ORDIN nr. 108 din 12 octombrie 2012
pentru aprobarea Directivei privind acreditarea de securitate a sistemelor informatice şi de comunicaţii (SIC) care stochează, procesează sau transmit informaţii clasificate - INFOSEC 13

EMITENT: OFICIUL REGISTRULUI NAŢIONAL AL INFORMAŢIILOR SECRETE DE STAT
PUBLICAT ÎN: MONITORUL OFICIAL nr. 716 din 22 octombrie 2012
Data intrarii in vigoare : 22 octombrie 2012

În temeiul art. 1 alin. (4) lit. b) şi art. 3 alin. (6) din Ordonanţa de urgenţă a Guvernului nr. 153/2002 privind organizarea şi funcţionarea Oficiului Registrului Naţional al Informaţiilor Secrete de Stat, aprobată prin Legea nr. 101/2003, cu modificările şi completările ulterioare, şi al art. 55 alin. (1) din Regulamentul privind procedurile, la nivelul Guvernului, pentru elaborarea, avizarea şi prezentarea proiectelor de documente de politici publice, a proiectelor de acte normative, precum şi a altor documente, în vederea adoptării/aprobării, aprobat prin Hotărârea Guvernului nr. 561/2009,

directorul general al Oficiului Registrului Naţional al Informaţiilor Secrete de Stat emite prezentul ordin.

ART. 1
Se aprobă Directiva privind acreditarea de securitate a sistemelor informatice şi de comunicaţii (SIC) care stochează, procesează sau transmit informaţii clasificate - INFOSEC 13, prevăzută în anexa care face parte integrantă din prezentul ordin.

ART. 2
La data intrării în vigoare a prezentului ordin se abrogă Ordinul directorului general al Oficiului Registrului Naţional al Informaţiilor Secrete de Stat nr. 386/2004 pentru aprobarea Ghidului pentru acreditarea de securitate a sistemelor informatice şi de comunicaţii naţionale care vehiculează informaţii NATO - DS 8, publicat în Monitorul Oficial al României, Partea I, nr. 1.081 din 19 noiembrie 2004, şi Ordinul directorului general al Oficiului Registrului Naţional al Informaţiilor Secrete de Stat nr. 172/2006 pentru aprobarea Directivei privind acreditarea de securitate a sistemelor informatice şi de comunicaţii (SIC) care stochează, procesează sau transmit informaţii clasificate - INFOSEC 13, publicat în Monitorul Oficial al României, Partea I, nr. 266 din 24 martie 2006.

ART. 3
Oficiul Registrului Naţional al Informaţiilor Secrete de Stat va duce la îndeplinire prevederile prezentului ordin.

Directorul general al Oficiului
Registrului Naţional al Informaţiilor Secrete de Stat,
Marius Petrescu

Bucureşti, 12 octombrie 2012.
Nr. 108.

ANEXĂ

DIRECTIVĂ
privind acreditarea de securitate a sistemelor informatice şi de comunicaţii (SIC) care stochează, procesează sau transmit informaţii clasificate - INFOSEC 13

CAP. I
Introducere

SECŢIUNEA 1
Domeniu de aplicabilitate

ART. 1

Directiva privind acreditarea de securitate a sistemelor informatice şi de comunicaţii (SIC) care stochează, procesează sau transmit informaţii clasificate - INFOSEC 13, denumită în continuare directivă, este aprobată de Oficiul Registrului Naţional al Informaţiilor Secrete de Stat (ORNISS), în aplicarea politicii naţionale, NATO şi UE de securitate privind protecţia informaţiilor clasificate.

ART. 2

Prezenta directivă se adresează ORNISS, structurilor de planificare, achiziţie şi implementare a SIC care procesează, stochează sau transmit informaţii clasificate, autorităţilor operaţionale ale SIC, structurilor responsabile cu stabilirea, implementarea şi menţinerea standardelor INFOSEC, entităţilor care, în cadrul procesului de acreditare de securitate a SIC, desfăşoară activităţi de evaluare/certificare, precum şi structurilor interne INFOSEC acreditate de ORNISS, denumite în continuare SII, stabilite în cadrul autorităţilor desemnate de securitate, denumite în continuare ADS.

ART. 3

Aplicarea prevederilor prezentei directive este obligatorie pentru SIC care stochează, procesează sau transmit informaţii clasificate.

SECŢIUNEA a 2-a
Definiţii

ART. 4

În cuprinsul prezentei directive, următorii termeni şi sintagme se definesc după cum urmează:

a) informaţii clasificate - informaţii naţionale clasificate secret de stat, informaţii NATO clasificate, informaţii UE clasificate sau informaţii echivalente care fac obiectul unor tratate, acorduri sau înţelegeri internaţionale la care România este parte;

b) sistem informatic şi de comunicaţii (SIC) - orice sistem care permite stocarea, procesarea sau transmiterea informaţiilor în format electronic. Un SIC cuprinde toate elementele care îi sunt necesare pentru a funcţiona, incluzând infrastructura, structurile organizaţionale, personalul şi resursele informaţionale;

c) acreditarea de securitate - autorizarea acordată unui SIC să proceseze, să stocheze sau să transmită informaţii clasificate în mediul său operaţional.

SECŢIUNEA a 3-a
Cerinţe de acreditare de securitate a SIC

ART. 5

Obiectivul principal al acreditării de securitate este acceptarea riscului de securitate rezidual asociat SIC şi autorizarea operării acestuia în conformitate cu termenii stabiliţi. Prin parcurgerea unui proces de acreditare de securitate se obţine asigurarea că măsurile de securitate implementate în SIC sunt conforme cu cerinţele politicilor de securitate specifice tipului de informaţii clasificate naţionale, NATO, UE şi altele asemenea şi ale documentaţiei cu cerinţele de securitate, denumită în continuare DCS, elaborată pentru respectivul SIC.

ART. 6

În conformitate cu prevederile legislației naționale, SIC care stochează, procesează sau transmit informații clasificate trebuie să facă obiectul unui proces de acreditare de securitate. În acest context se aplică următoarele prevederi:

a) pentru SIC care stochează, procesează sau transmit informații naționale clasificate secret de stat, procesul de acreditare de securitate este stabilit şi gestionat de către ORNISS prin Agenția de Acreditare de Securitate, denumită în continuare AAS, sau, după caz, de către SII din cadrul ADS, potrivit competențelor pentru care au fost acreditate de către ORNISS; luarea deciziei privind acreditarea revine ORNISS sau SII, după caz;

b) pentru SIC care stochează, procesează sau transmit informații naționale clasificate secret de serviciu, responsabilitatea acreditării de securitate revine persoanei juridice care are în responsabilitate SIC;

c) pentru interconectarea SIC care stochează, procesează sau transmit informații naționale clasificate secret de stat, procesul de acreditare de securitate este stabilit şi gestionat de către ORNISS prin AAS sau SII, după caz;

d) pentru SIC naționale care stochează, procesează sau transmit informații clasificate NATO CONFIDENTIAL sau cu un nivel superior, procesul de acreditare de securitate este stabilit şi gestionat de către ORNISS prin AAS, luarea deciziei privind acreditarea revenind ORNISS;

e) pentru SIC naționale care stochează, procesează sau transmit informații clasificate NATO RESTRICTED nu este necesar ca AAS să stabilească un proces de acreditare de securitate structurat, dar procesul de acreditare trebuie să reflecte importanța obiectivelor de securitate (confidențialitate, integritate şi disponibilitate), precum şi impactul pe care îl poate avea un eveniment nedorit asupra informațiilor, resurselor şi serviciilor sistemului; pentru aceste SIC, responsabilitatea stabilirii şi derulării procesului de acreditare de securitate, precum şi a luării deciziei privind acreditarea poate fi delegată de către ORNISS persoanei juridice care are în responsabilitate un astfel de sistem. Persoana juridică va respecta prevederile documentului prin care se stabilesc condițiile în care se realizează delegarea privind autoritatea de acreditare de securitate;

f) pentru interconectarea SIC naționale care stochează, procesează sau transmit informații NATO clasificate cu SIC NATO sau cu alte SIC naționale trebuie îndeplinite cerințele specifice stipulate în normele tehnice şi de implementare subsecvente şi în politicile de securitate ale respectivelor rețele, iar luarea deciziei privind acreditarea de securitate în vederea interconectării revine, după caz, ORNISS şi/sau organismelor NATO abilitate;

g) pentru SIC naționale care stochează, procesează sau transmit informații UE clasificate, procesul de acreditare de securitate trebuie să fie stabilit şi gestionat de către ORNISS prin AAS, iar luarea deciziei privind acreditarea revine ORNISS;

h) pentru interconectarea SIC naționale care stochează, procesează sau transmit informații UE clasificate cu SIC UE sau cu alte SIC naționale trebuie îndeplinite cerințele specifice stipulate în normele tehnice şi de implementare subsecvente şi în politicile de securitate ale respectivelor rețele, iar luarea deciziei privind acreditarea de securitate în vederea interconectării revine, după caz, ORNISS şi/sau organismelor UE abilitate;

i) pentru SIC naționale care stochează, procesează sau transmit informații echivalente care fac obiectul unor tratate, acorduri sau înțelegeri internaționale la care România este parte, procesul de acreditare este stabilit şi gestionat de către ORNISS prin AAS, iar luarea deciziei privind acreditarea de securitate revine ORNISS, prin aplicarea prevederilor naționale şi ale respectivelor tratate, acorduri sau înțelegeri internaționale la care România este parte.

