea optimă a rețelelor și sistemelor informatice care stau la baza furnizării serviciilor esențiale/digitale, vor fi identificate și prezentate în RASEC, în anexă, de către auditorul de securitate cibernetică.

4. Testarea și evaluarea securității rețelelor și sistemelor informatice.

Raportul va fi redactat în limba română și semnat numai de către un auditor de securitate cibernetică atestat pentru aplicarea activității de auditului speciale.

Raportul trebuie să cuprindă cel puțin următoarele:

a) sumar executiv, în care să fie redată opinia auditorului de securitate a rețelelor și sistemelor informatice referitoare la climatul general de securitate al ecosistemului evaluat;

b) concluzii privind impactul vulnerabilităților identificate asupra serviciilor esențiale/digitale;

c) recomandări generale de îmbunătățire a climatului de securitate a rețelelor și sistemelor informatice;

d) metodologia de testare folosită;

e) tipul fiecărei vulnerabilități identificate;

f) descriere generală a fiecărei vulnerabilități identificate;

g) impactul exploatării cu succes a fiecărei vulnerabilități identificate;

h) recomandări de eliminare/mitigare a fiecărei vulnerabilități identificate;

i) detalii tehnice ale fiecărei vulnerabilități identificate;

j) elemente tehnice specifice care să permită reproducerea fiecărei vulnerabilități identificate.

5. Concluzii ale echipei de audit de securitate/auditorului de securitate cibernetică privind respectarea cerințelor minime de securitate impuse de normele tehnice aplicabile operatorilor de servicii esențiale sau furnizorilor de servicii digitale.

Raportul trebuie să cuprindă cel puțin următoarele:

a) modul de respectarea a cerințelor minime de securitate impuse prin normele tehnice;

b) recomandări privind modul de remediere a neconformităților identificate;

c) termene privind remedierea și modul de raportate/notificare a ANSRSI sau altor autorități, după caz.

ANEXA Nr. 8 la Regulament

RECOMANDĂRI

privind furnizarea/desfășurarea auditului de securitate

I. Furnizarea unui serviciu de audit de securitate

(1) În cazul în care operatorul economic este o instituție publică centrală sau un deținător de infrastructuri cibernetice de interes național, acesta poate solicita sprijinul ANSRSI în procesul de definire/stabilire a specificațiilor care fac obiectul unei cereri de oferte sau al unui contract de audit de securitate.

(2) Operatorul economic trebuie să-și aleagă auditorul de securitate cibernetică atestat valabil din lista auditorilor de securitate cibernetică publicată de ANSRSI pe site-ul instituției pe pagina autorității.

(3) Pentru a beneficia de un serviciu de audit calificat, adică conform cu cerințele prezentului regulament, operatorul economic trebuie să:
- ✓ aleagă un auditor de securitate cibernetică din lista auditorilor de securitate cibernetică și;
- ✓ solicite auditorului de securitate cibernetică să stipuleze în contractul de audit că serviciul de audit furnizat este unul calificat.

Un auditor de securitate cibernetică atestat își păstrează dreptul de a efectua servicii necalificate. Utilizarea unui auditor de securitate cibernetică din lista auditorilor de securitate cibernetică atestați este, prin urmare, o condiție necesară, dar nu suficientă, pentru a beneficia de un serviciu de audit calificat.

(4) Auditorul de securitate cibernetică care furnizează un serviciu de audit de securitate trebuie să utilizeze produse de securitate și servicii de încredere.

(5) Operatorul economic trebuie să solicite auditorului de securitate care va furniza un serviciu de audit de securitate să îi trimită atestatul de securitate valabil eliberat de ANSRSI.

Prin atestat sunt identificate, în special, activitățile de audit pentru care auditorul de securitate cibernetică este atestat și perioada de valabilitate a atestării.

(6) Operatorul economic va solicita auditorului de securitate cibernetică care furnizează un serviciu de audit de securitate să îi trimită atestatele individuale ale fiecărui auditor de securitate cibernetică implicat în desfășurarea auditului de securitate.

(7) Operatorul economic poate, în conformitate cu prezentul regulament și Legea NIS, să depună o reclamație/ sesizare la ANSRSI împotriva unui auditor de securitate cibernetică atestat care furnizează un serviciu de audit de securitate în cazul în care consideră că acesta din urmă nu a respectat una sau mai multe cerințe din prezentul regulament ca parte a unui serviciu de audit calificat.

(8) Dacă, după examinarea reclamației/sesizării, se dovedește că auditor de securitate cibernetică nu a respectat una sau mai multe cerințe din prezentul regulament pe timpul furnizării unui serviciu de audit calificat și, în funcție de gravitate, ANSRSI poate revoca sau suspenda pe o perioadă de timp stabilită atestatul de auditor de securitate cibernetică.

(9) Atestatul unui auditor de securitate cibernetică nu atestă capacitatea acestuia de a accesa sau deține informații clasificate și, prin urmare, nu înlocuiește autorizația de acces la informații clasificate.

II. Recomandări generale privind auditul de securitate

(1) Auditul de securitate trebuie să fie cât mai cuprinzător și să țină seama de constrângerile bugetare și de timp alocate pentru desfășurarea acestuia.

(2) Stabilirea duratei auditului de securitate pentru echipa de audit/auditor trebuie adaptată în funcție de:
- ✓ sfera auditului și complexitatea acestuia;

- ✓ cerințele de securitate așteptate de la rețelele și sistemele informatice auditate.

