REGULAMENT din 22 martie 2021

pentru atestarea şi verificarea auditorilor de securitate cibernetică

EMITENT • **SECRETARIATUL GENERAL AL GUVERNULUI**

Publicat în **MONITORUL OFICIAL nr. 387 din 14 aprilie 2021**

Data intrării în vigoare 14-04-2021

Notă

Aprobat prin ORDINUL nr. 559 din 22 martie 2021, publicat în Monitorul Oficial, Partea I, nr. 387 din 14 aprilie 2021.

Capitolul I
Dispoziţii generale

Articolul 1

Aplicabilitate

(1) Prezentul regulament pentru atestarea şi verificarea auditorilor de securitate cibernetică, denumit în continuare regulament, stabileşte cadrul legal pentru atestarea auditorilor de securitate cibernetică pentru auditarea reţelelor şi sistemelor informatice ce susţin servicii esenţiale ori furnizează servicii digitale în condiţiile Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, cu modificările şi completările ulterioare, denumită în continuare Legea NIS.

(2) În înţelesul prezentului regulament, auditorii de securitate cibernetică pot fi persoane fizice atestate cetăţeni români, precum şi cetăţeni ai altui stat membru al Uniunii Europene ori al Spaţiului Economic European sau persoane juridice cu personal atestat, care îndeplinesc cerinţele prevăzute în prezentul regulament şi care doresc să desfăşoare o activitate prin care se realizează o evaluare sistematică a tuturor politicilor, procedurilor şi măsurilor de protecţie implementate la nivelul reţelelor şi sistemelor informatice, în vederea identificării disfuncţiilor şi vulnerabilităţilor şi a furnizării unor soluţii de remediere a acestora, activitate pe care să o exercite în România în mod independent sau ca angajaţi ai unor persoane juridice.

(3) Prezentul regulament nu se aplică la nivelul instituţiilor din sistemul de apărare, ordine publică şi securitate naţională, din domeniul protecţiei infrastructurilor critice şi nici la nivelul infrastructurilor cibernetice care vehiculează informaţii clasificate.

Articolul 2

Termeni, expresii şi abrevieri

(1) În cuprinsul prezentului regulament se utilizează următoarele abrevieri:

a) ANSRSI - Autoritatea competentă la nivel naţional pentru securitatea reţelelor şi sistemelor informatice care asigură furnizarea serviciilor esenţiale ori furnizează serviciile digitale, denumită şi Autoritatea competentă la nivel naţional;

b) CERT-RO - Centrul Naţional 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 esenţiale;

g) SOC - Centrul de operaţiuni de securitate cibernetică.

(2) În cuprinsul prezentului regulament, precum şi în activitatea specifică domeniului securităţii reţelelor şi sistemelor informatice se utilizează următoarele concepte:

a) auditor de securitate cibernetică (ASC) - persoană fizică atestată sau persoană juridică cu personal atestat care realizează activităţi de auditare a reţelelor şi sistemelor informatice ce susţin servicii esenţiale sau furnizează servicii digitale, conform reglementărilor şi bunelor practici în domeniu;

b) audit de securitate (ASEC) - activitatea prin care se realizează o evaluare sistematică a tuturor politicilor, procedurilor şi măsurilor de protecţie implementate la nivelul reţelelor şi sistemelor informatice în vederea identificării disfuncţiilor şi vulnerabilităţilor şi a furnizării unor soluţii de remediere a acestora;

c) atestat de auditor de securitate cibernetică (AASC) - document emis de autoritatea competentă la nivel naţional pentru securitatea reţelelor şi sistemelor informatice, cu valabilitate limitată de 3 ani, prin care se certifică îndeplinirea condiţiilor de către persoana atestată pentru desfăşurarea activităţilor de auditare a reţelelor şi sistemelor informatice aparţinând operatorilor de servicii esenţiale 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 şi reguli de conduită care trebuie să guverneze activitatea auditorului de securitate cibernetică;

f) domeniul auditului - mediul fizic, logic şi organizaţional în care se află reţelele şi sistemele informatice sau o parte a acestora şi pe care se efectuează un audit de securitate;

g) echipă de audit de securitate (EASEC) - formaţiune constituită din două sau mai multe persoane, condusă de un şef de echipă, ce este capabilă să efectueze auditul de securitate la nivelul unui operator de servicii esenţiale 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 şi a securităţii naţionale, precum şi a obligaţiilor asumate de România la nivelul Uniunii Europene. Activitatea este efectuată de ANSRSI cu sprijinul instituţiilor din COSC;

i) lista auditorilor de securitate cibernetică (LASC) - cuprinde toţi auditorii de securitate cibernetică valabil atestaţi de autoritatea competentă la nivel naţional pentru securitatea reţelelor şi sistemelor informatice şi este publicată pe site-ul instituţiei;

j) lista standardelor şi specificaţiilor europene şi internaţionale (LSSEINIS) - cuprinde toate standardele şi specificaţiile europene şi internaţionale utilizate în implementarea cerinţelor minime de securitate şi 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 sfârşitul activităţii de audit de securitate, prezentat operatorului economic auditat, respectiv operatorului de servicii esenţiale sau furnizorului de servicii digitale, şi care prezintă rezultatele auditului şi, în special, vulnerabilităţile descoperite/identificate, precum şi măsurile corective propuse;

l) registrul naţional al auditorilor de securitate cibernetică (RENASC) - document constituit şi administrat la nivelul autorităţii competente la nivel naţional pentru securitatea reţelelor şi sistemelor informatice care cuprinde evidenţa cronologică a atestărilor, suspendărilor şi revocărilor auditorilor de securitate cibernetică;

m) reţele şi sisteme informatice (RSI) - se definesc conform art. 3 lit. l) din Legea NIS; reprezintă o colecţie de resurse (hardware, software, personal, date/informaţii şi proceduri) aparţinând, după caz, operatorilor de servicii esenţiale sau furnizorilor de servicii digitale şi care stau la baza furnizării serviciilor esenţiale şi, respectiv, a serviciilor digitale;

n) sistem de control industrial (ICS) - un set de resurse umane şi materiale constituit în scopul controlului instalaţiilor tehnice utilizate în furnizarea unui serviciu esenţial sau digital compus din senzori şi dispozitive de acţionare;

o) solicitant de atestat de auditor de securitate cibernetică (SAASC) - o persoană care a absolvit un curs de specializare şi care solicită atestarea ca auditor de securitate cibernetică, de la data solicitării şi până la primirea atestatului;

p) testarea de penetrare - procesul de testare a reţelelor şi sistemelor informatice printr-o simulare a unui atac real asupra componentelor hardware şi software, inclusiv a aplicaţiilor informatice utilizate de operatorul de servicii esenţiale sau furnizorul de servicii digitale auditat, după caz, efectuată cu acordul operatorului economic auditat;

q) vulnerabilitate - o slăbiciune în proiectarea şi implementarea reţelelor şi sistemelor informatice sau a măsurilor de securitate aferente care poate fi exploatată de către o ameninţare sau de un grup de ameninţări.

Articolul 3

Autoritatea competentă la nivel naţional

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

(2) Autoritatea competentă la nivel naţional organizează şi gestionează procesul de atestare şi verificare a auditorilor de securitate cibernetică.

(3) CERT-RO, în calitate de autoritate competentă la nivel naţional, asigură:

a) menţinerea şi actualizarea permanentă a Registrului naţional 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 şi la activităţile de auditare a reţelelor şi sistemelor informatice, împreună cu instituţiile din COSC;

d) participarea la procesul de pregătire/specializare a auditorilor în vederea atestării ca auditori de securitate cibernetică, atât prin tematicile elaborate, cât şi în comisiile de examen/evaluare;

e) verificarea în urma sesizărilor sau din oficiu a îndeplinirii de către auditorii de securitate cibernetică atestaţi a obligaţiilor legale ce le revin.

Articolul 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 reţelelor şi sistemelor informatice care asigură furnizarea serviciilor esenţiale ori furnizează serviciile digitale în vederea identificării disfuncţiilor şi vulnerabilităţilor şi a furnizării unor soluţii de remediere a acestora.

(2) Auditorul de securitate cibernetică îşi desfăşoară activitatea individual sau în cadrul unei echipe de audit şi realizează cel puţin una dintre activităţile de audit de securitate, aşa cum sunt stabilite la art. 5 alin. (1).

(3) Auditorii de securitate cibernetică sunt atestaţi de autoritatea competentă la nivel naţional pentru securitatea reţelelor şi sistemelor informatice, iar evidenţa acestora este ţinută în Registrul naţional al auditorilor de securitate cibernetică.

(4) Calitatea de auditor de securitate cibernetică se dovedeşte prin atestatul de auditor valabil eliberat de către autoritatea competentă la nivel naţional pentru securitatea reţelelor şi sistemelor informatice.

(5) Atestatul de auditor de securitate cibernetică este nominal, netransmisibil şi are valabilitate 3 ani de la data emiterii. Modelul atestatului este prevăzut în anexa nr. 1.

Articolul 5

Activităţi de audit de securitate

(1) Activităţile de audit de securitate tratate în prezentul regulament sunt:

a) auditul arhitecturii [AS1] - constă în verificarea conformităţii măsurilor de securitate legate de alegerea, poziţionarea şi implementarea dispozitivelor hardware/software în reţelele şi sistemele informatice, cerinţele minime de securitate şi politicile interne ale operatorului economic. Auditul poate fi extins la interconectările cu reţele terţe, inclusiv internetul;

b) auditul de configurare [AS2] - constă în verificarea implementării măsurilor de securitate în conformitate cu stadiul tehnicii, cerinţele minime de securitate şi politicile de securitate în ceea ce priveşte configuraţia dispozitivelor hardware/software componente ale reţelelor şi sistemelor informatice. Aceste dispozitive pot fi în special echipamente de reţea, sisteme de operare (server sau staţie de lucru), aplicaţii sau produse de securitate;

c) auditul codului sursă [AS3] - constă în analiza totală sau parţială a codului sursă sau a condiţiilor de compilare ale unei aplicaţii pentru a descoperi vulnerabilităţile legate de practicile de programare neadecvate sau erorile logice care ar putea avea un impact asupra securităţii reţelelor şi sistemelor informatice;

d) auditul de penetrare sau testarea de penetrare [AS4] - constă în identificarea vulnerabilităţilor din reţelele şi sistemele informatice şi verificarea posibilităţilor de exploatare a acestora, precum şi a impactului exploatării acestora asupra reţelei, în condiţiile reale ale unui atac cibernetic asupra reţelelor şi sistemelor informatice. Activitatea de audit poate fi desfăşurată fie din afara reţelei (în special din internet sau din reţeaua interconectată a unei terţe părţi), fie din interiorul reţelei şi reprezintă o activitate care trebuie efectuată în complementaritate cu alte activităţi de audit pentru a le îmbunătăţi eficacitatea sau pentru a demonstra fezabilitatea exploatării vulnerabilităţilor descoperite;

e) auditul securităţii organizaţiei [AS5] - constă în auditul organizaţiei cu privire la securitatea logică şi fizică şi urmăreşte să se asigure că politicile şi procedurile de securitate definite de operatorul economic (operatorul de servicii esenţiale sau furnizorul de servicii digitale):

(i) sunt conforme cu nevoile de securitate ale operatorului economic auditat, nivelul tehnologic şi standardele în vigoare;

(ii) completează corect măsurile tehnice implementate;

(iii) sunt puse efectiv în practică.

De asemenea, auditorul de securitate cibernetică trebuie să se asigure că aspectele fizice ale securităţii reţelelor şi sistemelor informatice sunt acoperite corespunzător. Această activitate trebuie efectuată în complementaritate cu alte activităţi de audit pentru a le îmbunătăţi eficacitatea;

f) auditul sistemelor de control industrial [AS6] - constă în evaluarea nivelului de securitate al unui sistem de control industrial şi a dispozitivelor de control asociate. Evaluarea de securitate presupune aplicarea activităţilor de audit de la lit. a) la lit. e) din prezentul articol.

(2) Activităţile de audit de securitate se împart în:

a) activităţi speciale: [AS3] şi [AS4];

b) activităţi comune: [AS1], [AS2] şi [AS5];

c) activităţi mixte: [AS6].

(3) Activităţile mixte cuprind activităţile speciale şi normale/comune. În acest context, activitatea de audit a sistemelor de control industrial presupune desfăşurarea tuturor activităţilor, respectiv speciale şi comune.

(4) Corespondenţa dintre activităţile de audit şi evaluarea cerinţelor 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

Secţiunea 1
Noţiuni generale

Articolul 6

Noţiuni generale privind atestarea

(1) Atestarea auditorilor de securitate cibernetică se realizează de către Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO, în calitate de autoritate competentă la nivel naţional, 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 activităţile de audit, speciale şi comune, respectiv cele precizate la art. 5 alin. (1) lit. a)-e);

b) atestare tip special: numai pentru activităţile de audit speciale, respectiv cele precizate la art. 5 alin. (1) lit. c) şi d);

c) atestare tip comun: numai pentru activităţile de audit comune, respectiv cele precizate la art. 5 alin. (1) lit. a), b) şi e).

(3) În situaţia precizată la alin. (2) lit. a), auditorul de securitate cibernetică poate desfăşura toate activităţile de audit, inclusiv auditul sistemelor de control industrial [AS6].

(4) În situaţiile precizate la alin. (2) lit. b) şi c), auditorul de securitate cibernetică poate desfăşura numai activităţile de audit pentru care a fost atestat şi parţial activitatea de audit a sistemelor de control industrial [AS6], respectiv activităţi de audit speciale sau activităţi de audit comune.

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

Secţiunea a 2-a
Eliberarea atestatului de auditor de securitate cibernetică

Articolul 7

Documente necesare pentru atestare

(1) Atestatul de auditor de securitate cibernetică se obţine în baza cererii pentru emiterea atestatului de auditor de securitate cibernetică şi 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) adeverinţa medicală din care să rezulte starea de sănătate fizică şi psihică a solicitantului pentru exercitarea atribuţiilor de auditor de securitate cibernetică;

c) certificatul de cazier judiciar, aflat în termenul de valabilitate;

d) curriculum vitae - model europass, cu detalierea secţiunii „experienţă profesională“ ce va conţine justificarea privind experienţa în domeniu, în conformitate cu art. 25 alin. (2), prin detalii/descrieri şi anexarea de înscrisuri etc., respectiv cele care prezintă dovada a cel puţin:

(i) 2 ani de experienţă în domeniul administrării sau implementării reţelelor şi sistemelor informatice; sau

(ii) 2 ani de experienţă în domeniul securităţii reţelelor şi sistemelor informatice; sau

(iii) un an de experienţă în domeniul investigaţiilor, testării sau al auditului de securitate a tehnologiei informaţiei şi comunicaţiilor sau a reţelelor şi sistemelor informatice ori a sistemelor de control industrial;

e) certificări, în copii - în funcţie de tipul de atestat solicitat:

(i) atestare tip general - cel puţin două dintre certificările profesionale menţionate în anexa nr. 5 (dintre care cel puţin una dintre activităţile de audit comune şi cel puţin una dintre activităţile de audit speciale), în perioada de valabilitate;

(ii) atestare tip special - cel puţin una dintre certificările profesionale pentru activităţile de audit speciale menţionate în anexa nr. 5, în perioada de valabilitate;

(iii) atestare tip comun - cel puţin una dintre certificările profesionale pentru activităţile de audit comune menţionate în anexa nr. 5, în perioada de valabilitate; sau

(iv) certificat evaluare expertiză privind securitatea cibernetică eliberat de către CERT-RO, conform art. 25 alin. (3) şi (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 naţional, conform art. 32 din Legea NIS;

g) taxa de evaluare şi 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 înfiinţare/înregistrare al persoanei juridice, respectiv certificat de înregistrare în registrele naţionale, după caz, registrul comerţului, Registrul asociaţiilor şi fundaţiilor, Registrul federaţiilor etc.;

b) certificat constatator emis de instituţia care gestionează registrul în care se ţine evidenţa înfiinţării persoanei juridice, cu starea la zi a persoanei juridice, nu mai vechi de 30 de zile, în original sau în copie semnată şi cu menţiunea „conform cu originalul";

c) documentele de la alin. (2) pentru fiecare auditor de securitate cibernetică persoană fizică;

d) taxa de evaluare şi 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 naţional, în Strada Italiană nr. 22, cod poştal 020976, sectorul 2, Bucureşti, România, sau se transmite prin poştă, cu scrisoare cu valoare declarată şi confirmare de primire, sau prin e-mail în format electronic la nis@cert.ro.

(5) Documentaţia va fi în limba română, paginată şi însoţită de un opis.

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

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

Articolul 8

Iniţierea procedurii de evaluare şi atestare a auditorului

(1) După confirmarea primirii documentaţiei, autoritatea competentă la nivel naţional procedează la iniţierea procedurii de evaluare şi atestare a auditorului de securitate cibernetică.

(2) Procedura de evaluare şi atestare presupune parcurgerea a cinci etape procedurale, respectiv: evaluarea documentaţiei solicitantului (EEDS); evaluarea riscurilor de securitate cu privire la solicitant (EERS); evaluarea expertizei solicitantului (EEES); evidenţa auditorului de securitate cibernetică (EEAS); finalizarea procedurii de atestare (EFPA).

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

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

(5) Procedura de evaluare şi atestare, respectiv luarea în evidenţă a auditorului de securitate cibernetică sau refuzul privind înscrierea se finalizează la nivelul autorităţii competente la nivel naţional, în termen de maximum 60 de zile de la primirea documentaţiei complete de la solicitant.

Articolul 9

Evaluarea documentaţiei solicitantului (EEDS)

(1) Autoritatea competentă la nivel naţional constituie mapa auditorului de securitate cibernetică, evaluează documentele transmise de către solicitant, solicită date, informaţii sau înscrisuri suplimentare, dacă este cazul, şi în funcţie de situaţie dispune continuarea sau întreruperea procedurii de evaluare şi atestare.

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

(3) Autoritatea competentă la nivel naţional colaborează cu instituţii şi autorităţi din domeniul/sectorul învăţământ, sănătate şi aplicării legii în vederea evaluării înscrisurilor trimise de către solicitant.