CAP. II
Structurile implicate în procesul de acreditare de securitate a SIC

ART. 7

ORNISS prin AAS este responsabil de managementul procesului de acreditare de securitate a SIC, în conformitate cu prevederile art. 6.

ART. 8

În cuprinsul anexei nr. 2 sunt prezentate structurile implicate în procesul de acreditare de securitate a SIC. Atribuțiile acestora sunt precizate în Directiva privind structurile cu responsabilități în domeniul INFOSEC - INFOSEC 1, aprobată prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 482/2003.

ART. 9

(1) AAS se asigură că autoritatea operațională a SIC, denumită în continuare AOSIC, are autoritatea necesară pentru a gestiona aspectele de securitate în conformitate cu documentația de securitate.

(2) În cazul în care AOSIC nu are autoritatea necesară, AAS poate solicita luarea unor măsuri speciale, de exemplu:

a) escaladarea - în acest caz, AAS solicită să fie identificată o altă autoritate, care să fie desemnată de către conducătorul organizației drept AOSIC;

b) cooperarea - în acest caz, autoritățile reprezentând toate structurile care utilizează SIC cooperează în vederea implementării unui set comun de cerințe de securitate specifice sistemului, denumite în continuare CSSS. În această situație, autoritatea funcționează ca un comitet. Această cooperare trebuie susținută de un acord scris al membrilor şi face subiectul unui arbitraj al unei terțe părți, care este AAS. Cooperarea dintre statele membre şi structuri NATO/UE poate necesita identificarea unei terțe părți (cum ar fi: Oficiul de Securitate al NATO sau Secretariatul General al Consiliului UE); aceasta mai poate fi, de exemplu, un furnizor de informații având interes în protecția informațiilor stocate, procesate sau transmise şi care are posibilitatea stopării transmiterii informațiilor;

c) hegemonia - în acest caz, conducerea unei persoane juridice consimte să accepte autoritatea altei persoane juridice şi să implementeze CSSS. Această măsură operează similar cu aceea a cooperării, în cazul în care una dintre părțile acordului este dominantă, posibil datorită faptului că este furnizorul principal de informații, şi poate să impună un CSSS celeilalte părți fără a se recurge la arbitrajul unei terțe părți.

ART. 10

(1) În cazul interconectării SIC naționale care stochează, procesează sau transmit informații NATO/UE clasificate cu SIC NATO/SIC UE, când în administrarea şi acreditarea de securitate a SIC sunt implicate şi organisme NATO/UE, responsabilitatea acreditării de securitate nu se limitează numai la ORNISS.

(2) În situația prevăzută la alin. (1), ORNISS i se poate solicita să recunoască autoritatea unor structuri NATO/UE şi/sau să îşi coordoneze cu acestea responsabilitățile pe care le are la nivel național privind acreditarea.

ART. 11

(1) În cazul interconectării SIC naționale care stochează, procesează sau transmit informații clasificate, caz în care sunt implicate mai multe AOSIC şi structuri de securitate, se impune încheierea unor acorduri de securitate între AOSIC privind interconectarea.

(2) Aprobarea pentru interconectare prevăzută la alin. (1) este acordată de către ORNISS sau SII, după caz, responsabilitatea acreditării de securitate a fiecărui SIC care se interconectează revenind ORNISS sau SII, după caz.

ART. 12

(1) În vederea gestionării activităților stabilite prin strategia de acreditare de securitate a SIC se constituie o comisie de acreditare de securitate (CAS).

(2) CAS se constituie, la solicitarea AAS, la începutul ciclului de viață al proiectului şi îşi menține existența până în momentul acreditării de securitate.

(3) CAS este formată din reprezentanți ai tuturor structurilor care au responsabilități în asigurarea securității informațiilor, serviciilor şi resurselor SIC. Astfel, pe lângă AAS, al cărei reprezentat prezidează CAS, aceasta poate avea în componență:

a) reprezentanți ai altor structuri din cadrul ORNISS;

b) reprezentanți ai ADS pe domeniul de competență;

c) manageri de proiect;

d) reprezentanți ai AOSIC implicate;

e) reprezentanți ai structurilor de securitate ale entităților care administrează SIC;

f) reprezentanți ai structurilor de planificare şi implementare a SIC;

g) responsabili cu securitatea criptografică, a transmisiilor, a emisiilor etc.;

h) reprezentanți ai altor autorități având competențe relevante pentru securitatea SIC, cum ar fi, de exemplu, autorități de evaluare şi/sau certificare a unor componente ale SIC.

(4) În funcție de etapa de implementare a proiectului, AAS poate invita la reuniunile CAS şi alte structuri care pot sprijini luarea deciziei privind acreditarea de securitate a SIC.

(5) CAS poate fi reactivată de către AAS ori de câte ori se consideră necesar, de exemplu: schimbări semnificative în cerințele operaționale şi/sau în documentația de securitate, schimbări majore privind configurația SIC.

(6) Prin intermediul CAS, AAS poate cere tuturor celor responsabili de asigurarea securității SIC să se implice în procesul de acreditare de securitate.

(7) În cazul interconectării SIC naționale care stochează, procesează şi transmit informații clasificate, CAS este responsabilă pentru stabilirea documentației de securitate pentru SIC care se interconectează, pentru analiza şi aprobarea documentației privind cerințele de securitate comunitară, denumite în continuare CSC, precum şi pentru acreditarea de securitate a interconectării.

(8) În anexa nr. 3 este prezentat un exemplu de regulament de organizare şi funcționare a CAS.

CAP. III
Bazele acreditării de securitate

SECȚIUNEA 1
Generalități

ART. 13

Decizia privind acreditarea de securitate a unui SIC care stochează, procesează sau transmite informații clasificate se fundamentează pe rezultatele:

a) etapeide analiză a riscului de securitate şi concluziilor prezentate în raportul de analiză a riscului;

b) evaluării documentației de securitate, cum ar fi: raportul privind analiza riscului de securitate, DCS, procedurile operaționale de securitate;

c) verificării privind implementarea principiilor securității şi reglementărilor de securitate, de exemplu, prin aplicarea unui plan de testare şi evaluare a securității şi a analizei rezultatelor, precum şi menținerea acestora în acord cu cerințele de securitate;

d) identificării riscurilor reziduale şi reluării periodice a procesului de management al riscurilor de securitate.

SECȚIUNEA a 2-a
Procesul de management al riscului de securitate

ART. 14

(1) SIC naționale care stochează, procesează sau transmit informații clasificate trebuie supuse unui proces de management al riscului de securitate.

(2) Directiva privind managementul INFOSEC pentru sisteme informatice şi de comunicații - INFOSEC 3, aprobată prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 484/2003, stabileşte aspectele generale, procesele de analiză a riscului de securitate şi de management al riscului de securitate, precum şi necesitatea reluării procesului de management al riscului de securitate. Detaliile privind aplicarea acesteia sunt prezentate în ghidul "Metodologia privind managementul riscului de securitate pentru sistemele informatice şi de comunicații care stochează, procesează sau transmit informații clasificate - DS3", aprobată prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 389/2004.

SECȚIUNEA a 3-a
Documentația de securitate

ART. 15

(1) Un element important al procesului de acreditare de securitate îl constituie documentația de securitate, compusă din:

a) strategia de acreditare de securitate a SIC, document elaborat, după caz, de AAS sau SII, prin care se stabilesc activitățile necesar a fi derulate în cadrul procesului de acreditare de securitate a SIC, responsabilitățile şi termenele de realizare a acestora;

b) rezultatele procesului de management al riscului de securitate;

c) DCS prin care se definesc cerințele de securitate, mediile de securitate şi măsurile de securitate aplicabile SIC care trebuie acreditat;

d) procedurile operaționale de securitate (PrOpSec) care prezintă modul de implementare a măsurilor de securitate, a procedurilor operaționale referitoare la securitate ce trebuie urmate şi a responsabilităților personalului;

e) rapoarte de evaluare/certificare a securității informațiilor, resurselor sau serviciilor SIC, certificate de conformitate a produselor INFOSEC din compunerea SIC.

