



SR EN ISO /CEI 17021:2007

Cod: -

Editia: 1; Rev: 1

Intrat in vigoare: 13.12.2010

**Nume document: SCHEMA DE CERTIFICARE SMSI**

**Tip document: Scema de certificare**

**PROCERT LABORATORY: ORGANISM DE  
CERTIFICARE**

ELABORAT: Data: 13.12.2010	Director Tehnic Calitate, ELENA CIRJAN	AVIZAT/APROBAT: Data: 13.12.2010	Director General, SIMONA APOSTOL
Semnatura		Semnatura	

Exemplar nr.:

Copie controlată:

Copie necontrolată:

## 1 Scop

Prezenta procedură descrie responsabilitățile și metode utilizate pentru certificarea sistemelor de management al securității informației (conform SR ISO/CEI 27001:2006) în cadrul Procert Laboratory.

## 2 Domeniu de aplicare

Acest document se aplică pentru toate contractele de certificare / extindere a certificării pentru sisteme de management al securității informației.

## 3 Referințe normative

- SR EN ISO/CEI 17000:2005 - Evaluarea Conformității . Vocabular și principii generale;
- SR EN ISO / CEI 17021:2007 – Evaluarea Conformității. Cerințe pentru organisme care efectuează audit și certificare de sisteme de management;
- SR EN ISO 19011:2003 - Ghid pentru auditarea sistemelor de management al calității și mediului;
- [ISO 9001 Auditing Practices Group, Necesitatea abordării auditului în două faze;](#)
- SR EN ISO 19011:2003, „Ghid pentru auditarea sistemelor de management al calității și/sau mediu”;
- ISO/IEC 27001:2005 – Specificații ale Managementului pentru Securitatea Informației;
- [SR ISO/CEI 27006:2008, „Tehnologia informației. Tehnici de securitate. Cerințe pentru organismele care furnizează servicii de auditare și certificare”](#)
- [IAF MD 2:2007 - Transfer of Accredited Certification of Management Systems](#)
- [IAF MD 3:2008 - Advanced Surveillance and Recertification Procedures \(ASRP\)](#)
- [IAF MD 4:2008 - Use of Computer Assisted Auditing Techniques \("CAAT"\) for Accredited Certification of Management Systems](#)
- [IAF MD 5:2009 - IAF Mandatory Document For Duration of QMS and EMS Audits](#)

## 4 Definiții

**Schema de certificare** = cerințe specifice de certificare corelate anumitor categorii de persoane pentru care se aplică aceleași standarde, reguli și proceduri.

## 5 Rolurile și responsabilitățile în cadrul schemei de certificare

### 5.1 Directorul General

- analizează respectarea procedurilor de certificare;
- ia decizia de certificare pe baza Fișei de evaluare dosar și Dosar audit alături de membrii Comitetelor Tehnice;
- semnează certificatele emise de Procert Laboratory.

## 5.2 Directorul Tehnic Calitate

- analizeaza si avizeaza contractele de certificare;
- identifica impreuna cu Directorul General necesarul de resurse pentru indeplinirea cerintelor contractuale;
- planifica auditurile de certificare/supraveghere/urmarire/extindere/ recertificare ;
- se asigura de completitudinea informatiilor pentru desfasurarea in conditii optime a procesului de certificare (Comanda, Contract, Chestionar, Documentatie, alte informatii avute la dispozitie);
- selecteaza echipa de audit in functie de complexitatea domeniilor de activitate supuse certificarii si de disponibilitatea acestora;
- anunta clientul si membrii echipei de audit privind perioada estimata pentru desfasurarea auditului;
- constituie interfata intre Procort Laboratory, echipa de audit si Comitetul Tehnic;
- semnaleaza orice lipsuri din dosarele de audit (dovezi incomplete, inregistrari lipsa, incadrari constatari negative, etc.);
- convoaca Comitetul Tehnic in vederea evaluarii dosarelor de audit
- pun la dispozitia echipei de audit orice informatie necesara pentru desfasurarea in conditii optime a auditului (Comanda certificare, Chestionar evaluare preliminara, Rapoarte de audit precedente, Documentatie).
- stabileste necesarul de resurse pentru activitatile desfasurate (umane, materiale, financiare);
- identifica si semnaleaza Directorului General orice probleme legate de activitatea de certificare (amenintarea la asigurarea impartialitatii Procort Laboratory, conflicte interne, comunicare interna/externa, respectarea procedurii (ex. confidentialitate));
- stabileste programul de monitorizare si evaluare a auditorilor in baza feed-back-ului primit de la clienti, auditori si Resurse Umane.
- semnaleaza orice modificari privind procedurile de certificare/standardele/cerinte legale;
- gestioneaza baza de date aferenta propriei activitati.
- raporteaza saptamanal stadiul certificarilor/supraveghegerilor/reinnoirilor/extinderilor.
- raporteaza stadiul activitatilor Directorului General: probleme identificate, cauze, propuneri de imbunatatire, orice modificari aparute in cerintele legale si de reglementare, proceduri interne, dosarele ce urmeaza a fi analizate de catre Comitetul Tehnic, stadiul certificarilor/supraveghegerilor/ reinnoirilor/ extinderilor.

## 5.3 Comitetul Tehnic

- asigura competenta tehnica pentru evaluarea dosarelor organizatiilor auditate in vederea luarii deciziei de acordare / mentinere / suspendare / retragere certificarii;
- analizeaza in mod obiectiv si impartial dosarele de audit ale organizatiilor auditate si consemneaza concluziile in Fisa de evaluare a dosarului;
- ia decizia acordarii / mentinerii / suspendarii / retragerii certificarii si inregistreaza in Fisa de evaluare a dosarului
- efectueaza o evaluare continua a auditorilor din punct de vedere al completitudinii dosarelor de audit prezentate de acestia;
- evalueaza auditorii sefi / auditorii / expertii Procort Laboratory prin interviuri fata in fata sau telefonice din punct de vedere al competentelor pe domeniul solicitat;
- pastreaza confidentialitatea informatiilor si a datelor din dosarele organizatiilor auditate.

## 5.4 Director Comercial

- emite certificatele conform Registrului de eliberare certificate
- traduce domeniul de certificare;
- transmite Clientului Certificatele după ce au fost verificate de Directorul General și semnate de acesta;
- se preocupă de primirea certificatelor anulate / retrase și arivarea hol în dosarul de audit.

## 6 Etapele schemei de certificare

### 6.1 Analiza solicitării

Organizația care dorește să obțină certificarea sistemului/sistemelor de management de către Procort Laboratory trebuie să prezinte o comandă fermă (Comanda de certificare) împreună cu Chestionarul de evaluare preliminară.

Clientul poate solicita o certificare de grup pentru două sau mai multe organizații, atunci când una din condițiile de mai jos sunt îndeplinite:

- unul dintre acționari este comun pentru organizațiile care doresc certificarea de grup;
- organizațiile au un sistem de management similar;
- produsele și serviciile furnizate sunt identice sau comparabile și incluse în domeniul de certificare.

Procort Laboratory analizează cererea clientului și poate solicita/accesa și alte informații pentru a decide dacă Organismul de certificare poate oferi serviciile în conformitate cu cerințele ISO/CEI 17021:2005 și propriile politici și proceduri. În analiza cererii se ține cont de:

- 
- suficiența cunoștințelor referitoare la dezvoltările tehnologice și legale relevante pentru sistemul de management al securității informației organizației auditate
- rezolvarea diferentelor cunoscute de înțelegere dintre Procort Laboratory și organizația solicitantă;
- înțelegerea domeniului de activitate ale organizației auditate și riscurile asociate afacerii dacă există deficiențe necesare în cadrul Procort Laboratory, pentru certificare față de vulnerabilitățile și impacturile asupra organizației clientului privind securitatea informațiilor asupra resurselor
- competența și capacitatea personalului Procort Laboratory pentru a putea audita domeniul și locațiile solicitate (competența, timp, limba, condiții de securitate, amenințări asupra imparțialității).

