ANEXA NR. 1
la Metodologia
de acreditare

CRITERII DE ACREDITARE

A. MANAGEMENT

A.1 Cerințe privind statutul juridic

C1 Entitatea evaluatoare trebuie să aibă personalitate juridică.

A.2 Cerințe privind organizarea

C2 În cazul în care entitatea evaluatoare face parte dintr-o persoană juridică cu un obiect de activitate mai larg, responsabilitățile personalului de conducere care participă la activitățile pentru care entitatea evaluatoare solicită acreditarea sau care le poate influența trebuie clar definite, pentru a evita eventuale conflicte de interese.

C3 Entitatea evaluatoare şi personalul său nu trebuie să fie supuşi nici unor presiuni de ordin comercial, financiar sau de altă natură, care să le afecteze capacitatea de decizie sau calitatea activităților întreprinse.

De exemplu, orice presiune asupra deciziilor privind activitatea pentru care se solicită acreditarea, exercitată de persoane sau organizații din afara entității evaluatoare, trebuie exclusă.

C4 Entitatea evaluatoare nu trebuie să fie implicată în nici o activitate care poate avea un impact negativ asupra independenței activităților întreprinse. Procedurile aplicabile la nivelul entității evaluatoare trebuie să asigure respectarea acestei cerințe. Termenul de separare a activităților care pot influența evaluarea va fi de cel puțin 3 ani.

De exemplu, dacă entitatea evaluatoare oferă şi servicii de consultanță sau soluții de securitate IT acestea nu trebuie în nici un fel să afecteze independența evaluărilor derulate de entitatea evaluatoare prin oferirea unor astfel de servicii simultan cu evaluarea.

C5 Organizarea entității evaluatoare şi responsabilitățile acesteia trebuie atent şi clar definite. Atribuirea responsabilităților trebuie să fie făcută conform regulamentului intern de organizare şi funcționare. Acest regulament trebuie să specifice, suplimentar:

- Persoana juridică din care face parte entitatea evaluatoare şi care este modul de subordonare al acesteia;

- Modul de organizare generală a entității evaluatoare şi structura managementului, cu precizarea responsabilităților fiecărei poziții în activitățile pentru care se solicită acreditarea;
- Modul de organizare a activităților tehnice şi existența următoarelor funcții:
    - Director tehnic – responsabil de operațiile tehnice, gestionează resursele necesare asigurării calității activității de evaluare;
    - Director pentru asigurarea calității – (nu poate deține în acelaşi timp şi funcția de director tehnic) ce are responsabilitatea şi autoritatea de a asigura implementarea sistemului calității. Directorul pentru asigurarea calității trebuie să participe la procesul de luare a deciziilor privind probleme de politici sau legate de resursele entității evaluatoare;
    - Şeful structurii de securitate/funcționarul de securitate al entității evaluatoare – (nu poate deține în acelaşi timp şi funcția de director tehnic) este însărcinat cu definirea şi implementarea procedurilor de securitate în cadrul entității evaluatoare. El va verifica aplicarea procedurilor.

Aceeaşi persoană poate deține una sau mai multe funcții dacă acest lucru este aprobat de directorul general, cu excepția cazurilor menționate mai sus.

C6 Pentru a se asigura permanența îndeplinirii responsabilităților ce revin funcțiilor de conducere, acestea pot fi delegate unor persoane nominalizate în documentație.

C7 Responsabilitatea, autoritatea şi căile de raportare trebuie definite pentru toți membrii entității evaluatoare implicați în activitățile pentru care se solicită acreditarea.

C8 Conducerea entității evaluatoare trebuie să desemneze persoanele responsabile de întocmirea şi semnarea rapoartelor aferente activităților pentru care se solicită acreditarea.

C9 Toate detaliile comerciale privind activitățile pentru care se solicită acreditarea trebuie să fie stabilite prin contract între entitatea evaluatoare sau persoana juridică din care face parte, beneficiarul serviciilor prestate de entitatea evaluatoare şi în anumite cazuri, subcontractori.

A.3 Sistemul de asigurare a calității

C10 Entitatea evaluatoare trebuie să opereze şi să mențină un sistem de calitate adecvat pentru activitatea pentru care se solicită acreditarea. Deținerea unei certificări a calității emisă de o autoritate de certificare autorizată reprezintă un element în favoarea acordării certificatului de acreditare.