(2) DCS constituie baza acordului dintre AAS şi AOSIC în sensul operării SIC într-o manieră sigură. Aceasta stabileşte măsurile de securitate care asigură controlul şi responsabilitatea privind accesul individual al utilizatorilor SIC la informațiile clasificate. Acest document împreună cu PrOpSec stabileşte măsurile de securitate necesar a fi implementate, având în vedere:

a) aspectele relevante din punctul de vedere al securității, aflate în afara controlului AOSIC, adică mediul de securitate global, cum ar fi, de exemplu: elemente privind securitatea clădirii, securitatea întregului spațiu aflat sub controlul structurii/funcționarului de securitate, securitatea sistemelor interconectate şi mediul general de amenințări;

b) securitatea fizică, securitatea personalului, securitatea informațiilor şi măsuri de securitate procedurale aflate sub controlul AOSIC în mediul de securitate local;

c) mecanismele INFOSEC în SIC, adică mediul de securitate electronic, implementate într-o arhitectură dezvoltată pentru a corespunde funcționalității şi nivelului de asigurare de securitate necesar.

SECȚIUNEA a 4-a
Principiile securității

ART. 16

DCS, incluzând şi aspectele rezultate din analiza riscurilor de securitate, stabileşte modalitatea de obținere a protecției informațiilor, resurselor şi serviciilor SIC.

ART. 17

AAS analizează conformitatea cerințelor de securitate stabilite pentru SIC cu prevederile reglementărilor în domeniu şi cu necesitatea de contracarare a riscurilor de securitate generate de implementarea şi operarea SIC.

ART. 18

În cazul interconectării SIC, cerințele de securitate se aplică şi interfeței dintre sisteme. Pentru stabilirea cerințelor de securitate se au în vedere:

a) contracararea riscurilor de securitate inerente rezultate din necesitățile operaționale, referitoare la utilizatorii autorizați ai SIC, şi din folosirea canalelor de comunicație şi a echipamentelor necesare;

b) contracararea riscurilor de securitate din afara SIC, inclusiv a atacurilor inițiate de utilizatorii SIC cu care se interconectează.

ART. 19

Evaluarea cerințelor de securitate pentru contracararea riscurilor de securitate prevăzute la art. 18 lit. a) poate fi realizată într-o manieră clară întrucât elementele variabile sunt în mare măsură limitate, cum ar fi, de exemplu: locația SIC, numărul utilizatorilor, certificarea de securitate a acestora, volumul şi nivelul de clasificare de securitate a informațiilor stocate, procesate sau transmise.

ART. 20

(1) În evaluarea cerințelor de securitate pentru contracararea riscurilor de securitate prevăzute la art. 18 lit. b) există 3 scenarii privind configurația:

a) SIC care nu se interconectează direct cu alte SIC, dar există facilitatea de transfer off-line a informațiilor;

b) SIC care se interconectează şi care au diferite moduri de operare de securitate sau diferite niveluri de clasificare a informațiilor ori SIC sigur care se interconectează cu SIC nesigur, cum ar fi INTERNET sau rețele similare din domeniul public. În acest context este necesară adoptarea politicii de nod autoprotejat în vederea prevenirii riscurilor la adresa confidențialității, integrității şi disponibilității informațiilor, precum şi a integrității şi disponibilității resurselor şi serviciilor SIC;

c) un SIC acreditat care se interconectează cu alt SIC acreditat prin intermediul unei infrastructuri securizate, acestea putând coopera pentru a susține mutual securitatea.

(2) În situația prevăzută la alin. (1) lit. a) se au în vedere amenințările şi vulnerabilitățile unui SIC independent (neconectat - LAN). Cerințele de securitate trebuie să aibă în vedere funcționalitatea şi nivelul de încredere oferite de măsurile de securitate implementate în hardware şi software.

(3) În situațiile prevăzute la alin. (1) lit. b) şi c), DCS se stabileşte în funcție de fluxul informațiilor, amenințările şi vulnerabilitățile aferente interconectării şi utilizatorilor celuilalt SIC în termeni de securitate sau insecuritate. Factorii determinanți în stabilirea necesității de securitate se constituie din reglementările de securitate aplicate de celălalt SIC, structura şi rigoarea propriilor CSSS şi nivelul de încredere obținut prin măsurile de securitate implementate în hardware şi software.

SECȚIUNEA a 5-a
Testarea şi evaluarea de securitate

ART. 21

Pentru acreditarea de securitate a unui SIC care stochează, procesează sau transmite informații clasificate, AAS trebuie să aibă certitudinea că:

a) prin cerințele de securitate stabilite pentru SIC se realizează un echilibru corespunzător între riscul de securitate şi cerințele operaționale;

b) cerințele de securitate sunt implementate şi respectate conform documentației de securitate.

ART. 22

(1) Verificarea faptului că măsurile de securitate sunt implementate în conformitate cu cerințele de securitate implică efectuarea unor testări şi evaluări ale securității. Scopul acestora este de a identifica eventualele discrepanțe dintre măsurile de securitate aprobate şi cele implementate.

(2) Testarea şi evaluarea securității include aspectele privind managementul configurației pentru toate produsele hardware şi software relevante pentru securitate.

(3) Resursele necesare derulării procesului de testare şi evaluare a securității includ personalul de testare şi documentația relevantă pentru administrarea de securitate şi de sistem, cum ar fi DCS, PrOpSec şi datele de management al configurației.

(4) Planul de testare şi evaluare a securității trebuie să stabilească activitățile necesar a fi derulate, obiectivele fiecăreia dintre aceste activități, metoda de executare a testului şi rezultatele anticipate. Rezultatele activității de testare şi evaluare a securității contribuie la luarea unei decizii privind acreditarea de securitate, fiind cuprinse într-un document şi prezentate AOSIC.

ART. 23

(1) Activitățile de evaluare şi certificare de securitate a SIC sunt parte integrantă a procedurilor de management al întregului proiect. Pentru derularea acestor activități trebuie avute în vedere atât costurile, cât şi acordarea întregului sprijin necesar entităților de evaluare şi certificare, inclusiv prin punerea la dispoziție a unei documentații suplimentare, care să detalieze aspectele tehnice ale DCS, conform nivelului necesar de asigurare a securității.

(2) Responsabilitatea privind monitorizarea continuă a activităților de evaluare şi certificare revine AOSIC.

SECȚIUNEA a 6-a
Riscul rezidual

ART. 24

DCS, prin care se stabilesc măsurile de securitate necesar a fi aplicate, trebuie, de asemenea, să identifice orice riscuri reziduale asociate SIC, care nu pot fi contracarate, cum ar fi cele din motive tehnice, şi care sunt apreciate de către AOSIC şi AAS ca fiind acceptabile. Acestea constituie obiectul reluării procesului de management al riscului de securitate.

ART. 25

(1) În cadrul procesului de management al riscurilor se evaluează riscurile asociate configurației SIC, completate cu vulnerabilitățile identificate în timpul derulării testării şi evaluării securității. Rezultatul acestei analize va fundamenta decizia privind acreditarea de securitate.

(2) Cu ocazia reluării periodice a procesului de management al riscului de securitate trebuie efectuată o analiză a riscurilor de securitate, care să ia în considerare noile vulnerabilități şi amenințări identificate şi noile

măsuri de securitate capabile să elimine vulnerabilitățile care nu au fost contracarate anterior, stabilind dacă riscurile reziduale se mențin la un nivel acceptabil.

(3) Riscurile reziduale sunt asumate de către organizația care are în responsabilitate SIC.

