



ASOCIAȚIA DE ACREDITARE DIN ROMÂNIA
ORGANISMUL NAȚIONAL 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, SR ISO/IEC 27006:2016 și
ISO/IEC 27006:2015/Amd.1:2020

RENAR Cod: RS-5.2.6 SMSI

APROBAT

Pagina 1 din 9

Director general al structurii executive
Alina Elena TAINĂ

Ediția din data aprobării: 20.11.2020

Data intrării în vigoare: 20.11.2020

RENAR – Asociația de Accreditare din România Organismul Național de Accreditare	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, SR ISO/IEC 27006:2016 și ISO/IEC 27006: 2015/Amd.1: 2020	Cod: RS-5.2.6 SMSI Ediția din 20.11.2020
		Pagina 2 /9

CUPRINS

1. INTRODUCERE	3
2. DOMENIU DE APLICARE	3
3. TERMINOLOGIE, DEFINIȚII ȘI PRESCURTĂRI.....	3
3.1 Terminologie și definiții.....	3
3.2 Prescurtări.....	4
4. CERINȚE SPECIFICE PENTRU ACREDITARE.....	4
5. PREVEDERI SPECIFICE PRIVIND APLICAREA STANDARDELOR DE ACREDITARE SR EN ISO/CEI 17021-1:2015, SR ISO/IEC 27006:2016 și ISO/IEC 27006:2015/Amd.1:2020.....	5
6. PREVEDERI SPECIFICE REFERITOARE LA PROCESUL DE ACREDITARE	7
6.1 Inițierea acreditării.....	8
6.2 Solicitarea acreditării	8
6.3 Evaluarea prin asistare.....	8
6.4 Informarea RENAR	8
7. MODIFICĂRI FAȚĂ DE EDIȚIA ANTERIOARĂ.....	8
8. ISTORICUL DOCUMENTULUI.....	8

RENAR – Asociația de Acreditare din România Organismul Național 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, SR ISO/IEC 27006:2016 și ISO/IEC 27006: 2015/Amd.1: 2020	Cod: RS-5.2.6 SMSI Ediția din 20.11.2020
		Pagina 3 /9

1. INTRODUCERE

Cerințele pe care trebuie să le îndeplinească organismele care efectuează auditul și certificarea sistemelor de management al securității informației, pentru a obține și menține acreditarea sunt menționate în SR EN ISO/IEC 17021-1:2015 „Evaluarea conformității. Cerințe pentru organisme care efectuează audit și certificare de sisteme de management. Partea 1:Cerințe”, în SR ISO/IEC 27006:2016 [”Tehnologia informației. Tehnici de securitate. Cerințe pentru organismele care furnizează servicii de auditare și certificare a sistemelor de management al securității informației” și în ISO/IEC 27006:2015/Amd.1: 2020](#) ”Tehnologia informației. Tehnici de securitate. Cerințe pentru organismele care furnizează servicii de auditare și certificare a sistemelor de management al securității informației”.

La elaborarea și implementarea documentelor sistemului de management propriu, OEC trebuie să se ia în considerare ghidurile EA, IAF și 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 autorizația acordată de autoritățile competente pentru diferite activități, în condițiile legii.

Organismele acreditate poartă întreaga responsabilitate pentru activitățile pe care le desfășoară și documentele pe care le emit și nu pot utiliza acreditarea acordată de RENAR pentru a fi exonerate de răspundere sau pentru împărțirea responsabilității.

2. DOMENIU DE APLICARE

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

Acest document conține prevederi specifice privind aplicarea anumitor cerințe din standardul SR EN ISO/CEI 17021-1:2015, din standardul SR ISO/IEC 27006:2016, [precum și din ISO/IEC 27006: 2015/Amd.1: 2020](#), pentru a se asigura o aplicare unitară și consecventă în procesul de acreditare a organismelor care furnizează servicii de audit și certificare a sistemelor de management al siguranței informației față de cerințele SR EN ISO/IEC 27001:2018.