(3) Pentru a reduce volumul total al elementelor/componentelor rețelelor și sistemelor informatice care urmează să fie auditate și, prin urmare, costul auditului și, în același timp, menținerea domeniului relevant de audit, eșantionarea ar trebui efectuată respectând următoarele principii:

- ✓ pentru auditurile de configurare, sunt auditate doar serverele sensibile: controlere de domeniu Active Directory, servere de fișiere, servere de infrastructură (DNS, SMTP etc.), servere de aplicații etc.
- ✓ pentru auditul codului sursă, sunt auditate doar părțile sensibile ale codului sursă: gestionarea autentificării, gestionarea controalelor de acces ale utilizatorilor, accesul la bazele de date, controlul intrărilor utilizatorilor etc.

(4) Pentru auditul de penetrare este de preferat efectuarea testării de penetrare pe un mediu de testare (sau „pre-producție") pentru a evita consecințele unor eventuale defecțiuni într-un mediu de producție. Cu toate acestea, pentru a asigura relevanța auditului, auditorul de securitate cibernetică trebuie să se asigure că acest mediu este similar cu cel de producției.

Aplicabilitatea rezultatelor auditurilor tehnice în mediul de producție ar trebui verificată. Arhitectura, configurația, codul sursă și auditurile securității organizației ar trebui efectuate în mediul de producție.

(5) Definirea domeniului/sferei de audit trebuie să se bazeze pe o analiză prealabilă a riscurilor „afacerii" operatorului economic auditat. Se recomandă ca operatorul economic să indice auditorului de securitate cibernetică elementele sensibile ale rețelelor și sistemelor informatice (ținte) auditate. Această recomandare este fundamentală în cazul auditului sistemelor de control industrial.

III. Recomandări pe timpul desfășurării auditului de securitate

(1) Operatorul economic va desemna un responsabil pentru gestionarea relației cu auditorul de securitate cibernetică care furnizează serviciul de audit (echipa de audit) și monitorizarea procesului de desfășurare a misiunii de audit (planuri de lucru, autorizații etc.).

(2) Operatorul economic va lua toate măsurile de salvgardare necesare pentru a-și proteja rețelele și sistemele informatice, inclusiv datele/informațiile înainte și în timpul misiunii de audit. Acest proces trebuie să se desfășoare în colaborare cu auditorul de securitate cibernetică pentru a nu interfera cu activitățile de audit, în special specialiștii operatorului economic nu trebuie să submineze integritatea urmelor colectate.

(3) Pentru a evita orice denunțare a furtului sau a încălcării încrederii, operatorul economic va evita să ofere sau să accepte folosirea de către auditorul de securitate cibernetică echipamente non-proprietate pentru utilizarea în scopuri profesionale (BYOD[1]) în absența proprietarului echipamentului sau fără acordul său.

(4) Operatorul economic va informa, pe tot parcursul misiunii de audit, auditorul de securitate cibernetică cu privire la acțiunile pe care le efectuează asupra rețelelor și sistemelor informatice (operațiuni de administrare, garanții etc.) care ar putea afecta furnizarea serviciului de audit.

(5) Operatorul economic va implementa mijloace de comunicare sigure și dedicate pentru toate comunicările legate de audit, intern și cu auditorul de securitate cibernetică.

(6) Auditorul de securitate cibernetică care furnizează serviciul de audit va avea capacitatea de a renunța la sau de a înlocui orice auditor din echipa de audit.

IV. Tipuri de audit recomandate

(1) Autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice recomandă, auditorilor de securitate cibernetică să furnizeze/solicite înscrierea în contractul de audit pentru desfășurarea unui audit de securitate următoarele tipuri de audit:

- ✓ auditul unei aplicații informatice:
  - ➢ audit cod sursă;
  - ➢ audit de configurare (server de aplicații, server HTTP, bază de date etc.).

[1] Bring Your Own Device = Aduceți propriul dispozitiv.

- ✓ auditul unui centru de date:
  - audit arhitectură (legătură între diferitele zone și entități, filtrare etc.);
  - audit de configurare (echipamente de rețea și securitate, servere de infrastructură);
  - audit securitate organizație.
- ✓ auditul unei rețele informatice:
  - audit arhitectură;
  - audit de configurare (stații de lucru de birou, echipamente de rețea, servere de birou, servere AD etc.);
  - audit securitate organizație.
- ✓ auditul unei platforme de telefonie:
  - audit arhitectură;
  - audit de configurare (echipamente de rețea și securitate, IPBX, telefoane etc.).
- ✓ auditul unei platforme de virtualizare:
  - audit arhitectură;
  - audit de configurare (echipamente de rețea și securitate, sisteme de virtualizare etc.).
- ✓ audit unui sistem de control industrial, inclusiv sala de control:
  - audit arhitectură;
  - audit de configurare (controlere logice programabile industriale, senzori / activatori, servere de aplicații, stații operator, stații de inginerie, console de programare, echipamente de rețea și securitate, servere de autentificare etc.);
  - audit securitate organizație;
  - audit cod sursă (controlere logice programabile industriale, console, sisteme încorporate, aplicații de afaceri etc.)

Lista nu este exhaustivă și poate fi completată de auditorii de securitate cibernetică pe timpul furnizării unui serviciu de audit de securitate.

(2) Se recomandă ca pentru fiecare dintre tipurile de audituri descrise mai sus să includă activitatea de audit de penetrare (testarea de penetrare).

(3) Auditul de penetrare (testarea de penetrare) nu trebuie efectuat niciodat singur și fără nicio altă activitate de audit.

(4) Testarea de penetrare nu trebuie efectuată pe platformele de găzduire partajate decât dacă s-a convenit în mod expres de către gazdă și după ce riscurile au fost evaluate și controlate, iar responsabilitățile au fost stabilite în mod clar.

