Document IAF Obligatoriu

CERINȚE PENTRU TRANZIȚIA LA ISO/IEC 27001:2022

Ediția 2

(IAF MD 26:2023)

Emis: 15 februarie 2023 Data aplicării: 15 februarie 2023 IAF MD 26:2023, Ediţia 2

Declaraţia RENAR

RENAR are permisiunea IAF pentru traducerea în limba română şi publicarea pe pagina WEB a prezentului document.

RENAR recunoaşte şi respectă drepturile de autor ale IAF şi solicită utilizatorilor acestui document să nu-l folosească în alt mod sau în alte scopuri decât este stipulat „***Copyright – IAF***”.

În situaţia în care, între părţile interesate, apar divergenţe de interpretare a prevederilor prezentului document, datorate traducerii, definitorie este varianta în limba engleză a documentului. Documentul va fi publicat pe pagina WEB a RENAR, www.renar.ro, împreună cu varianta originală în limba engleză.

Traducerea din limba engleză: Lăcrămiora TUDOR

Forumul Internațional de Acreditare, Inc (IAF) facilitează comerțul și sprijină industria și autoritățile de reglementare prin operarea unui acord de recunoaștere reciprocă la nivel mondial între Organismele de Acreditare (OA) pentru ca rezultatele emise de Organismele de Evaluare a Conformității (OEC) acreditate de către membrii IAF să fie acceptate la nivel global.

Acreditarea reduce riscurile pentru mediul de afaceri şi clienţii săi asigurându-i că OEC acreditate sunt competente să desfăşoare activităţile specifice cuprinse în domeniul lor de acreditare. OA care sunt membre ale IAF şi OEC acreditate de acestea trebuie să îndeplinească cerinţele standardelor internaţionale adecvate şi ale documentelor IAF obligatorii, pentru o aplicare consecventă a acestor standarde.

OA semnatare ale Acordului de Recunoaștere Multilaterală (MLA) sunt evaluate cu regularitate de o echipă de omologi numită cu scopul de a furniza încredere în funcționarea programelor lor de acreditare. Structura IAF MLA este detaliată în IAF PL 3 – Politici și Proceduri privind Structura IAF MLA și Extinderea Domeniului IAF MLA. Domeniul de aplicare al IAF MLA este detaliat în documentul Statutul IAF MLA.

IAF MLA este structurat pe cinci niveluri: Nivelul 1 precizează criteriile obligatorii care se aplică tuturor organismelor de acreditare, ISO/IEC 17011. Combinarea unei/ unor activități de la Nivelul 2 cu documentul(tele) normative corespunzătoare de la Nivelul 3 se numește domeniul principal al MLA, iar combinarea documentelor normative relevante de la Nivelul 4 (dacă se aplică) și Nivelul 5 se numește un sub-domeniu al MLA.

- Domeniul principal MLA include activități, de ex. certificare de produs, și standardele obligatorii asociate, de ex. ISO/IEC 17065. Atestările efectuate de OEC la nivelul domeniului principal sunt considerate ca având acelaşi nivel de încredere.
- Subdomeniul MLA include cerințele pentru evaluarea conformității, de ex. ISO 9001 și cerințele specifice schemei, unde este aplicabil, de ex. ISO TS 22003-1. Atestările efectuate de OEC-uri la nivelul subdomeniului sunt considerate a fi echivalente.

IAF MLA furnizează încrederea necesară pentru acceptarea pe piață a rezultatelor evaluării conformității. O atestare emisă, în cadrul domeniului IAF MLA, de un organism acreditat de un OA semnatar IAF MLA poate fi recunoscută în toată lumea, facilitându-se astfel comerțul internațional.