Analiza Comenzii de certificare se face de către Directorul Tehnic Calitate, [Directorul Comercial](#) și Directorul General.

În urma analizei, Procort Laboratory identifică competența necesară și amplitudinea evaluărilor în vederea obținerii și menținerii certificării. Numărul de zile de evaluare pentru auditul inițial de certificare și pentru supravegheri sunt stabilite în funcție de procedura *Stabilirea numărului de zile om pentru efectuarea evaluărilor în vederea certificării / supravegherii / extinderii / restrângerii / reevaluării / recertificării*.

În cazul în care Procort Laboratory decide că poate furniza servicii de evaluare în vederea certificării se transmite Clientului Oferta sau proiectul de contract.

Etapele contractului de certificare sunt:

- Inițierea procesului de certificare;
- Audit faza 1;
- Audit faza 2 ;
- Luarea deciziei de certificare;
- Eliberarea certificatului;
- Supravegherea 1 (la 6 luni de la luarea deciziei de certificare) ;
- Supravegherea 2 (la 18 luni de la luarea deciziei de certificare) ;
- Supravegherea 3 (la 30 luni de la luarea deciziei de certificare).

Numărul de zile stabilite pentru efectuarea auditurilor de certificare și supraveghere poate fi modificat în urma Auditului faza 1, la recomandarea justificată a Auditorului Șef.

## 6.2 Desemnarea echipei de audit

Directorul Tehnic Calitate desemnează echipa de audit în vederea efectuării auditului. Echipa de audit este formată dintr-un Auditor Șef (conducătorul echipei de audit) și membrii (auditori și experți). În cadrul echipei de audit este obligatoriu ca Auditorul Șef să aibă o parte din competențe pe domeniul auditat. Experții tehnici lucrează sub supravegherea unui auditor. Auditorii trebuie să aibă competențe pe domeniul auditat sau domenii conexe. În cazul în care, domeniul de activitate al furnizorului de sistem de management este domeniu de risc, unul dintre membrii echipei trebuie să fie expert, altfel echipa se completează cu un membru expert. Planul și data auditului sunt acordate cu clientul.

## 6.3 Domeniul de aplicare al certificării

Echipa de audit auditează sistemul de management al securității informației al clientului, în conformitate cu domeniul de aplicare definit, în raport cu toate cerințele de certificare.

Procert Laboratory se asigură în timpul auditului că domeniul de aplicare și limitele sistemului de management al securității informației clientului sunt clar definite în termeni caracteristici ale afacerii, organizației, locației acestora, resursele și tehnologiei.

Procert Laboratory confirmă în domeniul de aplicare al sistemului de management al securității informației că organizația auditată abordează cerințele 4, 5, 6, 7 și 8 din standardul SR ISO/CEI 27001:2006.

Echipa de audit se asigură că evaluarea riscului de securitate a informațiilor clientului și tratarea riscurilor reflectă în mod corespunzător activitățile sale și se încadrează în limitele activităților sale. Procert Laboratory confirmă că acest lucru este reflectat în domeniul de activitate al organizației auditate, al sistemului de management al securității informației al acestora și în Declarația de Aplicabilitate în *Raportul de Audit*.

Echipa de audit se asigură că interfețele cu serviciile și activitățile, care nu sunt complet în domeniul de activitate al sistemului de management al securității informației, sunt abordate în cadrul sistemului care este subiectul certificării și sunt incluse și în evaluarea riscurilor referitoare la securitatea informațiilor organizației auditate.

## 6.4 Timpul de audit

Timpul de audit este luat in calcul la stabilirea numarului de zile de audit pentru auditul inițial de certificare și pentru supravegheri in procedura *Stabilirea numarului de zile om pentru efectuarea evaluarilor in vederea certificarii / supravegherii / extinderii / restrangerii / reevaluarii / recertificarii.*

## 6.5 Locatii multiple

Locatiile multiple sunt luate in calcul la stabilirea numarului de zile de audit pentru auditul inițial de certificare și pentru supravegheri in procedura *Stabilirea numarului de zile om pentru efectuarea evaluarilor in vederea certificarii / supravegherii / extinderii / restrangerii / reevaluarii / recertificarii.*

## 6.6 Auditul de certificare initiala

Dupa definitivarea si semnarea contractului, Procert Laboratory desfășoară etapa de audit inițial în vederea certificării sistemului de management. Echipa de audit desemnată pentru evaluare ține cont de competente și experiența specifică a auditorilor. Daca exista vreun conflict de interese, organizatia are dreptul a cere, justificat, inlocuirea auditorilor.

Auditul inițial de certificare presupune parcurgerea a două etape: auditul faza 1 și auditul faza 2.

**6.6.1. Auditul faza 1** se deruleaza, de regula, la sediul clientului.

**Obiectivul auditului faza 1** este acela de a cunoaste cât mai bine organizația solicitantă și de a analiza stadiul acesteia în raport cu referențialele. De aceea se urmaresc: evaluarea documentatiei sistemului de management al securitatii informatiei în raport cu referențiale solicitate (enunturi documentate ale politicii SMSI si obiective, domeniul de aplicabilitate al SMSI, proceduri si masuri de securitate pentru sustinerea SMSI, descrierea metodologiei de evaluare a riscului, raportul de analiza al riscului, planul de tratare al riscului, proceduri documentate, Declaratia de Aplicabilitate;)

- evaluarea sediului clientului si a conditiilor specifice locatiei, si derularea discutiilor cu personalul clientului pentru a determina nivelul de pregatire pentru etapa a doua a auditului;
- analiza stadiului clientului in raport cu cerintele SR ISO/CEI 27001:2006 si a intelegerii de catre client a acestor cerinte, in particular cu privire la identificarea performantelor cheie sau a aspectelor, proceselor, obiectivelor si operatiunilor semnificative ale sistemului de management al securitatii informatiei;
- evaluarea auditului intern si analizei efectuate de management;
- colectarea informatiilor necesare referitoare la domeniul de certificare, al proceselor si locatiei/locatiilor clientului cat si referitoare la aspectele legale aplicabile;
- furnizarea unui punct de plecare pentru planificarea auditului faza 2, confirmarea si stabilirea domeniului de aplicare, a criteriilor de audit si a locatiilor pentru care se solicita certificarea;
- sesizarea punctelor critice (problemelor) ale sistemului de management al securitatii informatiei care in timpul auditului faza 2 ar putea fi considerate neconformitati;

In anumite situatii Procert Laboratory poate decide ca Auditul faza 1 sa se deruleze fara vizitarea organizatiei, iar evaluarea documentatiei relevante a sistemului de management se face la sediul Procert Laboratory. Aceasta decizie este luata de catre Directorul Tehnic Calitate.

Decizia Procert Laboratory in aceasta situatie va fi justificata prin:

- dimensiunea organizatiei;
- localizarea organizatiei (ex. distanta foarte mare care implica costuri ridicate);

---

Nume document: Schema de certificare sisteme de management al securitatii informatiei, vers. 1.1

Cod document : -

Intrat in vigoare: 13.12.2010

- tipul activitatilor derulate de catre organizatie (ex. procese de o complexitate scăzută);
- eventuala cunoastere prealabila a organizatiei (ex. certificarea unui alt sistem de management realizata anterior ).

Constatarile Auditului faza 1 se consemneaza in Raportul de audit faza 1 care este comunicat imediat Clientului. Perioada de timp intre Auditul faza 1 si Auditul faza 2 este stabilita de comun acord cu clientul in functie de constatarile auditului faza 1.

Zonele critice (problemele) sesizate de echipa de audit în Auditul faza 1, care raman necorectate, pot conduce ca in faza 2 a auditului initial de certificare să fie sesizate ca neconformitati.