CAP. IV
Principalele etape ale procesului de acreditare de securitate

SECȚIUNEA 1
Generalități

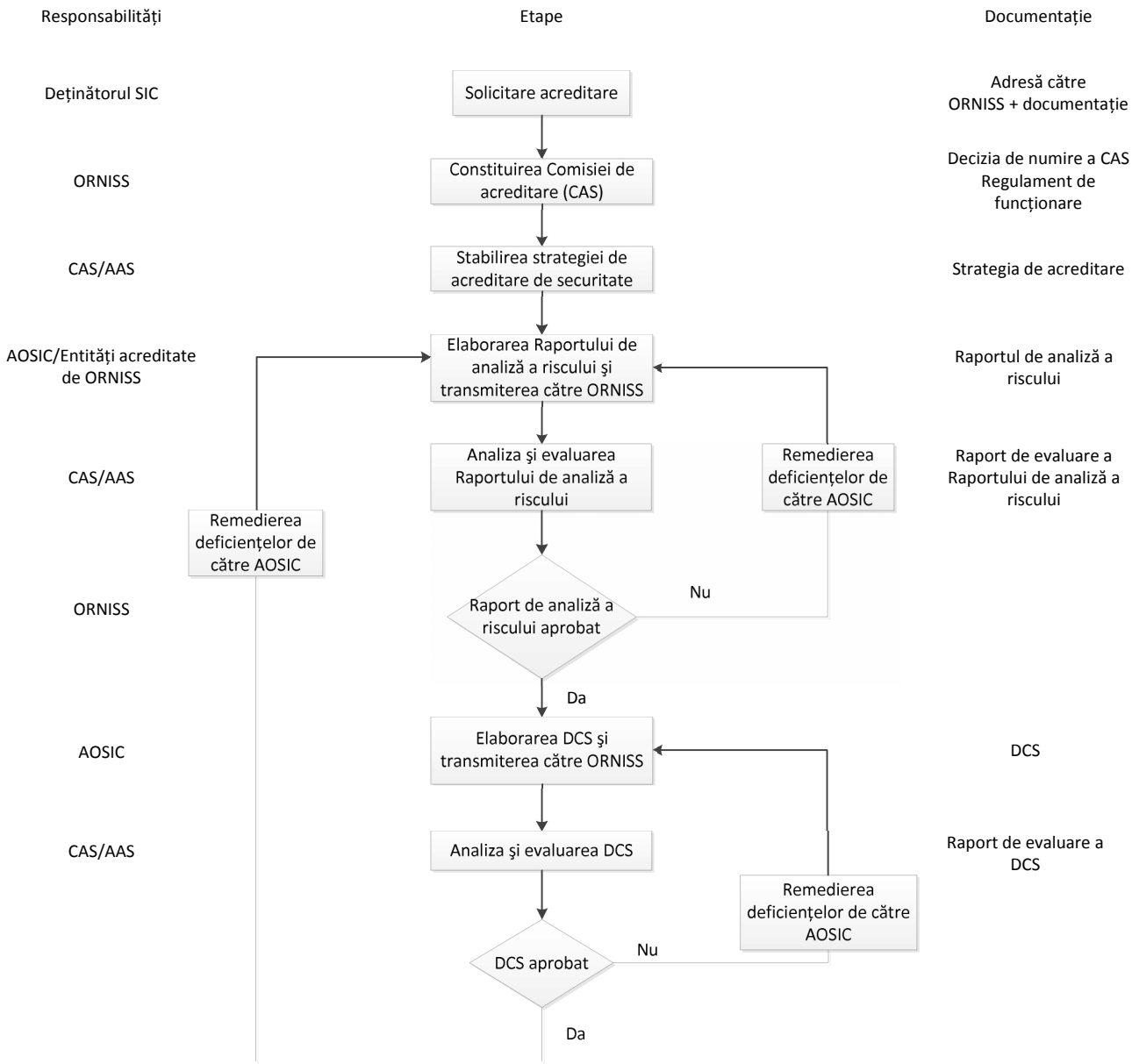
ART. 26

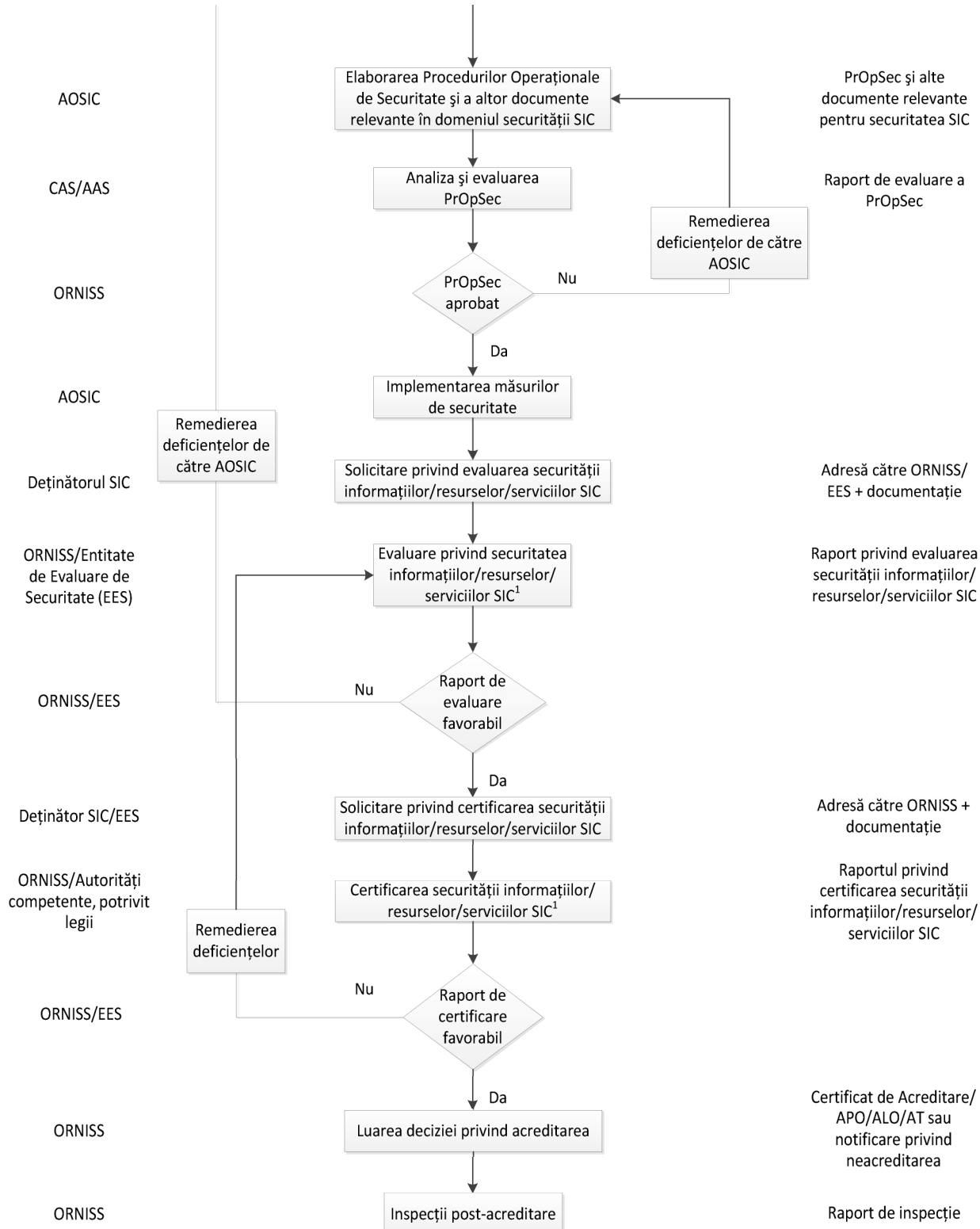
(1) Activitățile INFOSEC sunt derulate de-a lungul întregului ciclu de viață al SIC şi trebuie corelate cu procesul de acreditare de securitate în conformitate cu precizările din anexa nr. 1.

(2) Succesiunea etapelor în cadrul procesului de acreditare de securitate a SIC este iterativă şi continuă, ca urmare a modificărilor aduse acestuia de-a lungul ciclului său de viață, schimbări care impun reluarea procesului de management al riscurilor de securitate.

(3) Etapele principale ale procesului de acreditare de securitate a SIC sunt prezentate în următoarea figură:

Etapele procesului de acreditare de securitate





1 – Încadrarea acestei activități pe această poziție s-a realizat din considerente logice, neavând caracter obligatoriu din punct de vedere cronologic.

SECȚIUNEA a 2-a
Solicitarea acreditării

ART. 27

(1) Reprezentantul legal al persoanei juridice de drept public sau privat solicită, printr-o adresă oficială transmisă la ORNISS, declanşarea procesului de acreditare de securitate a SIC pe care îl are în responsabilitate.

(2) Cererea de acreditare de securitate a SIC va fi însoțită de următoarele precizări:

a) elemente care să susțină necesitatea de acces la informații clasificate, cum ar fi, de exemplu, o copie a hotărârii Guvernului prin care este aprobată lista proprie cuprinzând categoriile de informații secrete de stat pe niveluri de secretizare, documentație care să confirme demararea procedurilor de obținere a unui certificat de securitate industrială etc.;

b) nivelul maxim de clasificare a informațiilor care vor fi stocate, procesate sau transmise în SIC;

c) descrierea generală a SIC: scop, configurație hardware şi software, amplasare, interconectare etc.;

d) modul de operare de securitate al SIC;

e) abrevierea denumirii SIC;

f) datele de contact ale personalului având responsabilități în domeniul protecției informațiilor clasificate stocate, procesate sau transmise în format electronic.

(3) În cazul în care documentația care însoțeşte cererea privind acreditarea de securitate a SIC este completă, AAS inițiază demersurile de constituire a CAS şi de elaborare a strategiei de acreditare de securitate. În caz contrar, ORNISS va informa solicitantul în vederea furnizării informațiilor adiționale necesare.

SECȚIUNEA a 3-a
Constituirea CAS

ART. 28

Rolul CAS este de a gestiona implementarea strategiei de acreditare de securitate a SIC.

ART. 29

(1) Directorul General al ORNISS stabileşte, prin ordin, la propunerea AAS, componența CAS a SIC.

(2) Activitatea CAS se desfăşoară în conformitate cu regulamentul de organizare şi funcționare aprobat de directorul general al ORNISS.

SECȚIUNEA a 4-a
Elaborarea strategiei de acreditare de securitate

ART. 30

(1) CAS elaborează strategia de acreditare de securitate prin care se stabilesc condițiile în care SIC va fi acreditat.