Articolul 10

Evaluarea riscului de securitate cu privire la solicitant (EERS)

(1) Întrucât reţelele şi sistemele informatice care susţin serviciile esenţiale sau furnizează servicii digitale fac parte din domenii-cheie pentru securitatea naţională, având în vedere că securitatea cibernetică este componentă a securităţii naţionale şi ţinând cont de faptul că activitatea de audit de securitate presupune acces la informaţii critice pentru furnizarea serviciilor esenţiale/digitale (de exemplu: date cu caracter sensibil sau

confidenţiale; date/informaţii ce pot fi utilizate pentru derularea de atacuri cibernetice de natură să afecteze semnificativ funcţionarea serviciilor esenţiale/digitale la nivel naţional; vulnerabilităţi identificate etc.), evaluarea riscurilor de securitate cu privire la solicitant, inclusiv din perspectiva securităţii naţionale, este o etapă importantă în cadrul procedurii de evaluare şi atestare.

(2) Autoritatea competentă la nivel naţional cooperează cu instituţiile din COSC şi solicită efectuarea de verificări ale riscurilor de securitate, inclusiv din perspectiva securităţii naţionale, cu privire la solicitantul de atestat de auditor de securitate cibernetică.

(3) În urma informaţiilor/datelor primite, autoritatea competentă la nivel naţional evaluează riscurile de securitate şi în funcţie de situaţie dispune continuarea sau întreruperea procedurii de evaluare şi atestare.

Articolul 11

Evaluarea expertizei solicitantului (EEES)

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

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

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

Articolul 12

Evidenţa auditorului de securitate cibernetică (EEAS)

(1) Autoritatea competentă la nivel naţional întocmeşte 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 naţional emite atestatul de auditor de securitate cibernetică, ia în evidenţă auditorul de securitate cibernetică şi actualizează lista auditorilor de securitate cibernetică.

(3) Lista auditorilor de securitate cibernetică se publică pe site-ul instituţiei, pe pagina autorităţii.

(4) Evidenţa auditorilor de securitate cibernetică se ţine de către autoritatea competentă la nivel naţional, în format electronic, pe baza Registrului naţional al auditorilor de securitate cibernetică.

Articolul 13

Finalizarea procedurii de atestare (EFPA)

(1) Autoritatea competentă la nivel naţional transmite solicitantului atestatul de auditor de securitate cibernetică.

(2) Autoritatea competentă la nivel naţional actualizează bazele de date specifice şi 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 CERTRO, autoritatea competentă la nivel naţional, din Strada Italiană nr. 22, sectorul 2, cod poştal 020976, Bucureşti, sau în contul instituţiei.

(4) Neachitarea taxei duce la revocarea atestatului şi radierea auditorului de securitate cibernetică din evidenţele autorităţii competente la nivel naţional.

(5) Dosarele solicitanţilor care nu se încadrează în prevederile prezentului regulament, precum şi dosarele incomplete ale solicitanţilor care nu au fost completate în termenul stabilit la art. 8 alin. (3) se restituie acestora, fiind însoţite de o adresă de informare cu privire la restituire. Taxa de evaluare şi procesare în vederea atestării ca auditor de securitate cibernetică nu se restituie.

Secţiunea a 3-a
Revocarea atestatului de auditor de securitate cibernetică

Articolul 14

Revocarea atestatului

(1) CERT-RO, în calitate de autoritate competentă la nivel naţional, dispune revocarea atestatului de auditor de securitate cibernetică în următoarele situaţii:

a) încălcarea normelor privind incompatibilitatea specificate la art. 18 alin. (1);

b) nerespectarea în auditul de securitate a standardelor şi specificaţiilor europene şi internaţionale;

c) nerespectarea în întocmirea tematicilor de audit de securitate a normelor tehnice în vigoare privind cerinţele minime de asigurare a securităţii reţelelor şi sistemelor informatice ale operatorilor de servicii esenţiale şi ale furnizorilor de servicii digitale;

d) nerespectarea condiţiilor aplicabile activităţii de audit de securitate a reţelelor şi sistemelor informatice stabilite în cap. IV secţiunea a 3-a;

e) neachitarea taxelor de auditor de securitate cibernetică sau de reînnoire atestat;

f) neachitarea amenzilor contravenţionale stabilite de personalul de control din cadrul autorităţii competente la nivel naţional în urma controalelor impuse de sesizările primite, din oficiu sau în urma autosesizării ori încălcării de către auditorul de securitate cibernetică a obligaţiilor ce îi revin în temeiul Legii NIS;

g) nerespectarea cerinţelor impuse auditorilor de securitate cibernetică stabilite în cap. III secţiunea a 2-a;

h) încălcarea Codului etic al auditorului de securitate cibernetică;

i) după a 31-a zi de la primirea atestatului şi nesemnării/ netransmiterii declaraţiei/angajamentului 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 infracţiuni în domeniul securităţii cibernetice.

(2) La cererea expresă a auditorului de securitate cibernetică privind renunţarea la atestat, autoritatea competentă la nivel naţional dispune revocarea atestatului şi radierea auditorului de securitate cibernetică din registrul naţional. Modelele de cerere, persoană fizică sau juridică, sunt prezentate în anexa nr. 3.

(3) Ca urmare a revocării atestatului de auditor de securitate cibernetică, autoritatea competentă la nivel naţional informează persoana în cauză, radiază auditorul de securitate cibernetică din evidenţele autorităţii, respectiv din Registrul naţional al auditorilor de securitate cibernetică şi actualizează lista auditorilor de securitate cibernetică de pe site-ul instituţiei.

Secţiunea a 4-a
Reînnoirea atestatului de auditor

Articolul 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 naţional, reînnoirea atestatului prin completarea şi transmiterea unei cereri privind reînnoirea atestatului de auditor de securitate cibernetică, însoţită 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) şi g), actualizate la zi;

b) acte doveditoare privind participarea la activităţi de pregătire şi perfecţionare;

c) taxa de evaluare şi procesare (PF) în vederea reînnoirii atestatului de auditor de securitate cibernetică;

d) lista auditurilor de securitate desfăşurate 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) şi b), actualizate la zi;

b) documentele stabilite la alin. (2) lit. a) şi b), pentru fiecare auditor de securitate cibernetică persoană fizică;

c) taxa de evaluare şi procesare (PJ) în vederea reînnoirii atestatului de auditor de securitate cibernetică;

d) lista auditurilor de securitate desfăşurate pe perioada de valabilitate a atestatului, conform modelului prezentat în anexa nr. 12.

(4) În procedura de evaluare şi reînnoire a atestatului de securitate cibernetică, autoritatea competentă la nivel naţional aplică prevederile de la cap. II secţiunea a 2-a art. 8-13.

(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 CERTRO, autoritatea competentă la nivel naţional, din Strada Italiană nr. 22, sectorul 2, cod poştal 020976, Bucureşti, sau în contul instituţiei.

(6) Neachitarea taxei duce la revocarea atestatului şi radierea auditorului de securitate din Registrul naţional al auditorilor de securitate cibernetică.

Secţiunea a 5-a
Suspendarea atestatului de auditor de securitate cibernetică

Articolul 16
Suspendarea atestatului

(1) Autoritatea competentă la nivel naţional poate dispune suspendarea atestatului de auditor de securitate cibernetică, pentru o perioadă stabilită de autoritate, în următoarele situaţii:

a) în cazul descoperirii de către autoritatea competentă la nivel naţional a nerespectării de către un auditor de securitate cibernetică a unei obligaţii prevăzute de Legea NIS sau prezentul regulament sau de un act emis de autoritatea competentă la nivel naţional în baza Legii NIS - până la remedierea deficienţelor constatate şi 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-a zi de la data efectuării modificării şi până la îndeplinirea cerinţei stabilite, dar nu mai mult de 60 de zile;

c) în cazul nerespectării termenului stabilit la art. 20 alin. (2) - din a 11-a zi de la primirea atestatului şi până la transmiterea angajamentului semnat la autoritatea naţională, dar nu mai mult de 30 de 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 desfăşura activităţi de audit în condiţiile Legii NIS şi nici să semneze rapoarte de audit de securitate până la remedierea neregulilor şi intrarea în legalitate.

Secţiunea a 6-a
Registrul naţional al auditorilor de securitate cibernetică

Articolul 17

Constituirea, întreţinerea şi actualizarea registrului

(1) CERT-RO constituie, la nivelul autorităţii competente la nivel naţional, Registrul naţional al auditorilor de securitate cibernetică, care este întreţinut şi actualizat în permanenţă.

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

(3) Pentru informarea operatorilor de servicii esenţiale, furnizorilor de servicii digitale şi autorităţilor de reglementare şi administrare a sectoarelor şi subsectoarelor, în baza Registrului naţional al auditorilor de securitate cibernetică, autoritatea competentă la nivel naţional elaborează, actualizează în permanenţă şi publică pe site-ul instituţiei lista auditorilor de securitate cibernetică.

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

Capitolul III
Condiţii şi cerinţe pentru auditorii de securitate cibernetică

Secţiunea 1
Norme generale

Articolul 18

Norme privind activitatea auditorilor

(1) Constituie incompatibilităţi următoarele activităţi desfăşurate de către un auditor de securitate cibernetică:

a) efectuarea auditului de securitate la un operator de servicii esenţiale 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 relaţie contractuală ce nu este de tip audit;

b) efectuarea auditului de securitate pentru reţelele şi 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 cerinţă minimă de securitate în condiţiile Legii NIS (cel puţin odată la 2 ani), la un operator de servicii esenţiale sau furnizor de servicii digitale de 3 ori consecutiv;

d) efectuarea auditului de securitate la un operator de servicii esenţiale sau furnizor de servicii digitale în care deţine o participare la capitalul social al acestuia.

(2) Auditul de securitate se realizează numai de auditori de securitate cibernetică, atestaţi de CERT-RO, în calitate de autoritate competentă la nivel naţional, potrivit standardelor şi specificaţiilor europene şi internaţionale aplicabile în domeniu, în baza unor tematici de audit stabilite în conformitate cu normele tehnice în vigoare privind cerinţele minime de asigurare a securităţii reţelelor şi sistemelor informatice aplicabile operatorilor de servicii esenţiale, respectiv furnizorilor de servicii digitale şi după încheierea unui contract de audit.

(3) Auditul de securitate realizat în conformitate cu prevederile alin. (2) este un audit de securitate care se poate realiza şi la solicitarea autorităţii competente la nivel naţional şi reprezintă un audit de securitate în condiţiile Legii NIS.

(4) Pentru desfăşurarea auditului de securitate, auditorii de securitate cibernetică se pot organiza şi pot funcţiona şi în echipe de audit de securitate.

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

Secţiunea a 2-a
Cerinţe pentru auditorii de securitate cibernetică

Articolul 19

Cerinţe generale

(1) Pe timpul auditului de securitate, un auditor de securitate cibernetică poate desfăşura una sau mai multe activităţi de audit menţionate la art. 5 alin. (1).

(2) În desfăşurarea unei activităţi de audit de securitate, auditorul de securitate cibernetică trebuie:

a) să respecte legile şi reglementările în vigoare pe teritoriul naţional;

b) să descrie şi să organizeze activitatea cu operatorul economic supus auditului de securitate;

c) să îşi asume responsabilitatea pentru activităţile de audit de securitate pe care le desfăşoară şi, în special, orice daune cauzate entităţii auditate;

d) după caz, să încheie o asigurare profesională care să acopere daunele cauzate operatorului economic, atât infrastructurii, cât şi informaţiilor procesate, ca parte a auditului de securitate efectuat;

e) să se asigure că informaţiile pe care le furnizează, inclusiv publicitatea, nu sunt false sau înşelătoare;

f) să efectueze serviciul în mod imparţial, cu bună-credinţă şi cu respect pentru operatorul economic, personalul şi reţelele şi sistemele informatice ale acestuia;

g) să deţină licenţe valide pentru instrumentele (software sau hardware) utilizate pentru efectuarea activităţilor de audit de securitate;

h) să solicite/ceară operatorului economic să îl informeze cu privire la orice cerinţe legale şi de reglementare specifice la care este supus şi, în special, la cele legate de sectorul său de activitate;

i) să informeze operatorul economic atunci când acesta din urmă este obligat să raporteze un incident de securitate către CERT-RO şi trebuie să îl susţină în acest proces, dacă acesta din urmă solicită acest lucru;

j) să realizeze auditul de securitate pe baza unui contract de furnizare servicii de audit de securitate.

Articolul 20

Codul etic al auditorului de securitate cibernetică

(1) Auditorii de securitate cibernetică sunt obligaţi să respecte Codul etic al auditorului de securitate cibernetică prezentat în anexa nr. 13.

(2) După obţinerea atestatului de auditor de securitate cibernetică, auditorul de securitate cibernetică va lua act de codul etic şi va semna, olograf sau digital, declaraţia/ angajamentul privind respectarea Codului etic al auditorului de securitate cibernetică prevăzut(ă) la art. 10 din anexa nr. 13 şi o/îl va înainta la CERT-RO, autoritatea competentă la nivel naţional, în maximum 10 zile de la emiterea atestatului, folosind unul dintre modurile de transmitere prezentate la art. 7 alin. (4).

(3) Nesemnarea şi/sau netransmiterea declaraţiei/ angajamentului duce, după caz, la suspendarea atestatului după a 11-a zi de la emiterea atestatului, dar nu mai mult de 30 de zile sau la revocarea după cea de a 31-a zi de la emiterea atestatului.

Articolul 21

Managementul resurselor şi abilităţilor

(1) Pentru realizarea auditului de securitate, auditorul de securitate cibernetică poate să se asocieze cu alţi auditori de securitate cibernetică pentru a asigura pe deplin şi sub toate aspectele activităţile de audit pentru care se încheie contractul cu operatorul economic. În acest sens, pentru fiecare contract trebuie să se asigure că auditorii de securitate desemnaţi au calităţile şi abilităţile necesare. Fiecare auditor trebuie să deţină un atestat valabil eliberat de autoritatea competentă la nivel naţional pentru activităţile de audit pe care le efectuează.

(2) În vederea îmbunătăţirii abilităţilor şi îndeplinirii în bune condiţii a activităţilor de audit, auditorul de securitate cibernetică trebuie să participe, periodic, la activităţi de pregătire şi dezvoltare a capacităţilor profesionale prin seminare, prezentări şi exerciţii tehnice, cursuri de pregătire etc.

(3) Auditorul de securitate cibernetică este responsabil pentru metodele, instrumentele (software sau hardware) şi tehnicile utilizate pe timpul auditului de securitate, precum şi pentru utilizarea corectă a acestora (precauţii pentru utilizare, controlul configuraţiei etc.) în efectuarea activităţilor de audit. În acest sens trebuie:

a) să asigure actualizarea continuă a componentelor tehnice utilizate;

b) să utilizeze componente specifice şi relevante pentru fiecare tip de activitate de audit;

c) să deţină licenţe valide pentru instrumentele (software/hardware) utilizate pentru efectuarea activităţilor de audit.

Articolul 22

Protecţia informaţiilor

(1) Auditorul de securitate cibernetică trebuie să protejeze informaţiile referitoare la auditul de securitate şi, în special, dovezile, constatările şi rapoartele.

(2) Auditorul de securitate cibernetică trebuie să ia toate măsurile tehnice şi organizatorice în vederea protejării tuturor informaţiilor referitoare la activitatea de audit la nivel de procesare restricţionată.

(3) Auditorul de securitate cibernetică trebuie să implementeze un sistem de management al securităţii informaţiei (SMSI) în vederea protejării tuturor informaţiilor privitoare la auditurile de securitate efectuate, indiferent de forma în care sunt prezentate (de exemplu: verbal, pe hârtie sau în orice altă formă), inclusiv, dar fără a se limita la date, informaţii personale, proprietatea intelectuală, parole, informaţii cu privire la operatorii economici auditaţi, personalul, reţelele şi sistemele informatice ale acestuia, precum şi informaţiile care nu sunt încă publice cu privire la activităţile de audit desfăşurate etc.

Secţiunea a 3-a
Condiţii pentru auditorii de securitate cibernetică

Articolul 23

Abilităţi generale

(1) Auditorul de securitate cibernetică trebuie să cunoască legislaţia română în vigoare, aplicabilă auditului de securitate cibernetică.

(2) Auditorul de securitate cibernetică trebuie să aibă abilităţi de scriere, raportare şi sinteză şi să ştie să se exprime oral întrun mod clar şi uşor de înţeles, în limba română.

(3) Auditorul de securitate cibernetică trebuie să îşi îmbunătăţească în mod regulat abilităţile, inclusiv prin monitorizarea activă a standardelor profesionale, metodologiilor, tehnicilor şi instrumentelor utilizate în timpul activităţilor de audit desfăşurate.

Articolul 24

Abilităţi şi cunoştinţe specifice auditului de securitate

(1) Auditorul de securitate cibernetică trebuie să stăpânească cele mai bune practici şi metodologii de audit în conformitate cu lista standardelor şi specificaţiilor europene şi internaţionale.

(2) Auditorul de securitate cibernetică trebuie să presteze activitatea de audit în conformitate cu cerinţele stabilite în prezentul regulament.

(3) Auditorul de securitate cibernetică trebuie să aibă abilităţile/competenţele cerute de tipurile de activităţi de audit şi de funcţiile îndeplinite pe timpul unui audit de securitate, astfel cum sunt definite în anexa nr. 6.

Articolul 25

Experienţă

(1) Auditorul de securitate cibernetică trebuie să deţină expertiză în domeniul auditului de securitate cibernetică, ce va fi certificată prin deţinerea unei certificări profesionale conform listei din anexa nr. 5 sau, alternativ, prin absolvirea unui/unei examen/evaluări al/a expertizei privind securitatea cibernetică.

(2) Pentru desfăşurarea activităţilor de audit de securitate, auditorul de securitate cibernetică trebuie să aibă experienţă în domeniu, respectiv să îndeplinească cel puţin una dintre cerinţele de mai jos:

a) cel puţin 2 ani de experienţă în domeniul administrării sau implementării reţelelor şi sistemelor informatice;

b) cel puţin 2 ani de experienţă în domeniul securităţii reţelelor şi sistemelor informatice;

c) cel puţin un an de experienţă în domeniul investigaţiilor, testării sau al auditului de securitate a tehnologiei informaţiei şi comunicaţiilor sau al reţelelor şi sistemelor informatice sau al 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 şi 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 naţional.