ANEXA Nr. 9 la Regulament

CERINȚELE SPECIFICE
activităților de audit de securitate

Generalități

(1) Pe timpul desfășurării activităților de audit, desfășurate în baza contractului de audit, operatorul economic și auditorii de securitate cibernetică trebuie să respecte cerințele specifice stabilite în această anexă, respectiv de la [CAS1] la [CAS6].

(2) Activitățile tehnice descrise la [CAS1] până la [CAS4] nu exclud evaluarea securității organizației, respectiv securitatea logică și fizică a domeniului auditat. Această evaluare constă în verificarea faptului că politicile și procedurile de securitate definite pentru asigurarea cerințelor minime de securitate a rețelelor și sistemelor informatice auditate sunt conforme cu nivelul tehnicii.

(3) Activitățile tehnice de la [CAS6], auditul sistemelor de control industrial, presupune atingerea cerințelor specifice prin cerințele stabilite la [CAS1] până la [CAS5].

(4) Cerințele enunțate de la [CAS1] la [CAS5] sunt date cu titlu informativ și nu sunt exhaustive. În plus, acestea trebuie efectuate numai atunci când sunt aplicabile rețelelor și sistemelor informatice auditate.

[CAS1]. Cerințe specifice auditului arhitecturii

(1) **Acțiuni ale OE.** Operatorul economic trebuie să furnizeze auditorului de securitate cibernetică elementele de arhitectură și configurare a rețelelor și sistemelor informatice auditate.

(2) **Acțiuni tehnice ale ASI.** Auditorul de securitate cibernetică trebuie să:

- ✓ Revizuiască/auditeze următoarele documente atunci când acestea există:
  - ➢ diagramele arhitecturale de nivel 2 și 3 corespunzătoare Modelului OSI (Interconectarea Sistemelor Deschise / Open Systems Interconnection);
  - ➢ matricea fluxurilor;
  - ➢ regulile de filtrare;
  - ➢ configurarea echipamentelor de rețea (routere și comutatoare);
  - ➢ interconectări cu rețele terțe sau Internet;
  - ➢ analizele de risc ale rețelelor și sistemelor informatice;
  - ➢ documentele de arhitectură tehnică legate de ținta auditului.

(3) **Comunicarea dintre ASI și OE**. Auditorul de securitate cibernetică trebuie să poată organiza interviuri cu personalul implicat în stabilirea și administrarea rețelelor și sistemelor informatice auditate, în special în ceea ce privește procedurile de administrare.

[CAS2]. Cerințe specifice auditului de configurare

(1) **Acțiuni ale OE.** Operatorul economic trebuie să furnizeze auditorului de securitate cibernetică elementele de configurare ale rețelelor și sistemelor informatice auditate. Elementele de configurare pot fi identificate manual sau automat, folosind ”acces privilegiat”, sub formă de fișiere de configurare sau capturi de ecran.

Această acțiune poate fi întreprinsă direct de auditorul de securitate cibernetică după aprobarea operatorului economic supus auditului.

(2) **Acțiuni tehnice ale ASI.** Auditorul de securitate cibernetică trebuie să:

- ✓ Verifice securitatea configurațiilor, în conformitate cu stadiul tehnicii, cerințele minime de asigurare a securității rețelelor și sistemelor informatice și regulile specifice ale OE, respectiv a:
  - ➢ echipamentelor de rețea cu fir sau fără fir (cum ar fi switch-uri sau routere);

- echipamentelor de securitate (tip firewall sau releu invers, filtrare sau nu, și regulile lor de filtrare, criptare etc.);
- sistemelor de operare;
- sistemelor de gestionare a bazelor de date;
- serviciilor de infrastructură;
- serverelor de aplicații;
- stațiilor de lucru;
- echipamentelor de telefonie;
- mediilor de virtualizare.

(3) **Comunicarea dintre ASI și OE.** Auditorul de securitate cibernetică trebuie să poată organiza interviuri cu personalul implicat în stabilirea și administrarea rețelelor și sistemelor informatice auditate, în special în ceea ce privește standardele de configurare.

[CAS3]. Cerințe specifice auditului codului sursă

(1) **Acțiuni ale OE.** Operatorul economic trebuie să furnizeze auditorului de securitate cibernetică: codul sursă, documentația referitoare la implementare, metodele și rapoartele de testare și arhitectura rețelelor și sistemelor informatice auditate, precum și configurația elementelor de compilare și de execuție, în limitele drepturilor operatorului economic.

(2) **Acțiuni tehnice ale ASI.** Auditorul de securitate cibernetică trebuie să:

- ✓ Verifice securitatea părților din codul sursă referitoare la:
  - mecanisme de autentificare;
  - mecanisme criptografice;
  - gestionarea utilizatorilor;
  - controlul accesului la resurse;
  - interacțiuni cu alte aplicații;
  - relații cu sistemele de gestionare a bazelor de date;
  - respectarea cerințelor de securitate referitoare la mediul în care este implementată aplicația.
- ✓ Verifice cele mai frecvente vulnerabilități în următoarele domenii:
  - scripturi între site-uri,
  - injecții SQL,
  - falsificare a cererilor între site-uri,
  - erori logice ale aplicației,
  - depășirea buffer-ului,
  - executarea comenzilor arbitrare,
  - includerea fișierelor (local sau la distanță).
- ✓ Respecte regulile specifice de audit, respectiv trebuie să:
  - efectueze o analiză de securitate a aplicației auditate pentru a limita auditul la părțile critice ale codului său;
  - prevină scurgerile de informații și modificări în funcționarea rețelelor și sistemelor informatice;
  - efectueze activitate manual sau automat folosind instrumente specializate. Fazele automatizate, precum și instrumentele utilizate, trebuie identificate în livrabile și, în special, în raportul de audit.