3. TERMINOLOGIE, DEFINIȚII ȘI PRESCURTĂRI

3.1 Terminologie și definiții

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

- SR EN ISO/IEC 17011:2018 – Evaluarea conformității. Cerințe pentru organismele de acreditare care acreditează organisme de evaluarea a conformității
- [SR EN ISO/IEC 17000:2020 – Evaluarea conformității. Vocabular și principii generale](#)
- SR EN ISO/IEC 27000: 2017 - Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației. Privire de ansamblu și vocabular
- SR ISO/IEC 27006:2016 - Tehnologia informației. Tehnici de securitate. Cerințe pentru organismele care furnizează servicii de auditare și certificare a sistemelor de management al securității informației
- [ISO/IEC 27006: 2015/Amd.1: 2020- Tehnologia informației. Tehnici de securitate. Cerințe pentru organismele care furnizează servicii de auditare și certificare a sistemelor de management al securității informației](#)

RENAR – Asociația de Accreditare din România Organismul Național de Accreditare	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, SR ISO/IEC 27006:2016 și ISO/IEC 27006: 2015/Amd.1: 2020	Cod: RS-5.2.6 SMSI Ediția din 20.11.2020
		Pagina 4 /9

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. CERINȚE 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 conformității. Cerințe pentru organisme care efectuează audit și certificare de sisteme de management. Partea 1: Cerințe

SR ISO/IEC 27006:2016 – Tehnologia informației. Tehnici de securitate. Cerințe pentru organismele care furnizează servicii de auditare și certificare a sistemelor de management al securității informației

[ISO/IEC 27006: 2015/Amd.1: 2020 - Tehnologia informației. Tehnici de securitate. Cerințe pentru organismele care furnizează servicii de auditare și certificare a sistemelor de management al securității informației](#)

4.1.2 Documente pentru evaluarea conformității

SR EN ISO/IEC 27001:2018 – Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației. Cerințe

4.1.3 Ghiduri de aplicare a standardelor de acreditare (sunt luate în considerare edițiile în vigoare)

- IAF MD 1 - IAF Mandatory Document for the Audit and Certification of a Management System Operated by a Multi-Site Organization;
- IAF MD 2 - IAF Mandatory Document for the Transfer of Accredited Certification of Management Systems;
- IAF MD 4 - IAF Mandatory Document for the Use of Information and Communication Technology (ICT) for Auditing/Assessment Purposes;
- IAF MD 11 - IAF Mandatory Document for Application of ISO/IEC 17021 for Audits of Integrated Management Systems (IMS)
- IAF MD 12 - IAF Mandatory Document for Accreditation Assessment of Conformity Assessment Bodies with Activities in Multiple Countries;
- IAF MD 17 - IAF Mandatory Document for Witnessing Activities for the Accreditation of Management Systems Certification Bodies
- IAF MD 23 Control of Entities Operating on Behalf of Accredited Management Systems Certification Bodies

4.1.4 Alte referințe pentru SMSI

[SR EN ISO/IEC 27002:2018, Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației](#)

RENAR – Asociația de Accreditare din România Organismul Național de Accreditare	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, SR ISO/IEC 27006:2016 și ISO/IEC 27006: 2015/Amd.1: 2020	Cod: RS-5.2.6 SMSI Ediția din 20.11.2020
		Pagina 5 /9

SR ISO/IEC 27007:2016 – Tehnologia informației. Tehnici de securitate. Linii directoare pentru auditarea sistemelor de management al securității informației
ISO/IEC TS 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
P-16	Politica privind tratarea neconformităților constatate la evaluarea OEC
P-17	Politica privind supravegherea și reevaluarea
P-21	Politica privind suspendarea, restrângerea și retragerea acreditării
P-27	Politica privind tratarea apelurilor
RE-01	Regulament pentru acreditare
RE-02	Regulament privind utilizarea mărcii naționale de acreditare, referirea la statutul de acreditat al unui organism de evaluare a conformității și la statutul RENAR de semnatar al acordurilor de recunoaștere multilaterală
RS-5.2 SM	Regulament specific de acreditare în domeniul acreditării organismelor care efectuează audit și 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 tranziția la noi standarde internaționale P-07 și Politicii privind schimbarea condițiilor de acreditare P-08.

5. PREVEDERI SPECIFICE PRIVIND APLICAREA STANDARDELOR DE ACREDITARE SR EN ISO/CEI 17021-1:2015, SR ISO/IEC 27006:2016 și ISO/IEC 27006:2015/Amd.1:2020

Capitolul 5 urmărește ordinea articolelor din standardul SR EN ISO/CEI 17021-1:2015, completate de articolele din SR ISO/IEC 27006:2016 și din ISO/IEC 27006:2015/Amd.1:2020.