(4) Modul de organizare şi desfăşurarea examinării/evaluării expertizei în domeniul auditului de securitate cibernetică se va aproba prin Normele referitoare la autorizarea formatorilor şi furnizorilor de servicii de formare pentru auditorii de securitate cibernetică şi membrilor echipelor CSIRT.

Articolul 26

Angajamente

(1) Auditorul de securitate cibernetică ce va efectua un audit 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/entităţile 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
Condiţii aplicabile activităţii de audit de securitate

Secţiunea 1
Auditul de securitate

Articolul 27

Desfăşurarea auditului de securitate

(1) Auditul de securitate este unul dintre mijloacele disponibile oricărui operator economic pentru a testa şi asigura nivelul de securitate al reţelelor şi sistemelor informatice care stau la baza susţinerii serviciilor esenţiale sau furnizării de servicii digitale.

(2) Auditul de securitate se va desfăşura în baza unui contract încheiat între operatorul economic, respectiv operatorul de servicii esenţiale sau furnizorul de servicii digitale, şi un auditor de securitate, valabil atestat de autoritatea competentă la nivel naţional.

(3) Operatorul economic nu poate contracta servicii de audit de securitate cu acelaşi 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 cerinţele impuse pentru efectuarea auditului de securitate a reţelelor şi sistemelor informatice care stau la baza furnizării serviciilor esenţiale sau digitale, în conformitate cu prezentul regulament şi cu bunele practici în domeniu.

(5) Perioada supusă auditării reprezintă perioada cuprinsă între două audituri de securitate consecutive.

(6) Auditul de securitate se desfăşoară cu respectarea standardelor şi specificaţiilor europene şi internaţionale aplicabile în domeniu. Prima listă a standardelor şi specificaţiilor europene şi internaţionale a fost aprobată prin Decizia directorului general al Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO nr. 88/2020 privind aprobarea Listei standardelor şi specificaţiilor europene şi internaţionale şi publicată în Monitorul Oficial al României, Partea I.

(7) Tematicile de audit vor ţine seama de normele tehnice privind cerinţele minime de asigurare a securităţii reţelelor şi sistemelor informatice aplicabile, după caz, operatorilor de servicii esenţiale sau furnizorilor de servicii digitale.

(8) Pentru cazurile în care reţelele şi sistemele informatice care stau la baza furnizării serviciilor esenţiale sau digitale sunt situate în afara ţării, auditarea sistemului se va face astfel:

a) de către auditorul de securitate cibernetică - acesta va audita reţelele şi sistemele informatice din străinătate; sau

b) de către un auditor de securitate cibernetică acreditat de autoritatea competentă din acea ţară - în acest caz, auditorul de securitate cibernetică contractant agreează auditarea reţelelor şi sistemelor informatice din străinătate şi preia responsabilitatea auditării, anexând la raportul final raportul auditorului extern tradus în limba română.

(9) Autoritatea competentă la nivel naţional poate verifica derularea procesului de auditare, atât prin participarea la auditul desfăşurat de către auditorul de securitate, cât şi prin prisma evaluării dosarelor de emitere/reînnoire atestat de audit de securitate cibernetică.

Secţiunea a 2-a
Documente de audit de securitate

Articolul 28

Documente relevante pe timpul auditului de securitate

(1) La finalizarea auditului de securitate, auditorul de securitate cibernetică are obligaţia de a întocmi raportul de audit de securitate, în limba română, care va cuprinde, în anexă, rapoarte specifice pentru fiecare dintre activităţile de audit, aşa cum sunt stabilite la art. 5 alin. (1) lit. a)-f).

(2) La întocmirea raportului de audit de securitate, auditorul de securitate cibernetică va avea în vedere respectarea cerinţelor şi recomandărilor stabilite în anexa nr. 7.

(3) În termen de maximum 15 zile de la solicitarea scrisă a autorităţii competente la nivel naţional, auditorul de securitate cibernetică trebuie să comunice următoarele, fără a se limita la acestea:

a) orice raport sau document care a fost adus la cunoştinţa operatorului economic auditat;

b) motivaţia de încetare a contractului de audit, dacă aceasta a avut loc înainte de finalizarea auditării.

(4) Auditorul de securitate cibernetică notifică atât operatorului economic auditat, cât şi autorităţii competente la nivel naţional, prin e-mail (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 şi utilizarea în siguranţă a reţelelor şi sistemelor informatice care furnizează servicii esenţiale sau digitale;

b) poate conduce la o opinie de audit cu rezerve, negativă sau imposibilitatea exprimării acesteia.

Secţiunea a 3-a
Cerinţe referitoare la desfăşurarea unui audit de securitate

Articolul 29

Cerinţe generale privind auditul de securitate

(1) Definirea auditului de securitate şi descrierea activităţilor de audit de securitate solicitate se formulează în cererea de oferte.

(2) Cerinţe specifice şi recomandări cu privire la furnizarea serviciilor de audit de securitate şi la desfăşurarea auditului, precum şi tipurile de audit care urmează a fi efectuate în funcţie de sfera auditului sunt prezentate în anexa nr. 8.

(3) Auditorul de securitate cibernetică solicită şi 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 reţelele şi sistemele informatice de auditat, precum şi interdependenţele externe ale reţelelor şi sistemelor informatice.

(5) Auditorul de securitate cibernetică se asigură că auditul de securitate furnizat este adaptat la context şi la obiectivele dorite de operatorul economic. În caz contrar, auditorul de securitate cibernetică informează operatorul economic înainte de furnizarea auditului de securitate.

(6) Furnizarea şi desfăşurarea unui audit de securitate presupun atingerea următoarelor etape:

a) contractul de audit de securitate;

b) pregătirea auditului de securitate;

c) executarea auditului de securitate;

d) finalizarea auditului de securitate;

e) închiderea auditului de securitate.

Articolul 30

Contractul de audit de securitate

(1) Auditul de securitate a reţelelor şi sistemelor informatice se desfăşoară 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 şi de auditorul de securitate cibernetică contractant.

(3) Termenii serviciului. Contractul de audit:

a) descrie domeniul de aplicare a auditului, abordarea generală a auditului de securitate a reţelelor şi sistemelor informatice, activităţile de audit şi termenii auditului (obiective, locuri şi criterii ale auditului, etape, livrabile aşteptate ca input, condiţii prealabile etc.);

b) specifică dacă serviciul de audit este calificat sau nu;

c) specifică rezultatele aşteptate la finalizarea auditului, şedinţele de deschidere şi de închidere, publicul-ţintă, nivelul de confidenţialitate şi metodele asociate;

d) descrie mijloacele tehnice (echipamente şi instrumente) şi organizaţionale 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 şi operatorul economic;

f) prevede ce mijloace logistice vor fi puse la dispoziţia auditorului de securitate cibernetică de către operatorul economic (resurse materiale, umane, tehnice etc.);

g) defineşte 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 acţiunile care nu pot fi efectuate asupra reţelelor şi sistemelor informatice şi/sau informaţiilor colectate fără autorizarea expresă a operatorului economic şi, eventual, acordul sau prezenţa personalului operatorului economic, precum şi modalităţile asociate (implementare, persoane prezente, durată, interval program, planificări, descrierea datelor sensibile şi a acţiunilor autorizate etc.);

i) defineşte mijloacele care asigură trasabilitatea între operatorul economic şi auditorul de securitate a informaţiilor şi suporturilor materiale prezentate pentru analiză.

(4) Organizare. Contractul de audit trebuie:

a) să specifice numele responsabilului de legătură din partea operatorului economic cu auditorul de securitate cibernetică, precum şi pentru punerea în legătură a auditorului de securitate cu diferite persoane/furnizori implicaţi;

b) să specifice numele, rolurile, responsabilităţile, precum şi drepturile şi nevoile de cunoaştere a persoanelor-cheie desemnate de auditorul de securitate cibernetică şi de operatorul economic;

c) să stipuleze că auditorul de securitate cibernetică trebuie, acolo unde este cazul, să colaboreze cu furnizori de servicii terţi care lucrează în numele operatorului economic şi care au fost desemnaţi în mod specific de către operatorul economic şi să distingă clar responsabilităţile furnizorului de servicii terţ. Această cerinţă trebuie să permită în special auditorului de securitate cibernetică să colaboreze cu un furnizor de servicii de detectare a incidentelor de securitate;

d) să stipuleze că auditorul de securitate cibernetică nu implică alţi auditori care nu au nicio relaţie 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 sancţiuni, respectiv suspendare sau retragere atestat.

(5) Responsabilităţi. 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 acţiunile 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 şi accesul la domeniul de aplicare a auditului (reţele şi sisteme informatice, suporturi materiale etc.) sau că a obţinut acordul oricărui terţ şi, în special, al furnizorilor sau partenerilor săi de servicii, ale căror reţele şi sisteme informatice ar intra în sfera de aplicare;

e) stipulează că operatorul economic şi auditorul de securitate cibernetică îndeplinesc toate obligaţiile legale şi de reglementare necesare desfăşurării auditului;

f) stipulează că operatorul economic autorizează temporar auditorul de securitate cibernetică, cu scopul unic de a efectua auditul, să acceseze şi 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 şi să analizeze, în scopul efectuării auditului, date aparţinând reţelelor şi sistemelor informatice auditate;

h) defineşte responsabilităţile şi măsurile de precauţie obişnuite care trebuie respectate de către toate părţile cu privire la riscurile potenţiale asociate auditului, în ceea ce priveşte confidenţialitatea informaţiilor colectate şi analizate, precum şi în ceea ce priveşte disponibilitatea (de exemplu, refuzul de serviciu în timpul testării de penetrare, scanarea vulnerabilităţilor privind un sistem informatic sau a unui server) şi integritatea reţelelor şi sistemelor informatice vizate;

i) stabileşte dacă auditorul de securitate cibernetică are nevoie de o asigurare de practică profesională care acoperă daunele cauzate în timpul desfăşurării auditului şi, dacă este cazul, specifică acoperirea acestora şi include certificatul de asigurare.

(6) Confidenţialitate. Contractul de audit:

a) prevede regimul de distribuţie a raportului de audit (de exemplu, public, confidenţial etc.);

b) prevede o clauză explicită prin care raportul de audit poate fi transmis către ANSRSI, pe baza autorizaţiei scrise din partea operatorului economic;

c) stipulează că auditorul de securitate cibernetică poate, cu excepţia unui refuz formal şi scris din partea operatorului economic, să păstreze anumite tipuri de informaţii legate de audit odată ce acesta a fost finalizat. Auditorul de securitate cibernetică trebuie să identifice aceste tipuri de informaţii în contract (de exemplu: livrabile, informaţii, documente etc.);

d) stipulează că auditorul de securitate cibernetică anonimizează şi decontextualizează (ştergerea oricăror informaţii care identifică operatorul economic, orice informaţii cu caracter personal etc.) toate informaţiile pe care operatorul economic le autorizează să le păstreze;

e) stipulează că auditorul de securitate cibernetică distruge toate informaţiile referitoare la operatorul economic, cu excepţia celor pentru care a primit o autorizaţie de păstrare/stocare de la operatorul economic;

f) specifică metodele (conţinutul, forma, domeniul de aplicare etc.) pentru elaborarea recomandărilor;

g) prevede o procedură pentru obţinerea consimţământului personalului operatorului economic auditat şi al oricărui partener terţ pentru efectuarea auditului de securitate.

(7) Reglementări. Contractul de audit:

a) este scris în limba română;

b) stipulează că legea aplicabilă este legea română;

c) prevede cerinţele care trebuie îndeplinite de auditorul de securitate cibernetică în contextul unui caz judiciar, civil sau de arbitraj;

d) defineşte perioada de păstrare a informaţiilor legate de audit şi, în special, a evenimentelor colectate şi a incidentelor de securitate detectate. Dacă este necesar, se poate face o distincţie privind perioada de păstrare în funcţie de tipurile de informaţii. Perioada minimă de păstrare este de 6 luni, sub rezerva legislaţiei şi 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 şi a Legii NIS.

(9) Participare experţi. Contractul trebuie să specifice că auditorul de securitate cibernetică contractant poate implica alţi experţi în activităţile de audit de securitate executate în baza acestui regulament şi a Legii NIS, cu condiţia ca implicarea experţilor să nu depăşească 10% din volumul total al activităţii 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 excepţia 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 şi în alte limbi, versiunea în limba română prevalează.

(11) Conformitate. Contractul de audit:

a) indică faptul că auditul de securitate furnizat este:

(i) un serviciu de audit executat în condiţiile Legii NIS. În acest caz, auditorul de securitate cibernetică informează operatorul economic despre faptul că atât el, cât şi orice subcontractant deţin atestate de auditor de securitate cibernetică valabile eliberate de autoritatea competentă la nivel naţional;

(ii) un serviciu de audit executat în afara condiţiilor 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 deţin un atestat de auditor de securitate cibernetică individual pentru fiecare dintre activităţile de audit pentru care se efectuează misiunea de audit, inclusiv aceste atestate.

Articolul 31

Pregătirea auditului de securitate

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

(2) Şeful echipei de audit va constitui şi va conduce echipa de auditori, ce trebuie să aibă - în ansamblul său - cunoştinţele, experienţa şi abilităţile necesare pentru executarea auditului.

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

(4) Şeful echipei de audit sau auditorul de securitate cibernetică, acolo unde nu există constituită o echipă de audit, se asigură, împreună cu operatorul economic, că reprezentanţii legali ai entităţilor afectate de audit au fost anunţaţi în prealabil şi că şi-au dat acordul.

(5) Şeful echipei de audit sau 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 şi criteriile auditului, componenta tehnică şi organizatorică a serviciului de audit, datele şi locurile în care vor fi desfăşurate activităţile de audit şi, în special, cele posibile auditate, informaţii generale despre şedinţele de începere şi de închidere a misiunii de audit, auditorii de securitate care alcătuiesc echipa de audit, confidenţialitatea datelor colectate şi anonimizarea constatărilor şi rezultatelor.

(6) Tematica de audit va ţine seama de cerinţele minime de asigurare a securităţii reţelelor şi sistemelor informatice aplicabile operatorilor de servicii esenţiale, respectiv furnizorilor de servicii digitale.

(7) Obiectivele, criteriile şi programul auditului, precum şi activităţile de audit aplicate trebuie definite între auditorul de securitate cibernetică contractant şi operatorul economic, ţinând seama de constrângerile de funcţionare ale reţelelor şi sistemelor informatice. Aceste elemente trebuie incluse în planul de audit.

(8) În funcţie de activitatea de audit, echipa de audit/auditorul trebuie să obţină mai întâi toată documentaţia existentă de la operatorul economic (exemple: politica de securitate, analiza riscurilor, proceduri de securitate etc.), referitoare la reţelele şi sistemele informatice auditate în scopul evaluării şi revizuirii acesteia.

(9) Auditul de securitate va începe numai după o şedinţă oficială în timpul căreia şeful echipei de audit sau auditorul de securitate cibernetică, acolo unde nu există constituită o echipă de audit, şi reprezentanţii autorizaţi ai operatorului economic îşi confirmă contractul cu privire la toţi termenii serviciului de audit furnizat. Această întâlnire poate fi şi 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 conştientizeze operatorul economic despre valoarea backup-ului şi păstrării datelor, aplicaţiilor şi sistemelor de operare din reţelele şi sistemele informatice auditate.

(11) În prealabil şi în cazul specific al testării de penetrare, trebuie semnat un formular de autorizare de către operatorul economic, entităţile auditate şi orice terţi. În formularul de autorizare vor fi specificate, în special:

a) lista infrastructurilor auditate (adrese IP, nume de domenii etc.);

b) lista adreselor IP din care provin testele;

c) data şi orele exclusive ale testelor;

d) durata autorizaţiei.

Articolul 32

Executarea auditului de securitate

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

(2) Auditul de securitate trebuie efectuat cu respect pentru activitatea, reputaţia, personalul, precum şi pentru reţelele şi sistemele informatice ale operatorului economic.

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

(4) Auditorul de securitate cibernetică trebuie să notifice imediat, direct sau prin şeful de echipă, când este constituită echipa de audit, conducerea managerială proprie şi operatorul economic, în conformitate cu clauzele de confidenţialitate stabilite în contractul de audit, cu privire la concluziile activităţii de audit.

(5) Orice modificare adusă reţelelor şi sistemelor informatice auditate, în timpul auditului, trebuie urmărită, iar la sfârşitul auditului, reţelele şi sistemele informatice în cauză trebuie să revină într-un stadiu a cărui securitate nu este degradată în comparaţie cu starea iniţială.

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

(7) Auditorul de securitate cibernetică trebuie să ia toate măsurile de precauţie necesare pentru a păstra confidenţialitatea documentelor şi informaţiilor referitoare la operatorul economic.

(8) Operatorul economic va urmări logurile acţiunilor şi rezultatele auditorilor de securitate cu privire la reţelele şi sistemele informatice auditate, precum şi datele de finalizare a acestora. Aceste loguri pot fi utilizate pentru a stabili cauzele unui posibil incident tehnic care a avut loc în timpul auditului.

(9) Detalierea cerinţelor impuse auditorului de securitate şi operatorului economic pe timpul executării auditului de securitate este specificată în anexa nr. 9.

Articolul 33

Finalizarea auditului de securitate

(1) La finalizarea auditului şi fără a aştepta finalizarea raportului de audit, şeful echipei de audit sau auditorul de securitate cibernetică, acolo unde nu există constituită o echipă de audit, trebuie să informeze operatorul economic cu privire la constatările şi concluziile iniţiale ale auditului.

(2) Acolo unde este cazul, auditorul de securitate cibernetică prezintă vulnerabilităţile majore şi critice care ar necesita o acţiune rapidă şi 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 activităţile de audit stabilite la art. 5 alin. (1), în funcţie de serviciile de audit contractate, şi să îl trimită operatorului economic, în format electronic sau hârtie.