C11 Entitatea evaluatoare trebuie să dezvolte şi să aplice proceduri şi instrucțiuni, pentru a asigura calitatea activităților pentru care solicită acreditarea. Personalul trebuie să aibă acces la această

documentație, să o studieze, să o înțeleagă şi să o implementeze. Toți membrii implicați în activități pentru care se solicită acreditarea trebuie să cunoască sistemul de asigurare a calității implementat în cadrul entității evaluatoare.

C12 Obiectivele sistemului de asigurare a calității trebuie să fie definite într-o politică de calitate (Manualul calității). Manualul calității trebuie să includă un angajament al conducerii entității evaluatoare privind asigurarea unei practici profesionale bune şi a unei calități superioare a activităților pentru care se solicită acreditarea. De asemenea, trebuie să includă obiectivele sistemului de calitate şi obligația ca personalul entității evaluatoare să cunoască documentația şi să aplice procedurile. Manualul trebuie, de asemenea, să conțină angajamentul conducerii de a respecta criteriile de acreditare.

C13 Manualul calității trebuie să stabilească structura documentației legate de sistemul de asigurare a calității şi trebuie să conțină sau să facă referire la procedurile implementate în cadrul entității evaluatoare (incluzând procedurile tehnice).

C14 Manualul calității trebuie să stabilească rolurile şi responsabilitățile personalului de conducere şi ale celui din poziții cheie pentru activitățile pentru care se solicită acreditarea.

C15 Entitatea evaluatoare trebuie să definească procedurile necesare administrării tuturor documentelor referitoare la sistemul de asigurare a calității, cum sunt regulamentele, standardele, metodele de evaluare şi alte documente aferente (instrucțiuni, manuale etc.). În special trebuie definite procedurile referitoare la modificări, aprobări şi circuitul documentelor.

A.4 Cerințe de securitate

C16 Entitatea evaluatoare trebuie să definească o politică de securitate, specificând metodele şi condițiile referitoare la protecția informațiilor clasificate aflate în posesia sa. Politica de securitate trebuie aprobată de Oficiul Registrului Național al Informațiilor Secrete de Stat (ORNISS), iar implementarea sa este responsabilitatea funcționarului de securitate/structurii de securitate. Toate persoanele participante la activitățile pentru care se solicită acreditarea trebuie să cunoască şi să respecte această politică.

A.4.1 Proceduri de securitate

C17 Politica de securitate trebuie să definească:

- Obiectivele securității;
  - Structura desemnată cu realizarea acestor obiective;
  - Procedurile de securitate pentru:
    - Protecția/securitatea locației;
    - Securitatea personalului;

- Conştientizarea personalului implicat în activitățile pentru care se solicită acreditarea;
- Protecția informațiilor legate de activitățile pentru care se solicită acreditarea;
- Controlul accesului la informații;
- Protecția arhivelor şi a comunicațiilor;
- Accesul vizitatorilor în entitatea evaluatoare.

Lista nu este exhaustivă, fiind prezentată cu titlu exemplificativ.

- Prevederile referitoare la situațiile anormale identificate în aplicarea politicii şi acțiunile corective ce se impun în aceste situații.

C18 Politica de securitate trebuie să prevadă managementul informațiilor clasificate, indiferent de formatul acestora (hârtie, electronic).

A.4.2 Securitatea personalului

C19 Dacă în cursul activităților pe care le desfăşoară, personalul entității evaluatoare trebuie să aibă acces la informații clasificate, acesta trebuie să dețină certificat de securitate, conform prevederilor legislației naționale în domeniul protecției informațiilor clasificate secret de stat.

C20 Personalul implicat în activitățile pentru care se solicită acreditarea trebuie să semneze un angajament din care să reiasă că a luat cunoştință de şi se angajează să aplice prevederile legislației naționale în domeniul protecției informațiilor clasificate secret de stat şi procedurile de securitate aplicabile în entitatea evaluatoare.

C21 Personalul trebuie să fie instruit să aplice procedurile de securitate stabilite prin politica de securitate.