(3) **Comunicarea dintre ASI și OE.** Auditorul de securitate cibernetică va efectua interviuri cu unul dintre dezvoltatori/programatori sau persoana responsabilă de implementarea codului sursă auditat pentru a avea informații referitoare la contextul aplicației, nevoile de securitate și practicile de dezvoltare.

[CAS4]. Cerințe specifice auditului de penetrare (Testarea de penetrare)

(1) **Acțiuni ale OE.** Operatorul economic trebuie să aprobe activitatea.

(2) **Acțiuni tehnice ale ASI.** Auditorul de securitate cibernetică trebuie să:

- ✓ Efectueze una sau mai multe dintre următoarele faze:

- Faza 1 – ”Black box” (cutie neagră). Auditorul nu are alte informații decât adresele IP și adresele URL asociate țintei auditate. Această fază este în general precedată de descoperirea informațiilor și identificarea țintei prin interogarea serviciilor DNS, scanarea porturilor deschise, descoperirea prezenței echipamentelor de filtrare etc. .
- Faza 2 – ”Gray box” (cutie gri). Auditorul are cunoștință despre un utilizator standard al rețelelor și sistemelor informatice (autentificare legitimă, stație de lucru „standard” etc.). Identificatorii pot aparține diferitelor profiluri de utilizator pentru a testa diferite niveluri de privilegii.
- Faza 3 – ”White box” (cutie albă). Auditorul dispune de cât mai multe informații tehnice (arhitectură, cod sursă, contacte telefonice, identificatori etc.) înainte de a începe analiza. De asemenea, are acces la contacte tehnice legate de rețelele și sistemele informatice țintă.

În cazul în care sunt efectuate mai multe dintre faze, se recomandă păstrarea ordinii de execuție descrisă mai sus.

- ✓ Definească un profil de atacator simulat.
- ✓ Exploateze vulnerabilitățile descoperite numai cu acordul operatorului economic, atunci când știe că rețelele și sistemele informatice auditate vor fi instabile sau chiar va fi provocat un refuz de serviciu.
- ✓ Indice și justifice în raportul de audit absența oricărei încercări de exploatare vulnerabilităților.
- ✓ Comunice ANSRSI vulnerabilitățile non-publice descoperite în timpul auditului.

(3) **Comunicarea dintre ASI și OE.** Auditorul de securitate cibernetică trebuie să aibă un contact permanent cu operatorul economic și să avertizeze/informeze operatorul economic înainte de orice acțiune care ar putea duce la o defecțiune sau chiar la o refuzare a serviciului rețelelor și sistemelor informatice auditate.

[CAS5]. Cerințe specifice auditului securității organizației

(1) **Acțiuni ale OE.** Operatorul economic trebuie să pună la dispoziția auditorului de securitate cibernetică toate documentele și înscrisurile necesare desfășurării activității de audit.

(2) **Acțiuni tehnice ale ASI.** Auditorul de securitate cibernetică trebuie să:
- ✓ Analizeze organizarea securității rețelelor și sistemelor informatice pe baza standardelor tehnice și de reglementare stabilite în LSSEINIS, în conformitate cu cerințele minime de securitate aplicabile operatorilor de servicii esențiale, respectiv furnizorilor de servicii digitale.
- ✓ Respecte regulile specifice de audit, respectiv trebuie să:
  - permită măsurarea conformității rețelelor și sistemelor informatice auditate cu privire la parametrii de referință și identificarea abaterilor care prezintă vulnerabilități majore ale acestora.
  - integreze analiza elementelor legate de securitatea aspectelor fizice ale rețelelor și sistemelor informatice, în special, protecția spațiilor care găzduiesc componente ale rețelelor și sistemelor informatice și a datelor/ informațiilor auditate sau controlul acces la aceste componente.

(3) **Comunicarea dintre ASI și OE.** Auditorul de securitate cibernetică trebuie să aibă un contact permanent cu operatorul economic, să poată avea discuții/ interviuri cu managerii de proces și responsabilii cu securitate, inclusiv responsabilii NIS.

[CAS6]. Cerințe specifice auditului sistemelor de control industrial

(1) **Acțiuni ale OE.** Operatorul economic trebuie să pună la dispoziția auditorului de securitate cibernetică documente și înscrisuri, precum și accesul la elementele/componentele care urmează a fi supuse auditului tehnic.

(2) **Acțiuni tehnice ale ASI.** Auditorul de securitate cibernetică trebuie să desfășoare următoarele activități în cadrul sistemului de control industrial [ISC] și, după caz, al centrului său de control [SCADA]:
- ✓ audit arhitectură;
- ✓ audit de configurare;
- ✓ audit securitate logică și fizică.

(3) **Comunicarea dintre ASI și OE.** Auditorul de securitate cibernetică trebuie să:
- ✓ poată organiza interviuri cu personalul implicat în securitatea sistemului de control industrial, managerul operațional al sistemului și, după caz, administratorii tehnici.

- ✓ să informeze operatorul economic cu privire la riscurile efectuării testărilor de penetrare într-un mediu care cuprinde sisteme de control industrial.

ANEXA Nr. 10 la Regulament

SCALA

impactului vulnerabilităților

(1) În procesul de stabilire a impactului vulnerabilităților, se utiliza o scală de clasificare a vulnerabilităților.

(2) Vulnerabilitățile, de origine tehnică sau organizațională, sunt clasificate în funcție de riscul pe care îl prezintă pentru rețelele și sistemele informatice adică în funcție de impactul vulnerabilității asupra acestora și dificultatea de furnizare a serviciului esențial/digital.