(2) Strategia de acreditare de securitate este aprobată de directorul general al ORNISS şi include următoarele aspecte:

a) scopul şi obiectivele procesului de acreditare de securitate;

b) descrierea SIC;

c) documentația care trebuie elaborată în vederea luării deciziei privind acreditarea de securitate;

d) autoritățile şi structurile implicate în procesul de acreditare de securitate şi responsabilitățile acestora;

e) cerințele privind derularea procesului de management al riscului de securitate;

f) cerințele privind etapele de evaluare şi certificare a securității informațiilor, resurselor şi serviciilor SIC;

g) graficul activităților care trebuie desfăşurate în cadrul procesului de acreditare de securitate;

h) procesele menite să asigure menținerea acreditării de securitate a SIC.

(3) ORNISS transmite strategia de acreditare de securitate aprobată tuturor celor implicați în procesul de acreditare de securitate a SIC, în termen de maximum 30 de zile de la data înregistrării la ORNISS a documentației complete prevăzute la art. 27 alin. (2).

SECȚIUNEA a 5-a
Elaborarea raportului de analiză a riscului

ART. 31

Procesul de management al riscului de securitate se desfăşoară pe toată durata ciclului de viață al SIC şi constă în parcurgerea etapelor de analiză a riscului şi de reducere a acestuia la un nivel acceptabil.

ART. 32

Managementul riscului de securitate este obligatoriu pentru toate SIC naționale care stochează, procesează sau transmit informații clasificate.

ART. 33

Analiza riscului de securitate poate fi desfăşurată de persoana juridică ce administrează SIC supus procesului de acreditare de securitate sau de către o entitate acreditată de ORNISS pentru realizarea acestui tip de activitate. Este foarte important ca analiza riscului să fie desfăşurată de o echipă de experți bine pregătiți în domeniile: administrarea şi organizarea securității, securitatea fizică, securitatea personalului, securitatea documentelor, INFOSEC.

ART. 34

La finalizarea procesului de analiză a riscului se întocmeşte raportul privind analiza riscului de securitate care prezintă riscurile privind producerea unor evenimente nedorite, nivelurile asociate acestora, cum ar fi, de exemplu, mic, mediu, mare, recomandările privind măsurile de securitate care conduc la reducerea lor, precum şi nivelurile riscurilor reziduale rezultate.

SECȚIUNEA a 6-a
Analizarea, evaluarea şi aprobarea raportului de analiză a riscului

ART. 35

(1) Raportul de analiză a riscului de securitate va fi supus unei analize de către CAS, care va transmite reprezentantului legal al persoanei juridice care are în responsabilitate SIC şi entității acreditate de ORNISS, după caz, un document care are drept obiect evaluarea acestui raport sau raportul de analiză a riscului aprobat. Documentul de evaluare întocmit de ORNISS sau raportul de analiză a riscului aprobat va fi transmis în termen de maximum 30 zile de la data înregistrării raportului de analiză a riscului la ORNISS.

(2) Raportul de analiză a riscului de securitate este:

a) asumat de reprezentantul legal al persoanei juridice care are în responsabilitate SIC;

b) dacă este cazul, asumat de reprezentantul legal al entității acreditate de ORNISS care a efectuat analiza riscului;

c) aprobat de ORNISS.

SECȚIUNEA a 7-a
Elaborarea DCS

ART. 36

(1) DCS se întocmeşte pentru toate SIC care stochează, procesează sau transmit informații clasificate.

(2) DCS este elaborată de AOSIC, în colaborare cu toate structurile implicate în proiect, cum ar fi: structura de securitate, structura de planificare şi implementare a SIC, managerul de proiect.

(3) DCS, reprezentând acordul obligatoriu între AOSIC şi AAS, se constituie într-o documentație completă şi explicită a principiilor de securitate care trebuie avute în vedere şi a cerințelor detaliate de securitate care trebuie îndeplinite.

(4) În elaborarea DCS trebuie să se aibă în vedere următoarele criterii:

a) politica națională/NATO/UE de securitate, după caz;

b) rezultatele procesului de management al riscului de securitate, inclusiv parametrii impuşi care se referă la mediul operațional, cum ar fi: cel mai scăzut nivel al certificatului de securitate al personalului, cel mai ridicat nivel de clasificare a informațiilor stocate, procesate sau transmise, modul de operare de securitate sau cerințele pentru utilizatori;

c) politicile de securitate ale rețelelor care se interconectează.

(5) DCS poate fi revizuită în fiecare etapă a ciclului de viață al SIC, de la planificarea şi până la scoaterea din uz a acestuia.

(6) DCS poate fi alcătuită din unul sau mai multe documente, în funcție de natura şi complexitatea SIC, astfel:

(i) CSSS - prezintă aspectele de securitate specifice fiecărui SIC;

(ii) CSC - în cazul în care comunitatea de interese este alcătuită din mai multe SIC interconectate sau când o organizație are un număr de SIC care operează în cadrul aceluiaşi mediu global de securitate. În plus, CSC trebuie să faciliteze însumarea unei serii bilaterale de documente cu cerințe de securitate pentru interconectarea sistemelor, denumite CSIS, şi trebuie să stabilească standardele de securitate care trebuie aplicate oricărui SIC care urmează să se alăture comunității;

(iii) CSIS - prezintă aspectele de securitate ale interconectării efective între diferite SIC.

(7) Componența DCS se stabileşte prin strategia de acreditare de securitate.

ART. 37

În cazul interconectării SIC, CAS va stabili responsabilitățile privind elaborarea CSC şi a CSIS, în funcție de structura care asigură managementul proiectului. Această structură va asigura şi transmiterea către ORNISS a documentației de securitate privind interconectarea.

ART. 38

CSSS şi PrOpSec vor îndeplini cerințele din CSC şi CSIS şi vor fi elaborate de autoritatea operațională a fiecărui SIC care se interconectează, având în vedere condițiile de securitate din mediul operațional al fiecărui sistem.

SECȚIUNEA a 8-a
Analizarea, evaluarea şi aprobarea DCS

ART. 39

(1) În cadrul acestei etape, CAS analizează şi evaluează DCS pentru a stabili dacă aceasta este elaborată în acord cu criteriile stabilite la art. 36 alin. (4). Având în vedere faptul că DCS poate fi modificată pe parcursul ciclului de viață al SIC, versiunile actualizate ale DCS vor fi transmise AAS.

(2) CAS întocmeşte şi transmite solicitantului un raport de analiză a DCS sau DCS aprobată, în termen de maximum 30 de zile de la data înregistrării la ORNISS a DCS.

SECȚIUNEA a 9-a
Elaborarea PrOpSec şi a altor documente relevante în domeniul securității SIC

ART. 40

(1) PrOpSec reprezintă descrierea precisă a implementării cerințelor de securitate definite anterior în DCS, a procedurilor operaționale care trebuie urmate şi responsabilităților personalului SIC.

(2) PrOpSec sunt întocmite de către AOSIC, în conformitate cu normele INFOSEC emise de ORNISS şi cu documentația specifică rețelelor cu care se interconectează, după caz. Acest document este înaintat către AAS pentru analiză, evaluare şi aprobare.

(3) În funcție de configurația SIC, în cadrul strategiei de acreditare de securitate a SIC se vor preciza şi alte documente relevante pentru securitatea SIC, necesar a fi întocmite în susținerea procesului de acreditare.

SECȚIUNEA a 10-a
Analizarea, evaluarea şi aprobarea PrOpSec

ART. 41

(1) În cadrul acestei etape, documentul privind PrOpSec este analizat şi evaluat de către CAS pentru a stabili dacă cerințele de securitate sunt îndeplinite prin stabilirea corespunzătoare a procedurilor operaționale respective.

(2) CAS întocmeşte şi transmite solicitantului un raport de analiză a PrOpSec sau PrOpSec aprobate, în termen de maximum 30 de zile de la data înregistrării la ORNISS a PrOpSec.

SECȚIUNEA a 11-a
Implementarea măsurilor de securitate

ART. 42

Responsabilitatea implementării măsurilor de securitate aprobate prin documentația de securitate revine AOSIC.

SECȚIUNEA a 12-a
Testarea şi evaluarea securității informațiilor, resurselor şi serviciilor SIC

ART. 43

Prin strategia de acreditare de securitate a SIC se stabilesc responsabilitățile privind desfăşurarea activităților de testare şi evaluare a securității informațiilor, resurselor şi serviciilor SIC.

ART. 44

(1) Testarea şi evaluarea securității este o activitate de analiză, evaluare şi testare comprehensivă a măsurilor de securitate tehnice şi nontehnice, operaționale şi de management al securității informațiilor, resurselor şi serviciilor SIC, în vederea stabilirii gradului în care măsurile satisfac cerințele de securitate stabilite prin DCS, sunt corect implementate, sunt eficiente şi a gradului în care sunt respectate procedurile de securitate aprobate pentru sistem.

(2) Testarea şi evaluarea securității au rolul de a stabili măsura în care sistemul de protecție implementat îndeplineşte obiectivele securității informațiilor, resurselor şi serviciilor SIC.