Perioada pentru corectarea potentialelor neconformitati trebuie sa fie direct proportionala cu:

- necesitatile Clientului de a rezolva potentialele neconformitati;
- complexitatea proceselor;
- numarul de anagajati.

In cazul in care nu se depisteaza potentiale neconformitati in Auditul faza 1, Auditorul Sef poate preda Clientului Planul de audit convenit pentru Auditul faza 2 si poate incepe desfasurarea Auditului faza 2. In acest caz, Auditorul Sef este obligat sa anunte Directorul Tehnic Calitate. Directorul Tehnic Calitate trebuie sa se asigure de disponibilitatea tuturor resurselor (ex. disponibilitatea tuturor membrilor echipei de audit) pentru efectuarea auditului faza 2.

#### **6.6.2 Echipa de audit**

Echipa de audit luata in ansamblu, trebuie sa indeplineasca urmatoarele cerinte:

- cel putin un membru al echipei de audit trebuie sa satisfaca cerintele Procet Laboratory in fiecare dintre urmatoarele domenii:
  - managementul echipei
  - sisteme si procese de management aplicabile sistemului de management al securitatii informatiei
  - cunoasterea cerintelor legislative si de reglementare in domeniul specific al securitatii informatiei
  - identificarea tendintelor referitoare la incidentele si amenintarile legate de securitatea informatiei
  - identificarea vulnerabilitatii organizatiei auditate si intelegerea probabilitatii de exploatare a lor, impactul, reducerea si controlul lor
  - cunostinte referitoare la masurile de securitate ale sistemului de management al securitatii informatiilor si a implementarii lor
  - cunoasterea analizei eficacitatii sistemului de management al securitatii informatiei si masurarea eficientei masurilor de securitate
  - standardele sistemului de management al securitatii informatiei asociate si/sau relevante, cele mai bune practici industriale, politici si proceduri de securitate
  - cunostinte privind metodele de tratare a incidentelor si de continuitate a afacerii
  - cunostinte referitoare la resursele informatiilor tangibile si intangibile si analiza impactului
  - cunostinte referitoare la tehnologii curente, in care securitatea poate fi relevant sau poate fi o problema
  - cunostinte privind procesele si metodele pentru managementul riscurilor.

- Echipa de audit trebuie sa fie competenta pentru a asocia indiciile referitoare la incidentele de securitate in sistemul de management al securitatii informatiei din organizatia auditata cu elementele corespunzatoare ale acestui sistem

### 6.6.3. Auditul faza 2 se derulează obligatoriu la sediul-sediile clientului.

**Obiectivele auditului faza 2** sunt urmatoarele:

- a confirma ca Clientul adera la politicile, obiectivele si procedurile proprii
- a confirma ca sistemul de management al securitatii informatiei este conform tuturor cerintelor normative ale standardului ISO/IEC 27001 si realizeaza obiectivele politicii Clientului.

Auditul se desfasoara in baza Planului de audit elaborat de către Auditorul Șef si acceptat de catre client.

Sedinta de deschidere este prima etapa a Auditului faza 2 si trebuie sa urmareasca:

- participarea participantilor, inclusiv o scurta descriere a acestora;
- confirmarea si stabilirea domeniului de aplicare, a criteriilor de audit si a locatiilor pentru care se solicita certificarea;
- metodele si procedurile utilizate in timpul auditului, inclusiv cele de esantionare;
- stabilirea si confirmarea canalelor de comunicare;
- confirmarea resurselor si facilitatilor necesare desfasurarii auditului;
- confirmarea limbii utilizate in timpul auditului;
- confirmarea aspectelor referitoare la confidentialitate si raportare a rezultatelor auditului;
- informarea cu privire la conditiile in care auditul poate fi terminat;

Pentru a indeplinii obiectivele **auditului faza 2**, echipa de audit se va focaliza pe urmatoarele aspecte ale organizatiei Clientului:

- evaluarea riscurilor legate de securitatea informatiilor si daca evaluarile produc rezultate comparabile si reproductibile;
- cerintele privind documentatia;
- selectarea obiectivelor de control si a masurilor de securitate
- examinari ale eficacitatii sistemului de management al securitatii informatiilor si masurari ale eficacitatiimasurilor de securitate privind securitatea informatiilor, raportare si examinare fata de obiectivele stabilite
- audituri interne si analize efectuate de management
- responsabilitatea managementului pentru politica de securitate a informatiilor
- corespondenta intre masurile de securitate selectate si implementate, Declaratia de Aplicabilitate, rezultatele examinarii riscurilor si procesul de tratare a riscurilor, politica si obiectivele sistemului de management al securitatii informatiei
- implementarea unor masuri de securitate, luand in considerare masuratorile organizatiei privind eficienta masurilor de securitate, pentru a determina daca masurile de securitate sunt implemnetate si eficiente pentru a atinge obiectivele declarate;
- programe, procese, proceduri, inregistrari, audituri interne si examinari ale eficientei sistemului de management al securitatii informatiei pentru a se asigura ca acestea pot fi urmarite in deciziile de management si in politica si obiectivele sistemului de management.

Pe parcursul auditului, echipa de audit verifica daca:

- organizatia auditata este consecventa in mentinerea procedurilor pentru identificarea, examinarea si evaluarea amenintarilor pentru securitatea informatiilor, referitoare la resurse, a vulnerabilitatilor si a impacturilor asupra organizatiei auditate.
- analiza amenintarile legate de securitate este relevanta si adecvata pentru functionarea organizatiei si daca procedurile organizatiei (pentru identificarea, examinarea si evaluarea

amenintarilor legate de securitatea informatiei, pentru resurse, vulnerabilitati si impacturi) si rezultatele aplicarii lor sunt coerente cu politica, obiectivele si tintele organizatiei auditate.

- procedurile folosite in analiza semnificatiei acestora sunt complete si implementate in mod corespunzator.
- organizatia auditata are un sistem de management pentru a atinge conformitatea legala si de reglementare, aplicabil riscurilor si impacturilor asociate securitatii informatiei

#### **6.6.4. Raport de audit de certificare**

Auditul de certificare se finalizeaza cu sedinta de inchidere in care echipa de audit furnizeaza:

- o indicatie scrisa sau verbala care priveste conformitatea sistemului de management al securitatii informatiei al organizatiei auditate cu cerintele de certificare particulare
- o oportunitate pentru client de a pune intrebari despre constatari si fundamentarea lor

Echipele de audit furnizeaza organismului de certificare Raportul de audit care contine urmatoarele informatii:

- o relatare asupra auditului de certificare, asupra analizei riscurilor privind securitatea informatiei organizatiei auditate
- timpul total de audit utilizat si specificarea detaliata a timpului consumat pentru evaluarea analizei riscurilor, auditarea la fata locului si elaborarea raportului de audit
- chestionarele de audit care au fost urmarite, justificarea selectarii lor si metodologia folosita
- ariile acoperite de audit, inclusiv piste de audit semnificative urmate si metodologiile de audit utilizate
- detaliile asupra oricaror neconformitati identificate, sustinute de o dovada obiectiva si o referinta a acestor neconformitati la cerintele standardului ISO/IEC 27001.
- comentariile referitoare la conformitatea sistemului de management al securitatii informatiei cu cerintele de certificare, cu o declaratie clara a neconformitatii, o referinta la versiunea Declaratiei de Aplicabilitate.
- adecvarea organizarii interne si procedurile adoptate de organizatia auditata pentru a oferi incredere in sistemul de management al securitatii informatiei.
- gradul de incredere care se poate acorda auditurilor interne si analizelor efectuate de management;
- un rezumat al celor mai importante observatii, atat pozitive cat si negative privind implementarea si eficacitatea sistemului de management al securitatii informatiei
- recomandarea echipei de audit daca sistemul de management al organizatiei auditate ar trebui certificat sau nu, impreuna cu informatiile care sa fundamenteze aceasta recomandare

Echipele de audit va inregistra eventualele neconformitati fata de documentele de referinta, in Rapoarte de constatare.