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. 5.3.1](#) și [Art. 5.3.3](#) din RS-5.2 SM, precum și prevederile de la [pct. IS 5.2 din SR ISO/IEC 27006:2016](#).

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 și practici de securitate a informațiilor, de tehnologiile și activitățile referitoare la informații și comunicare legate de selectarea

RENAR – Asociația de Accreditare din România Organismul Național de Accreditare	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, SR ISO/IEC 27006:2016 și ISO/IEC 27006: 2015/Amd.1: 2020	Cod: RS-5.2.6 SMSI Ediția din 20.11.2020
		Pagina 6 /9

controalelor de securitate adecvate și proporționale, care protejează resursele informatice, de standardele sectoriale, de legislația specifică.

Exemple de tehnologii ITC

- tehnologii de rețelistică și comunicații cu spectru larg de aplicabilitate
- tehnologii și aplicații generice pentru întreprinderi precum sisteme pentru asistarea deciziei, managementul proceselor, managementul conținutului, managementul relațiilor cu clienții, planificarea resurselor (DSS, CMS, CRM, ERP etc.)
- tehnologii și aplicații generice de management al identității
- tehnologii SCADA
- tehnologii de automatizare computerizată (monitorizare flote, măsurarea utilităților etc.)
- tehnologii web
- comerțul electronic - sisteme de plăți on-line
- aplicații de comunicații de date și voce (de exemplu, poșta electronică, chat, VoIP)

Exemple de măsuri de SI

- controlul accesului în rețele de date
 - interceptarea comunicațiilor și monitorizarea datelor
 - antivirus, firewall
 - SIEM, IDS, IPS, DLP
 - monitorizarea comunicațiilor de date și a aplicațiilor (logging)
 - colectarea probelor electronice
 - criptare, structuri PKI, semnături electronice
 - teste de penetrare (ethical hacking)
- (2) OEC trebuie să aibă un proces documentat pentru a determina competența necesară pentru fiecare funcție din procesul de certificare (a se vedea Anexa A din SR EN ISO/CEI 17021-1:2015, [pct. IS 7.1.1 și IS 7.1.2](#) și Anexa A din SR ISO/IEC 27006:2016 și [art. 5.4.1 din RS-5.2.SM](#)), pentru toate domeniile tehnice pe care și le-a stabilit și identificarea competențelor necesare și asigurarea acestora pentru fiecare audit în parte.
- (3) Datele de ieșire ale procesului trebuie să fie exprimate în cunoștințe și abilități, astfel încât să se demonstreze îndeplinirea eficientă a activităților de audit și certificare.
- (4) OEC este responsabil pentru stabilirea competenței personalului implicat în activități de management, audit și certificare în conformitate cu propriile proceduri și 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 competență.

- (5) Competența auditorilor OEC trebuie confirmată prin cel puțin 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 deține înregistrări pentru a demonstra cum a fost evaluat personalul și care a fost rezultatul evaluării;
- că deține înregistrări care să demonstreze că toate criteriile de competență au fost evaluate.

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

Se aplica prevederile cap. 5 Art. [5.4.2](#) din RS-5.2 SM.

OEC trebuie să dețină toate dovezile relevante și înregistrările prin care să demonstreze competența fiecărui angajat (personal operațional sau managerial) în raport cu activitatea de

RENAR – Asociația de Accreditare din România Organismul Național de Accreditare	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, SR ISO/IEC 27006:2016 și ISO/IEC 27006: 2015/Amd.1: 2020	Cod: RS-5.2.6 SMSI Ediția din 20.11.2020
		Pagina 7 /9

certificare pe care o desfășoară conform prevederilor din Anexa A a standardului SR EN ISO/CEI 17021-1:2015.

Personalul OEC-ului implicat în conducerea și efectuarea activităților de audit trebuie să acopere ca și competență, toate domeniile tehnice stabilite de OEC pentru care OEC a solicitat acreditarea sau este acreditat.