(4) Raportul de audit trebuie să conţină în special:

a) o menţiune privind destinatarul raportului de audit şi regimul de distribuţie a acestui raport (de exemplu, public, confidenţial, clasificat etc.);

b) o menţiune privind standardele profesionale, metodologiei sau cadrului utilizat pentru executarea auditului de securitate cibernetică;

c) un rezumat întocmit într-un limbaj accesibil şi persoanelor nontehnice care specifică:

(i) contextul şi domeniul de aplicare a serviciului de audit de securitate furnizat;
(ii) vulnerabilităţi critice, tehnice sau organizaţionale şi măsurile corective propuse;
(iii) evaluarea nivelului de securitate a reţelelor şi sistemelor informatice auditate în comparaţie cu stadiul tehnicii şi ţinând cont de domeniul de aplicare a auditului;
d) un tabel rezumat al rezultatelor auditului care specifică:
(i) un rezumat al vulnerabilităţilor identificate, clasificate în funcţie de o scară valorică;
(ii) rezumatul măsurilor corective propuse, clasificate după nivelul critic şi după complexitate, sau costul estimat al corecţiei;
e) la efectuarea unei testări de penetrare, o descriere a cursului liniar al testelor de penetrare şi a metodologiei utilizate pentru a detecta vulnerabilităţile şi, dacă este cazul, a le exploata;
f) o concluzie/opinie generală a auditorului privind securitatea reţelelor şi sistemelor informatice auditate, care prezintă rezultatele diferitelor activităţi de audit desfăşurate.
(5) Raportul de audit trebuie adaptat în funcţie de activitatea de audit desfăşurată de auditorul de securitate cibernetică.
(6) Vulnerabilităţile, de origine tehnică sau organizaţională, trebuie clasificate în funcţie de impactul lor asupra securităţii reţelelor şi sistemelor informatice şi de dificultatea lor de exploatare. Se va utiliza scala stabilită de CERT-RO, în calitate de autoritate competentă la nivel naţional, în anexa nr. 10.
(7) Fiecare vulnerabilitate trebuie să fie asociată cu una sau mai multe recomandări adaptate reţelelor şi sistemelor informatice ale operatorului economic. Recomandările descriu soluţii pentru rezolvarea temporară sau permanentă a vulnerabilităţii şi îmbunătăţirea nivelului de securitate.
(8) Raportul de audit poate prezenta, de asemenea, recomandări generale care nu au legătură cu vulnerabilităţile şi sunt destinate să consilieze operatorul economic cu privire la acţiunile pe care le poate întreprinde acesta pentru asigurarea unui nivel sporit al securităţii reţelelor şi sistemelor informatice proprii.
(9) Raportul de audit trebuie să menţioneze rezervele legate de exhaustivitatea rezultatelor auditului (referitoare la termenele alocate, disponibilitatea informaţiilor solicitate, colaborarea operatorului economic etc.) sau relevanţa reţelelor şi sistemelor informatice auditate.
(10) Raportul de audit trebuie să includă numele şi detaliile de contact ale auditorilor, şefului echipei de audit, dacă este cazul, şi 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 şi să specifice activităţile de audit asociate.

Articolul 34

Închiderea auditului de securitate

(1) Pentru închiderea auditului şi finalizarea contractului de audit, auditorul de securitate cibernetică va organiza, împreună cu operatorul economic, o şedinţă (fizic sau online) de închidere a auditului de securitate la predarea raportului de audit. În timpul întâlnirii se vor prezenta rezumatul raportului de audit, concluziile auditului, recomandările auditorului şi se va răspunde întrebărilor ridicate de reprezentanţii operatorului economic. De asemenea, este o oportunitate a auditorului de securitate cibernetică de a explica recomandări complexe şi, eventual, de a sugera alte soluţii mai uşor de implementat.
(2) Toate datele, înregistrările, informaţiile sau documentele referitoare la reţelele şi sistemele informatice auditate obţinute de auditorul de securitate cibernetică trebuie returnate operatorului economic sau, la cererea acestuia, distruse în conformitate cu contractul de audit. După caz, şeful echipei de audit sau auditorul de securitate cibernetică, acolo unde nu există constituită o echipă de audit, întocmeşte un raport privind distrugerea datelor, pe care îl transmite operatorului economic şi în care specifică datele distruse şi modul în care acestea au fost distruse.
(3) Contractul de audit este considerat finalizat atunci când au fost efectuate toate activităţile planificate şi 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 activităţii auditorilor de securitate cibernetică

Articolul 35

Verificarea activităţii auditorilor de securitate cibernetică

(1) CERT-RO, în calitate de autoritate competentă la nivel naţional, verifică modul de îndeplinire a activităţii de către auditorii de securitate cibernetică, în baza planului de control anual, a sesizărilor primite sau a activităţii 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 naţional 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 naţional, 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 obligaţiilor legale ce le revin şi dispune, după caz, măsuri de remediere, suspendarea activităţii 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 naţional, în format electronic, la adresa de e-mail nis@cert.ro - o situaţie a auditurilor de securitate desfăşurate în anul calendaristic precedent, respectiv numărul, beneficiarii, perioadele, neregulile grave constatate şi vulnerabilităţile constatate. Modelul de situaţie se regăseşte în anexa nr. 11.

Capitolul VI
Dispoziţii finale

Articolul 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 şi furnizorilor de servicii de formare pentru auditorii de securitate cibernetică pe site-ul instituţiei.

(2) După această dată, auditorul de securitate cibernetică are la dispoziţie 6 luni pentru finalizarea cursului de specializare auditor şi transmiterea la autoritatea competentă la nivel naţional a copiei certificatului de specializare auditor prin una dintre modalităţile specificate la art. 7 alin. (4).

(3) Dacă după termenul stabilit la alin. (2) auditorul de securitate cibernetică nu transmite la autoritatea competentă la nivel naţional 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 evidenţele autorităţii naţionale şi lista auditorilor de securitate cibernetică este actualizată.

Articolul 37

Anexe

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

Anexa nr. 1

la regulament

Simplitatea este o complexitate rezolvată

CENTRUL NAŢIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ - CERT-RO
AUTORITATEA COMPETENTĂ LA NIVEL NAŢIONAL PENTRU SECURITATEA REŢELELOR ŞI SISTEMELOR INFORMATICE
ATESTAT
AUDITOR DE SECURITATE CIBERNETICĂ (S/N) ..../..... din ...../...../20....

În aplicarea dispoziţiilor art. 20 lit. p) din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, cu modificările şi completările ulterioare,
în temeiul prevederilor art. 11 din Regulamentul pentru atestarea şi verificarea auditorilor de securitate cibernetică, aprobat prin Ordinul secretarului general al Guvernului nr. 559/2021,
în baza Raportului final de evaluare nr. ..... din ..../.../20..., întocmit de Autoritatea competentă la nivel naţional pentru securitatea reţelelor şi sistemelor informatice (ANSRSI),
.....,
(denumirea persoanei juridice/numele şi prenumele)
cu sediul/domiciliul în localitatea ....., judeţul ....., CUI/CNP ....., seria/nr. înregistrare RC/CI ....., este atestat ca:
AUDITOR DE SECURITATE CIBERNETICĂ

Înscris în Registrul naţional al auditorilor de securitate cibernetică/IDASC .....
Perioada de valabilitate: ...../...../20.... - ...../..../20.....
TIP ATESTAT: [ ] general/[ ] special/[ ] comun
Restricţii privind desfăşurarea activităţilor de audit speciale: [ ] Nu/[ ] Da
Activităţi de audit speciale calificate:
Audit cod sursă [AS3] [ ] Nu/[ ] Da | Audit de penetrare [AS4] [ ] Nu/[ ] Da

Director general, CERT-RO,
.....
(prenumele şi numele, semnătura şi ştampila)
Director, CERT-RO/ANSRSI,
.....
(prenumele şi numele, 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
.....
(numele şi prenumele)
DOMICILIU
Adresa .....
(strada nr., bl./clădire, et., ap., cod poştal)
Localitatea ...../Judeţul/Municipiul ...../Sectorul .....
DATE DE IDENTIFICARE
CNP ...../BI/CI ..... Seria ...../Număr .....
DATE DE CONTACT
Telefon ...../Fax ...../
E-mail ...../Web .....
ADRESĂ CORESPONDENŢĂ^1
^1 Se va completa numai dacă diferă de sediul/domiciliul solicitantului (specificat mai sus).
Adresa
.....
(strada nr., bl./clădire, et., ap., cod poştal)
Localitatea ...../Judeţul/Municipiul ...../Sectorul .....

B. Solicitare

În temeiul Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, cu modificările şi completările ulterioare (Legea NIS), solicit:
[ ] emiterea atestatului de auditor de securitate cibernetică.
Solicit următorul tip de atestat^2: [ ] general/[ ] special/[ ] comun.
^2 Se va marca cu „X“ tipul de atestat solicitat: general - pentru toate activităţile de audit ([AS1]-[AS5]) şi implicit [AS6]; special - numai pentru activităţile speciale ([AS3] şi [AS4]) şi parţial [AS6]; comun - pentru activităţile comune ([AS1], [AS2] şi [AS5]) şi parţial [AS6].

C. Acord prelucrare date^3

C.T.C.E. Piatra Neamţ

^3 În procesele interne, ANSRSI protejează interesele de securitate şi comerciale ale solicitanţilor/auditorilor de securitate cibernetică, precum şi confidenţialitatea informaţiilor furnizate de către aceştia.
Îmi exprim acordul cu privire la prelucrarea datelor cu caracter personal şi procesarea electronică a datelor de către Autoritatea competentă la nivel naţional pentru securitatea reţelelor şi sistemelor informatice (ANSRSI) în procesul de implementare şi 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

Numele şi prenumele: .....
Data: .....
Semnătura: .....

Informaţiile prelucrate în sensul îndeplinirii obligaţiilor de la art. 32 din Legea NIS nu fac parte din categoria informaţiilor de interes public aşa cum acestea sunt reglementate în Legea nr. 544/2001 privind liberul acces la informaţiile de interes public, cu modificările şi completările ulterioare.

CERERE
pentru emiterea atestatului de auditor de securitate cibernetică

Tip persoană: [ ] [juridică]

A. Date generale (identificare solicitant)

SOLICITANT
.....
(denumirea persoanei juridice)
SEDIUL
Adresa .....
(strada nr., bl./clădire, et., ap., cod poştal)
Localitatea ...../Judeţul/Municipiul ...../Sectorul .....
DATE DE IDENTIFICARE
CUI ...../Nr. înregistrare RN^1 .....
^1 Registrul comerţului; Registrul asociaţiilor şi fundaţiilor; Registrul federaţiilor etc.
DATE DE CONTACT
Telefon ...../Fax ...../
E-mail ...../Web .....
ADRESĂ CORESPONDENŢĂ^2
^2 Se va completa numai dacă diferă de sediul/domiciliul solicitantului (specificat mai sus).
Adresa
.....
(strada nr., bl./clădire, et., ap., cod poştal)
Localitatea ...../Judeţul/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 reţelelor şi sistemelor informatice, cu modificările şi completările ulterioare (Legea NIS), solicit:
[ ] emiterea atestatului de auditor de securitate cibernetică.
Solicit următorul tip de atestat^3: [ ] general/[ ] special/[ ] comun.
^3 Se va marca cu „X" tipul de atestat solicitat: general - pentru toate activităţile de audit ([AS1]-[AS5]) şi implicit [AS6]; special - numai pentru activităţile speciale ([AS3] şi [AS4]) şi parţial [AS6]; comun - pentru activităţile comune ([AS1], [AS2] şi [AS5]) şi parţial [AS6].
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

^4 În procesele interne, ANSRSI protejează interesele de securitate şi comerciale ale solicitanţilor/auditorilor de securitate cibernetică, precum şi confidenţialitatea informaţiilor furnizate de către aceştia.
Informaţiile prelucrate în sensul îndeplinirii obligaţiilor de la art. 32 din Legea NIS nu fac parte din categoria informaţiilor de interes public, aşa cum acestea sunt reglementate în Legea nr. 544/2001 privind liberul acces la informaţiile de interes public, cu modificările şi completările ulterioare.
Îmi exprim acordul cu privire la prelucrarea datelor cu caracter personal şi procesarea electronică a datelor de către Autoritatea competentă la nivel naţional pentru securitatea reţelelor şi sistemelor informatice (ANSRSI) în procesul de implementare şi 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

Numele şi prenumele: .....
Data: .....
Semnătura: .....

Anexa nr. 3

la regulament

CERERE
pentru renunţarea la atestatul de auditor de securitate cibernetică

Tip persoană: [ ] [fizică]

A. Date generale (identificare auditor)

SOLICITANT
Numele/prenumele .....
(numele şi prenumele)
IDASC^1 .....
^1 IDASC - Codul unic de identificare a auditorului de securitate cibernetică.
ADRESĂ CORESPONDENŢĂ
Adresa .....
(strada nr., bl./clădire, et., ap., cod poştal)
Localitatea ...../Judeţul/Municipiul ...../Sectorul .....
E-mail .....

B. Solicitare

În temeiul Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, cu modificările şi completările ulterioare (Legea NIS), solicit:
[ ] renunţarea la atestatul de auditor de securitate cibernetică.
Solicit renunţarea la următorul tip de atestat^2: [ ] general/[ ] special/[ ] comun.
^2 Se va marca cu „X" tipul de atestat solicitat: general - pentru toate activităţile de audit ([AS1] - [AS5]) şi implicit [AS6]; special - numai pentru activităţile speciale ([AS3] şi [AS4]) şi parţial [AS6]; comun - pentru activităţile comune ([AS1], [AS2] şi [AS5]) şi parţial [AS6].

C. Acord prelucrare date^3

^3 În procesele interne, ANSRSI protejează interesele de securitate şi comerciale ale auditorilor de securitate cibernetică, precum şi confidenţialitatea informaţiilor furnizate de către aceştia.
Îmi exprim acordul cu privire la prelucrarea datelor cu caracter personal şi procesarea electronică a datelor de către Autoritatea competentă la nivel naţional pentru securitatea reţelelor şi sistemelor informatice (ANSRSI) în procesul de implementare şi monitorizare a Legii NIS. [ ] Da

Numele şi prenumele: .....
Data: .....
Semnătura: .....

Informaţiile prelucrate în sensul îndeplinirii obligaţiilor de la art. 32 din Legea NIS nu fac parte din categoria informaţiilor de interes public, aşa cum acestea sunt reglementate în Legea nr. 544/2001 privind liberul acces la informaţiile de interes public, cu modificările şi completările ulterioare.

CERERE
pentru renunţarea la atestatul de auditor de securitate cibernetică

Tip persoană: [ ] [juridică]

A. Date generale (identificare auditor)

SOLICITANT

Denumire .....

(denumirea persoanei juridice)

IDASC^1 .....

^1 IDASC - codul unic de identificare a auditorului de securitate cibernetică.

ADRESĂ CORESPONDENŢĂ

Adresa .....

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

Localitatea ...../Judeţul/Municipiul ...../Sectorul .....

E-mail .....

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

1. Numele/prenumele ..... CNP ..... CI (S/N) ..... IDASC .....

....

n. Numele/prenumele ..... CNP ..... CI (S/N) ..... IDASC .....

C. Solicitare

În temeiul Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, cu modificările şi completările ulterioare (Legea NIS), solicit:

[ ] renunţarea la atestatul de auditor de securitate cibernetică.

Solicit renunţarea la următorul tip de atestat^2: [ ] general/[ ] special/[ ] comun.

^2 Se va marca cu „X“ tipul de atestat solicitat: general - pentru toate activităţile de audit ([AS1] - [AS5]) şi implicit [AS6]; special - numai pentru activităţile speciale ([AS3] şi [AS4]) şi parţial [AS6]; comun - pentru activităţile comune ([AS1], [AS2] şi [AS5]) şi parţial [AS6].

Solicitări privind personalul pentru care se solicită renunţarea atestat:

1. .../tip atestat la care se renunţă: [ ] general/[ ] special/[ ] comun;

....

n. .../tip atestat la care se renunţă: [ ] general/[ ] special/[ ] comun.

D. Acord prelucrare date^3

^3 În procesele interne, ANSRSI protejează interesele de securitate şi comerciale ale auditorilor de securitate cibernetică, precum şi confidenţialitatea informaţiilor furnizate de către aceştia.

Informaţiile prelucrate în sensul îndeplinirii obligaţiilor de la art. 32 din Legea NIS nu fac parte din categoria informaţiilor de interes public aşa cum acestea sunt reglementate în Legea nr. 544/2001 privind liberul acces la informaţiile de interes public, cu modificările şi completările ulterioare.

Îmi exprim acordul cu privire la prelucrarea datelor cu caracter personal şi procesarea electronică a datelor de către Autoritatea competentă la nivel naţional pentru securitatea reţelelor şi sistemelor informatice (ANSRSI) în procesul de implementare şi monitorizare a Legii NIS. [ ] Da

Numele şi prenumele: .....

Data: .....

Semnătura: .....

Anexa nr. 4

la regulament

CERERE

pentru reînnoirea atestatului de auditor de securitate cibernetică

Tip persoană: [ ] [fizică]

A. Date generale (identificare auditor)

SOLICITANT

Numele/prenumele .....

(numele, prenumele)

IDASC^1 .....

^1 IDASC - codul unic de identificare a auditorului de securitate cibernetică.

ADRESĂ CORESPONDENŢĂ

Adresa .....

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

Localitatea ...../Judeţul/Municipiul ...../Sectorul .....
E-mail .....

B. Solicitare

În temeiul Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, cu modificările şi completările ulterioare (Legea NIS), solicit:

[ ] reînnoirea atestatului de auditor de securitate cibernetică.

Solicit reînnoirea următorului tip de atestat^2: [ ] general/[ ] special/[ ] comun.

^2 Se va marca cu „X" tipul de atestat solicitat: general - pentru toate activităţile de audit ([AS1] - [AS5]) şi implicit [AS6]; special - numai pentru activităţile speciale ([AS3] şi [AS4]) şi parţial [AS6]; comun - pentru activităţile comune ([AS1], [AS2] şi [AS5]) şi parţial [AS6].

C. Acord prelucrare date^3

^3 În procesele interne, ANSRSI protejează interesele de securitate şi comerciale ale auditorului de securitate cibernetică, precum şi confidenţialitatea informaţiilor furnizate de către aceştia.