(3) În vederea verificării faptului dacă măsurile de securitate sunt implementate şi respectate în conformitate cu cerințele de securitate, în cadrul activității de evaluare se efectuează testări privind securitatea SIC sau a componentelor sale, după caz, în baza unui plan de testare şi evaluare.

(4) Rezultatele activității de testare şi evaluare a securității sunt prezentate într-un raport, care trebuie să conțină constatările verificării, să identifice deficiențele existente în implementarea măsurilor de securitate sau în asigurarea obiectivelor securității şi să formuleze recomandările privind măsurile corective necesare.

(5) Dacă în cadrul etapei de testare şi evaluare a securității se identifică noi riscuri de securitate care pot afecta obiectivele securității informațiilor, resurselor şi serviciilor SIC, aceste riscuri vor fi evidențiate în cadrul raportului privind testarea şi evaluarea securității SIC, care va cuprinde şi recomandări privind măsuri de securitate suplimentare care să conducă la reducerea acestor riscuri.

SECȚIUNEA a 13-a
Certificarea securității informațiilor, resurselor şi serviciilor SIC

ART. 45

(1) Prin strategia de acreditare de securitate a SIC se stabilesc responsabilitățile privind desfăşurarea activităților de certificare privind securitatea informațiilor, resurselor şi serviciilor SIC.

(2) Certificarea securității informațiilor, resurselor şi serviciilor SIC reprezintă activitatea care are drept scop verificarea rezultatelor obținute în cadrul etapei de testare şi evaluare a securității informațiilor, resurselor şi serviciilor SIC, precum şi modalitatea în care s-a desfăşurat aceasta.

(3) În cadrul procesului de certificare, care constă într-o analiză independentă a rezultatelor obținute în urma etapei de testare şi evaluare de securitate, precum şi a modalității în care s-a desfăşurat această activitate, trebuie să se analizeze următoarele aspecte:

a) resursele folosite în cadrul testării şi evaluării de securitate, cum ar fi, timpul, banii etc.;

b) personalul care a realizat testarea şi evaluarea de securitate (calificare, obiectivitate, imparțialitate etc.);

c) procesele derulate în cadrul testării şi evaluării (mecanismele tehnice de evaluare, coordonarea corespunzătoare a constatărilor şi recomandărilor, tehnicile şi instrumentele utilizate, alocarea resurselor pentru utilizarea instrumentelor, realizarea analizelor şi prezentarea concluziilor);

d) raportul privind testarea şi evaluarea (recomandările şi concluziile sunt corespunzătoare; activitatea de evaluare a fost concentrată pe elementele relevante; analizarea ariilor cu probleme majore de securitate; existența unor măsuri de securitate neevaluate care ar putea influența concluziile; stabilirea recomandărilor în funcție de priorități şi baza pe care s-au stabilit prioritățile; vulnerabilități reziduale identificate; recomandările şi opiniile sunt rezultatul unei informări corespunzătoare).

(4) Rezultatele activității de certificare de securitate vor face obiectul unui raport.

(5) Dacă, în urma activității de certificare, se constată deficiențe în procesul de evaluare de securitate, atunci raportul se transmite entității de evaluare de securitate în vederea remedierii acestora.

SECȚIUNEA a 14-a
Luarea deciziei privind acreditarea de securitate a SIC

ART. 46

După parcurgerea activităților necesare luării unei decizii privind acreditarea de securitate a SIC, la propunerea CAS, directorul general al ORNISS are la dispoziție următoarele opțiuni:

a) acreditarea deplină (AD) - decizie de acreditare pentru o perioadă specificată de timp, pentru mediul operațional stabilit inițial, atunci când nu trebuie să fie îndeplinite condiții specificate în prealabil. În urma acordării AD, se emite certificatul de acreditare de securitate, pentru o perioadă de maximum 3 ani;

b) aprobarea limitată de operare (ALO) - pentru operarea SIC în afara mediului operațional stabilit inițial, cum ar fi, de exemplu: modificarea conținutului inițial al misiunii SIC, gestionarea unei situații de criză, operațiuni mai restrictive, misiuni unice cu durată limitată;

c) aprobarea provizorie de operare (APO) - decizie de acreditare prin care sunt identificate foarte clar condițiile pentru APO, activitățile ce vor fi întreprinse şi realizate înainte de obținerea AD, cum ar fi, de exemplu: contramăsurile adiționale care vor fi implementate, aprobarea versiunii finale a documentației de securitate. Perioada pentru care se acordă acest tip de acreditare poate fi de maximum 12 luni calendaristice;

d) aprobarea pentru testare (AT) - decizie de acreditare prin care sunt identificate foarte clar condițiile, cum ar fi: sfera de acțiune în care SIC va fi testat, nivelul maxim de clasificare a informațiilor implicate în testare;

e) neacreditarea - decizie datorată identificării unor deficiențe grave referitoare la securitatea SIC. AAS va recomanda perioada în care trebuie să se desfăşoare activitățile de corectare a deficiențelor constatate.

ART. 47

Certificatul de acreditare de securitate emis de ORNISS confirmă faptul că măsurile de securitate sunt conforme cu legislația în domeniu şi rezultatele analizei riscurilor de securitate sunt implementate corespunzător şi asigură nivelul de încredere corespunzător pentru SIC în condițiile prezentate în documentația de securitate.

ART. 48

Reprezentantul legal al persoanei juridice care deține SIC are obligația de a remite la ORNISS certificatul/aprobarea expirată sau anulată de către ORNISS, în termen de maximum 10 zile de la data expirării/anulării acestora.

CAP. V
Acreditarea de securitate a unui SIC într-un mediu de achiziție şi implementare etapizat

ART. 49

(1) În numeroase situații, organizațiile care exploatează un SIC adoptă o politică de achiziție şi implementare în mai multe faze, ceea ce conduce la un proces de acreditare de securitate etapizat.

(2) Într-un mediu de achiziție şi implementare etapizat pot exista două situații:

a) SIC în care etapele de dezvoltare sunt planificate de la începutul proiectului, cerințele finale care trebuie îndeplinite fiind cunoscute;

b) SIC în care achizițiile nu urmează un plan prestabilit.

ART. 50

(1) În situația prevăzută la art. 49 alin. (2) lit. a), procesul etapizat de acreditare de securitate este uşor de aplicat. DCS pentru un astfel de SIC trebuie să descrie aspectele finale privind rolul şi configurația SIC, mediile de securitate, cerințele de securitate şi măsurile de securitate, precum şi aspectele de detaliu ale cerințelor şi măsurilor de securitate pentru fiecare etapă de dezvoltare.

(2) Pentru fiecare etapă planificată, DCS trebuie să prezinte restricțiile ce sunt necesare a fi aplicate şi condițiile care trebuie îndeplinite în etapele ulterioare, pentru ca aceste restricții să fie ridicate.

ART. 51

(1) În situația prevăzută la art. 49 alin. (2) lit. a), acreditarea de securitate trebuie obținută după fiecare etapă de dezvoltare prevăzută în DCS aprobată. Acest scenariu reflectă faptul că acreditarea de securitate este un proces continuu.

(2) Într-un mediu de achiziție şi implementare etapizat, procesul de acreditare de securitate poate fi întrerupt în orice moment dacă etapele ulterior planificate pentru dezvoltarea SIC nu sunt realizate. În acest caz SIC va fi acreditat în configurația realizată în urma ultimei achiziții.

ART. 52

În situația prevăzută la art. 49 alin. (2) lit. b), procesul de acreditare de securitate nu este planificat din faza de debut a proiectului prevăzut a se desfăşura etapizat, reprezentând în general situațiile în care pentru un SIC existent apare necesitatea operațională de extindere sau de interconectare. În această situație, este necesar a se evalua starea de securitate a SIC, prin derularea procesului de management al riscului de securitate, stabilindu-se cerințele şi măsurile de securitate adiționale, care vor fi documentate în DCS.

CAP. VI
Activități postacreditare

SECȚIUNEA 1
Activități principale

ART. 53

Măsurile de securitate stabilite prin documentația de securitate a SIC trebuie menținute şi testate de către AOSIC, de-a lungul perioadei de acreditare de securitate a SIC.

ART. 54

După acordarea autorizării de funcționare a SIC, AAS desfăşoară periodic inspecții în vederea stabilirii gradului în care măsurile de securitate implementate sunt conforme cu reglementările în vigoare, rezultatele managementului riscului de securitate şi documentația de securitate a SIC.

ART. 55

(1) Structurile de planificare şi implementare ale SIC şi AOSIC au responsabilitatea să informeze ORNISS cu privire la propunerile de modificare a configurației SIC, schimbările în cerințele operaționale ale sistemului, schimbările privind nivelul de clasificare a informațiilor stocate, procesate sau transmise în SIC ori oricare alte modificări aduse sistemului.

(2) Modificările vor fi efectuate numai după aprobarea acestora de către ORNISS.

(3) ORNISS oferă consultanță cu privire la implicațiile pe care le pot avea asupra securității modificările propuse. În acest scop, condițiile pentru reacreditarea de securitate trebuie să fie clar definite în DCS.