Se aplică și prevederile de la pct. IS 7.2 din SR ISO/IEC 27006:2016 așa cum au fost modificate și completate prin ISO/IEC 27006:2015/Amd.1:2020.

5.3.3 *Art. 7.3 din SR EN ISO/CEI 17021-1:2015*

Se aplică și prevederile de la pct. IS 7.3 din SR ISO/IEC 27006:2016.

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. 5.5.1 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 așa cum au fost modificate prin ISO/IEC 27006:2015/Amd.1:2020.

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

Se aplică prevederile cap. 5 Art. 5.5.3 din RS-5.2 SM și prevederile de la pct. IS 8.4 din SR ISO/IEC 27006: 2016.

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. 5.6.1, Art. 5.6.2, Art. 5.6.3 și Art. 5.6.4 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 9.1.4 (așa cum a fost modificat prin ISO/IEC 27006:2015/Amd.1 : 2020) și IS 9.1.6 din SR ISO/IEC 27006:2016. În cazul în care OEC decide reduceri ale tarifelor conform politicilor și procedurilor sale, acest fapt nu trebuie să determine și reduceri ale timpului de audit.
- (3) OEC trebuie să aplice eșantionarea locațiilor în conformitate cu IAF MD1 cu respectarea IS 9.1.5 din SR ISO/IEC 27006:2016 și Art. 5.6.5 din RS-5.2 SM.
- (4) OEC trebuie să aibă acorduri contractuale cu clienții săi care să-i permită să efectueze audituri speciale în cazul în care organizația client a avut incidente de securitate a informațiilor sau în cazul oricăror altor modificări majore ce pun sub semnul întrebării eficacitatea sistemului de management al securității informațiilor.

Se aplică prevederile de la pct. IS 9.1.1, IS 9.1.3 (așa cum a fost modificat prin ISO/IEC 27006:2015/Amd.1:2020), IS 9.1.4, IS 9.1.5, IS 9.1.6, IS 9.2.1, IS 9.2.2, IS 9.3.1, IS 9.4, IS 9.5, IS 9.6.2, IS 9.6.3, IS 9.6.4 din SR ISO/IEC 27006:2016.

6. PREVEDERI SPECIFICE REFERITOARE LA PROCESUL DE ACREDITARE

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

RENAR – Asociația de Accreditare din România Organismul Național de Accreditare	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, SR ISO/IEC 27006:2016 și ISO/IEC 27006: 2015/Amd.1: 2020	Cod: RS-5.2.6 SMSI Ediția din 20.11.2020
		Pagina 8 /9

6.1 Inițierea acreditării

Mapa de documente informative aferente domeniului de acreditare față de SR EN ISO/CEI17021-1:2015 se găsește pe site-ul RENAR: www.renar.ro, la secțiunea 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 și certificare a sistemelor de management al securității informațiilor este tratată ca o extindere. RENAR ia în considerare toate informațiile aferente acreditărilor anterioare.

6.3 Evaluarea prin asistare

- (1) Într-un ciclu de acreditare, evaluările prin asistare se desfășoară, de regulă, la clienții 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 auditați 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 puțin un audit de certificare inițială sau de recertificare.
- (4) Atunci când selectează auditurile care vor fi asistate, RENAR nu va evalua prin asistare aceiași auditori care au fost asistați anterior sau un audit efectuat la aceeași organizație client al OEC.
- (5) Echipa de evaluare RENAR are dreptul să consulte documentele sistemului de management ale clientului OEC, inclusiv Declarația 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

RENAR – Asociația de Acreditare din România Organismul Național 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, SR ISO/IEC 27006:2016 și ISO/IEC 27006: 2015/Amd.1: 2020	Cod: RS-5.2.6 SMSI Ediția din 20.11.2020
		Pagina 9 /9

22.04.2019	(M) Claudia BUCUR, Evaluator șef	Ovidiu Cantemir DUMITRU, MCR Cezar MILITARU, Director DAOCI
02.04.2020	(M) Marian POROSCHIANU, Director DAOCI Claudia BUCUR, Evaluator șef	Ovidiu Cantemir DUMITRU, Manager Calitate și Risc
20.11.2020	(M) Marian POROSCHIANU, Director DAOCI Claudia BUCUR, Evaluator Șef	Ovidiu Cantemir DUMITRU, Manager Calitate și Risc