(3) Nivelul de risc asociat cu fiecare vulnerabilitate este evaluat în funcție de următoarea scală de valori:

- ✓ **Scăzut:** risc scăzut pentru rețelele și sistemele informatice –> poate necesita corecție;
- ✓ **Moderat:** risc moderat asupra rețelele și sistemele informatice –> necesită corecție pe termen mediu;
- ✓ **Major:** risc major pentru rețelele și sistemele informatice –> necesită corecție pe termen scurt;
- ✓ **Critic:** risc critic pentru rețelele și sistemele informatice –> necesită corecție imediată sau oprirea imediată a serviciului furnizat.

(4) Ușurința în exploatare a vulnerabilităților printr-un atac corespunde nivelului de expertiză și mijloacelor necesare pentru a efectua atacul cibernetic folosind vulnerabilitățile identificate. Se evaluează pe următoarea scală de exploatare:

- ✓ **Ușor:** operare banală –> nu necesită instrumente speciale;
- ✓ **Redus:** operare simplă –> necesită tehnici simple și instrumente disponibile publicului;
- ✓ **Înalt:** operare abilitată –> necesită abilități în securitatea rețelelor și sistemelor informatice și dezvoltarea instrumentelor simple pentru exploatarea vulnerabilităților publice;
- ✓ **Dificil:** operare expertiză –> necesită expertiză în securitatea rețelelor și sistemelor informatice și dezvoltarea instrumentelor specifice pentru exploatarea vulnerabilităților nepublicate.

(5) Impactul corespunde consecințelor pe care exploatarea vulnerabilității le poate avea asupra rețelelor și sistemelor informatice auditate. Se evaluează conform următoarei scale de impact:

- ✓ **Minim:** nicio consecință directă asupra securității rețelelor și sistemelor informatice;
- ✓ **Mediu:** consecințe izolate asupra anumitor puncte ale rețelelor și sistemelor informatice;
- ✓ **Maxim:** consecințe limitate asupra unei părți a rețelelor și sistemelor informatice;
- ✓ **Critic:** consecințe generalizate asupra întregilor rețele și sisteme informatice.

(6) Tabelul următor indică nivelul de risc inerent fiecărei vulnerabilități descoperite, în funcție de dificultatea lor de exploatare și de impactul presupus:

Ușurința în exploatare / Impact	Dificil	Înalt	Redus	Ușor
Minim	Scăzut	Scăzut	Moderat	Major
Mediu	Scăzut/Moderat[1]	Moderat	Moderat	Major
Maxim	Moderat	Major	Major	Critic
Critic	Moderat	Major	Critic	Critic

[1] În cazul sistemelor de control industrial ale operatorilor de importanță critică națională, pentru un impact Mediu, nivelul riscului este estimat la Moderat, chiar și pentru o ușurință în exploatare estimată la Dificil.

ANEXA Nr. 11 la Regulament

SITUAȚIA

Auditurilor de securitate desfășurate în anul ...

Auditor de securitate cibernetică persoană: ☐ [juridică] / ☐ [fizică]

Auditor de securitate cibernetică: ..... / IDASC: .....

(Numele/prenumele PF / Denumire PJ)

#	Beneficiar	Tip beneficiar	Zile misiune	Taxă audit (mii lei)	Activități de audit		Nereguli grave constatate	Vulnerabilități constatate
1.	ABC Energy	OSE	12	10	Comune	Da/ Nu	a)...	1)... 2)...
					Speciale	Da/ Nu	a)...	1)... 2)...
					Mixte	Da/ Nu	a)...	1)... 2)...
...	...	...		...	...		...	...
Situație centralizatoare								
A.	OSE	n	29	2000	-	-	59	50
B.	FSD	m	5	500	-	-	15	11
C.	TOTAL	(n+m)	34	2500	-	-	74	61

ANEXA Nr. 12 la Regulament

LISTA

Auditurilor de securitate desfășurate pe perioada de valabilitate a atestatului[1]

Auditor de securitate cibernetică persoană: ☐ [juridică] / ☐ [fizică]

Perioada – de la data de: ...../...../20....

la data de: ...../...../20....

Secțiunea 1. Persoană fizică

#1. Auditor de securitate cibernetică: ..... / IDASC: .....
(numele/prenumele)

#	Beneficiar	Anul	Zile audit	Tip contract		Activități de audit		
				Individual	Asociere	Comune	Speciale	Mixte
I.	Operatori de servicii esențiale							
1.	ABC Energy	20...	21		x	x	x	
...	...	...	...	x				x
Subtotal OSE		-	**TZM**	**Z(c1)**	**Z(c2)**	**Z(a1)**	**Z(a2)**	**Z(a3)**
II.	Furnizori de servicii digitale							
1.	XYZ Cloud	20...	15	x		x	x	
...	...	...	...		x	x		
Subtotal FSD		-	**TZM**	**Z(c'1)**	**Z(c'2)**	**Z(a'1)**	**Z(a'2)**	**Z(a'3)**

Secțiunea 2. Persoană juridică[2]

#1. Auditor de securitate cibernetică: ..... / IDASC: .....
(numele/prenumele)

#2. Auditor de securitate cibernetică: ..... / IDASC: .....
(numele/prenumele)

...

#n. Centralizator (PJ): ..... / IDASC: .....
(Denumire PJ)

#	Tip beneficiari	Anul	Zile audit	Tip contract		Activități de audit		
				Individual	Asociere			
I.	Operatori de servicii esențiale	-	TZM	Z(c1)	Z(c2)	Z(a1)	Z(a2)	Z(a3)
II.	Furnizori de servicii digitale	-	TZM	Z(c'1)	Z(c'2)	Z(a'1)	Z(a'2)	Z(a'3)

[1] Perioada de valabilitate a atestatului – perioada cuprinsă între data emiterii atestatului și până la data solicitării reînnoirii atestatului.
[2] Se completează pentru fiecare auditor de securitate persoană fizică – câte un tabel ca și la Secțiunea 1. Persoană fizică – și se centralizează datele pentru fiecare tip de beneficiar, respectiv operatori de servicii esențiale și furnizori de servicii digitale.