Îmi exprim acordul cu privire la prelucrarea datelor cu caracter personal şi procesarea electronică a datelor de către Autoritatea competentă la nivel naţional pentru securitatea reţelelor şi sistemelor informatice (ANSRSI) în procesul de implementare şi 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

Numele şi prenumele: .....
Data: .....
Semnătura: .....

Informaţiile prelucrate în sensul îndeplinirii obligaţiilor de la art. 32 din Legea NIS nu fac parte din categoria informaţiilor de interes public aşa cum acestea sunt reglementate în Legea nr. 544/2001 privind liberul acces la informaţiile de interes public, cu modificările şi completările ulterioare.

CERERE
pentru reînnoirea atestatului de auditor de securitate cibernetică

Tip persoană: [ ] [juridică]

A. Date generale (identificare entitate solicitantă)

SOLICITANT

Denumire .....
(denumirea persoanei juridice)
IDASC^1 .....

^1 IDASC - Codul unic de identificare a auditorului de securitate cibernetică.

ADRESĂ CORESPONDENŢĂ

Adresa .....
(strada nr., bl./clădire, et., ap., cod poştal)
Localitatea ...../Judeţul/Municipiul ...../Sectorul .....
E-mail .....

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

1. Numele/prenumele ..... CNP ..... CI (S/N) ..... IDASC .....
....
n. Numele/prenumele ..... CNP ..... CI (S/N) ..... IDASC .....

C. Solicitare

În temeiul Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, cu modificările şi completările ulterioare (Legea NIS), solicit:

[ ] reînnoirea atestatului de auditor de securitate cibernetică.

Solicit reînnoirea următorului tip de atestat^2: [ ] general/[ ] special/[ ] comun.

^2 Se va marca cu „X" tipul de atestat solicitat: general - pentru toate activităţile de audit ([AS1] - [AS5]) şi implicit [AS6]; special - numai pentru activităţile speciale ([AS3] şi [AS4]) şi parţial [AS6]; comun - pentru activităţile comune ([AS1], [AS2] şi [AS5]) şi parţial [AS6].

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

^3 În procesele interne, ANSRSI protejează interesele de securitate şi comerciale ale auditorului de securitate cibernetică, precum şi confidenţialitatea informaţiilor furnizate de către aceştia.

Îmi exprim acordul cu privire la prelucrarea datelor cu caracter personal şi procesarea electronică a datelor de către Autoritatea competentă la nivel naţional pentru securitatea reţelelor şi sistemelor informatice (ANSRSI) în procesul de implementare şi 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

Numele şi prenumele: .....

Data: .....

Semnătura: .....

Informaţiile prelucrate în sensul îndeplinirii obligaţiilor de la art. 32 din Legea NIS nu fac parte din categoria informaţiilor de interes public aşa cum acestea sunt reglementate în Legea nr. 544/2001 privind liberul acces la informaţiile de interes public, cu modificările şi completările ulterioare.

Anexa nr. 5

la regulament

LISTA

certificărilor profesionale^1

^1 Lista certificărilor profesionale va fi completată/actualizată, permanent, în baza evaluării realizate de Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO, în calitate de autoritate competentă la nivel naţional, şi vor fi publicate pe site-ul instituţiei.

#	Certificare	Activităţi 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

Anexa nr. 6

la regulament

ABILITĂŢI, APTITUDINI ŞI ACŢIUNI
specifice auditorilor de securitate cibernetică

I. Abilităţi

1. Comportament profesional

1.1. Auditorul de securitate cibernetică trebuie să posede abilităţi necesare pentru a-i permite să acţioneze în conformitate cu principiile auditului.

1.2. Auditorul de securitate cibernetică trebuie să prezinte un comportament profesional adecvat în timpul desfăşurării activităţilor de audit, iar în acest sens trebuie să fie:

a) etic - corect, veridic, sincer, cinstit şi discret;

b) raţional - dispus să ia în considerare idei sau puncte de vedere alternative;

c) diplomatic - tacticos în relaţiile cu indivizii;

d) observator - observarea activă a mediului fizic şi a activităţilor;

e) perceptiv - conştient şi capabil să înţeleagă situaţiile;

f) versatil - capabil să se adapteze cu uşurinţă la diferite situaţii;

g) tenace - persistent şi axat pe atingerea obiectivelor;

h) decisiv - capabil să ajungă la concluzii în timp util pe baza raţionamentului şi analizei logice;

i) autonom - capabil să acţioneze şi să funcţioneze independent în timp ce interacţionează eficient cu ceilalţi;

j) ferm - capabil să acţioneze responsabil şi etic, chiar dacă aceste acţiuni nu pot fi întotdeauna populare şi pot duce uneori la dezacord sau confruntare;

k) responsabil - dispus să înveţe din situaţii;

l) sensibil - observator şi respectuos faţă de cultura organizaţională a operatorului economic auditat;

m) cooperant - interacţionează eficient cu alţii, inclusiv cu membrii echipei de audit şi personalul operatorului economic auditat.

2. Cunoştinţe şi abilităţi

2.1. Auditorul de securitate cibernetică trebuie să aibă cunoştinţe şi abilităţi în domeniile:

a) Principii, procese şi metode de audit

Cunoştinţele şi abilităţile din acest domeniu permit auditorului de securitate cibernetică să se asigure că activităţile de audit sunt efectuate într-un mod consecvent şi sistematic, iar în acest sens trebuie:

– să înţeleagă tipurile de riscuri şi oportunităţi asociate activităţii de audit, precum şi principiile abordării auditului bazate pe managementul riscurilor;

– să planifice şi să organizeze munca eficient;

– să efectueze activitatea de audit în termenele convenite prin contractul de audit;

– să acorde prioritate şi să se concentreze pe chestiuni importante;

– să comunice eficient, oral şi în scris (fie personal, fie prin utilizarea interpreţilor);

– să colecteze informaţii prin interviuri eficiente, ascultare, observare şi revizuire a informaţiilor documentate, inclusiv înregistrări şi date;

– să înţeleagă şi să ia în considerare opiniile experţilor tehnici;

– să auditeze un proces de la început până la sfârşit, inclusiv interacţiunile cu alte procese şi diferite funcţii, după caz;

– să verifice relevanţa şi acurateţea informaţiilor colectate;

– să confirme suficienţa şi adecvarea dovezilor pentru a susţine constatările, concluziile şi recomandările pe timpul şi după misiunea de audit;

– să evalueze factorii care pot afecta fiabilitatea constatărilor, recomandărilor şi concluziilor auditului;

– să documenteze activităţile de audit, constatările pe timpul misiunii de audit şi raportul de audit;

– să păstreze confidenţialitatea şi securitatea informaţiilor.

b) Standarde şi specificaţii

Cunoştinţele şi abilităţile din acest domeniu permit auditorului de securitate cibernetică să înţeleagă sfera auditului de securitate, să aplice criteriile de audit şi să acopere următoarele:
– standardele sistemului de management sau alte documente normative sau de orientare/susţinere utilizate pentru stabilirea criteriilor sau metodelor de audit;
– standardele şi specificaţiile europene şi internaţionale utilizate în implementarea cerinţelor minime de securitate şi în activitatea auditorilor de securitate;
– aplicarea standardelor şi specificaţiilor europene şi internaţionale de către operatorul economic, respectiv operatorul de servicii esenţiale sau furnizorul de servicii digitale;
– relaţiile şi interacţiunile la nivelul reţelelor şi sistemelor informatice care stau la baza furnizării serviciilor esenţiale sau digitale;
– înţelegerea importanţei şi priorităţii multiplelor standarde sau referinţe;
– aplicarea standardelor sau referinţelor la diferite situaţii de audit.

c) Organizaţia şi contextul acesteia

Cunoştinţele şi abilităţile din acest domeniu permit auditorului de securitate cibernetică să înţeleagă structura, scopul şi practicile de management ale operatorului economic şi, în acest sens, trebuie să acopere următoarele:
– nevoile şi aşteptările părţilor interesate relevante care au impact asupra sistemului de management;
– tipul de organizaţie, guvernanţa, dimensiunea, structura, funcţiile şi relaţiile operatorului economic;
– concepte generale de afaceri şi management, procese şi terminologii conexe (inclusiv planificarea, bugetarea şi gestionarea resurselor umane) care stau la baza furnizării serviciilor esenţiale/digitale;
– aspectele culturale şi sociale ale operatorului economic.

d) Legalitate şi reglementare aplicabile

Cunoştinţele şi abilităţile din acest domeniu permit auditorului de securitate cibernetică să fie conştient de cerinţele organizaţiei şi de modul de organizare a activităţilor de lucru în cadrul acesteia. Cunoştinţele şi abilităţile specifice jurisdicţiei sau activităţilor, proceselor, produselor şi serviciilor auditate trebuie să acopere următoarele:
– cerinţele statutare, de reglementare şi guvernanţa acestora;
– terminologia juridică de bază;
– contracte şi răspunderi.

II. Aptitudini şi acţiuni specifice rolurilor echipei de audit

1. Şeful echipei de audit^1

^1 Rolul de şef 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 activităţile de audit conform art. 6 alin. (2) lit. a) din Regulament].

1.1. Acţiuni/Sarcini

1.1.1. Acţiuni:
– constituirea şi structurarea echipei de audit adaptată obiectivelor serviciului de audit furnizat în baza unui contract de audit.
– gestionarea misiunii de audit, prin/inclusiv:
• identificarea, stabilirea şi gestionarea priorităţilor pentru fiecare membru al echipei de audit;
• utilizarea eficientă a resurselor;
• gestionarea incertitudinii de atingere a obiectivelor auditului;
• protejarea sănătăţii şi siguranţei membrilor echipei de audit în timpul misiunii de audit, inclusiv asigurarea conformităţii auditorilor cu dispoziţiile relevante privind sănătatea şi securitatea în muncă;
• coordonarea şi controlul membrilor echipei de audit;
• prevenirea şi rezolvarea conflictelor şi problemelor care pot apărea în timpul auditului, inclusiv a celor din cadrul echipei de audit, după caz;
• dezvoltarea şi menţinerea unei relaţii de colaborare între membrii echipei de audit;
– sprijinirea operatorului economic în evaluarea impactului asupra reţelelor şi sistemelor informatice a ameninţărilor care ar putea exploata potenţialele vulnerabilităţi descoperite în timpul serviciului de audit furnizat, în special în ceea ce priveşte confidenţialitatea, integritatea şi disponibilitatea serviciului esenţial sau digital furnizat de către OE;
– formularea de recomandări adecvate pentru remedierea riscurilor care decurg din vulnerabilităţile descoperite;
– controlul calităţii produselor şi livrabilelor destinate informării operatorului economic, inclusiv pregătirea şi completarea raportului de audit de securitate.

1.2. Aptitudini

1.2.1. Competenţe:
– aprofundate în majoritatea domeniilor necesare auditorilor pe care îi supraveghează.

1.2.2. Calităţi:
– gestionarea unei echipe de auditori de securitate cibernetică;
– managementul priorităţilor;
– sintetizarea şi prezentarea informaţiilor utile pentru personalul tehnic şi nontehnic;
– scrierea unei documentaţii adaptate unor niveluri diferite de interlocutori (structuri tehnice, organisme de conducere, management instituţional etc.).

1.3. Abilităţi necesare pentru auditul sistemelor de control industrial

1.3.1. Competenţe:
– arhitecturi funcţionale bazate pe automate de comandă şi reglare programabile, respectiv sisteme de control industrial (ICS), sisteme pentru monitorizare, control şi achiziţie de date (SCADA) şi sisteme de control distribuite (DCS); controlere logice programabile (PLC);
– reţele industriale şi protocoale:
• topologia reţelelor industriale;
• partiţionarea reţelelor industriale faţă de alte reţele şi sisteme informatice;
• protocoale de transmisie şi comunicaţie utilizate de controlere logice programabile şi echipamente industriale (Modbus, S7, EtherNetIP, Profibus, Profinet, IEC 61850, OPC - clasic şi UA - etc.);
• tehnologii radio şi wireless din mediul industrial (inclusiv protocoale bazate pe stratul 802.15.4, respectiv Modelul OSI: nivelul 1 - Fizic şi nivelul 2 - Legături de date);
– funcţionalitatea diferitelor echipamente din sistemele de control industrial.

2. Auditorul pentru auditul arhitecturii

2.1. Acţiuni/Sarcini

2.1.1. Acţiuni:
– adoptarea unei viziuni globale a reţelelor şi sistemelor informatice pentru a identifica:
• vulnerabilităţile şi orice cale de atac asociată;
• elementele/componentele relevante care urmează a fi auditate;
– identificarea şi colectarea elementelor de arhitectură şi echipamentelor de reţea care urmează să fie auditate;
– auditarea configuraţiei echipamentelor de reţea alese anterior;
– dezvoltarea de instrumente adaptate ţintelor auditului, dacă este cazul;
– realizarea de interviuri cu administratorii de reţea;
– identificarea vulnerabilităţilor prezente în arhitectură şi în configuraţia echipamentului auditat;
– formularea de recomandări adecvate pentru remedierea riscurilor care decurg din vulnerabilităţile descoperite;
– valorificarea cunoştinţelor dobândite, oferirea de feedback şi răspunsuri către OE, precum şi elaborarea şi prezentarea unui raport de audit.

2.2. Aptitudini

2.2.1. Competenţe.
– reţele şi protocoale:
• protocoale şi infrastructuri de reţea;
• servicii de infrastructură;
• configurarea şi securizarea principalelor echipamente de reţea de pe piaţă;
• reţele de telecomunicaţii;
• tehnologie wireless;
• telefonie;
– echipamente şi software de securitate:
• firewall („ziduri de protecţie“);
• sisteme de backup („rezervă“);
• sisteme de stocare partajate;
• dispozitive de criptare a comunicaţiilor;
• servere de autentificare;
• servere proxy inversate;
• soluţii de gestionare a exploatării/utilizării reţelelor şi sistemelor informatice;
• sisteme/soluţii de detecţie şi prevenirea intruziunilor.

2.2.2. Calităţi:
– sintetizarea şi prezentarea informaţiilor utile pentru personalul tehnic şi non-tehnic;
– scrierea unei documentaţii adaptate unor niveluri diferite de interlocutori (structuri tehnice, organisme de conducere, management instituţional etc.);
– lucrul în echipă (schimb de cunoştinţe, colaborare tehnică şi ajutor reciproc).

2.3. Abilităţi necesare pentru auditul sistemelor de control industrial

2.3.1. Competenţe:
– arhitecturi funcţionale bazate pe automate de comandă şi reglare programabile, respectiv sisteme de control industrial (ICS), sisteme pentru monitorizare, control şi achiziţie de date (SCADA) şi sisteme de control distribuite (DCS); controlere logice programabile (PLC);
– reţele industriale şi protocoale:
• topologia reţelelor industriale;
• partiţionarea reţelelor industriale faţă de alte reţele şi sisteme informatice;
• protocoale de transmisie şi comunicaţie utilizate de controlere logice programabile şi echipamente industriale (Modbus, S7, EtherNetIP, Profibus, Profinet, IEC 61850, OPC - clasic şi UA - etc.);
• tehnologii radio şi wireless din mediul industrial (inclusiv protocoale bazate pe stratul 802.15.4, respectiv Modelul OSI: nivelul 1 - Fizic şi nivelul 2 - Legături de date);
– funcţionalitatea diferitelor echipamente din sistemele de control industrial.

3. Auditorul pentru auditul de configurare

3.1. Acţiuni/Sarcini:

3.1.1. Acţiuni:
– adoptarea unei viziuni globale a reţelelor şi sistemelor informatice pentru:
• a înţelege rolul infrastructurii care urmează să fie auditată;
• a identifica elementele/componentele relevante care urmează să fie auditate;
– identificarea şi colectarea elementelor de configurare ale echipamentelor de reţea care urmează să fie auditate;
– auditarea configuraţiei echipamentelor de reţea alese anterior;
– dezvoltarea de instrumente adaptate ţintelor auditului, dacă este cazul;
– realizarea de interviuri cu administratorii de sistem şi/sau de aplicaţii;
– identificarea vulnerabilităţilor prezente în configuraţia elementelor auditate;
– formularea de recomandări adecvate pentru remedierea riscurilor care decurg din vulnerabilităţile descoperite;
– valorificarea cunoştinţelor dobândite, oferirea de feedback şi răspunsuri către OE, precum şi elaborarea şi prezentarea unui raport de audit.

3.2. Aptitudini

3.2.1. Competenţe:
– reţele şi protocoale:
• protocoale şi infrastructuri de reţea;
• servicii de infrastructură;
• configurarea şi securizarea principalelor echipamente de reţea de pe piaţă;
• reţele de telecomunicaţii;
• tehnologie wireless;
• telefonie;
– echipamente şi software de securitate:
• firewall („ziduri de protecţie“);
• sisteme de backup („rezervă“);
• sisteme de stocare partajate;
• dispozitive de criptare a comunicaţiilor;
• servere de autentificare;
• servere proxy inversate;
• soluţii de gestionare a exploatării/utilizării reţelelor şi sistemelor informatice;
• sisteme/soluţii de detecţie şi prevenire a intruziunilor;
• software/soluţii de securitate client/server etc.;
– sisteme de operare (mediu şi avansat):
• sisteme Microsoft;
• sisteme UNIX/Linux;
• sisteme centralizate (de exemplu, bazate pe OS/400 sau z/OS);
• soluţii de virtualizare;
– aplicaţii (Model OSI: nivelul 7 - Aplicaţie):
• aplicaţii de tip client/server;
• limbaje de programare utilizate pentru configurare (de exemplu: scripturi, filtre WMI etc.);
• mecanisme criptografice;
• baze de date şi aplicaţii:
– servere web;
– servere de aplicaţii;

– sisteme de gestionare a bazelor de date;
– pachete software;
– tehnici de intruziune.

3.2.2. Calităţi:
– sintetizarea şi prezentarea informaţiilor utile pentru personalul tehnic şi nontehnic;
– scrierea unei documentaţii adaptate unor niveluri diferite de interlocutori (structuri tehnice, organisme de conducere, management instituţional etc.);
– lucrul în echipă (schimb de cunoştinţe, colaborare tehnică şi ajutor reciproc).