A.4.3 Securitatea informațiilor

C22 Entitatea evaluatoare trebuie să dezvolte şi să aplice proceduri prin care să asigure protecția informațiilor vehiculate în cursul activităților pentru care se solicită acreditarea. Aceste proceduri trebuie să includă următoarele, dar să nu se limiteze la acestea:

- Securitatea conturilor de utilizatori (securitatea intrărilor în sistem, proceduri de autentificare, parole etc.);
- Separarea accesului la date (separarea datelor aferente activităților acreditate de cele aferente altor activități, separarea datelor provenite de la diferite activități acreditate, protejarea datelor transmise în afara entității evaluatoare, inclusiv prin mecanisme criptografice etc.);

- Securitatea comunicațiilor dintre entitatea evaluatoare şi partenerii săi (beneficiari, subcontractanți), dacă este cazul, sau dintre angajații entității evaluatoare, atunci când aceştia transmit informații clasificate prin intermediul unor rețele nesecurizate;
- Protecția datelor (arhivare, copii de siguranță, refacerea datelor etc.).

C23 Toți membrii entității evaluatoare trebuie să asigure protecția informațiilor referitoare la contract, la client şi la activitățile pentru care se solicită acreditarea.

C24 Entitatea evaluatoare trebuie să asigure protecția informațiilor clasificate, cu respectarea principiului „nevoii de a cunoaşte".

A.5 Subcontractarea

C25 Subcontractarea unor procese aferente activităților pentru care se solicită acreditarea trebuie să se realizeze numai în situații de excepție şi trebuie notificată la ORNISS.

C26 Dacă subcontractarea este necesară, aceasta se va realiza numai cu entități acreditate de ORNISS. Dacă subcontractantul nu este o entitate evaluatoare acreditată, trebuie ca activitățile subcontractate să nu presupună acces la informații clasificate.

B. LOCAȚIILE ŞI ECHIPAMENTUL ENTITĂȚII EVALUATOARE

B.1 Locaţiile şi mediul

C27 Entitatea evaluatoare trebuie să dețină locații tehnice speciale pentru activitățile pentru care solicită acreditarea (birouri, platforme pentru testări, săli de şedințe, etc.).

C28 Măsurile de securitate fizică şi controalele de mediu implementate trebuie să fie în concordanță cu activitățile pentru care se solicită acreditarea.

B.2 Instrumente şi echipamente

C29 Toate echipamentele necesare desfăşurării activităților pentru care se solicită acreditarea trebuie să fie disponibile în cadrul entității evaluatoare. Entitatea evaluatoare trebuie să aibă suficiente resurse pentru desfăşurarea activității solicitate.

C30 Dacă, în mod excepțional, entitatea evaluatoare trebuie să utilizeze echipamente din afara persoanei juridice, trebuie să demonstreze faptul că echipamentele utilizate oferă calitatea şi măsurile de securitate necesare. Personalul entității evaluatoare trebuie să fie calificat pentru utilizarea echipamentelor. În plus, trebuie să se definească clar, în proceduri, măsurile de protecție a informațiilor clasificate procesate de echipamente.

C31 Toate instrumentele utilizate în activitățile pentru care se solicită acreditarea trebuie să fie marcate şi înregistrate (ex.: un cod unic).

Trebuie implementat un management al configurației şi amplasării echipamentelor.

Sistemul de management al configurației trebuie să permită auditarea schimbărilor aduse instrumentelor.

Fiecare echipament sau produs software ce poate influența activitățile pentru care se solicită acreditarea trebuie înregistrat.

Trebuie să se asigure repetabilitatea şi reproductibilitatea rezultatelor evaluării.

C32 Echipamentele pot fi utilizate numai de către personalul autorizat. Accesul la instrumentele evaluatoare trebuie să fie controlat. Operarea şi administrarea instrumentelor trebuie să se execute conform unor instrucțiuni cunoscute de către personalul autorizat.

C. PREGĂTIREA PERSONALULUI ÎN DOMENIUL TEHNIC

C33 Entitatea evaluatoare trebuie să aibă personal cu experiența necesară pentru desfăşurarea activităților pentru care se solicită acreditarea.

Personalul angajat

C34 Personalul entității evaluatoare trebuie să aibă competența şi experiența necesară în domeniul tehnologiei informației şi în cel al evaluării produselor şi/sau soluțiilor de securitate IT.