ANEXA Nr. 13 la Regulament

CODUL ETIC AL AUDITORULUI DE SECURITATE CIBERNETICĂ

Capitolul I. Introducere

Articolul 1

Codul etic al auditorului de securitate cibernetică reprezintă un ansamblu de principii și reguli de conduită care trebuie să guverneze activitatea auditorului de securitate cibernetică.

Articolul 2

Prevederile Codului etic al auditorului de securitate cibernetică se aplică tuturor auditorilor de securitate cibernetică, atestați de Autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice a atestatului de securitate cibernetică (ANSRSI), care desfășoară activități de audit de securitate a rețelelor și sistemelor informatice care stau la baza furnizării de servicii esențiale și/sau digitale.

Articolul 3

Scopul Codului etic al auditorului de securitate cibernetică este crearea cadrului etic necesar desfășurării activității de auditor de securitate cibernetică, astfel încât acesta să își îndeplinească cu profesionalism, loialitate, corectitudine și în mod imparțial îndatoririle de serviciu și să se abțină de la orice faptă care ar putea să aducă prejudicii instituției – atunci când este angajat la un auditor persoană juridică – și operatorului economic (operator de servicii esențiale sau furnizor de servicii digitale) – atunci când desfășoară activități de audit de securitate.

Articolul 4

În vederea atingerii scopului Codului etic al auditorului de securitate cibernetică, auditorul de securitate cibernetică va îndeplini următoarele obiective:

1) performanța – desfășurarea unei activități de audit de securitate se va realiza la cei mai ridicați parametri, în scopul îndeplinirii cerințelor stabilite în Regulamentul pentru atestarea și verificarea auditorilor de securitate cibernetică (RENASC), în condiții de economicitate, eficacitate și eficiență;

2) profesionalismul – presupune existența unor capacități intelectuale și experiențe dobândite prin pregătire și educație și printr-un cod de valori și conduită comun tuturor auditorilor de securitate cibernetică;

3) calitatea serviciilor – constă în competența auditorului de securitate cibernetică de a-și realiza sarcinile ce i revin cu obiectivitate, responsabilitate, sârguință și onestitate;

4) încrederea – auditorul de securitate cibernetică trebuie să promoveze cooperarea și bunele relații cu ceilalți auditori de securitate cibernetică – când face parte dintr-o echipă de audit. Sprijinul și cooperarea profesională, echilibrul și corectitudinea sunt elemente esențiale ale activității desfășurate de către un de auditor de securitate cibernetică;

5) conduita – auditorul de securitate cibernetică trebuie să aibă o conduită ireproșabilă atât pe plan profesional, cât și personal;

6) corectitudinea – metodele, instrumentele și tehnicile utilizate trebuie să fie valide și actualizate la nivel cu noutățile în domeniu securității cibernetice;

7) credibilitatea – informațiile furnizate de rapoartele, opiniile și recomandările auditorului de securitate cibernetică trebuie să fie fidele realității și de încredere.

Articolul 5

Codul etic al auditorului de securitate cibernetică este structurat în două componente esențiale:

1) principii fundamentale privind practicarea auditului de securitate cibernetică;

2) reguli de conduită care impun normele de comportament pentru auditorul de securitate cibernetică.

Capitolul II. Principii fundamentale

Articolul 6

În desfășurarea activității auditorul de securitate cibernetică este obligat să respecte următoarele principii fundamentale:

A. Integritatea

- ✓ Auditorul de securitate cibernetică trebuie să fie corect, onest și incoruptibil, integritatea fiind suportul încrederii și credibilității acordate raționamentului auditorului de securitate cibernetică.

B. Independența și obiectivitatea

- ✓ Independența. Independența față de operatorul economic (operator de servicii esențiale sau furnizor de servicii digitale) și oricare alte grupuri de interese este indispensabilă. În acest sens, auditorul de securitate cibernetică trebuie să:
  - o depună toate eforturile pentru a fi independent în tratarea problemelor aflate în analiză;
  - o fie independent și imparțial atât în teorie, cât și în practică;
  - o nu fie afectat de interese personale sau exterioare;
  - o nu se implice în acele activități în care au un interes legitim/întemeiat.
- ✓ Obiectivitatea. În activitatea sa auditorul de securitate cibernetică trebuie să:
  - o manifeste obiectivitate și imparțialitate în redactarea rapoartelor, care trebuie să fie precise și obiective;
  - o formuleze concluzii și opinii bazate exclusiv pe documentele obținute și analizate conform listei standardelor și specificațiilor internaționale și europene în domeniu;
  - o folosească toate informațiile utile primite de la operatorul economic auditat și din alte surse;
  - o analizeze punctele de vedere exprimate de operatorul economic auditat și, în funcție de pertinența acestora, să formuleze opiniile și recomandările proprii;
  - o facă o evaluare echilibrată a tuturor circumstanțelor relevante și să nu fie influențat de propriile interese sau de interesele altora în formarea propriei opinii.

C. Confidențialitatea

- ✓ Auditorul de securitate cibernetică este obligat să:
  - o păstreze confidențialitatea în legătură cu faptele, informațiile sau documentele despre care ia cunoștință în exercitarea atribuțiilor lor; este interzis să utilizeze în interes personal sau în beneficiul unui terț informațiile dobândite în exercitarea atribuțiilor de serviciu.
  - o protejeze informațiile referitoare la auditul de securitate și, în special, dovezile, constatările și rapoartele.
- ✓ În cazuri excepționale auditorul de securitate cibernetică poate furniza aceste informații numai în condițiile expres prevăzute de normele legale în vigoare sau cu autorizația scrisă din partea operatorului economic auditat.