Constatările evaluărilor pot avea următoarele încadrări:

- conformitate;
- neconformitate;
- observație.

La sfarsitul sedintei de inchidere, Auditorul Șef va comunica clientului domeniul si locatiile pentru care se va propune acordarea certificarii, in functie de constatările auditului.

În cazul în care au existat constatări negative, Clientul trebuie să stabilească corecții și acțiuni corective in maxim 2 saptamani de la luarea la cunostinta a constatarilor negative. Termenul de rezolvare al corecțiilor-acțiunilor corective nu va fi mai mare de 3 luni. Auditorul Șef analizează propunerile Clientului și decide modul adecvat de verificare a închiderilor corecțiilor și acțiunilor corective.

In cazul in care este necesar un audit suplimentar pentru verificarea închiderii acestora, costul va fi suportat de către Client.

Raportarea rezultatelor auditului se face prin Sinteza auditului, completata de Auditorul Sef ce contine propunerea privind acordarea sau neacordarea certificării.

Informatiile si documentele rezultate in timpul auditului sunt predate Directorului Tehnic Calitate, care urmareste compeltitudinea Dosarului de audit. Atunci cand Dosarul de audit este complet intrunieste Comitetului Tehnic.

## 6.7 Decizia de certificare

Rezolutia privind acordarea certificării pentru activitatile economice și locațiile Clientului, se adoptă de către Directorul General al Procet Laboratory impreuna cu membrii Comitetului Tehnic, pe baza recomandarilor Auditorului Sef.

Certificarea se acorda atunci cand:

- solicitantul prezinta dovezi suficiente pentru demonstrarea implementarii, mentinerii si eficacitatii sistemului de management al securitatii informatiei implementat in raport cu SR ISO/CEI 27001:2006;
- solicitantul prezinta dovezi ale efectuarii a minimum unui audit intern pe an;
- solicitantul prezinta dovezi ale efectuarii a minimum unei analiza efectuate de management pe an;
- solicitantul respecta prezentele *Regulile de certificare Procet Laboratory* si prevederile Contractului de certificare;
- solicitantul a inchis toate neconformitatile identificate in timpul auditului faza 1 si faza 2, in termenul stabilit cu echipa de audit.

Decizia de certificare se ia in baza evaluarii constatarilor si concluziilor auditului si a altor informații relevante (ex: site, mass media, reclamatii).

Astfel, în primă fază, dosarul este analizat din punct de vedere tehnic de catre membrii Comitetului Tehnic in functie de domeniile solicitate.

Decizia Directorului General urmareste confirmarea sau infirmarea conformarii procesului de certificare cu procedurile Procet Laboratory si ține cont de concluziile echipei de audit, si decizia Comitetului Tehnic cat si de respectarea procedurilor în vigoare în vederea luarii deciziei de certificare. Directorul General nu poate contrazice decizia luata de membrii Comitetului Tehnic desemnati.

Decizia de certificare este inscrisa in Registrul de eliberare certificate si comunicata Clientului scris.

Solicitantii nemultumiti de decizia adoptata pot formula apeluri ale deciziei de certificare, adresata Directorului General.

În cazul deciziei favorabile de certificare, Procet Laboratory va elibera Clientului Certificatul/ Certificatele, Anexa la certificate (daca este cazul), mărcile de certificare Procet Laboratory și Regulile de utilizare a mărcilor de certificare Procet Laboratory.

Certificatul eliberat de Procert Laboratory conține următoarele informații:

- standardul de referință;
- numele și adresa (inclusiv punctele de lucru) organizației certificate;
- activitățile pentru care s-a acordat certificarea;
- data eliberării / data expirării certificatului;
- numărul și seria certificatului.
- Referire la versiunea specifică a Declarației de Aplicabilitate

Anexa la certificat conține următoarele informații:

- standardul de referință
- numărul și seria certificatului aferent;
- adresele și domeniul certificat;
- data eliberării / data expirării certificatului.

Seria certificatului este marcată printr-o literă în funcție de standardul adoptat, astfel: SI = securitatea informației.

Numărul certificatului este format din 5 cifre, certificatele numerotându-se în ordine crescătoare de la 00001 la 0000n.

După acordarea certificatului/ certificatelor, Procert Laboratory va înregistra lunar pe site-ul Procert Laboratory ([www.procertlaboratory.ro](http://www.procertlaboratory.ro)) certificatele emise.

Transmiterea certificatelor, anexei și marilor și a Regulilor de utilizare a mărcilor de certificare Procert Laboratory se face pe baza de proces verbal, utilizând servicii postale sau înmănare directă.

## 6.8 Valabilitatea și reînnoirea certificării sistemelor de management

Certificatele emise de Procert Laboratory sunt valabile pe o perioadă de 3 ani de la data emiterii, cu condiția respectării programului de supravegheri transmis de către Procert Laboratory la eliberarea certificatului.

Modificările (ex: schimbare punct de lucru, modificare procese, modificare mod de lucru, etc...) apărute în sistemul de management al securității informației Clientului certificat, trebuie notificate către Procert Laboratory.

În acest sens, Procert Laboratory trebuie să reevalueze organizația și poate planifica audituri de supraveghere suplimentare în vederea evaluării continuității conformării sistemului de management al securității informației al organizației. Costurile acestor evaluări vor fi suportate de organizație.

În cazul în care se modifică cerințele de certificare ale Procert Laboratory și este necesară o reevaluare, conform Politicii de tranziție, Clientul trebuie să accepte reevaluarea, suportând costurile, pentru menținerea certificării.

Drepturile și obligațiile Clienților pe perioada valabilității Certificatelor sunt următoarele:

- drepturi:
  - să folosească marca/ mărcile de certificare Procert Laboratory pentru promovarea imaginii organizației numai pentru activitățile și punctele de lucru pentru care a obținut certificarea;
  - să accepte programul auditurilor de supraveghere ;
  - să solicite prin adresă scrisă restrângerea și / sau extinderea domeniului certificării;

- sa renunțe in orice moment la certificare (cu plata tarifelor prevazute in contractul de certificare pana in momentul respectiv).
- obligații:
  - sa mentina sistemul de management al securitatii informatiei;
  - sa respecte toate prevederile Regulilor de utilizare a marilor de conformitate Procet Laboratory;
  - sa mențină proceduri adecvate pentru a se asigura ca informatiile catre organism sunt actualizate;
  - sa pună la dispoziția Procet Laboratory situația apelurilor si reclamațiilor primite din partea clientilor, reclamații legate de functionarea sistemul de management al securitatii informatiei;
  - sa isi dea acordul pentru toate auditurile de supraveghere, planificate sau neplanificate, cooperând cu echipa de audit, cu asigurarea documentelor / înregistrărilor, accesului necesar si securității echipei;
  - sa respecte prevederile Contractului de certificare si ale Regulilor de certificare sisteme de management.

Certificarea Procet Laboratory nu absolvă organizația de obligațiile sale legale si contractuale legate de produsele si / sau serviciile furnizate.

## 6.9 MENTINEREA CERTIFICARII

Mentinerea certificarii pe perioada de valabilitate a certificatului se face in urma audurilor de supraveghere.

Scopul audurilor de supraveghere este de a verifica faptul ca sistemul de management al securitatii informatiei certificat continua sa fie implementat, de a lua in considerare implicatiile modificarilor asupra sistemului, si de a ratifica o conformitate continua cu cerintele privind certificarea. Audurile de supraveghere planificate au loc astfel:

- Supravegherea I – la 6 luni de la auditul de certificare
- Supravegherea II – la 1 an de la supravegherea I
- Supravegherea III – la 1 an de la supravegherea II

Termenele pentru efectuarea evaluarilor in vederea mentinerii certificarii se pot devansa sau prelungi cu cel mult 60 de zile lucratoare fata de termenele planificate, asa cum este prezentat mai sus. Primul audit de supraveghere nu trebuie sa depaseasca 12 luni de la ultima zi a auditului faza 2.