ART. 56

ORNISS acordă asistență AOSIC pentru investigarea oricăror încălcări ale măsurilor de securitate şi a situațiilor în care se suspectează încălcarea acestora.

ART. 57

Situațiile care conduc la necesitatea reacreditării de securitate a SIC sunt următoarele, fără a se limita la acestea:

a) schimbarea nivelului de clasificare a informațiilor, care are ca efect o schimbare a măsurilor de securitate;

b) schimbarea cerințelor de securitate, ca urmare a schimbării politicii naționale de securitate;

c) schimbarea amenințărilor la adresa SIC sau a vulnerabilităților SIC ori ale unui SIC cu care acesta este conectat;

d) modificări ale mediului de securitate global, mediului de securitate local sau mediului de securitate electronic, cum ar fi schimbări ale componentelor software de securitate sau ale celor relevante pentru securitate, după caz. Relevanța modificărilor asupra securității sistemului se analizează şi se evaluează de către AOSIC şi se notifică AAS;

e) încălcarea normelor de securitate, violarea securității SIC sau un eveniment nedorit care poate determina anularea aprobării de funcționare prin descoperirea unor breşe în proiectarea securității;

f) schimbarea semnificativă a măsurilor de securitate fizică implementate sau a conținutului documentului PrOpSec;

g) schimbarea semnificativă a configurației SIC, de exemplu, conectarea unor stații de lucru la un SIC, în afara configurației aprobate;

h) pentru rețele, includerea unui alt SIC, acreditat separat, sau modificarea/înlocuirea SIC conectate;

i) rezultatele unei verificări efectuate de către AAS.

ART. 58

(1) În situația în care pentru un SIC care deține un certificat de acreditare de securitate există necesitatea de a stoca, de a procesa sau de a transmite informații clasificate şi după termenul de valabilitate al acestuia, persoana juridică ce are în responsabilitate SIC va solicita reacreditarea de securitate a SIC.

(2) Solicitarea prevăzută la alin. (1) va fi transmisă la ORNISS cu minimum 3 luni înainte de expirarea termenului de valabilitate a certificatului de acreditare de securitate şi va cuprinde datele prevăzute la art. 27 alin. (2).

ART. 59

ORNISS poate decide anularea/suspendarea aprobării de funcționare acordate unui SIC când, după caz, se constată încălcarea gravă a normelor de securitate, încetarea activității persoanei juridice de drept public sau privat care deține SIC, modificarea domeniului de activitate al acesteia, apariția unor modificări în cadrul persoanei juridice care conduc la neavizarea Programului de prevenire a scurgerii de informații clasificate sau orice altă situație care poate afecta grav obiectivele securității SIC.

ART. 60

CAS stabileşte, prin strategia de reacreditare de securitate, activitățile necesar a fi derulate în vederea obținerii unei noi aprobări, în funcție de modificările suferite în SIC.

ART. 61

AAS asigură evidența la nivel național a informațiilor referitoare la acreditarea tuturor SIC naționale ce stochează, procesează sau transmit informații clasificate.

SECȚIUNEA a 2-a
Încetarea funcționării SIC/dezafectarea echipamentelor

ART. 62

În cazul în care un SIC național care stochează, procesează sau transmite informații clasificate îşi încetează activitatea sau echipamentele sale sunt dezafectate, AOSIC adresează o solicitare ORNISS sau entității de evaluare de securitate, care va acorda consultanță pentru a se asigura că:

a) documentele, inclusiv mediile de stocare fixe şi amovibile asociate SIC, precum şi informațiile necesare evidenței sunt, după caz, arhivate, declasificate sau distruse în conformitate cu prevederile legale în vigoare;

b) dezafectarea şi distrugerea produselor, sistemelor criptografice şi materialelor asociate se realizează în conformitate cu procedurile legale;

c) echipamentele din care s-au extras mediile de stocare se utilizează în medii controlate şi securizate.

ART. 63

Anexa nr. 4 prezintă o bibliografie a reglementărilor şi documentelor cu relevanță în domeniu.

ART. 64

Anexele nr. 1-4 fac parte integrantă din prezenta directivă.

ANEXA 1
la directivă

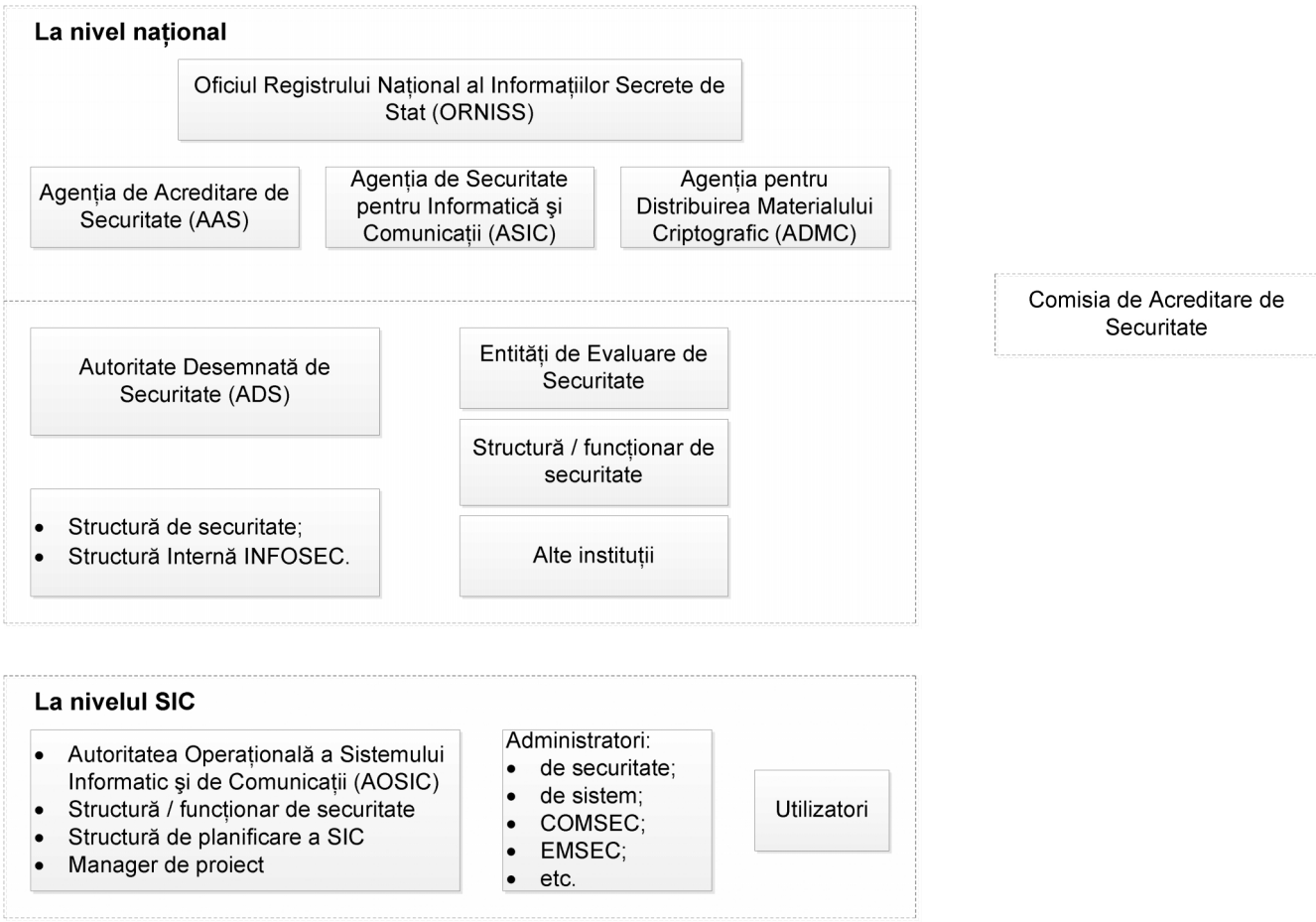
Corelația dintre activitățile INFOSEC de-a lungul întregului ciclu de viață al SIC şi procesul de acreditare de securitate a SIC