3.3. Abilităţi necesare pentru auditul sistemelor de control industrial

3.3.1. Competenţe:
– reţele industriale şi protocoale:
• protocoale de transmisie şi comunicaţie utilizate de controlere logice programabile şi echipamente industriale (Modbus, S7, EtherNetIP, Profibus, Profinet, IEC 61850, OPC - clasic şi UA - etc.);
• tehnologii radio şi wireless din mediul industrial (inclusiv protocoale bazate pe stratul 802.15.4, respectiv Modelul OSI: nivelul 1 - Fizic şi nivelul 2 - Legături de date);
– echipamente:
• configurarea şi securizarea principalelor controlere logice programabile (PLC) şi echipamente de control industriale de pe piaţă.

4. Auditorul pentru auditul codului sursă

4.1. Acţiuni/Sarcini

4.1.1. Acţiuni:
– adoptarea unei viziuni globale a reţelelor şi sistemelor informatice pentru a înţelege rolul aplicaţiei care urmează a fi auditată;
– identificarea în cadrul aplicaţiei a elementelor relevante care urmează a fi auditate în cadrul codului sursă;
– auditarea codului sursă;
– dezvoltarea de instrumente adaptate ţintelor auditului, dacă este cazul;
– realizarea de interviuri cu dezvoltatorii de aplicaţii;
– utilizarea de tehnici de inginerie inversă, dacă este cazul;
– identificarea vulnerabilităţilor prezente în codul sursă auditat;
– formularea de recomandări adecvate pentru remedierea riscurilor care decurg din vulnerabilităţile descoperite;
– valorificarea cunoştinţelor dobândite, oferirea de feedback şi răspunsuri către OE, precum şi elaborarea şi prezentarea unui raport de audit.

4.2. Aptitudini

4.2.1. Competenţe:
– aplicaţii (Model OSI: nivelul 7 - Aplicaţie):
• ghiduri şi principii de dezvoltare a securităţii/siguranţei aplicaţiei;
• arhitecturi de aplicaţii [client/server, multinivel („n-tier“) etc.];
• limbaje de programare;
• mecanisme criptografice;
• mecanisme de comunicare (interne sistemului şi prin reţea) şi protocoale asociate;
• baze de date/aplicaţii:
– servere web;
– servere de aplicaţii;
– sisteme de gestionare a bazelor de date;
– pachete software;
– atacuri cibernetice:
• principiile şi metodele de intruziune în aplicaţii;
• eludarea măsurilor de securitate software;
• exploatarea vulnerabilităţilor şi eliminarea tehnicilor de privilegii.

4.2.2. Calităţi:
– sintetizarea şi prezentarea informaţiilor utile pentru personalul tehnic şi non-tehnic;
– scrierea unei documentaţii adaptate unor niveluri diferite de interlocutori (structuri tehnice, organisme de conducere, management instituţional etc.);
– lucrul în echipă (schimb de cunoştinţe, colaborare tehnică şi ajutor reciproc).

4.3. Abilităţi necesare pentru auditul sistemelor de control industrial

4.3.1. Competenţe:
– arhitecturi funcţionale bazate pe controlere logice programabile (PLC);

– arhitecturi de aplicaţii SCADA (bazate sau nu pe un pachet software);
– arhitecturi de aplicaţii ale programelor de utilizator prezente în controlere programabile industriale;
– reţele industriale şi protocoale:
• protocoale de transmisie şi comunicaţie utilizate de controlere logice programabile şi echipamente industriale (Modbus, S7, EtherNetIP, Profibus, Profinet, IEC 61850, OPC - clasic şi UA - etc.).

5. Auditorul pentru auditul de penetrare

5.1. Acţiuni/Sarcini

5.1.1. Acţiuni:
– adoptarea unei viziuni globale a sistemului informaţional pentru a identifica:
• ţintele 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 permiţând executarea scenariilor de atac alese;
– efectuarea de atacuri relevante asupra infrastructurii ţintă;
– dezvoltarea de instrumente adaptate ţintelor atacate, dacă este necesar;
– utilizarea de tehnici de inginerie inversă, după caz;
– identificarea vulnerabilităţilor prezente în orice element al infrastructurii care permite efectuarea atacurilor;
– formularea de recomandări adecvate pentru remedierea riscurilor care decurg din vulnerabilităţile descoperite;
– valorificarea cunoştinţelor dobândite, oferirea de feedback şi răspunsuri către OE, precum şi elaborarea şi prezentarea unui raport de audit.

5.2. Aptitudini

5.2.1. Competenţe:
– reţele şi protocoale:
• protocoale şi infrastructuri de reţea;
• servicii de infrastructură;
• configurarea şi securizarea principalelor echipamente de reţea de pe piaţă;
• reţele de telecomunicaţii;
• tehnologie wireless;
• telefonie;
– echipamente şi software de securitate:
• firewall („ziduri de protecţie“);
• sisteme de backup („rezervă“);
• sisteme de stocare partajate;
• dispozitive de criptare a comunicaţiilor;
• servere de autentificare;
• servere proxy inversate;
• soluţii de gestionare a exploatării/utilizării reţelelor şi sistemelor informatice;
• sisteme/soluţii de detecţie şi prevenirea intruziunilor;
• software/soluţii de securitate client/server etc.;
– sisteme de operare:
• sisteme Microsoft;
• sisteme UNIX/Linux;
• sisteme centralizate (de exemplu, bazate pe OS/400 sau z/OS);
• soluţii de virtualizare;
– aplicaţii (Model OSI: nivelul 7 - Aplicaţie):
• ghiduri şi principii de dezvoltare a securităţii/siguranţei;
• aplicaţii de tip client/server;
• limbaje de programare pentru auditurile de cod;
• mecanisme criptografice;
• mecanisme de comunicare (interne sistemului şi prin reţea) şi protocoale asociate;
• baze de date şi aplicaţii:
– servere web;
– servere de aplicaţii;
– sisteme de gestionare a bazelor de date;
– pachete software;
– atacuri cibernetice:
• principiile şi metodele de intruziune în aplicaţii;
• eludarea măsurilor de securitate software;

• exploatarea vulnerabilităţilor şi eliminarea tehnicilor de privilegii.

5.2.2. Calităţi:

– sintetizarea şi prezentarea informaţiilor utile pentru personalul tehnic şi non-tehnic;

– scrierea unei documentaţii adaptate unor niveluri diferite de interlocutori (structuri tehnice, organisme de conducere, management instituţional etc.);

– lucrul în echipă (schimb de cunoştinţe, colaborare tehnică şi ajutor reciproc).

5.3. Abilităţi necesare pentru auditul sistemelor de control industrial

Competenţe:

– arhitecturi funcţionale bazate pe controlere logice programabile (PLC):

– reţele industriale şi protocoale:

• topologia reţelelor industriale;

• partiţionarea reţelelor industriale faţă de alte reţele şi sisteme informatice;

• protocoale de transmisie şi comunicaţie utilizate de controlere logice programabile şi echipamente industriale (Modbus, S7, EtherNetIP, Profibus, Profinet, IEC 61850, OPC - clasic şi UA - etc.);

• tehnologii radio şi wireless din lumea industrială (inclusiv protocoale bazate pe stratul 802.15.4, respectiv Modelul OSI: nivelul 1 - Fizic şi nivelul 2 - Legături de date);

– echipamente:

• configurarea şi securizarea principalelor controlere logice programabile (PLC) şi echipamente de control industriale de pe piaţă.

6. Auditorul pentru auditul securităţii organizaţiei

6.1. Acţiuni/Sarcini

6.1.1. Acţiuni:

– adoptarea unei viziuni globale a organizaţiei pentru a identifica:

• politicile şi procesele relevante care urmează să fie auditate;

• locurile relevante care urmează să fie auditate;

• vulnerabilităţile şi orice cale de atac fizică asociată;

– colectarea documentelor asociate proceselor care urmează să fie auditate;

– auditarea proceselor şi locaţiilor alese anterior;

– desfăşurarea de interviuri cu managerii de proces şi responsabilii cu securitatea, inclusiv responsabilii NIS;

– identificarea vulnerabilităţilor prezente în procesele şi arhitectura fizică a locurilor auditate;

– formularea de recomandări adecvate pentru remedierea riscurilor care decurg din vulnerabilităţile descoperite;

– valorificarea cunoştinţelor dobândite, oferirea de feedback şi răspunsuri către OE, precum şi elaborarea şi prezentarea unui raport de audit.

6.2. Aptitudini

6.2.1. Competenţe:

– cunoaşterea şi stăpânirea standardelor tehnice;

– cunoaşterea şi stăpânirea cadrului normativ:

• lista standardelor şi specificaţiilor europene şi internaţionale (LSSEINIS);

• actele de reglementare referitoare la securitatea reţelelor şi sistemelor informatice, la activitatea de audit de securitate cibernetică, precum şi cele conexe^2;

^2 În special normele referitoare la protecţia datelor cu caracter personal, la secretul profesional, la protecţia corespondenţei, la atacurile asupra intereselor fundamentale ale naţiunii, la terorism şi atacurile asupra siguranţei publice, la proprietatea intelectuală privind utilizarea mijloacelor de criptografie, patrimoniul ştiinţific şi tehnic naţional.

– cunoaşterea şi stăpânirea domeniilor legate de organizarea securităţii reţelelor şi sistemelor informatice:

• analiza riscurilor;

• politica de securitate a reţelelor şi sistemelor informatice;

• lanţuri de responsabilitate pentru asigurarea securităţii reţelelor şi sistemelor informatice;

• securitatea resursei umane;

• gestionarea funcţionării şi administrării reţelelor şi sistemelor informatice;

• control logic al accesului la reţelele şi sistemele informatice;

• dezvoltarea şi întreţinerea aplicaţiilor informatice;

• gestionarea incidentelor de securitate a informaţiei;

• gestionarea planului de continuitate a activităţii organizaţiei;

• securitate fizică;

– cunoaşterea şi stăpânirea practicilor legate de audit:

• întreţinere;

• vizită la faţa locului;

• analiză documentară.

6.2.2. Calităţi;

– sintetizarea şi prezentarea informaţiilor utile pentru personalul tehnic şi nontehnic;

– scrierea unei documentaţii adaptate unor niveluri diferite de interlocutori (structuri tehnice, organisme de conducere, management instituţional etc.);

– lucrul în echipă (schimb de cunoştinţe, colaborare tehnică şi ajutor reciproc).

6.3. Abilităţi necesare pentru auditul sistemelor de control industrial

6.3.1. Competenţe:

– să fie familiarizat cu următoarele subiecte:

• standarde de siguranţă/securitate funcţională pentru sistemele de control industrial;

• arhitecturi funcţionale bazate pe controlere logice programabile (PLC);

• rolurile şi utilizarea protocoalelor industriale;

• cunoaşterea rolului funcţional al diferitelor echipamente.

Anexa nr. 7

la regulament

CERINŢE ŞI RECOMANDĂRI
privind întocmirea raportului de audit de securitate

I. Cerinţe privind conţinutul raportului de audit de securitate

#	CERINŢE	OBSERVAŢII
1.	Titlul raportului	Raport de audit de securitate (RASEC) ....
2.	Beneficiarii /Destinatarii raportului, restricţii privind conţinutul şi circulaţia raportului	Se vor preciza datele cu privire la contractul de furnizare servicii de audit, destinatarul(ii) RASEC şi modul de circulaţie a acestuia.
3.	Identificarea operatorului economic	Identificarea operatorului economic (operator de servicii esenţiale - OSE sau furnizor de servicii digitale - FSD) supus misiunii de audit (denumirea/CUI/numărul de înregistrare la Oficiul Naţional al Registrului Comerţului/adresa etc.) Identificarea serviciilor esenţiale şi digitale furnizate pe baza reţelelor şi sistemelor informatice auditate Includerea afirmaţiei că reţelele şi sistemele informatice au fost auditate ca urmare a obligaţiei legale impuse de Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, cu modificările şi completările ulterioare (Legea NIS), de Normele tehnice privind cerinţele minime de asigurare a securităţii reţelelor şi sistemelor informatice aplicabile operatorilor de servicii esenţiale, respectiv furnizorilor de servicii digitale şi de Regulamentul pentru atestarea şi verificarea auditorilor de securitate cibernetică.
4.	Tipul serviciului de audit furnizat/ efectuat	Se va preciza tipul de serviciu de audit efectuat, respectiv în condiţiile Legii NIS sau în afara condiţiilor Legii NIS. Aşa 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 responsabilităţii conducerii operatorului economic	Se va preciza faptul că managementul operatorului economic (reprezentanţii legali) îşi asumă responsabilităţile cu privire la implementarea recomandărilor stabilite prin auditul efectuat asupra reţelelor şi sistemelor informatice şi reducerea riscurilor de securitate.
6.	Responsabilitatea auditorilor de securitate cibernetică	RASEC va include cel puţin afirmaţiile că: - „este responsabilitatea auditorului de securitate cibernetică să exprime o opinie cu privire la conformitatea reţelelor şi sistemelor informatice cu prevederile Normelor tehnice privind cerinţele minime de asigurare a securităţii reţelelor şi sistemelor informatice aplicabile operatorilor de servicii esenţiale, respectiv furnizorilor de servicii digitale şi ale prezentului regulament..."; - „raportul de audit de securitate a fost elaborat în conformitate cu standardul de audit utilizat, respectiv ..... (menţionarea acestuia)".
7.	Identificare auditori de securitate cibernetică	Datele de identificare ale şefului echipei de audit, precum şi ale membrilor echipei: - numele, prenumele, telefon, fax, adresa de e-mail şi adresa unde îşi desfăşoară activitatea etc.
8.	Semnături	Semnătura şefului echipei de audit şi a auditorilor pentru fiecare activitate de audit de securitate desfăşurată
9.	Obiectivele auditului de securitate	Obiectivele generale şi individualizate pe fiecare activitate de audit ([AS1] ÷ [AS6])
10.	Perioada desfăşurării auditului de securitate	Se va preciza perioada în care s-a realizat auditul.
11.	Data elaborării şi prezentării raportului de audit de securitate	Se va preciza data întocmirii RASEC, precum şi data şedinţei de închidere şi prezentare a acestuia.

12.	Locaţii de desfăşurare a auditului de securitate	Se vor specifica locaţiile, pe fiecare activitate de audit, unde s-a desfăşurat misiunea de audit; adresa sediului central /sucursalei/filialei etc.
13.	Descrierea domeniului/sferei de audit	Identificarea reţelelor şi sistemelor informatice utilizate de către operatorul economic pentru furnizarea serviciilor esenţiale sau digitale ..... (menţionarea denumirii SE/SD) Pentru reţelele şi sistemele informatice supuse auditului de securitate se vor menţiona următoarele: - măsurile organizatorice: politicile aplicabile şi procedurile implementate; - un sumar conţinând analiza riscurilor aferente furnizării de SE/SD, a posibilelor deficienţe ale reţelelor şi sistemelor auditate şi a măsurilor de reducere a riscurilor asociate, în baza cerinţelor minime de securitate implementate conform prevederilor Normelor tehnice privind cerinţele minime de asigurare a securităţii reţelelor şi sistemelor informatice aplicabile operatorilor de servicii esenţiale, 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/acţiune asumat de operatorul economic rezultat în urma activităţii de audit de securitate anterioare, dacă este cazul Se va verifica modul de implementare a măsurilor şi respectarea termenelor asumate prin RASEC anterior.
15.	Evaluarea anuală a riscurilor operaţionale	Referiri cu privire la modul de efectuare de către operatorul economic a evaluării anuale a riscurilor operaţionale generate de utilizarea reţelelor şi sistemelor informatice importante Se va verifica şi opina cu privire la plauzibilitatea metodologiei/tehnicilor utilizate, precum şi asupra măsurilor de control implementate în vederea gestionării riscurilor operaţionale identificate.
16.	Testarea de penetrare	Se vor menţiona/prezenta date cu privire la rezultatul obţinut în urma efectuării testării de penetrare. Conform raportului de securitate a testării şi evaluare a securităţii reţelelor şi sistemelor informatice - auditul de penetrare, se consemnează în RASEC următoarele elemente: - nr. de înregistrare/data raportului privind testarea de penetrare: - perioada în care s-au desfăşurat testări de penetrare; - descrierea metodologiei/tehnicilor utilizate; - menţionarea rezultatelor obţinute în urma testării; - concluziile raportului; - recomandările transmise operatorului economic şi răspunsul managementului acestuia.
17.	Opinia auditorului de securitate cibernetică	Afirmaţia 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 desfăşurată. Alte anexe

II. Recomandări privind întocmirea raportului de audit de securitate

1. Sumarul observaţiilor

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

a) descrierea neconformităţii/constatării;

b) importanţa neconformităţii/constatării;

c) riscurile asociate;

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

e) planul de acţiune asumat de către operatorul economic auditat, care conţine măsurile propuse, termenul de implementare şi persoanele responsabile de implementare.

2. Analiza şi managementul riscurilor

În ceea ce priveşte analiza internă şi 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 reţelelor şi 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 informaţiei şi comunicaţiilor externalizate pentru reţelele şi sistemele informatice auditate

Serviciile furnizate de terţi pentru funcţionarea optimă a reţelelor şi sistemelor informatice care stau la baza furnizării serviciilor esenţiale/digitale vor fi identificate şi prezentate în RASEC, în anexă, de către auditorul de securitate cibernetică.

4. Testarea şi evaluarea securităţii reţelelor şi sistemelor informatice

Raportul va fi redactat în limba română şi semnat numai de către un auditor de securitate cibernetică atestat pentru aplicarea activităţii de audit speciale.

Raportul trebuie să cuprindă cel puţin următoarele:

a) sumar executiv, în care să fie redată opinia auditorului de securitate a reţelelor şi sistemelor informatice referitoare la climatul general de securitate al ecosistemului evaluat;
b) concluzii privind impactul vulnerabilităţilor identificate asupra serviciilor esenţiale/digitale;
c) recomandări generale de îmbunătăţire a climatului de securitate a reţelelor şi sistemelor informatice;
d) metodologia de testare folosită;
e) tipul fiecărei vulnerabilităţi identificate;
f) descriere generală a fiecărei vulnerabilităţi identificate;
g) impactul exploatării cu succes a fiecărei vulnerabilităţi identificate;
h) recomandări de eliminare/mitigare a fiecărei vulnerabilităţi identificate;
i) detalii tehnice ale fiecărei vulnerabilităţi identificate;
j) elemente tehnice specifice care să permită reproducerea fiecărei vulnerabilităţi identificate.

