ASOCIAŢIA DE ACREDITARE DIN ROMÂNIA
ORGANISMUL NAŢIONAL DE ACREDITARE

REGULAMENT SPECIFIC DE ACREDITARE

în domeniul acreditării organismelor care efectuează audit și certificare a sistemelor de management al securității informației conform SR EN ISO/CEI 17021-1:2015 și SR ISO/IEC 27006:2016

RENAR Cod: **RS-5.2.6 SMSI**

APROBAT

Director general al structurii executive
Alina Elena TAINĂ

Ediția din data aprobării: 22.04.2019

Data intrării în vigoare: 22.04.2019

CUPRINS

1. INTRODUCERE

Cerinţele pe care trebuie să le îndeplinească organismele care efectuează auditul şi certificarea sistemelor de management al securității informației, pentru a obţine și menține acreditarea sunt menționate în SR EN ISO/IEC 17021-1:2015 „Evaluarea conformităţii. Cerinţe pentru organisme care efectuează audit şi certificare de sisteme de management. Partea 1: Cerințe” și în SR ISO/IEC 27006:2016 ”Tehnologia informaţiei. Tehnici de securitate. Cerinţe pentru organismele care furnizează servicii de auditare şi certificare a sistemelor de management al securităţii informaţiei”.

La elaborarea şi implementarea documentelor sistemului de management propriu, OEC trebuie să se ia în considerare ghidurile EA, IAF şi ISO aplicabile. Aceste documente pot fi găsite la următoarele adrese de web: www.european-accreditation.org, www.iaf.nu, www.iso.org.

Solicitarea acreditării este voluntară. Acreditarea acordată de RENAR nu este echivalentă cu autorizaţia acordată de autoritățile competente pentru diferite activităţi, în condiţiile legii.

Organismele acreditate poartă întreaga responsabilitate pentru activităţile pe care le desfăşoară şi documentele pe care le emit şi nu pot utiliza acreditarea acordată de RENAR pentru a fi exonerate de răspundere sau pentru împărţirea responsabilităţii.

2. DOMENIU DE APLICARE

Acest document este aplicabil organismelor care auditează şi certifică sisteme de management al securităţii informaţiilor şi care solicită acreditarea sau sunt acreditate de RENAR, în domeniul voluntar (nereglementat).

Acest document conţine prevederi de aplicare ale anumitor cerinţe din standardul SR EN ISO/CEI 17021-1:2015, precum și din standardul SR ISO/IEC 27006:2016, pentru a se asigura o aplicare unitară şi consecventă în procesul de acreditare a organismelor care furnizează servicii de audit şi certificare a sistemelor de management al siguranței informației faţă de cerințele SR EN ISO/IEC 27001:2018.

3. TERMINOLOGIE, DEFINIȚII ȘI PRESCURTĂRI

3.1 Terminologie şi definiţii

Se aplică definiţiile din documentele de referință de la capitolul 4, precum și din:

- SR EN ISO/CEI 17011:2005 – Evaluarea conformităţii. Cerinţe generale pentru organismele de acreditare care acreditează organisme de evaluarea a conformităţii
- SR EN ISO/CEI 17000:2005 – Evaluarea conformităţii. Vocabular şi principii generale
- SR ISO/IEC 27000: 2017 - Tehnologia informaţiei. Tehnici de securitate. Sisteme de management al securităţii informaţiei. Privire de ansamblu şi vocabular
- SR ISO/IEC 27006:2016 - Tehnologia informaţiei. Tehnici de securitate. Cerinţe pentru organismele care furnizează servicii de auditare şi certificare a sistemelor de management al securităţii informaţiei

3.2 Prescurtări

EA – European Cooperation for Accreditation
IAF – International Accreditation Forum

OEC – Organism de evaluare a conformității
SMSI – Sistem de management al securității informației

4. CRITERII SPECIFICE PENTRU ACREDITARE

4.1 OEC trebuie să îndeplinească cerințele din versiunile în vigoare ale documentelor de referință menționate mai jos:

4.1.1 Standarde pentru acreditare

SR EN ISO/CEI 17021-1:2015 – Evaluarea conformităţii. Cerinţe pentru organisme care efectuează audit şi certificare de sisteme de management. Partea 1: Cerințe

SR ISO/IEC 27006:2016 – Tehnologia informaţiei. Tehnici de securitate. Cerinţe pentru organismele care furnizează servicii de auditare şi certificare a sistemelor de management al securităţii informaţiei