D. Competența profesională

- ✓ Auditorul de securitate cibernetică este obligat să își îndeplinească atribuțiile pe timpul activității de audit de securitate cu profesionalism, competență, imparțialitate și la standarde internaționale, aplicând cunoștințele, aptitudinile și experiența dobândite.
- ✓ Auditorul de securitate cibernetică este obligat să respecte legile și reglementările naționale aplicabile, precum și cele mai bune practici legate de activitățile de audit de securitate.

E. Neutralitatea politică

- ✓ Auditorul de securitate cibernetică trebuie să fie neutru din punct de vedere politic, în scopul îndeplinirii în mod imparțial a activităților; în acest sens el trebuie să își mențină independența față de orice influențe politice.
- ✓ Auditorul de securitate cibernetică are obligația ca în exercitarea atribuțiilor ce i revin să se abțină de la exprimarea sau manifestarea convingerilor lui politice.

Capitolul III. Reguli de conduită

Articolul 7

Regulile de conduită sunt norme de comportament pentru auditorul de securitate cibernetică și reprezintă un ajutor pentru interpretarea principiilor și aplicarea lor practică, având rolul să îndrume din punct de vedere etic auditorul de securitate cibernetică.

A. Integritatea

- ✓ exercitarea profesiei cu onestitate, bună-credință și responsabilitate;
- ✓ respectarea legii și acționarea în conformitate cu cerințele activității de audit de securitate;
- ✓ respectarea și contribuția la obiectivele etice legitime ale instituției din care provine;
- ✓ se interzice auditorului de securitate cibernetică să ia parte cu bună știință la activități ilegale și angajamente care discreditează îndeplinirea atribuțiilor de auditor de securitate cibernetică sau instituția din care face parte.

B. Independența și obiectivitatea

- ✓ se interzice implicarea auditorului de securitate cibernetică în activități sau în relații care ar putea să fie în conflict cu interesele instituției supuse activității de audit de securitate și care ar putea afecta o evaluare obiectivă;
- ✓ se interzice auditorului de securitate cibernetică să asigure unui operator economic auditat alte servicii decât cele de audit și consultanță;
- ✓ se interzice auditorului de securitate cibernetică, în timpul activității de audit, să primească din partea operatorului economic auditat avantaje de natură materială sau personală care ar putea să afecteze obiectivitatea evaluării;
- ✓ auditorului de securitate cibernetică este obligat să prezinte în rapoartele lui orice documente sau fapte cunoscute de el, care în caz contrar ar afecta activitatea operatorului economic auditat.

C. Confidențialitatea

- ✓ se interzice folosirea de către auditorului de securitate cibernetică a informațiilor obținute în cursul activității de audit de securitate în scop personal sau într-o manieră care poate fi contrară legii ori în detrimentul obiectivelor legitime și etice ale operatorului economic auditat.

D. Competența:

- ✓ auditorul de securitate cibernetică trebuie să se comporte într-o manieră profesională în toate activitățile pe care le desfășoară, să aplice standarde și norme profesionale și să manifeste imparțialitate în îndeplinirea atribuțiilor cu privire la activitatea de audit de securitate;
- ✓ auditorul de securitate cibernetică trebuie să se angajeze numai în acele activități de audit pentru care au cunoștințele, aptitudinile și experiența necesare;
- ✓ auditorul de securitate cibernetică trebuie să utilizeze metode și practici de cea mai bună calitate în activitățile pe care le realizează; în desfășurarea auditului și în elaborarea rapoartelor auditorul de securitate cibernetică are datoria de a adera la postulatele de bază și la standardele de audit general acceptate;
- ✓ auditorul de securitate cibernetică trebuie să își îmbunătățească în mod continuu cunoștințele, eficiența și calitatea activității lui:

- în cazul persoanelor juridice, acestea trebuie să asigure condițiile necesare pregătirii profesionale a auditorilor de securitate cibernetică, perioada alocată în acest scop fiind de minimum 15 zile lucrătoare pe an;
- în cazul persoanelor fizice, acestea trebuie să desfășoare activități de pregătire profesională de minimum 15 zile lucrătoare pe an;

✓ auditorul de securitate cibernetică trebuie să aibă un nivel corespunzător de studii de specialitate, pregătire și experiență profesionale elocvente;

✓ auditorul de securitate cibernetică trebuie să cunoască legislația de specialitate și să se preocupe în mod continuu de creșterea nivelului de pregătire, conform standardelor internaționale;

✓ se interzice auditorului de securitate cibernetică să își depășească atribuțiile de serviciu.

Capitolul IV. Dispoziții finale

Articolul 8

ANSRSI verifică respectarea prevederilor Codului etic al auditorului de securitate cibernetică de către auditorii de securitate cibernetică, persoane fizice și persoane juridice, și poate iniția măsurile corective necesare, inclusiv revocarea atestatului de auditor de securitate cibernetică.

Articolul 9

În conformitate cu art. 20 alin. (1) din Regulamentul pentru atestarea și verificarea auditorilor de securitate cibernetică, prevederile Codului etic al auditorului de securitate cibernetică sunt obligatorii pentru toți auditorii de securitate cibernetică, persoane fizice și juridice, valabil atestați, care au obligația de a-l lua la cunoștință.

Articolul 10

După obținerea atestatului de auditor de securitate cibernetică, auditorul va semna o declarație/angajament prin care ia act de Codul etic al auditorului de securitate cibernetică și se angajează să respecte prevederile acestuia.

Articolul 11

Nerespectarea Codului etic al auditorului de securitate cibernetică duce la revocarea de către Autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice a atestatului de securitate cibernetică a atestatului de auditor de securitate cibernetică.