C35 Entitatea evaluatoare are responsabilitatea de a asigura instruirea angajaților desemnați să utilizeze instrumente specifice, să îndeplinească activități pentru care se solicită acreditarea şi să semneze rapoartele de evaluare. Angajații aflați în perioada de instruire trebuie supravegheați de personal cu experiență.

C36 Procedura de recrutare a personalului entității evaluatoare trebuie să reflecte responsabilitățile ce revin entității evaluatoare ca urmare a acreditării. Procedura va include o verificare a candidaților, pentru a se asigura faptul că întrunesc criteriile de acreditare.

C37 Fiecare angajat al entității evaluatoare trebuie înştiințat de responsabilitățile sale. Acest lucru implică o definire a tuturor responsabilităților legate de activitățile pentru care se solicită acreditarea.

C38 Entitatea evaluatoare trebuie să precizeze obiectivele programelor de instruire şi perfecționare a angajaților săi. Pentru identificarea nevoilor de instructaj şi pentru realizarea unui program de instruire coerent, trebuie elaborate şi aplicate proceduri specifice. Sesiunile de perfecționare trebuie legate de activitățile pentru care se solicită acreditarea.

Notă: programul trebuie să includă o instruire asupra criteriilor de evaluare şi a tehnologiilor asociate.

C39 Entitatea evaluatoare trebuie să păstreze actualizate fişele posturilor pentru personalul de conducere, personalul tehnic şi cei cu posturi cheie ce participă la activitățile pentru care se solicită acreditarea.

Notă: ORNISS trebuie informat de activitatea personalului entității evaluatoare, pentru a se asigura că asemenea activitate este compatibilă cu domeniul acreditării.

C40 Entitatea evaluatoare trebuie să ia măsuri cu privire la schimbarea personalului.

Este importantă evitarea încheierii unui număr prea mare de contracte pe termen scurt şi a angajării persoanelor fără experiență în domeniu.

C41 Activitatea de bază a angajaților entității evaluatoare trebuie să fie cea de evaluare a produselor şi soluțiilor de securitate IT, servicii de consultanță sau instructaje de securitate. Angajații entității evaluatoare pot fi implicați în alte activități decât cele menționate anterior, pe perioade limitate, dar activitatea lor trebuie să fie compatibilă cu activitatea pentru care se solicită acreditarea.

D. METODE ŞI PROCEDURI DE LUCRU

D.1 Metode

C42 Entitatea evaluatoare trebuie să dețină o metodologie pentru fiecare activitate inclusă în aria de acoperire a acreditării. Metodologia trebuie să fie cuprinsă într-un standard internațional sau național.

C43 Entitatea evaluatoare poate dezvolta metode proprii, dacă nu există alte metode sau dacă nu a fost adaptată o metodă generală. Cercetarea metodelor trebuie să fie o activitate planificată şi va fi realizată de personal calificat şi care dispune de resurse adecvate.

C44 Entitatea evaluatoare trebuie să aprobe la nivel intern metodele de evaluare (incluzând testarea şi atacurile) ce au fost cercetate, în scopul confirmării faptului că sunt indicate pentru utilizarea cerută. Aprobarea se realizează cu ajutorul proiectelor pilot.

C45 Trebuie întocmită o documentație completă pentru toate metodele, procedurile sau instrucțiunile utilizate pentru desfăşurarea activităților pentru care se solicită acreditarea.

C46 Pe parcursul desfăşurării activităților pentru care se solicită acreditarea, entitatea evaluatoare trebuie să respecte metodele aprobate.

D.2 Registre

C47 Toate registrele ce conțin date referitoare la activitățile pentru care se solicită acreditarea (observații, date, etc.) trebuie păstrate. Aceste registre trebuie să conțină suficiente informații pentru a permite repetarea activităților la parametrii cât mai apropiați de original. De asemenea, în registru trebuie să se specifice şi persoana care a realizat activitatea.

D.3 Rapoarte de evaluare

C48 Toate rapoartele de evaluare trebuie aprobate în cadrul entității evaluatoare, înainte de a fi oferite solicitanților.

C49 Toate rapoartele evaluărilor, inclusiv rapoartele transmise în format electronic, înaintate solicitanților şi ORNISS, trebuie semnate de o persoană autorizată (conform criteriului 8).

C50 Rapoartele de evaluare trebuie păstrate de entitatea evaluatoare pe o perioadă de minim 10 ani.