CUPRINS

Ediţia Nr. 2
Elaborat de: Comitetul Tehnic IAF
Aprobat de: Membrii IAF Data: 03 februarie 2023
Data emiterii: 15 februarie 2023 Data aplicării: 15 februarie 2023
Persoană de contact: Elva Nilsen
IAF Corporate Secretary
Telefon: +1 613 454-8159
Email: secretary@iaf.nu

Introducere la documentele IAF obligatorii

Termenul “ar trebui” este utilizat pentru a indica mijloacele recunoscute pentru îndeplinirea cerințelor standardului. Un Organism de Evaluare a Conformității (OEC) le poate îndeplini într-o manieră echivalentă cu condiția ca aceasta să poată fi demonstrată unui Organism de Acreditare (OA). Termenul “trebuie” este utilizat în acest document pentru a indica acele prevederi care, reflectând cerințele standardului relevant, sunt obligatorii.

Cerințe pentru tranziția la ISO/IEC 27001:2022

1. INTRODUCERE

Toate documentele care furnizează informații privind tranzițiile documentelor normative vor fi documente obligatorii, de urmat de organismele de acreditare (OA) semnatare ale IAF MLA și de Organisme de Evaluare a Conformității (OEC) acreditate, cu domeniul de aplicare așa cum se detaliază în acest document. Acest document este elaborat de un grup de lucru numit de Comitetul Tehnic IAF în conformitate cu IAF PR 7:2022 – "Cerințe pentru elaborarea documentelor IAF obligatorii privind tranzițiile".

Acest document furnizează cerințe privind tranziția de mai jos și este obligatoriu pentru organismele de acreditare semnatare ale acordului IAF MLA și pentru OEC acreditate de acestea, pentru domeniul în cauză:

Document normativ:	ISO/IEC 27001:2022
Înlocuiește:	ISO/IEC 27001:2013
Statut curent (la data publicării documentului obligatoriu):	IS
Perioada de tranziție:	3 Years (36 months)

2. REZUMATUL MODIFICĂRILOR PRINCIPALE

2.1 Istoric

Conform politicii ISO aferente, ISO/IEC FDIS 27001:2022 a fost elaborat prin integrarea ISO/IEC 27001:2013 cu ISO/IEC 27001:2013/COR 1:2014, ISO/IEC 27001:2013/COR 2:2015 și ISO /IEC 27001:2013/DAmd1 în iulie 2022. În plus, ISO a cerut ISO/IEC FDIS 27001:2022 să se alinieze la structura armonizată pentru standardele sistemului de management (MSS) definită în Anexa SL a Directivelor ISO/IEC, Partea 1, Supliment ISO consolidat, 2022. Pe baza rezultatului votului FDIS, ISO a publicat ISO/IEC 27001:2022 la 25 octombrie 2022.

Nota 1: ISO/IEC 27001:2013/DAmd1 a fost elaborat pentru a se alinia cu ISO/IEC 27002:2022, care a actualizat Anexa A și notele de la Clauza 6.1.3 c). DAmd este abrevierea pentru proiectul de amendament.

Nota 2: Nu vor fi publicate mai mult de două documente separate sub formă de amendamente care modifică un standard internațional actual (a se vedea Directiva ISO/IEC Partea 1, 2022, Clauza 2.10.3), prin urmare, noua ediție a ISO/IEC 27001 trebuia publicată după elaborarea ISO/IEC 27001:2013/DAmd1.

2.2 Principalele modificări

În comparație cu ISO/IEC 27001:2013, principalele modificări ale ISO/IEC 27001:2022 includ, dar nu se limitează la:

1) Anexa A face referire la controalele de securitate a informațiilor din ISO/IEC 27002:2022, care includ informațiile despre denumirea si tipul de control.
2) Notele Clauzei 6.1.3 c) sunt revizuite editorial, inclusiv ștergerea obiectivelor de control și utilizarea „controlul securității informațiilor” pentru a înlocui „controlul”.
3) Formularea clauzei 6.1.3 d) este reorganizată pentru a elimina eventualele ambiguități.
4) Adăugarea unui nou punct 4.2 c) pentru a determina cerințele părților interesate luate în considerare într-un sistem de management al securității informațiilor (SMSI).
5) Adăugarea unei noi subclauze 6.3 - Planificarea modificărilor, care definește că modificările la SMSI trebuie efectuate de către organizație într-o manieră planificată.
6) Păstrarea consecvenței verbului folosit în legătură cu informațiile documentate, de exemplu, folosirea formulării „Informațiile documentate trebuie să fie disponibile ca dovadă a XXX” în clauzele 9.1, 9.2.2, 9.3.3 și 10.2.
7) Utilizarea „proceselor, produselor sau serviciilor furnizate din exterior” pentru a înlocui „procesele externalizate” din Clauza 8.1 și ștergerea termenului „externalizare”.
8) Denumirea și reordonarea subclauzelor de la Clauza 9.2 - Audit intern și 9.3 – Analiza efectuată de management.
9) Schimbarea ordinii celor două subclauze de la Clauza 10 - Îmbunătățire.
10) Actualizarea ediției documentelor conexe enumerate în Bibliografie, cum ar fi ISO/IEC 27002 și ISO 31000.
11) Unele abateri ale ISO/IEC 27001:2013 de la structura de nivel înalt, textul de bază identic, termenii comuni și definițiile de bază ale MSS sunt revizuite pentru a fi consecvente cu structura armonizată pentru MSS, de exemplu, Clauza 6.2 d).

Nota 1: Primele două elemente provin din ISO/IEC 27001:2013/DAmd1, al treilea element este din ISO/IEC 27001:2013/COR 2:2015, iar celelalte modificări rezultă din structura armonizată pentru MSS.

Nota 2: În comparație cu ediția anterioară, numărul de controale de securitate a informațiilor din ISO/IEC 27002:2022 scade de la 114 controale în 14 clauze la 93 controale în 4 clauze. Pentru controalele din ISO/IEC 27002:2022, 11 controale sunt noi, 24 de controale sunt comasate cu controalele existente și 58 de controale sunt actualizate. Mai mult, este revizuită structura de control, care introduce „atribut" și „scop" pentru fiecare control și nu mai folosește „obiectiv" pentru un grup de controale.

Nota 3: ISO/IEC 27001:2013/COR 1:2014 este asociat cu Anexa A și se suprapune cu ISO/IEC 27001:2013/DAMD1.

2.3 Impactul

Impactul modificărilor din ISO/IEC 27001:2022 include, dar nu se limitează la introducerea unei noi Anexe A și a Clauzei 6.3 - Planificarea modificărilor deoarece:

1) ISO/IEC 27001:2013/COR 2:2015 a fost deja publicat și implementat.
2) Anexa A este normativă.
3) Structura armonizată pentru MSS este considerată ca o revizuire minoră pentru structura la nivel înalt, text de bază identic, termeni comuni și definiții de bază ale MSS, în care majoritatea modificărilor sunt considerate editoriale.

Cerințele din ISO/IEC 27001 care utilizează controlul de referință stabilit în Anexa A sunt procesul de comparare între controalele de securitate a informațiilor determinate de organizație și cele din Anexa A (6.1.3 c)) și elaborarea unei Declarații de Aplicabilitate (6.1.3 d)). Prin compararea controalelor necesare securității informațiilor cu cele din Anexa A, organizația poate confirma că orice control necesar al securității informațiilor din referința stabilită în Anexa A la ISO/IEC 27001:2022 nu este omis din neatenție.

O astfel de comparație ar putea să nu conducă la descoperirea vreunui control necesar al securității informațiilor care a fost omis din greșeală. Cu toate acestea, dacă sunt descoperite controale necesare de securitate a informațiilor omise din greșeală, organizația trebuie să își actualizeze planurile de tratare a riscurilor pentru a adapta și implementa controalele suplimentare necesare de securitate a informațiilor.

După cum este sugerat mai sus, impactul ISO/IEC 27001:2022 asupra organizațiilor care au implementat SMSI nu trebuie să fie semnificativ.