Articolul 12

Modelul de declarație/angajament privind respectarea Codului etic al auditorului de securitate cibernetică

DECLARAȚIE/ANGAJAMENT

PRIVIND RESPECTAREA CODULUI ETIC AL AUDITORULUI DE SECURITATE CIBERNETICĂ

Auditor de securitate cibernetică: .....

IDASC: .....

Subsemnatul ..... (nume și prenume), atestat ca auditor de securitate cibernetică având IDASC: ….....,
posesor al actului de identitate seria ..... nr. ....., CNP .....,

Cunoscând dispozițiile art. 326 din Codul penal cu privire la falsul în declarații,

declar pe propria răspundere că am luat cunoștință de Codul etic al auditorului de securitate cibernetică și mă anagajez să-l respect pe întreg parcursul perioadei de valabilitate a atestatului de securitate cibernetică.

Dau prezenta declarație în conformitate cu art. 20 din Regulamentul pentru atestarea și verificarea auditorilor de securitate cibernetică, aprobat prin Ordinul secretarului general al Guvernului nr. .../2021, fiindu-mi necesară la CERT-RO/ANSRSI pentru înscrierea ca auditor de securitate cibernetică în Registrul național al auditorilor de securitate cibernetică.

Semnătura auditorului de securitate cibernetică .....

Numele și prenumele semnatarului .....

Data .....

ANEXA Nr. 14 la Regulament

GRILE CORESPONDENȚĂ

privind evaluarea cerințelor minime de securitate

I. Evaluarea cerințelor minime de securitate pentru operatorii de servicii esențiale

Domenii de securitate	Categorii de activități de securitate	Măsuri de securitate	Activități de audit		
			Comune	Speciale	Mixte
GUVERNANȚĂ	Managementul securității informației	Analizarea și evaluarea riscurilor	x	x	x
		Realizarea planurilor de securitate. Politica de securitate	x	x	x
		Acreditarea de securitate	x	x	x
		Indicatori de securitate	x		x
		Verificarea conformității cu privire la securitatea informației. Audit de securitate	x	x	x
		Testarea și evaluarea securității rețelelor și sistemelor informatice		x	x
		Asigurarea securității personalului	x		x
		Conștientizarea și instruirea utilizatorilor	x		x
		Gestionarea activelor	x		x
	Managementul ecosistemului	Cartografierea ecosistemului	x	x	x
		Relațiile ecosistemului	x		x
PROTECȚIE	Managementul arhitecturii	Managementul configurației rețelelor și sistemelor informatice	x		x
		Managementul suporților de memorie externă	x		x
		Segregarea și segmentarea rețelelor și sistemelor informatice	x		x
		Filtrarea traficului	x		x
		Asigurarea protecției produselor și serviciilor aferente rețelelor și sistemelor informatice	x	x	x
		Protecția împotriva malware	x	x	x
	Managementul administrării	Administrarea conturilor	x		x
		Administrarea rețelelor și sistemelor informatice	x		x
		Managementul accesului de la distanță	x		x
	Managementul identității și accesului	Managementul identificării și autentificării utilizatorilor	x		x
		Managementul drepturilor de acces	x		x
	Managementul mentenanței	Mentenanța rețelelor și sistemelor informatice	x		x
		Sisteme control industrial. SCADA – Monitorizare, Control și Achiziții de Date	x	x	x
	Managementul securității fizice	Asigurarea protecției fizice a rețelelor și sistemelor informatice	x		x
APĂRARE CIBERNETICĂ	Managementul detecției	Managementul vulnerabilităților și alertelor de securitate	x	x	x
		Înregistrarea evenimentelor	x		x
		Jurnalizarea și asigurarea trasabilității activităților în cadrul rețelelor și sistemelor informatice	x		x
	Managementul incidentelor de securitate	Răspuns la incidente de securitate	x		x
		Raport incidente	x		x
		Comunicarea cu Autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice (ACNNISS) și CSIRT Național	x		x

Domenii de securitate	Categorii de activități de securitate	Măsuri de securitate	Activități de audit		
			Comune	Speciale	Mixte
REZILIENȚĂ	Managementul continuității afacerii	Asigurarea disponibilității serviciului esențial și a funcționării rețelelor și sistemelor informatice	x		x
		Managementul recuperării datelor în caz de dezastre	x		x
	Managementul crizelor	Organizarea gestionării crizelor	x		x
		Procesul de gestionare a crizelor	x		x

II. Tipuri de audit recomandate/activități de audit

#	Tipuri de audit recomandate	Activități de audit				
		[AS1]	[AS2]	[AS3]	[AS4]	[AS5]
1.	Auditul unei aplicații informatice		x	x	x	
2.	Auditul unui centru de date	x	x		x	x
3.	Auditul unei rețele informatice	x	x		x	x
4.	Auditul unei platforme de telefonie	x	x		x	
5.	Auditul unei platforme de virtualizare	x	x		x	
6.	Auditul unui sistem de control industrial	x	x	x	x	x

III. Tipuri de atestate de securitate/activități de audit

#	Atest de securitate cibernetică	Activități de audit					
		[AS1]	[AS2]	[AS3]	[AS4]	[AS5]	[AS6]
1.	Atestat tip general	x	x	x	x	x	x
2.	Atestat tip comun	x	x			x	x[1]
3.	Atestat tip special			x	x		x[2]

[1] Activitate de audit [AS6] desfășurată parțial, respectiv pentru activitățile comune: [AS1], [AS2] și [AS5].
[2] Activitate de audit [AS6] desfășurată parțial, respectiv pentru activitățile speciale: [AS3] și [AS4].