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

Raportul trebuie să cuprindă cel puţin următoarele:
a) modul de respectare a cerinţelor minime de securitate impuse prin normele tehnice;
b) recomandări privind modul de remediere a neconformităţilor identificate;
c) termene privind remedierea şi modul de raportare/ notificare a CERT-RO în calitate de autoritate competentă la nivel naţional pentru securitatea reţelelor şi sistemelor informatice sau a altor autorităţi, după caz.

Anexa nr. 8

la regulament

RECOMANDĂRI
privind furnizarea/desfăşurarea auditului de securitate

I. Furnizarea unui serviciu de audit de securitate

1. În cazul în care operatorul economic este o instituţie publică centrală sau un deţinător de infrastructuri cibernetice de interes naţional, acesta poate solicita sprijinul Autorităţii competente la nivel naţional pentru securitatea reţelelor şi sistemelor informatice (ANSRSI) în procesul de definire/stabilire a specificaţiilor care fac obiectul unei cereri de oferte sau al unui contract de audit de securitate.

2. Operatorul economic trebuie să îşi aleagă auditorul de securitate cibernetică atestat valabil din lista auditorilor de securitate cibernetică publicată de ANSRSI pe site-ul instituţiei la pagina autorităţii.

3. Pentru a beneficia de un serviciu de audit calificat, adică conform cerinţelor prezentului regulament, operatorul economic trebuie:
– să aleagă un auditor de securitate cibernetică din lista auditorilor de securitate cibernetică; şi
– să 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 îşi păstrează dreptul de a efectua servicii necalificate. Utilizarea unui auditor de securitate cibernetică din lista auditorilor de securitate cibernetică atestaţi este, prin urmare, o condiţie 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 şi 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, activităţile de audit pentru care auditorul de securitate cibernetică este atestat şi 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 desfăşurarea auditului de securitate.

7. Operatorul economic poate, în conformitate cu prezentul regulament şi Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, cu modificările şi completările ulterioare - Legea NIS, să depună o reclamaţie/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 cerinţe din prezentul regulament ca parte a unui serviciu de audit calificat.

8. Dacă, după examinarea reclamaţiei/sesizării, se dovedeşte că auditorul de securitate cibernetică nu a respectat una sau mai multe cerinţe din prezentul regulament pe timpul furnizării unui serviciu de audit calificat, în funcţie 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 deţine informaţii clasificate şi, prin urmare, nu înlocuieşte autorizaţia de acces la informaţii clasificate.

II. Recomandări generale privind auditul de securitate

1. Auditul de securitate trebuie să fie cât mai cuprinzător şi să ţină seama de constrângerile bugetare şi de timp alocate pentru desfăşurarea acestuia.

2. Stabilirea duratei auditului de securitate pentru echipa de audit/auditor trebuie adaptată în funcţie de:

– sfera auditului şi complexitatea acestuia;

– cerinţele de securitate aşteptate de la reţelele şi sistemele informatice auditate.

3. Pentru a reduce volumul total al elementelor/ componentelor reţelelor şi sistemelor informatice care urmează să fie auditate şi, prin urmare, costul auditului şi, în acelaşi timp, menţinerea domeniului relevant de audit, eşantionarea ar trebui efectuată respectând următoarele principii:

– pentru auditurile de configurare sunt auditate doar serverele sensibile: controlere de domeniu Active Directory, servere de fişiere, servere de infrastructură (DNS, SMTP etc.), servere de aplicaţii etc.;

– pentru auditul codului sursă sunt auditate doar părţile 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 „preproducţie“) pentru a evita consecinţele unor eventuale defecţiuni într-un mediu de producţie. Cu toate acestea, pentru a asigura relevanţa auditului, auditorul de securitate cibernetică trebuie să se asigure că acest mediu este similar cu cel de producţie.

Aplicabilitatea rezultatelor auditurilor tehnice în mediul de producţie ar trebui verificată. Arhitectura, configuraţia, codul sursă şi auditurile securităţii organizaţiei ar trebui efectuate în mediul de producţie.

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 reţelelor şi sistemelor informatice (ţinte) auditate. Această recomandare este fundamentală în cazul auditului sistemelor de control industrial.

III. Recomandări pe timpul desfăşurării auditului de securitate

1. Operatorul economic va desemna un responsabil pentru gestionarea relaţiei cu auditorul de securitate cibernetică care furnizează serviciul de audit (echipa de audit) şi monitorizarea procesului de desfăşurare a misiunii de audit (planuri de lucru, autorizaţii etc.).

2. Operatorul economic va lua toate măsurile de salvgardare necesare pentru a-şi proteja reţelele şi sistemele informatice, inclusiv datele/informaţiile înainte şi în timpul misiunii de audit. Acest proces trebuie să se desfăşoare în colaborare cu auditorul de securitate cibernetică pentru a nu interfera cu activităţile de audit; în special specialiştii operatorului economic nu trebuie să submineze integritatea urmelor colectate.

3. Pentru a evita orice denunţare a furtului sau a încălcării încrederii, operatorul economic va evita să ofere sau să accepte folosirea de către auditorul de securitate cibernetică de echipamente nonproprietate pentru utilizarea în scopuri profesionale (BYOD^1) în absenţa proprietarului echipamentului sau fără acordul său.

^1 Bring Your Own Device = Aduceţi propriul dispozitiv.

4. Operatorul economic va informa, pe tot parcursul misiunii de audit, auditorul de securitate cibernetică cu privire la acţiunile pe care le efectuează asupra reţelelor şi sistemelor informatice (operaţiuni de administrare, garanţii etc.) care ar putea afecta furnizarea serviciului de audit.

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

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

IV. Tipuri de audit recomandate

1. Autoritatea competentă la nivel naţional pentru securitatea reţelelor şi sistemelor informatice recomandă auditorilor de securitate cibernetică să furnizeze/solicite înscrierea în contractul de audit pentru desfăşurarea unui audit de securitate următoarele tipuri de audit:

– auditul unei aplicaţii informatice:

• audit cod sursă;

• audit de configurare (server de aplicaţii, server HTTP, bază de date etc.);

– auditul unui centru de date:

• audit arhitectură (legătură între diferitele zone şi entităţi, filtrare etc.);

• audit de configurare (echipamente de reţea şi securitate, servere de infrastructură);

• audit securitate organizaţie;
– auditul unei reţele informatice:
• audit arhitectură;
• audit de configurare (staţii de lucru de birou, echipamente de reţea, servere de birou, servere AD etc.);
• audit securitate organizaţie;
– auditul unei platforme de telefonie:
• audit arhitectură;
• audit de configurare (echipamente de reţea şi securitate, IPBX, telefoane etc.);
– auditul unei platforme de virtualizare:
• audit arhitectură;
• audit de configurare (echipamente de reţea şi securitate, sisteme de virtualizare etc.);
– auditul unui sistem de control industrial, inclusiv sala de control:
• audit arhitectură;
• audit de configurare (controlere logice programabile industriale, senzori/activatori, servere de aplicaţii, staţii operator, staţii de inginerie, console de programare, echipamente de reţea şi securitate, servere de autentificare etc.);
• audit securitate organizaţie;
• audit cod sursă (controlere logice programabile industriale, console, sisteme încorporate, aplicaţii de afaceri etc.)
Lista nu este exhaustivă şi 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 se includă activitatea de audit de penetrare (testarea de penetrare).
3. Auditul de penetrare (testarea de penetrare) nu trebuie efectuat niciodată singur şi 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 şi după ce riscurile au fost evaluate şi controlate, iar responsabilităţile au fost stabilite în mod clar.

Anexa nr. 9

la regulament

CERINŢELE SPECIFICE
activităţilor de audit de securitate

Generalităţi

1. Pe timpul desfăşurării activităţilor de audit, desfăşurate în baza contractului de audit, operatorul economic şi auditorii de securitate cibernetică trebuie să respecte cerinţele specifice stabilite în această anexă, respectiv de la [CAS1] la [CAS6].
2. Activităţile tehnice descrise la [CAS1] până la [CAS4] nu exclud evaluarea securităţii organizaţiei, respectiv securitatea logică şi fizică a domeniului auditat. Această evaluare constă în verificarea faptului că politicile şi procedurile de securitate definite pentru asigurarea cerinţelor minime de securitate a reţelelor şi sistemelor informatice auditate sunt conforme cu nivelul tehnicii.
3. Activităţile tehnice de la [CAS6], auditul sistemelor de control industrial, presupun atingerea cerinţelor specifice prin cerinţele stabilite la [CAS1] până la [CAS5].
4. Cerinţele enunţate de la [CAS1] la [CAS5] sunt date cu titlu informativ şi nu sunt exhaustive. În plus, acestea trebuie efectuate numai atunci când sunt aplicabile reţelelor şi sistemelor informatice auditate.

[CAS1]. Cerinţe specifice auditului arhitecturii

1. Acţiuni ale OE
Operatorul economic trebuie să furnizeze auditorului de securitate cibernetică elementele de arhitectură şi configurare a reţelelor şi sistemelor informatice auditate.
2. Acţiuni tehnice ale ASI
Auditorul de securitate cibernetică trebuie să revizuiască/ auditeze următoarele documente atunci când acestea există:
– diagramele arhitecturale de nivel 2 şi 3 corespunzătoare Modelului OSI (interconectarea sistemelor deschise /Open Systems Interconnection);
– matricea fluxurilor;
– regulile de filtrare;
– configurarea echipamentelor de reţea (routere şi comutatoare);

– interconectări cu reţele terţe sau internet;
– analizele de risc ale reţelelor şi sistemelor informatice;
– documentele de arhitectură tehnică legate de ţinta auditului.

3. Comunicarea dintre ASI şi OE

Auditorul de securitate cibernetică trebuie să poată organiza interviuri cu personalul implicat în stabilirea şi administrarea reţelelor şi sistemelor informatice auditate, în special în ceea ce priveşte procedurile de administrare.

[CAS2]. Cerinţe specifice auditului de configurare

1. Acţiuni ale OE

Operatorul economic trebuie să furnizeze auditorului de securitate cibernetică elementele de configurare ale reţelelor şi sistemelor informatice auditate. Elementele de configurare pot fi identificate manual sau automat, folosind „acces privilegiat“, sub formă de fişiere de configurare sau capturi de ecran.

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

2. Acţiuni tehnice ale ASI

Auditorul de securitate cibernetică trebuie să verifice securitatea configuraţiilor, în conformitate cu stadiul tehnicii, cerinţele minime de asigurare a securităţii reţelelor şi sistemelor informatice şi regulile specifice ale OE, respectiv a:

– echipamentelor de reţea cu fir sau fără fir (cum ar fi switchuri sau routere);
– echipamentelor de securitate (tip firewall sau releu invers, filtrare sau nu, şi regulile lor de filtrare, criptare etc.);
– sistemelor de operare;
– sistemelor de gestionare a bazelor de date;
– serviciilor de infrastructură;
– serverelor de aplicaţii;
– staţiilor de lucru;
– echipamentelor de telefonie;
– mediilor de virtualizare.

3. Comunicarea dintre ASI şi OE

Auditorul de securitate cibernetică trebuie să poată organiza interviuri cu personalul implicat în stabilirea şi administrarea reţelelor şi sistemelor informatice auditate, în special în ceea ce priveşte standardele de configurare.

[CAS3]. Cerinţe specifice auditului codului sursă

1. Acţiuni ale OE

Operatorul economic trebuie să furnizeze auditorului de securitate cibernetică: codul sursă, documentaţia referitoare la implementare, metodele şi rapoartele de testare şi arhitectura reţelelor şi sistemelor informatice auditate, precum şi configuraţia elementelor de compilare şi de execuţie, în limitele drepturilor operatorului economic.

2. Acţiuni tehnice ale ASI

Auditorul de securitate cibernetică trebuie:

– să verifice securitatea părţilor din codul sursă referitoare la:
• mecanisme de autentificare;
• mecanisme criptografice;
• gestionarea utilizatorilor;
• controlul accesului la resurse;
• interacţiuni cu alte aplicaţii;
• relaţii cu sistemele de gestionare a bazelor de date;
• respectarea cerinţelor de securitate referitoare la mediul în care este implementată aplicaţia;
– să verifice cele mai frecvente vulnerabilităţi în următoarele domenii:
• scripturi între site-uri;
• injecţii SQL;
• falsificare a cererilor între site-uri;
• erori logice ale aplicaţiei;
• depăşirea bufferului;
• executarea comenzilor arbitrare;
• includerea fişierelor (local sau la distanţă);
– să respecte regulile specifice de audit, respectiv trebuie:
• să efectueze o analiză de securitate a aplicaţiei auditate pentru a limita auditul la părţile critice ale codului său;

• să prevină scurgerile de informaţii şi modificări în funcţionarea reţelelor şi sistemelor informatice;
• să efectueze activitate manual sau automat folosind instrumente specializate. Fazele automatizate, precum şi instrumentele utilizate trebuie identificate în livrabile şi, în special, în raportul de audit.

3. Comunicarea dintre ASI şi OE

Auditorul de securitate cibernetică va efectua interviuri cu unul dintre dezvoltatori/programatori sau persoana responsabilă de implementarea codului sursă auditat pentru a avea informaţii referitoare la contextul aplicaţiei, nevoile de securitate şi practicile de dezvoltare.

[CAS4]. Cerinţe specifice auditului de penetrare (testarea de penetrare)

1. Acţiuni ale OE

Operatorul economic trebuie să aprobe activitatea.

2. Acţiuni 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 informaţii decât adresele IP şi adresele URL asociate ţintei auditate. Această fază este în general precedată de descoperirea informaţiilor şi identificarea ţintei prin interogarea serviciilor DNS, scanarea porturilor deschise, descoperirea prezenţei echipamentelor de filtrare etc.;
• faza 2 - „Gray box“ (cutie gri). Auditorul are cunoştinţă despre un utilizator standard al reţelelor şi sistemelor informatice (autentificare legitimă, staţie de lucru „standard“ etc.). Identificatorii pot aparţine diferitelor profiluri de utilizator pentru a testa diferite niveluri de privilegii;
• faza 3 - „White box“ (cutie albă). Auditorul dispune de cât mai multe informaţii tehnice (arhitectură, cod sursă, contacte telefonice, identificatori etc.) înainte de a începe analiza. De asemenea, are acces la contacte tehnice legate de reţelele şi sistemele informatice ţintă.

În cazul în care sunt efectuate mai multe dintre faze, se recomandă păstrarea ordinii de execuţie descrise mai sus;

– să definească un profil de atacator simulat;
– să exploateze vulnerabilităţile descoperite numai cu acordul operatorului economic, atunci când ştie că reţelele şi sistemele informatice auditate vor fi instabile sau chiar va fi provocat un refuz de serviciu;
– să indice şi să justifice în raportul de audit absenţa oricărei încercări de exploatare a vulnerabilităţilor;
– să comunice ANSRSI vulnerabilităţile nonpublice descoperite în timpul auditului.

3. Comunicarea dintre ASI şi OE

Auditorul de securitate cibernetică trebuie să aibă un contact permanent cu operatorul economic şi să avertizeze /să informeze operatorul economic înainte de orice acţiune care ar putea duce la o defecţiune sau chiar la o refuzare a serviciului reţelelor şi sistemelor informatice auditate.

[CAS5]. Cerinţe specifice auditului securităţii organizaţiei

1. Acţiuni ale OE

Operatorul economic trebuie să pună la dispoziţia auditorului de securitate cibernetică toate documentele şi înscrisurile necesare desfăşurării activităţii de audit.

2. Acţiuni tehnice ale ASI

Auditorul de securitate cibernetică trebuie:

– să analizeze organizarea securităţii reţelelor şi sistemelor informatice pe baza standardelor tehnice şi de reglementare stabilite în Lista standardelor şi specificaţiilor europene şi internaţionale (LSSEINIS), în conformitate cu cerinţele minime de securitate aplicabile operatorilor de servicii esenţiale, respectiv furnizorilor de servicii digitale;
– să respecte regulile specifice de audit, respectiv trebuie:
• să permită măsurarea conformităţii reţelelor şi sistemelor informatice auditate cu privire la parametrii de referinţă şi identificarea abaterilor care prezintă vulnerabilităţi majore ale acestora;
• să integreze analiza elementelor legate de securitatea aspectelor fizice ale reţelelor şi sistemelor informatice, în special protecţia spaţiilor care găzduiesc componente ale reţelelor şi sistemelor informatice şi a datelor /informaţiilor auditate sau controlul acces la aceste componente.

3. Comunicarea dintre ASI şi OE

Auditorul de securitate cibernetică trebuie să aibă un contact permanent cu operatorul economic, să poată avea discuţii/ interviuri cu managerii de proces şi responsabilii cu securitatea, inclusiv responsabilii NIS.

[CAS6]. Cerinţe specifice auditului sistemelor de control industrial

1. Acţiuni ale OE

Operatorul economic trebuie să pună la dispoziţia auditorului de securitate cibernetică documente şi înscrisuri, precum şi accesul la elementele/componentele care urmează a fi supuse auditului tehnic.