4.1.2 Documente pentru evaluarea conformității

SR EN ISO/IEC 27001:2018 – Tehnologia informaţiei. Tehnici de securitate. Sisteme de management al securităţii informaţiei. Cerinţe

4.1.3 Ghiduri de aplicare a standardelor de acreditare

IAF MD 1 – Certification of Multiple Sites Based on Sampling, ediția în vigoare
IAF MD 2 – Transfer of Accredited Certification of Management Systems, ediția în vigoare
IAF MD 3 – IAF Mandatory Document for Advanced Surveillance and Recertification Procedures, ediția în vigoare
IAF MD 4 – IAF Mandatory Document for the use of Computer Assisted AuditingTechniques (“CAAT”) for Accredited Certification of Management Systems, ediția în vigoare
IAF MD 11 – IAF Mandatory Document for the Application of ISO/IEC 17021 for Audits of Integrated Management Systems, ediția în vigoare
IAF MD 12 – Accreditation Assessment of Conformity Assessment Bodies with Activities in Multiple Countries, ediția în vigoare

4.1.4 Alte referințe pentru SMSI

SR ISO/IEC 27007:2016 – Tehnologia informaţiei. Tehnici de securitate. Linii directoare pentru auditarea sistemelor de management al securităţii informaţiei
ISO/IEC TR 27008:2019 – Information technology -- Security techniques -- Guidelines for auditors on information security controls
Alte standarde din seria ISO/CEI 27000 aplicabile

4.1.5 Documente RENAR

P-13	Politica privind tratarea reclamațiilor și apelurilor
P-16	Politica privind tratarea neconformităților constatate la evaluarea OEC
P-17	Politica privind supravegherea și reevaluarea
P-21	Politica privind suspendarea și retragerea acreditării
RE-01	Regulament pentru acreditare
RE-02	Regulament privind utilizarea mărcii naţionale de acreditare, referirea la statutul de acreditat al unui organism de evaluare a conformității și la statutul RENAR de

semnatar al acordurilor de recunoaştere multilaterală

RS-5.2 SM Regulament specific de acreditare în domeniul acreditării organismelor care efectuează audit şi certificare de sisteme de management – calitate, mediu, sănătate și securitate ocupațională, dispozitive medicale conform SR EN ISO/CEI 17021-1:2015

4.2 Cerințele pentru acreditare pot fi modificate, fie ca urmare a revizuirii sau înlocuirii standardului de acreditare, fie ca urmare a unor schimbări survenite în cadrul legislativ.

RENAR va adopta aceste modificări în propriile documente, conform Politicii privind tranziţia la noi standarde internaţionale P-07 şi Politicii privind schimbarea condiţiilor de acreditare P-08.

5. PREVEDERI SPECIFICE PRIVIND APLICAREA STANDARDELOR DE ACREDITARE SR EN ISO/CEI 17021-1:2015 ȘI SR ISO/IEC 27006:2016

Capitolul 5 urmăreşte ordinea articolelor din standardul SR EN ISO/CEI 17021-1:2015, completate de articolele din SR ISO/IEC 27006:2016.
Notă: Articolele din standard pentru care nu au fost necesare prevederi specifice nu sunt menționate.

5.1 OEC care solicită acreditarea trebuie să îndeplinească prevederile articolelor din standardele de acreditare SR EN ISO/CEI 17021-1:2015 ȘI SR ISO/IEC 27006:2016 și următoarele prevederi specifice:

5.2 *Art. 5 din SR EN ISO/CEI 17021-1:2015 și Art. 5 din SR ISO/IEC 27006:2016*
Se aplica prevederile cap. 5 Art. 5.1.1 și Art. 5.1.2 din RS-5.2 SM.

5.3 *Art. 7 din SR EN ISO/CEI 17021-1:2015 și Art. 7 din SR ISO/IEC 27006:2016*

5.3.1 *Art. 7.1 din SR EN ISO/CEI 17021-1:2015*

(1) OEC trebuie să-și stabilească domeniile tehnice care se referă, spre exemplu, la cerințele de competență în funcție de categoriile de tehnologii şi practici de securitate a informaţiilor, de tehnologiile şi activităţile referitoare la informaţii şi comunicare legate de selectarea controalelor de securitate adecvate şi proporţionale, care protejează resursele informatice, de standardele sectoriale, de legislația specifică.