Procesul de evaluare periodica a sistemelor de management al securitatii informatiei presupune efectuarea evaluarilor de supraveghere la fata locului, pentru a permite monitorizarea indeplinirii continue a cerintelor de certificare

In cadrul audurilor de supraveghere se verifica si analizeaza urmatoarele: verificarea actiunilor corective luate in urma neconformitatilor de la auditul anterior.

- verificarea inchiderii observatiilor identificate in cadrul auditului anterior;
- verificarea a 1/3 din sistemul de management implementat in cadrul organizatiei auditate (elementele selectate din ISO/IEC 27001)

- elementele de mentinere ale sistemului (auditul intern, analiza efectuata de management: cel putin anual, actiuni corective, actiuni preventive)
- comunicările din partea partilor externe
- modificari in sistemul documentat
- zonele care sunt subiectul schimbarii
- alte domenii corespunzatoare selectate
- analiza actiunilor intreprinse pentru neconformitatile identificate in timpul auditului anterior;
- eficacitatea sistemului de management cu privire la realizarea obiectivelor politicii de securitate;
- functionarea procedurilor pentru evaluarea periodica si revizuirea conformitatii cu legislatia si reglementarile referitoare la securitatea informatiei
- imbunatatirea continua;
- *inregistrările referitoare la apeluri si reclamatii aduse in fata organismului de certificare*
- utilizarea marcilor si a certificatelor.

Etapele desfasurarii unui audit de supraveghere sunt aceleasi ca la orice audit.

*Raport de audit de supraveghere trebuie sa contina informatile referitoare la eliminarea neconformitatilor descoperite anterior*

In cazul in care echipa de audit nu ridica neconformitati in timpul auditului de supraveghere, mentinerea certificatului se face pe baza recomandarii Auditorului Sef.

In cazul identificarii de neconformitati in cadrul auditurilor de supraveghere Directorul Tehnic Calitate convoaca membrii Comitetului Tehnic in vederea analizei dosarului de supraveghere.

In functie de recomandarea membrilor Comitetului Tehnic, Director General ia decizia mentinerii sau suspendarii certificarii.

In cazul deciziei de suspendare este obligatorie urmarirea inchiderii neconformitatilor. Decizia de retragere sau restrangere este luata de membrii Comitetul Tehnic si Directorul General pe baza recomandarilor Auditorului Sef.

Auditurile neplanificate (de urmarire) se inițiază de Procert Laboratory in următoarele cazuri:

- modificări majore ale sistemului de management al organizației certificate, inclusiv a statutului legal;
- modificarea cerintelor Procert Laboratory;
- reclamații privind funcționarea sistemului de management privind activitățile certificate;
- reclamații privind utilizarea abuziva a mărcilor de certificare.

In cazul identificarii de neconformitati in cadrul auditurilor de supraveghere neprogramate Directorul Tehnic Calitate convoaca membrii Comitetului Tehnic in vederea analizei dosarului de supraveghere.

In functie de recomandarea Auditorului Sef Comitetului Tehnic si Director General ia decizia mentinerii sau suspendarii certificarii.

In cazul deciziei de suspendare este obligatorie urmarirea inchiderii neconformitatilor. Rezultatul inchiderii neconformitatilor este evaluat de Comitetul Tehnic si Directorul General in vederea luarii deciziei de retragere sau restrangere a domeniului certificat.

## 6.10 Recertificarea

Recertificarea este similara certificarii sistemului de management al securitatii informatiei. Procesul de recertificare are loc la 3 ani de la certificare si presupune incheierea unui act aditional, cu acordul ambelor parti.

Cu cel putin trei luni inainte de expirarea termenului de valabilitate a Certificatului, Procet Laboratory va anunta organizatia cu privire la valabilitatea certificatului. In cazul in care organizatia este de acord, se va incheia un act aditional la contract.

Evaluarea in vederea recertificarii se va programa cu cel putin 2 luni inainte de expirarea termenului de valabilitate al certificatului.

In cazul mentinerii certificatului se mentine acelasi numar de certificat, precedat de litera "R" = recertificare.

## 6.11 Renuntarea la certificare; extinderea sau restrangerea domeniului de certificare; suspendarea sau retragerea certificarii

### Renunțarea la certificare

Organizațiile certificate pot renunța la certificare:

- la cerere scrisa;
- la expirarea termenului de valabilitate a certificatelor, prin neprezentarea Comenzii de recertificare;
- in cazul modificării standardului de referința pentru certificare;
- in cazul neacceptării modificărilor aduse prezentelor reguli si / sau condițiilor financiare prin renunțarea unilaterală la contract.

Renunțarea devine efectiva imediat.

In urma renunțării la certificare, organizația se obliga:

- sa restituie originalul certificatului Procet Laboratory;
- sa nu realizeze o eventuala copie sau o alta reproducere a certificatelor;
- sa elimine orice referința la certificare si sa înceteze utilizarea mărcii Procet Laboratory.

Prin renuntarea la certificatul Procet Laboratory, organizatia respectiva va fi scoasa din lista organizatiilor certificate de Procet Laboratory.

### **Extinderea sau restrângerea certificării**

Extinderea domeniului certificării se realizeaza ca urmare a unui audit de extindere solicitat in scris de organizatia certificata, auditul fiind desfasurat fie independent - la cerere, fie in completare la un audit de supraveghere. Extinderea domeniului va fi mentionata intr-un act aditional la contract si se mentioneaza in Sinteza audit intocmita de Auditorul sef.

Auditul de extindere este tratat:

- ca un audit initial de certificare (sau de recertificare): programul acoperind toate capitolele din referential, in conformitate cu procedurile referitoare la evaluarea sistemelor de management
- ca un audit de supraveghere, in cazul unei extinderi de mica amploare, in conformitate cu prezenta procedura.

In cazul deciziei favorabile, se inscrie in *Registrul de eliberare certificate*. Noul certificat are acelasi numar si aceeasi durata de valabilitate cu cel initial, dar cu domeniul sau standardul modificat sau cu

introducerea noilor filiale. De asemenea, data emiterii noului certificat va fi precizata intr-o paranteza, in continuarea datei initiale de emitere a certificatului, fiind precedata de litera E.

Procert Laboratory contacteaza organizatia si solicita returnarea certificatului. Noul certificat se transmite numai dupa primirea de catre Procert Laboratory a vechiului certificat, prin inscrierea acestuia in *Registrul eliberare certificate*.

Auditul de restrangere a domeniului certificarii se realizeaza la cererea organizatiei certificate ca urmare a restrangerii activitatii, inchiderii unor filiale, etc. si se trateaza ca un audit initial de certificare sau ca un audit de supraveghere in functie de impactul modificarilor asupra sistemului de management aplicabil. Acest aspect se precizeaza intr-un act aditional la contract.

Restrangerea domeniului se poate face la solicitarea clientului sau la propunerea Auditorului Sef care la un audit de supraveghere programat atunci cand constata ca organizatia nu mai dispune de capacitatea tehnica de a satisface conditiile de certificare pentru toate activitatile din domeniul certificat.

Noul certificat are acelasi numar si aceeasi durata de valabilitate cu cel initial, dar cu domeniul restrans. De asemenea, data emiterii noului certificat va fi precizata intr-o paranteza, in continuarea datei initiale de emitere a certificatului, fiind precedata de litera S.

Procert Laboratory inscrie in *Registrul eliberare certificate*, seria si numarul de ordine al certificatului. Procert Laboratory contacteaza Clientul si solicita returnarea certificatului. Noul certificat se emite numai dupa primirea de catre Procert Laboratory a vechiului certificat.

### **Suspendarea certificării**

Suspendarea Certificatului este actiunea de retragere pe o perioada precizata de timp a deciziei cu privire la mentinerea certificarii datorita nerespectarii referentialului sau conditiilor contractuale.