2. Acţiuni tehnice ale ASI

Auditorul de securitate cibernetică trebuie să desfăşoare următoarele activităţi în cadrul sistemului de control industrial (ISC) şi, după caz, al centrului său de control (SCADA):
– audit arhitectură;
– audit de configurare;
– audit securitate logică şi fizică.
3. Comunicarea dintre ASI şi OE
Auditorul de securitate cibernetică trebuie:
– să poată organiza interviuri cu personalul implicat în securitatea sistemului de control industrial, managerul operaţional al sistemului şi, 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 vulnerabilităţilor

1. În procesul de stabilire a impactului vulnerabilităţilor se va utiliza o scală de clasificare a vulnerabilităţilor.
2. Vulnerabilităţile, de origine tehnică sau organizaţională, sunt clasificate în funcţie de riscul pe care îl prezintă pentru reţelele şi sistemele informatice, adică în funcţie de impactul vulnerabilităţii asupra acestora şi dificultatea de furnizare a serviciului esenţial/digital.
3. Nivelul de risc asociat cu fiecare vulnerabilitate este evaluat în funcţie de următoarea scală de valori:
– scăzut: risc scăzut pentru reţelele şi sistemele informatice - poate necesita corecţie;
– moderat: risc moderat asupra reţelelor şi sistemelor informatice - necesită corecţie pe termen mediu;
– major: risc major pentru reţelele şi sistemele informatice - necesită corecţie pe termen scurt;
– critic: risc critic pentru reţelele şi sistemele informatice - necesită corecţie imediată sau oprirea imediată a serviciului furnizat.
4. Uşurinţa în exploatare a vulnerabilităţilor printr-un atac corespunde nivelului de expertiză şi mijloacelor necesare pentru a efectua atacul cibernetic folosind vulnerabilităţile identificate. Se evaluează pe următoarea scală de exploatare:
– uşor: operare banală - nu necesită instrumente speciale;
– redus: operare simplă - necesită tehnici simple şi instrumente disponibile publicului;
– înalt: operare abilitată - necesită abilităţi în securitatea reţelelor şi sistemelor informatice şi dezvoltarea instrumentelor simple pentru exploatarea vulnerabilităţilor publice;
– dificil: operare expertiză - necesită expertiză în securitatea reţelelor şi sistemelor informatice şi dezvoltarea instrumentelor specifice pentru exploatarea vulnerabilităţilor nepublicate.
5. Impactul corespunde consecinţelor pe care exploatarea vulnerabilităţii le poate avea asupra reţelelor şi sistemelor informatice auditate. Se evaluează conform următoarei scale de impact:
– minim: nicio consecinţă directă asupra securităţii reţelelor şi sistemelor informatice;
– mediu: consecinţe izolate asupra anumitor puncte ale reţelelor şi sistemelor informatice;
– maxim: consecinţe limitate asupra unei părţi a reţelelor şi sistemelor informatice;
– critic: consecinţe generalizate asupra întregilor reţele şi sisteme informatice.
6. Tabelul următor indică nivelul de risc inerent fiecărei vulnerabilităţi descoperite, în funcţie de dificultatea lor de exploatare şi de impactul presupus:

Uşurinţa în exploatare Impact	Dificil	Înalt	Redus	Uşor
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 importanţă critică naţională, pentru un impact mediu, nivelul riscului este estimat la moderat, chiar şi pentru o uşurinţă în exploatare estimată la dificil.

Anexa nr. 11

la regulament

SITUAŢIA
auditurilor de securitate desfăşurate în anul ...

Auditor de securitate cibernetică persoană:[ ] [juridică]/[ ] [fizică]
Auditor de securitate cibernetică: ...../IDASC:.....
(numele/prenumele PF/denumire PJ)

Nr. crt.	Beneficiar	Tip beneficiar	Zile misiune	Taxă audit (mii lei)	Activităţi de audit		Nereguli grave constatate	Vulnerabilităţi constatate
1.	A B C Energy	OSE	12	10	Comune	Da/Nu	a)...	1)... 2)...
					Speciale	Da/Nu	a)...	1)... 2)...
					Mixte	Da/Nu	a)...	1)... 2)...
...	...	...		...	...		...	...
Situaţie centralizatoare								
A.	OSE	n	29	2.000	-	-	59	50
B.	FSD	m	5	500	-	-	15	11
C.	TOTAL	(n+m)	34	2.500	-	-	74	61

Anexa nr. 12

la regulament

LISTA
auditurilor de securitate desfăşurate pe perioada de valabilitate a atestatului^1

^1 Perioada de valabilitate a atestatului - perioada cuprinsă între data emiterii atestatului şi data solicitării reînnoirii atestatului.
Auditor de securitate cibernetică persoană:[ ] [juridică]/[ ] [fizică]
Perioada - de la data de: ...../...../20....
la data de: ...../...../20....

Secţiunea 1.
Persoană fizică

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

Nr. crt.	Beneficiar	Anul	Zile audit	Tip contract		Activităţi de audit		
				Individual	Asociere	Comune	Speciale	Mixte
I.	Operatori de servicii esenţiale							
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)

Secţiunea 2.
Persoană juridică^2

^2 Se completează pentru fiecare auditor de securitate persoană fizică - câte un tabel ca şi la secţiunea I. Persoană fizică - şi se centralizează datele pentru fiecare tip de beneficiar, respectiv operatori de servicii esenţiale şi furnizori de servicii digitale.

1. Auditor de securitate cibernetică: ...../IDASC:.....
(numele/prenumele)
2. Auditor de securitate cibernetică: ...../IDASC:.....
(numele/prenumele)
...
n. Centralizator (PJ): ...../IDASC:.....
(denumire PJ)

Nr. crt.	Tip beneficiari	Anul	Zile audit	Tip contract		Activităţi de audit		
				Individual	Asociere			
I.	Operatori de servicii esenţiale	-	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)

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 şi 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, atestaţi de Autoritatea competentă la nivel naţional pentru securitatea reţelelor şi sistemelor informatice a atestatului de securitate cibernetică (ANSRSI), care desfăşoară activităţi de audit de securitate a reţelelor şi sistemelor informatice care stau la baza furnizării de servicii esenţiale şi/sau digitale.

Articolul 3
Scopul Codului etic al auditorului de securitate cibernetică este crearea cadrului etic necesar desfăşurării activităţii de auditor de securitate cibernetică, astfel încât acesta să îşi îndeplinească cu profesionalism, loialitate, corectitudine şi în mod imparţial îndatoririle de serviciu şi să se abţină de la orice faptă care ar putea să aducă prejudicii instituţiei - atunci când este angajat la un auditor persoană juridică - şi operatorului economic (operator de servicii esenţiale sau furnizor de servicii digitale) - atunci când desfăşoară activităţi 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. performanţa - desfăşurarea unei activităţi de audit de securitate se va realiza la cei mai ridicaţi parametri, în scopul îndeplinirii cerinţelor stabilite în Regulamentul pentru atestarea şi verificarea auditorilor de securitate cibernetică (RENASC), în condiţii de economicitate, eficacitate şi eficienţă;

2. profesionalismul - presupune existenţa unor capacităţi intelectuale şi experienţe dobândite prin pregătire şi educaţie şi printr-un cod de valori şi conduită comun tuturor auditorilor de securitate cibernetică;

3. calitatea serviciilor - constă în competenţa auditorului de securitate cibernetică de a-şi realiza sarcinile ce îi revin cu obiectivitate, responsabilitate, sârguinţă şi onestitate;

4. încrederea - auditorul de securitate cibernetică trebuie să promoveze cooperarea şi bunele relaţii cu ceilalţi auditori de securitate cibernetică - când face parte dintr-o echipă de audit. Sprijinul şi cooperarea profesională, echilibrul şi corectitudinea sunt elemente esenţiale ale activităţii desfăşurate de către un auditor de securitate cibernetică;

5. conduita - auditorul de securitate cibernetică trebuie să aibă o conduită ireproşabilă atât pe plan profesional, cât şi personal;

6. corectitudinea - metodele, instrumentele şi tehnicile utilizate trebuie să fie valide şi actualizate la nivel cu noutăţile în domeniul securităţii cibernetice;

7. credibilitatea - informaţiile furnizate de rapoartele, opiniile şi recomandările auditorului de securitate cibernetică trebuie să fie fidele realităţii şi de încredere.

Articolul 5
Codul etic al auditorului de securitate cibernetică este structurat în două componente esenţiale:

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 desfăşurarea activităţii auditorul de securitate cibernetică este obligat să respecte următoarele principii fundamentale:

a) integritatea - auditorul de securitate cibernetică trebuie să fie corect, onest şi incoruptibil, integritatea fiind suportul încrederii şi credibilităţii acordate raţionamentului auditorului de securitate cibernetică;

b) independenţa şi obiectivitatea:

– independenţa - independenţa faţă de operatorul economic (operator de servicii esenţiale sau furnizor de servicii digitale) şi oricare alte grupuri de interese este indispensabilă. În acest sens, auditorul de securitate cibernetică trebuie:
• să depună toate eforturile pentru a fi independent în tratarea problemelor aflate în analiză;
• să fie independent şi imparţial atât în teorie, cât şi în practică;
• să nu fie afectat de interese personale sau exterioare;
• să nu se implice în acele activităţi în care are un interes legitim/întemeiat;
– obiectivitatea - în activitatea sa auditorul de securitate cibernetică trebuie:
• să manifeste obiectivitate şi imparţialitate în redactarea rapoartelor, care trebuie să fie precise şi obiective;
• să formuleze concluzii şi opinii bazate exclusiv pe documentele obţinute şi analizate conform listei standardelor şi specificaţiilor internaţionale şi europene în domeniu;
• să folosească toate informaţiile utile primite de la operatorul economic auditat şi din alte surse;
• să analizeze punctele de vedere exprimate de operatorul economic auditat şi, în funcţie de pertinenţa acestora, să formuleze opiniile şi recomandările proprii;
• să facă o evaluare echilibrată a tuturor circumstanţelor relevante şi să nu fie influenţat de propriile interese sau de interesele altora în formarea propriei opinii;
c) confidenţialitatea:
– auditorul de securitate cibernetică este obligat:
• să păstreze confidenţialitatea în legătură cu faptele, informaţiile sau documentele despre care ia cunoştinţă în exercitarea atribuţiilor lor; este interzis să utilizeze în interes personal sau în beneficiul unui terţ informaţiile dobândite în exercitarea atribuţiilor de serviciu;
• să protejeze informaţiile referitoare la auditul de securitate şi, în special, dovezile, constatările şi rapoartele;
– în cazuri excepţionale auditorul de securitate cibernetică poate furniza aceste informaţii numai în condiţiile expres prevăzute de normele legale în vigoare sau cu autorizaţia scrisă din partea operatorului economic auditat;
d) competenţa profesională:
– auditorul de securitate cibernetică este obligat să îşi îndeplinească atribuţiile pe timpul activităţii de audit de securitate cu profesionalism, competenţă, imparţialitate şi la standarde internaţionale, aplicând cunoştinţele, aptitudinile şi experienţa dobândite;
– auditorul de securitate cibernetică este obligat să respecte legile şi reglementările naţionale aplicabile, precum şi cele mai bune practici legate de activităţile 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 imparţial a activităţilor; în acest sens el trebuie să îşi menţină independenţa faţă de orice influenţe politice;
– auditorul de securitate cibernetică are obligaţia ca în exercitarea atribuţiilor ce îi revin să se abţină 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 şi reprezintă un ajutor pentru interpretarea principiilor şi aplicarea lor practică, având rolul să îndrume din punct de vedere etic auditorul de securitate cibernetică.
a) integritatea:
– exercitarea profesiei cu onestitate, bună-credinţă şi responsabilitate;
– respectarea legii şi acţionarea în conformitate cu cerinţele activităţii de audit de securitate;
– respectarea şi contribuţia la obiectivele etice legitime ale instituţiei din care provine;
– se interzice auditorului de securitate cibernetică să ia parte cu bună ştiinţă la activităţi ilegale şi angajamente care discreditează îndeplinirea atribuţiilor de auditor de securitate cibernetică sau instituţia din care face parte;
b) independenţa şi obiectivitatea:
– se interzice implicarea auditorului de securitate cibernetică în activităţi sau în relaţii care ar putea să fie în conflict cu interesele instituţiei supuse activităţii de audit de securitate şi 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 şi consultanţă;
– se interzice auditorului de securitate cibernetică, în timpul activităţii de audit, să primească din partea operatorului economic auditat avantaje de natură materială sau personală care ar putea să afecteze obiectivitatea evaluării;

– auditorul 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) confidenţialitatea - se interzice folosirea de către auditorul de securitate cibernetică a informaţiilor obţinute în cursul activităţii de audit de securitate în scop personal sau întro manieră care poate fi contrară legii ori în detrimentul obiectivelor legitime şi etice ale operatorului economic auditat;

d) competenţa:

– auditorul de securitate cibernetică trebuie să se comporte într-o manieră profesională în toate activităţile pe care le desfăşoară, să aplice standarde şi norme profesionale şi să manifeste imparţialitate în îndeplinirea atribuţiilor cu privire la activitatea de audit de securitate;

– auditorul de securitate cibernetică trebuie să se angajeze numai în acele activităţi de audit pentru care are cunoştinţele, aptitudinile şi experienţa necesare;

– auditorul de securitate cibernetică trebuie să utilizeze metode şi practici de cea mai bună calitate în activităţile pe care le realizează; în desfăşurarea auditului şi în elaborarea rapoartelor auditorul de securitate cibernetică are datoria de a adera la postulatele de bază şi la standardele de audit general acceptate;

– auditorul de securitate cibernetică trebuie să îşi îmbunătăţească în mod continuu cunoştinţele, eficienţa şi calitatea activităţii lui:

• în cazul persoanelor juridice, acestea trebuie să asigure condiţiile 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 desfăşoare activităţi 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 şi experienţă profesionale elocvente;

– auditorul de securitate cibernetică trebuie să cunoască legislaţia de specialitate şi să se preocupe în mod continuu de creşterea nivelului de pregătire, conform standardelor internaţionale;

– se interzice auditorului de securitate cibernetică să îşi depăşească atribuţiile de serviciu.

Capitolul IV
Dispoziţii finale

Articolul 8

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

Articolul 9

În conformitate cu art. 20 alin. (1) din Regulamentul pentru atestarea şi verificarea auditorilor de securitate cibernetică, prevederile Codului etic al auditorului de securitate cibernetică sunt obligatorii pentru toţi auditorii de securitate cibernetică, persoane fizice şi juridice, valabil atestaţi, care au obligaţia de a-l lua la cunoştinţă.

Articolul 10

După obţinerea atestatului de auditor de securitate cibernetică, auditorul va semna o declaraţie/un angajament prin care ia act de Codul etic al auditorului de securitate cibernetică şi 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 naţional pentru securitatea reţelelor şi sistemelor informatice a atestatului de securitate cibernetică a atestatului de auditor de securitate cibernetică.

Articolul 12

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

DECLARAŢIE/ANGAJAMENT
privind respectarea Codului etic al auditorului de securitate cibernetică

Auditor de securitate cibernetică: .....
IDASC: .....
Subsemnatul, ... (nume şi prenume), atestat ca auditor de securitate cibernetică având IDASC: .....,
posesor al actului de identitate seria ..... nr....., CNP.....,
cunoscând dispoziţiile art. 326 din Codul penal cu privire la falsul în declaraţii,

declar pe propria răspundere că am luat cunoştinţă de Codul etic al auditorului de securitate cibernetică şi mă angajez să îl respect pe întreg parcursul perioadei de valabilitate a atestatului de securitate cibernetică.
Dau prezenta declaraţie în conformitate cu art. 20 din Regulamentul pentru atestarea şi verificarea auditorilor de securitate cibernetică, aprobat prin Ordinul secretarului general al Guvernului nr. 559/2021, fiindu-mi necesară la CERT-RO/ANSRSI pentru înscrierea ca auditor de securitate cibernetică în Registrul naţional al auditorilor de securitate cibernetică.
Semnătura auditorului de securitate cibernetică .....
Numele şi prenumele semnatarului .....
Data .....

Anexa nr. 14

la regulament

GRILE CORESPONDENŢĂ
privind evaluarea cerinţelor minime de securitate

I. Evaluarea cerinţelor minime de securitate pentru operatorii de servicii esenţiale

Domenii de securitate	Categorii de activităţi de securitate	Măsuri de securitate	Activităţi de audit		
			Comune	Speciale	Mixte
GUVERNANŢĂ	Managementul securităţii informaţiei	Analizarea şi 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 conformităţii cu privire la securitatea informaţiei. Audit de securitate	x	x	x
		Testarea şi evaluarea securităţii reţelelor şi sistemelor informatice		x	x
		Asigurarea securităţii personalului	x		x
		Conştientizarea şi instruirea utilizatorilor	x		x
		Gestionarea activelor	x		x
	Managementul ecosistemului	Cartografierea ecosistemului	x	x	x
		Relaţiile ecosistemului	x		x
PROTECŢIE	Managementul arhitecturii	Managementul configuraţiei reţelelor şi sistemelor informatice	x		x
		Managementul suporţilor de memorie externă	x		x
		Segregarea şi segmentarea reţelelor şi sistemelor informatice	x		x
		Filtrarea traficului	x		x
		Asigurarea protecţiei produselor şi serviciilor aferente reţelelor şi sistemelor informatice	x	x	x
		Protecţia împotriva malware	x	x	x
	Managementul administrării	Administrarea conturilor	x		x
		Administrarea reţelelor şi sistemelor informatice	x		x
		Managementul accesului de la distanţă	x		x
	Managementul identităţii şi accesului	Managementul identificării şi autentificării utilizatorilor	x		x
		Managementul drepturilor de acces	x		x
	Managementul mentenanţei	Mentenanţa reţelelor şi sistemelor informatice	x		x
		Sisteme control industrial. SCADA - monitorizare, control şi achiziţii de date	x	x	x
	Managementul securităţii fizice	Asigurarea protecţiei fizice a reţelelor şi sistemelor informatice	x		x
APĂRARE CIBERNETICĂ	Managementul detecţiei	Managementul vulnerabilităţilor şi alertelor de securitate	x	x	x
		Înregistrarea evenimentelor	x		x
		Jurnalizarea şi asigurarea trasabilităţii activităţilor în cadrul reţelelor şi 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 naţional pentru securitatea reţelelor şi sistemelor informatice (ANSRSI) şi CSIRT naţional	x		x
REZILIENŢĂ	Managementul continuităţii afacerii	Asigurarea disponibilităţii serviciului esenţial şi a funcţionării reţelelor şi 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/activităţi de audit

#	Tipuri de audit recomandate	Activităţi de audit				
		[AS1]	[AS2]	[AS3]	[AS4]	[AS5]
1.	Auditul unei aplicaţii informatice		x	x	x	
2.	Auditul unui centru de date	x	x		x	x
3.	Auditul unei reţele 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/activităţi de audit

#	Atest de securitate cibernetică	Activităţi 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] desfăşurată parţial, respectiv pentru activităţile comune [AS1], [AS2] şi [AS5].

^2 Activitate de audit [AS6] desfăşurată parţial, respectiv pentru activităţile comune [AS3] şi [AS4].

C.J.A.P. Piatra Neamţ