Etapa ciclului de viață al SIC	Procesele ciclului de viață al SIC	Cerințe de acreditare de securitate	Produse INFOSEC
Planificarea SIC	1. Stabilirea cerințelor operaționale şi de securitate 2. Procesul de definire a Pachetului de Capacități şi a documentației asociate	1. Evaluarea inițială a riscului 2. Versiunea inițială a documentației de securitate	Instrumente manuale sau automate de evaluare a riscului şi de management al riscului
Dezvoltarea şi achiziția SIC	1. Procesul de definire a categoriilor de costuri şi a costului estimat 2. Procesul de elaborare a specificațiilor 3. Dezvoltarea SIC 4. Achiziția SIC	1. Evaluarea detaliată a riscului 2. Îmbunătățirea DCS (de exemplu, CSC, CSSS, CSIS) 3. Stabilirea cerințelor pentru testarea şi evaluare a securității şi elaborarea planului de testare şi evaluare a securității	1. Instrumente de definire a cerințelor de securitate 2. Standarde de evaluare a securității IT 3. Alegerea Profilului de Protecție (PP). 4. Pachete de protecție 5. Ținta de securitate 6. Instrumente manuale sau automate de evaluare a riscului şi de management al riscului
Implementarea SIC şi acreditarea de securitate	Operaționalizarea SIC - implementarea sistemului - testarea de acceptanță - finalizarea documentației proiectului	1. Managementul riscului la adresa securității 2. Verificarea implementării securității 3. Acreditarea de securitate	1. Produsele INFOSEC 2. Catalogul național de pachete, produse şi profile de protecție INFOSEC
Exploatarea SIC	Exploatarea operațională a SIC	1. Proceduri Operaționale de Securitate (PrOpSec) 2. Continuarea procesului de management al riscului la adresa securității 3. Inspecții / verificări de securitate.	Instrumente de securitate

Etapa ciclului de viață al SIC	Procesele ciclului de viață al SIC	Cerințe de acreditare de securitate	Produse INFOSEC
Dezvoltarea/ Modificarea SIC	1. Procese specifice de dezvoltare 2. Achiziția SIC 3. Operaționalizarea SIC - Implementarea modificărilor - Testarea securității	1. Managementul riscului la adresa securității 2. Actualizarea documentației de securitate (de exemplu, CSC, CSSS, CSIS, PrOpSec) 3. Stabilirea cerințelor de testare şi evaluare a securității şi a planului de testare şi evaluare a securității 4. Verificarea implementării securității 5. Reacreditarea de securitate	1. Instrumente de definire a cerințelor de securitate 2. Standarde de evaluare a securității IT 3. Alegerea PP 4. Pachete de protecție 5. Ținta de securitate 6. Produse INFOSEC 7. Catalogul național de pachete, produse şi profile de protecție INFOSEC
Scoaterea SIC din exploatare	1. Arhivarea/declasificarea/ distrugerea documentelor, inclusiv a mediilor de stocare 2. Scoaterea din uz şi distrugerea produselor şi sistemelor criptografice	Actualizarea evidențelor	Catalogul național de pachete, produse şi profile de protecție INFOSEC

ANEXA 2
la directivă

Structuri implicate în procesul de acreditare de securitate a SIC



ANEXA 3
la directivă

COMISIA DE ACREDITARE DE SECURITATE (CAS)
Regulament de organizare şi funcționare

- model -

I. Introducere
Referințe:
1. Standardele naționale de protecție a informațiilor clasificate în România, aprobate prin Hotărârea Guvernului nr. 585/2002, cu modificările şi completările ulterioare
2. Normele privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România, aprobate prin Hotărârea Guvernului nr. 353/2002, cu modificările ulterioare
3. Directiva privind acreditarea de securitate a sistemelor informatice şi de comunicații (SIC) care stochează, procesează sau transmit informații clasificate - INFOSEC 13, aprobată prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 108/2012
4. Alte documente relevante
II. Se va realiza o prezentare generală a SIC (de către AOSIC)
Compunerea CAS pentru ..... (denumirea SIC)
III. CAS pentru ..... (denumirea SIC) este stabilită în conformitate cu cerințele documentelor de referință prevăzute la pct. I sub conducerea ....., având următoarea componență (după caz):
a) reprezentanți ORNISS;
b) reprezentanți ai ADS pe domeniul de competență;
c) managerii de proiect;
d) reprezentanții AOSIC implicate;
e) reprezentanți ai structurilor de securitate ai SIC;
f) reprezentanți ai structurilor de planificare şi implementare a SIC;
g) responsabilii cu securitatea criptografică, a transmisiilor, a emisiilor etc.;
h) reprezentanți ai altor autorități având competențe (de exemplu: autorități de certificare a unor componente ale SIC).
IV. Misiunea CAS pentru ..... (denumirea SIC)
Principala misiune a CAS pentru ..... (denumirea SIC) este de a obține acreditarea ..... (denumirea SIC). În plus, misiunea CAS pentru (denumirea SIC) este de a oferi consultanță în vederea stabilirii unui sistem efectiv de protecție a informațiilor vehiculate prin ..... (denumirea SIC) care să asigure confidențialitatea, integritatea şi disponibilitatea informațiilor clasificate. CAS pentru ..... (denumirea SIC) va exista pe întreaga perioadă a ciclului de viață a sistemului.
V. Responsabilitățile CAS pentru ..... (denumirea SIC)
CAS pentru ..... (denumirea SIC) are următoarele responsabilități, după caz:
a) asigură asistență şi îndrumare în domeniul INFOSEC pentru conducerea proiectului ..... (denumirea SIC);
b) asigură asistență şi îndrumare structurilor de securitate a ..... (denumirea SIC) cu privire la condițiile de acreditare şi reacreditare;
c) elaborează strategia de acreditare de securitate a ..... (denumirea SIC) şi gestionează implementarea acesteia. Procesul de acreditare poate varia în funcție de situație, dar trebuie să fie în conformitate cu cerințele prevăzute de legislația în domeniu;
d) recomandă standardele minime de securitate pentru implementarea specifică;
e) recomandă cerințele pentru evaluarea şi certificarea securității;
f) asigură consultanță în procesul de evaluare a securității pentru ..... (denumirea SIC);
g) analizează şi evaluează documentația de securitate a ..... (denumirea SIC);
h) acordă consultanță cu privire la conținutul viitoarelor versiuni ale documentației de securitate a ..... (denumirea SIC);
i) acordă consultanță cu privire la strategia propusă pentru îndeplinirea cerințelor de securitate;

j) acordă asistență structurilor de securitate în abordarea aspectelor de securitate ale cerințelor operaționale, pe baza CSC şi a documentației de securitate aprobate de către ORNISS;

k) acordă consultanță managerului de proiect al ..... (denumirea SIC) cu privire la implicațiile pe care schimbările configurației SIC, cerințelor operaționale sau nivelului de clasificare a informațiilor vehiculate în SIC le au asupra securității;

l) asigură consultanță pentru stabilirea memorandumurilor de înțelegere privind aspectele de management al securității şi pentru definirea şi acceptarea responsabilităților de către părțile implicate în cazul interconectării;

m) formulează propunerile privind luarea deciziei;

n) elaborează documentul oficial privind acreditarea de securitate a SIC;

o) stabileşte cerințele pentru evaluările periodice privind menținerea eficienței măsurilor de securitate.

VI. Raportarea

CAS pentru ..... (denumirea SIC) va raporta periodic AAS aspectele legate de derularea procesului de acreditare de securitate a ..... (denumirea SIC).

VII. Reuniunile de lucru

CAS pentru ..... (denumirea SIC) se reuneşte ori de câte ori este necesară rezolvarea unor aspecte aferente procesului de acreditare de securitate a SIC.

ANEXA 4
la directivă

Bibliografie

1. Legea nr. 182/2002 privind protecția informațiilor clasificate, cu modificările şi completările ulterioare.
2. North Atlantic Council, Security within the North Atlantic Treaty Organisation (NATO) C-M (2002) 49.
3. Decizia 2011/292/UE a Consiliului din 31 martie 2011 privind normele de securitate pentru protecția informațiilor UE clasificate.
4. Ordonanța de urgență a Guvernului nr. 153/2002 privind organizarea şi funcționarea Oficiului Registrului Național al Informațiilor Secrete de Stat, aprobată prin Legea nr. 101/2003, cu modificările şi completările ulterioare.
5. Standardele naționale de protecție a informațiilor clasificate în România, aprobate prin Hotărârea Guvernului nr. 585/2002, cu modificările şi completările ulterioare.
6. Normele privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România, aprobate prin Hotărârea Guvernului nr. 353/2002, cu modificările ulterioare.
7. North Atlantic Council, INFOSEC Management Directive for CIS, AC 35/-D/2005 - Rev. 2, oct. 2010.
8. North Atlantic Council, Guidelines for the Security Accreditation of CIS, AC/35 - D/1021 - Rev. 3, ianuarie 2012.
9. Council of the European Union, IA Security Guidelines on CIS Security Accreditation IASG 1-01, martie 2012.
10. Directiva privind structurile cu responsabilități în domeniul INFOSEC - INFOSEC 1, aprobată prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 482/2003.
11. Directiva principală privind domeniul INFOSEC - INFOSEC 2, aprobată prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 483/2003.
12. Directiva privind managementul INFOSEC pentru sisteme informatice şi de comunicații - INFOSEC 3, aprobată prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 484/2003.
13. Metodologia de acreditare a entităților pentru evaluarea produselor de securitate IT şi a sistemelor informatice şi de comunicații - INFOSEC 12, aprobată prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 23/2012.
14. Metodologia privind acreditarea structurilor interne INFOSEC din cadrul autorităților desemnate de securitate - INFOSEC 11, aprobată prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 12/2006.