Suspendarea certificatului este decizia Directorului General si este luata in urmatoarele conditii :

- sistemul de management al clientilor certificati are esecuri repetate si serioase in ceea ce priveste indeplinirea cerintelor certificarii, inclusiv a cerintelor pentru eficacitatea sistemului de management (esecuri identificate fie in cadrul auditurilor de supraveghere programate, fie neprogramate fie datorita reclamatilor primite de la beneficiari);
  - Clientul nu permite efectuarea auditurilor de supraveghere sau recertificare la frecventa ceruta
  - nerespectarea termenelor prevazute in Planificarea in vederea mentinerii certificatului cu maxim 60 de zile lucratoare;
  - abateri de la Reguli de utilizare a marcilor de conformitate Procert Laboratory, cod PO - 8.4 - 1, pe care organizatia si le asuma si stabileste termene de rezolvare in mai putin de o luna;
  - modificarea majora a sistemului/sistemelor de management fara a planifica un audit de evaluare in termen de maxim 60 de zile de la data anuntarii Procert Laboratory cu privire la acestea;
  - cerere voluntara de suspendare;

Suspendarea nu trebuie sa depasesca 3 luni.

### **Anularea certificării/ retragerea certificatelor**

Retragerea este actiunea de suspendare pe perioada nelimitata a deciziei de mentinere a certificarii datorita unor abateri care afecteaza imaginea Procert Laboratory, datorita nerespectarii referentialului sau a conditiilor contractuale. Retragerea certificatului este decizia Directorului General si este luata in urmatoarele conditii:

- esecul rezolvării problemelor care au dus la suspendarea certificării, în timpul stabilit de organismul de certificare;
- nerespectarea repetată a termenilor contractuali;
- la expirarea termenului de valabilitate a certificatului, prin neprezentarea unei cereri de reînnoire cu cel puțin trei luni înainte de expirarea certificatului;
- renunțarea unilaterală la contract.
- neacceptarea modificărilor aduse la procedurile Procert Laboratory.
- încetarea activităților pentru care s-a obținut certificarea sistemului de management;
- faliment sau lichidare pe cale juridică.

Membrii Comitetului Tehnic evaluează recomandarea Auditorului Șef retragere / restrângere a certificării. Procert Laboratory comunică organizației printr-o scrisoare decizia de suspendare/retragere. În cazul deciziei de retragere este solicitată returnarea Certificatului eliberat și se renunță la Contract. Clientul este obligat să returneze Certificatele eliberate în original și este obligat să înceteze folosirea marilor de certificare.

## 6.12 Managementul imparțialității

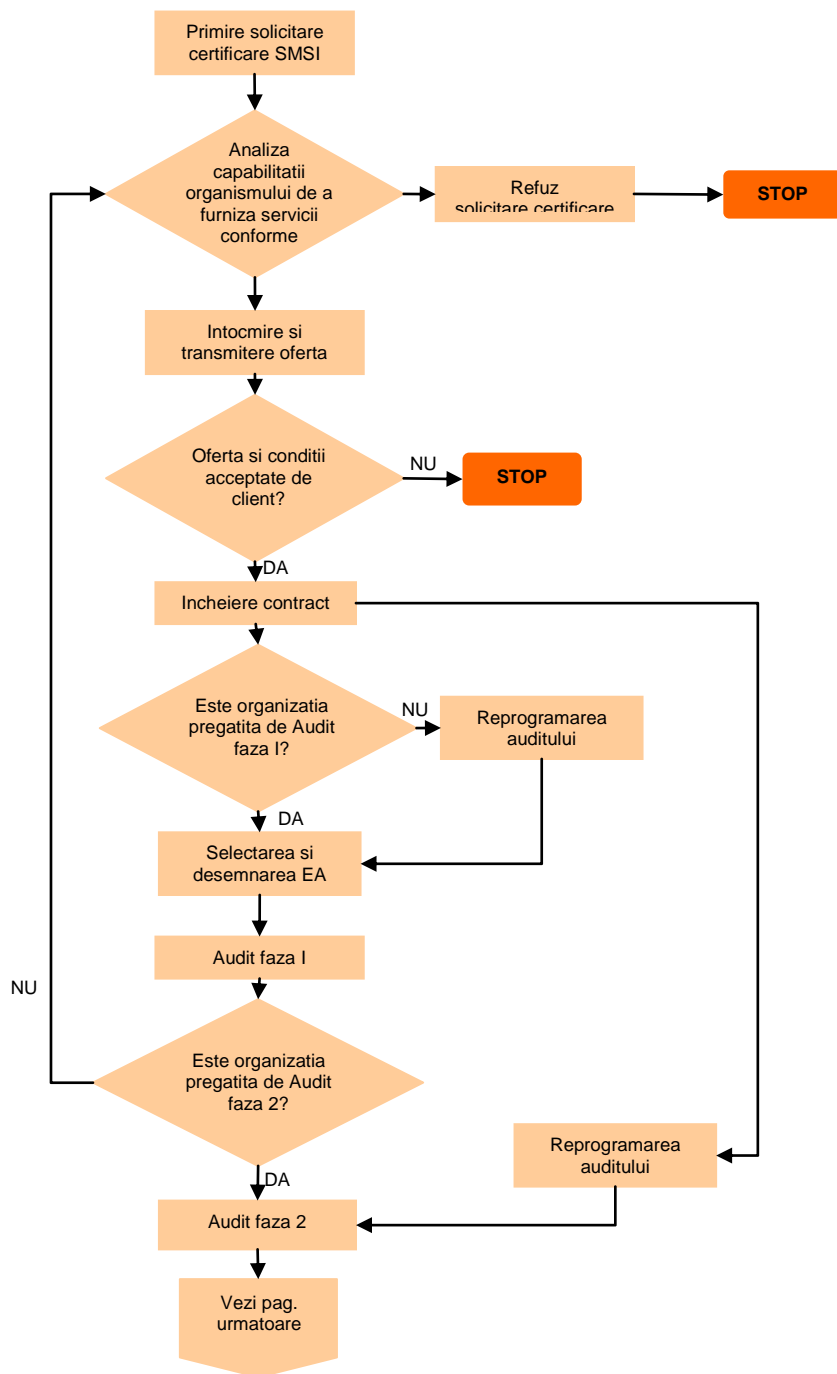
Pentru asigurarea imparțialității Procert Laboratory urmărește următoarele principii:

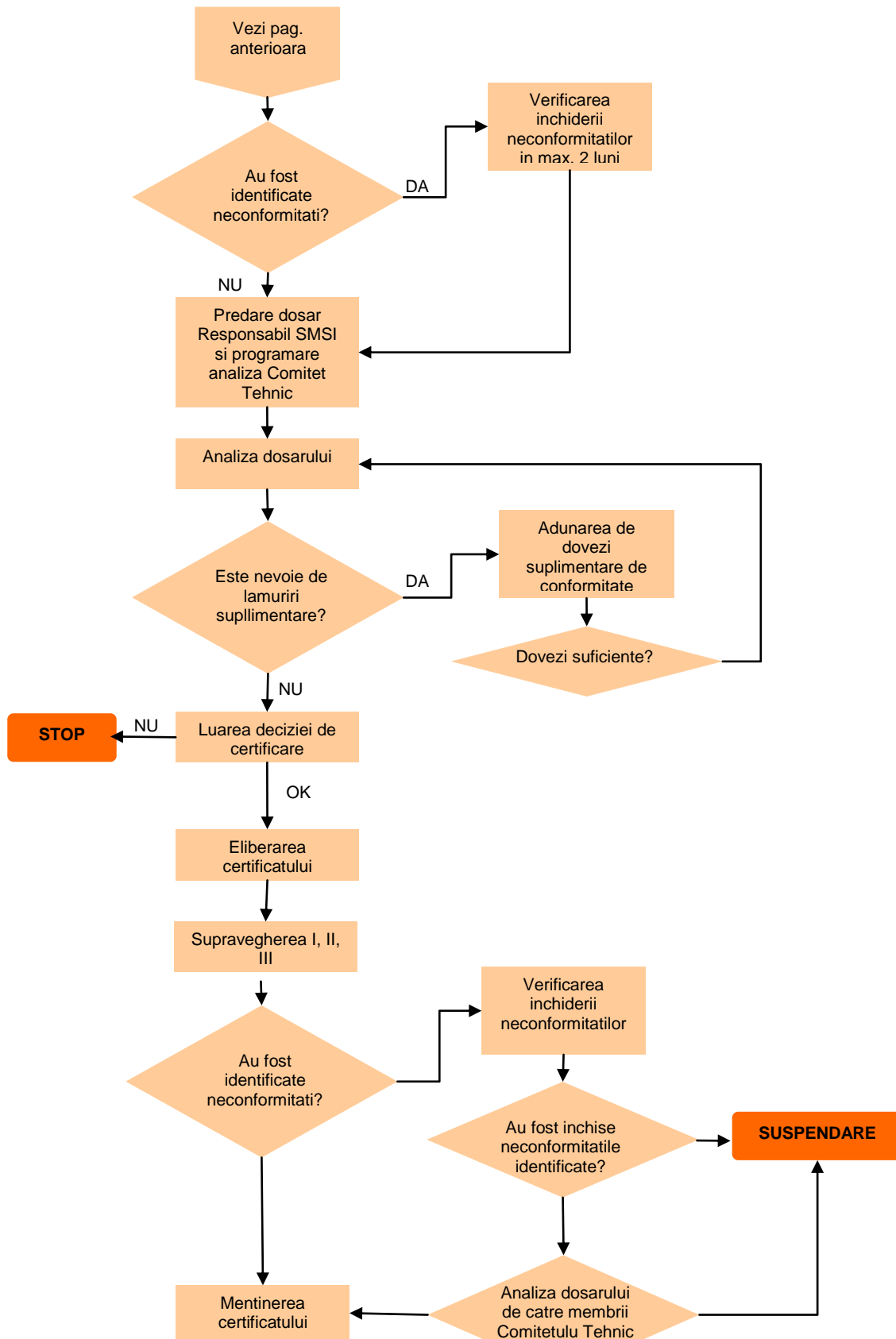
1. Procert Laboratory, prin statutul său nu acordă servicii de consultanță;
2. Procert Laboratory formează o structură la cel mai înalt nivel care trebuie să asigure imparțialitatea activităților organismului de certificare;
3. Procert Laboratory nu acordă certificate pentru firmele la care personalul de conducere (Director General, Director Tehnic Calitate) a acordat consultanță în ultimii 2 ani.
4. Persoanele implicate în procesul de certificare nu trebuie să fie furnizate consultanță, inclusiv cei care activează la nivel managerial, în ultimii doi ani, pentru clientul evaluat în vederea certificării/mentinerii certificării.
5. Procert Laboratory nu subcontractează unei firme de consultanță auditurile de certificare / supraveghere.
6. Anual, Procert Laboratory evaluează riscurile legate de imparțialitate;

De aceea personalul implicat în activitatea de certificare trebuie să declare ori de câte ori apar conflicte de interese.

Directorul Tehnic Calitate și Directorul General trebuie să se asigure de desfășurarea activităților cu imparțialitate, fără a permite presiuni comerciale, financiare sau de altă natură asupra personalului implicat în certificare.

## 7 Schema de certificare





## 8 Personalul implicat in schema de certificare

### 8.1 Directorul General

#### Studii

- studii post universitare;

#### Instruiri specifice procesului de certificare

- absolvirea cursurilor de auditor extern pentru securitatea informatiei;
- cunoasterea documentatiei Procert Laboratory;
- cunostinte relevante referitoare la sistemele de management al securitatii informatiei.

#### Experienta de lucru

- minim 4 ani de experienta in munca;
- minim 1 an de experienta in munca intr-un post de conducere;

#### Abilitati

- capacitatea de a lucra in echipa, de a comunica, de a raporta corect informatiile, de a forma personal.

### 8.2 Directorul Tehnic Calitate

#### Studii

- studii universitare tenice;

#### Instruiri specifice procesului de certificare

- cunoasterea documentatiei Procert Laboratory;
- absolvirea cursurilor de auditor extern pentru securitatii informatiei;
- capacitatea de a intelege si a aprecia complexitatea proceselor si aspectele legale domeniilor de certificare;
- cunostinte solide referitoare la sistemul de management al securitatii informatiei;
- cunoasterea tehnicilor de audit;
- capabilitatea de a aplica principiile, procedurile si tehnicile de audit;

#### Experienta de lucru

- minim 6 ani de experienta in munca;
- minim 1 an de experienta in munca intr-un post de conducere;
- minim 1 an experienta in gestionarea sistemelor de management al securitatii informatiei;

#### Abilitati si competente

- capacitatea de a intelege si a aprecia complexitatea proceselor si aspectele legale domeniilor de certificare;
- capabilitatea de a aplica principiile, procedurile si tehnicile de audit;
- capabilitatea de a forma personal;
- capacitatea de a lucra in echipa, de a comunica, de a raporta corect informatiile
- apacitatea de a-si planifica activitatile si de a urmari respectarea termenelor;

## 8.3 Membrii Comitetului Tehnic

### Studii

- minim studii superioare;

### Instruiri specifice procesului de certificare

- cunoscător al tehnicilor de audit;
- cunoasterea documentatiei Procert Laboratory;

### Experienta de lucru

- experienta profesionala totala de minim 5 ani vechime;
- *experienta profesionala in tehnologia informatiei 4 ani (cu norma intreaga);*
- *experienta profesionala in securitatea informatiei 2 ani (cu norma intreaga) din cei 4 de mai sus;*

### Abilitati si competente

- capacitatea de a intelege sistemul de management al securitatii informatiei in diverse organizatii, interactiunile intre componentele acestora;
- cunostarea contextului regional in care se desfasoara activitatile organizatiei evaluate;
- sa aiba cunostinte in domeniul de tehnologie corespunzator auditului inclusiv trebuie sa cunoasca modalitatile de evaluare si procedurile Procert Laboratory;
- cunostinte referitoare la procese, produse, inclusiv servicii aferente domeniului sau de competenta pentru a intelege contextul tehnologic in care s-a desfasurat auditul.
- capacitatea de a lucra in echipa, de a comunica, de a raporta corect informatiile, de a forma personal.

## 8.4 Auditori

### Studii

- *minim studii medii;*

### Instruiri specifice procesului de certificare

- *absolvent al unui/ unor curs / cursuri de minim 5 zile de auditor in domeniul securitatii informatiei, conform SR ISO/CEI 27001:2006*
- cunoasterea documentatiei Procert Laboratory;

### Experienta de lucru

- *experienta de munca de minim 4 ani vechime (cu norma intreaga) in tehnologia informatiei;*
- *minim 2 ani experienta intr-o functie in legatura cu securitatea informatiilor*
- experienta relevanta de minim 1 an in domeniul de competenta.