Exemple de tehnologii ITC
- tehnologii de reţelistică şi comunicaţii cu spectru larg de aplicabilitate
- tehnologii şi aplicaţii generice pentru întreprinderi precum sisteme pentru asistarea deciziei, managementul proceselor, managementul conţinutului, managementul relaţiilor cu clienţii, planificarea resurselor (DSS, CMS, CRM, ERP etc.)
- tehnologii şi aplicaţii generice de management al identităţii
- tehnologii SCADA
- tehnologii de automatizare computerizată (monitorizare flote, măsurarea utilităţilor etc.)
- tehnologii web
- comerţul electronic - sisteme de plăţi on-line
- aplicaţii de comunicaţii de date şi voce (de exemplu, poşta electronică, chat, VoIP)

Exemple de măsuri de SI
- controlul accesului în reţele de date
- interceptarea comunicaţiilor şi monitorizarea datelor
- antivirus, firewall

- SIEM, IDS, IPS, DLP
- monitorizarea comunicaţiilor de date şi a aplicaţiilor (logging)
- colectarea probelor electronice
- criptare, structuri PKI, semnături electronice
- teste de penetrare (etical hacking)

(2) OEC trebuie să aibă un proces documentat pentru a determina competenţa necesară pentru fiecare funcţie din procesul de certificare (a se vedea Anexa A din SR EN ISO/CEI 17021-1:2015 şi Anexa A din SR ISO/IEC 27006:2016), pentru toate domeniile tehnice pe care şi le-a stabilit și identificarea competenţelor necesare şi asigurarea acestora pentru fiecare audit în parte.

(3) Datele de ieşire ale procesului trebuie să fie exprimate în cunoştinţe şi abilităţi, astfel încât să se demonstreze îndeplinirea eficientă a activităţilor de audit și certificare.

(4) OEC este responsabil pentru stabilirea competenţei personalului implicat în activităţi de management, audit şi certificare în conformitate cu propriile proceduri şi criterii.

Un auditor nu trebuie să fie declarat competent de către OEC doar pentru că acesta a fost declarat competent de către un alt OEC (acreditat). OEC trebuie să prezinte înregistrări privind verificarea îndeplinirii propriilor criterii de competenţă.

(5) Competenţa auditorilor OEC trebuie confirmată prin cel puţin două metode de evaluare (a se vedea anexa B din SR EN ISO/CEI 17021-1:2015 pentru fiecare criteriu de competență documentat.
OEC trebuie să demonstreze:

- ca metodele de evaluare alese sunt adecvate criteriilor de evaluare stabilite;
- că deţine înregistrări pentru a demonstra cum a fost evaluat personalul şi care a fost rezultatul evaluării;
- că deţine înregistrări care să demonstreze că toate criteriile de competenţă au fost evaluate.

5.3.2 *Art. 7.2 din SR EN ISO/CEI 17021-1:2015*

Se aplica prevederile cap. 5 Art. 5.2.2 din RS-5.2 SM.

OEC trebuie să deţină toate dovezile relevante şi înregistrările prin care să demonstreze competenţa fiecărui angajat (personal operaţional sau managerial) în raport cu activitatea de certificare pe care o desfăşoară conform prevederilor din Anexa A a standardului SR EN ISO/CEI 17021-1:2015.
Personalul OEC-ului implicat în conducerea şi efectuarea activităţilor de audit trebuie să acopere ca şi competenţă, toate domeniile tehnice stabilite de OEC pentru care OEC a solicitat acreditarea sau este acreditat.

5.4 *Art. 8 din SR EN ISO/CEI 17021-1:2015 și Art. 8 din SR ISO/IEC 27006:2016*

5.4.1 *Art. 8.1 din SR EN ISO/CEI 17021-1:2015*

Se aplică prevederile cap. 5 Art. 5.3.1 din RS-5.2 SM.

5.4.2 *Art.8.2 din SR EN ISO/CEI 17021-1:2015*

Se aplică prevederile de la pct. IS 8.2 ISMS din SR ISO/IEC 27006: 2016.

5.4.3 *Art. 8.4 din SR EN ISO/CEI 17021-1:2015*

Se aplică prevederile cap. 5 Art. 5.3.3 din RS-5.2 SM.