### Experienta de audit

- *sa fi participat ca auditor in formare la cel putin 4 audituri de certificare, pentru cel putin 20 de zile de audit, care sa include examinarea documentatiei si analiza riscurilor, evaluarea implementarii si raportul de audit;*

### Abilitati si competente

- capacitatea de a aplica principiile, procedurile si tehnicile de audit;

- cunoasterea contextului regional in care se desfasoara activitatile organizatiei evaluate;
  - capacitatea de a planifica si organiza activitatea in mod eficace si de a se incadra in termenele stabilite;
  - capacitatea de a identifica si colecta informatii relevante pentru verificarea conformitatii cu cerintele standardului;
  - capacitatea de a intelege sistemele de management al securitatii informatiei in diverse organizatii, interactiunile intre componentele acestora;
  - capacitatea de a intelege evaluarea riscurilor si a managementului riscurilor, din perspectiva afacerii
  - capacitatea de a intelege cerintele de reglementare aplicabile sistemului de management al securitatii informatiei din cadrul organizatiei clientului
  - capacitatea de a intelege organizatia clientului, managementul aspectelor care privesc securitatea informatiilor referitoare la activitatile, produsele si serviciile acestora.
  - capacitatea de a recunoaste diferentele dintre documentele de referinta si prioritatile acestora cat si aplicarea lor in diverse situatii de audit;
  - capacitatea de a pune operatii complexe intr-o perspectiva larga si de a intelege rolul unitatilor individuale in organizatiile clientilor mai mari;
- cunostinte referitoare la standardele sistemului de management al securitatii informatiei, la cerintele de reglementare si la alte documente normative relevante domeniului de competenta;
- cunostinte referitoare la procese, produse, inclusiv servicii aferente domeniului sau de competenta pentru a intelege contextul tehnologic in care se efectueaza auditul;
- cunostinte asupra legilor, reglementarilor si altor cerinte legale relevante domeniului de competenta;
- cunostinte pentru urmatoarele subiecte privind:
    - aspectele de audit
      - riscul auditului
      - analiza proceselor de securitate a informatiei
      - ciclul Deming (PDCA) pentru imbunatatirea continua
      - auditul intern pentru securitatea informatiei
    - cerintele de reglementare
      - proprietatea intelectuala
      - continutul, protectia si pastrarea inregistrarilor organizatiei
      - protectia datelor si confidentialitatea
      - reglementarea masurilor de securitate si criptare
      - lupta impotriva terorismului
      - comertul electronic
      - semnaturile electronice si digitale
      - supravegherea locului de munca
      - interceptarea telecomunicatiilor si monitorizarea datelor
      - infractiunile prin intermediul calculatorului
      - colectarea probelor electronice
      - testele de penetrare

- cerintele specifice sectorului, nationale si international
  - tratarea
  - cerintele de management
    - tratarea riscurilor referitoare la securitatea informatiilor
    - riscurile de securitate privind externalizarea ICT
    - riscurile privind securitatea informatiilor pe lantul de aprovizionare
- cunostinte tehnice corespunzatoare referitoare la activitatile specifice din cadrul domeniului de activitate al sistemului de management al securitatii informatiei, potentialele riscuri de securitate a informatiilor aferente;
- cunostinte referitoare la analiza eficacitatii sistemului de management al securitatii informatiei si la masurarea eficacitatii masurilor de securitate
- sa aiba urmatoarele caracteristici personale: obiectiv, matur, cu capacitate de discernamant, analitic, tenace si realist;
- capacitatea de a lucra in echipa, de a comunica, de a raporta corect informatiile, de a forma personal.
- comportamnet etic, receptiv, diplomat, cu spirit de observatie, perceptiv, flexibil, tenace, hotarat, cu siguranta de sine.

## 8.5 Auditori Sefi

### Studii

- minim studii medii;

### Instruiri specifice procesului de certificare

- *absolvent al unui/ unor curs / cursuri de minim 5 zile de auditor in domeniul securitatii informatiei;*
- cunoasterea documentatiei Procert Laboratory;

### Experienta de lucru

- *experienta de munca de minim 4 ani vechime (cu norma intreaga) in tehnologia informatiei ;*
- *minim 2 ani experienta intr-o functie in legatura cu securitatea informatiilor*
- experienta relevanta de minim 1 an in domeniul de competenta.

### Experienta de audit

- *3 audituri SMSI complete.*

### Abilitati si competente

- capabilitatea de a aplica principiile, procedurile si tehnicile de audit;
- capabilitatea de a planifica si utiliza eficace resurse pe durata unui audit;
- cunostarea contextului regional in care se desfasoara activitatile organizatiei evaluate;
- capabilitatea de a organiza si orienta membrii echipei de audit;
- capabilitatea de a preveni si rezolva conflictele ce pot aparea in cadrul echipei de audit sau intre echipa de audit si organizatia auditata;
- capabilitatea de a conduce echipa de audit pentru a obtine concluziile auditului;
- capabilitatea de a pregati si finaliza raportul de audit;

- capabilitateade a identifica si colecta informatii relevante pentru verificarea conformitatii cu cerintele standardului;
- capabilitatea de a intelege sistemele de management al securitatii informatiei in diverse organizatii, interactiunile intre componentele acestora;
- capabilitatea de a intelege organizatia clientului, managementul aspectelor care privesc securitatea informatiilor referitoare la activitatile, produsele si serviciile acestora.
- capabilitatea de a intelege cerintele de reglementare aplicabile sistemului de management al securitatii informatiei din cadrul organizatiei clientului
- capabilitatea de a recunoaste diferentele dintre documentele de referinta si prioritatile acestora cat si aplicarea lor in diverse situatii de audit;
- capabilitatea de a pune operatii complexe intr-o perspectiva larga si de a intelege rolul unitatilor individuale in organizatiile clientilor mai mari;
- cunostinte asupra legilor, reglementarilor si altor cerinte legale relevante domeniului de competenta;
- cunostinte referitoare la procese, produse, inclusiv servicii aferente domeniului sau de competenta pentru a intelege contextul tehnologic in care se efectueaza auditul;
- cunostinte referitoare la analiza eficacitatii sistemului de management al securitatii informatiei si la masurarea eficacitatii masurilor de securitate
- cunostinte tehnice corespunzatoare referitoare la activitatile specifice din cadrul domeniului de activitate al sistemului de management al securitatii informatiei, potentialele riscuri de securitate a informatiilor aferente;
- sa aiba urmatoarele caracteristici personale: obiectiv, matur, cu capacitate de discernamant, analitic, tenace si realist, comunicativ, lucru in echipa, bun conciliant;
- capacitatea de a lucra in echipa, de a comunica, de a raporta corect informatiile, de a forma personal.
- comportament etic, receptiv, diplomat, cu spirit de observatie, perceptiv, flexibil, tenace, hotarat, cu siguranta de sine.

## 8.6 Experti

### Studii

- minim studii superioare sau postuniversitare pe domeniul de competenta, pentru nivelurile de risc;

### Instruiri specifice procesului de certificare

- cunoasterea standardului SR ISO/CEI 27001:2006;
- cunoasterea procedurilor si tehnicilor de audit;
- cunoasterea documentatiei Procert Laboratory;

### Experienta de lucru

- experienta profesionala totala de minim 5 ani vechime;
- experienta profesionala in tehnologia informatiei 4 ani (cu norma intreaga);
- experienta profesionala in securitatea informatiei 2 ani (cu norma intreaga) din cei 4 de mai sus;

---

## Abilitati si competente

- cunostarea contextului regional in care se desfasoara activitatile organizatiei evaluate;
- capacitatea de a identifica si colecta informatii relevante pentru verificarea conformitatii cu cerintele standardului;
- capacitatea de a intelege sistemele de management al securitatii informatiei in diverse organizatii, interactiunile intre componentele acestora;
- capacitatea de a recunoaste diferentele dintre documentele de referinta si prioritatile acestora cat si aplicarea lor in diverse situatii de audit;
- capacitatea de a pune operatii complexe intr-o perspectiva larga si de a intelege rolul unitatilor individuale in organizatiile clientilor mai mari;
- cunostinte asupra legilor, reglementarilor si altor cerinte legale relevante domeniului de competenta;
- cunostinte referitoare la procese, produse, inclusiv servicii aferente domeniului sau de competenta pentru a intelege contextul tehnologic in care se efectueaza auditul;
- cunostinte specifice privind procesul, problemele de securitate a informatiilor si legislatia care afecteaza organizatia client;sa aiba urmatoarele caracteristici personale: obiectiv, matur, cu capacitate de discernamant, analitic, tenace si realist, comunicativ, bun conciliant;
- capacitatea de a lucra in echipa, de a comunica, de a raporta corect informatiile, de a forma personal.