5.5 *Art. 9 din SR EN ISO/CEI 17021-1:2015 și Art. 9 din SR ISO/IEC 27006:2016*

(1) Se aplică prevederile cap. 5 Art. 5.4.1, Art. 5.4.2, Art. 5.4.3 și Art. 5.4.4 din RS-5.2 SM din RS-5.2 SM.
(2) OEC trebuie să aibă proceduri de stabilire a timpului auditului conform Anexei B a standardului SR EN ISO/IEC 27006:2016, prevederi pentru auditurile integrate conform IAF MD 11, cu respectarea IS 9.1.6. În cazul în care OEC decide reduceri ale tarifelor conform politicilor şi procedurilor sale, acest fapt nu trebuie să determine şi reduceri ale timpului de audit.
(3) OEC trebuie să aplice eşantionarea locaţiilor în conformitate cu IAF MD1.
(4) OEC trebuie să aibă acorduri contractuale cu clienţii săi care să-i permită să efectueze audituri speciale în cazul în care organizaţia client a avut incidente de securitate a informatiilor sau în cazul oricăror altor modificări majore ce pun sub semnul întrebării eficacitatea sistemului de management al securităţii informaţiilor.

6. PREVEDERI SPECIFICE REFERITOARE LA PROCESUL DE ACREDITARE

Procesul de acreditare se derulează conform RE-01 cu următoarele precizări:

6.1 Iniţierea acreditării

Mapa de documente informative aferente domeniului de acreditare faţă de SR EN ISO/CEI17021-1:2015 se găseşte pe site-ul RENAR: www.renar.ro, la secţiunea Procesul de acreditare.

6.2 Solicitarea acreditării

În cazul în care solicitantul are deja o acreditare pe baza standardului SR EN ISO/CEI 17021-1:2015 acordată de către RENAR, solicitarea de acreditare pentru audit şi certificare a sistemelor de management al securităţii informaţiilor este tratată ca o extindere. RENAR ia în considerare toate informaţiile aferente acreditărilor anterioare.

6.3 Evaluarea prin asistare

(1) Într-un ciclu de acreditare, evaluarile prin asistare se desfășoară, de regulă, la clienți ai OEC cu SMSI complexe, pentru diferite domenii de activitate (de ex. telecomunicații, energie, sănătate, financiar-bancar).
(2) În vederea efectuării evaluării prin asistare, OEC transmite la RENAR clienții programați a fi auditati în următoarele 4 luni, iar RENAR stabilește clientul la care va avea loc această evaluare în funcție de complexitatea SMSI a clientului.
(3) Într-un ciclu de acreditare, RENAR asistă cel puţin un audit de certificare inițială sau de recertificare.
(4) Atunci când selectează auditurile care vor fi asistate, RENAR nu va evalua prin asistare aceeaşi auditori care au fost asistaţi anterior sau un audit efectuat la aceeaşi organizaţie client al OEC.
(5) Echipa de evaluare RENAR are dreptul să consulte documentele sistemului de management ale clientului OEC, inclusiv Declaraţia de Aplicabilitate, în condiții de confidențialitate cerute atât de OEC, cât și de clientul OEC-ului. În cazul în care OEC nu asigură accesul la această documentație, RENAR are dreptul să înceteze procesul de acreditare.

6.4 Informarea RENAR

OEC trebuie să informeze în maxim 2 săptămâni RENAR despre orice modificări care afectează capacitatea de a îndeplini sarcinile de evaluare a conformității pentru care a fost acreditat (de exemplu: orice schimbare în statut, organizare, managementul la cel mai înalt nivel și personalul cheie ș.a.).

7. MODIFICĂRI FAȚĂ DE EDIȚIA ANTERIOARĂ

Modificările sunt identificate în text prin font de culoare albastră.

8. ISTORICUL DOCUMENTULUI

Ediția din data	Elaborat (E) /Modificat (M) de	Verificat de
15.05.2013	(E) Niculina TURCAN, Director Tehnic	Comitet Tehnic Certificare și Inspecție
12.10.2016	(M) Claudia BUCUR, Evaluator șef Virginica PEAGU, Evaluator șef Marian POROSCHIANU, Evaluator șef	Sorin CALOTĂ, Director DAOCI Alina TAINĂ, Director General Adjunct
25.05.2018	(M) Claudia BUCUR, Evaluator șef	Ovidiu Cantemir DUMITRU, DGA Cezar MILITARU, Director DAOCI Daniela IONESCU, Director DMC
22.04.2019	(M) Claudia BUCUR, Evaluator șef	Ovidiu Cantemir DUMITRU, MCR Cezar MILITARU, Director DAOCI