3. CALENDAR

Activitate	**Termen**
OA	
OA să fie pregătit să evalueze ISO/IEC 27001:2022 cel mai târziu	la 6 luni de la finalul lunii de publicare a documentului ISO/IEC 27001:2022 (de exemplu 30 aprilie 2023)
Acreditarea inițială de către OA numai față de ISO/IEC 27001:2022 să înceapă **nu mai târziu de**	6 luni de la finalul lunii de publicare a ISO/IEC 27001:2022 (de exemplu 30 aprilie 2023)
Tranzițiile OA pentru OEC să fie finalizate în	12 luni de la finalul lunii de publicare a ISO/IEC 27001:2022 (de exemplu 31 octombrie 2023)
OEC	
OEC să utilizeze pentru certificări inițiale și recertificări numai ISO/IEC 27001:2022 **nu mai târziu de**	18 luni de la finalul lunii de publicare a ISO/IEC 27001:2022 (de exemplu 30 aprilie 2024)
Tranzițiile OEC pentru clienții certificați să fie finalizate în	36 luni de la finalul lunii de publicare a ISO/IEC 27001:2022 (de exemplu 31 octombrie 2025)

4. ACȚIUNI PRIVIND PROCESUL DE TRANZIȚIE

4.1 Acțiuni ale OA

Activitate	***Da/ Nu***	***Note***
Aranjamente ale OA	Da	1) OA trebuie să stabilească aranjamentul de tranziție la ISO/IEC 27001:2022 având în vedere cerințele acestui document. 2) Aranjamentul de tranziție trebuie să abordeze ceea ce trebuie să facă OA și OEC. OA poate avea mai multe documente separate privind aranjamentul de tranziție. 3) Aranjamentul de tranziție trebuie să includă cel puțin luarea în considerare a următoarelor: • Schimbările din ISO/IEC 27001 și analiza GAP. • Personalul relevant este competent pentru ISO/IEC 27001:2022 și procesul de tranziție.

		Notă: Echipa de evaluare, în ansamblu, trebuie să aibă cunoștințe privind tehnologiile și practicile de securitate a informațiilor (a se vedea IAF MD 13:2020, 4.2). Cum știm cu toții, ISO/IEC 27002 oferă un set de referință de controale de securitate a informațiilor generice, inclusiv îndrumare pentru implementare. • Sunt identificate procesele și documentele OA afectate de modificarea ISO/IEC 27001, precum și sistemele informatice pentru gestionarea activităților de acreditare, dacă este aplicabil. • Programul de evaluare în vederea tranziției. • Există o comunicare în timp util către OEC referitoare la programul de evaluare în vederea tranziției, cum ar fi cronologia și abordarea evaluării tranziției și consecinţele nefinalizării tranziţiei până la termenul limită. 4) OA sunt încurajate să planifice și să înceapă acțiunile necesare cât mai curând posibil.
Analiza documentelor OEC	Nu	
Analiza documentelor tehnice ale OEC	Da	1) OA trebuie să efectueze revizuirea documentelor tehnice pentru a confirma dacă OEC sunt sau nu competente pentru ISO/IEC 27001:2022. 2) OA trebuie să determine adecvarea aranjamentului OEC pentru tranziție și, dacă este aplicabil, eficacitatea implementării acestuia prin revizuirea următoarelor informații transmise de OEC: • Analiza GAP pentru schimbările din ISO/IEC 27001:2022. • Aranjamentul de tranziție și dovezi de implementare a acestuia. • Autorizarea personalului implicat. • Celelalte informații relevante considerate necesare de către OA.
Evaluare tehnică la sediul	Dacă	Dacă OA poate să obțină dovezi suficiente prin

central al OEC (la fața locului sau la distanță)	este aplicabil	analiza documentelor tehnice ale OEC, atunci nu este necesară o evaluare la sediul central al OEC. Dacă OA nu poate verifica implementarea eficace și conformarea cu aranjamentul de tranziție al OEC, atunci este necesară o evaluare la sediu.
Evaluarea (evaluări) prin asistare ale OEC	Nu	
Este posibil să fie necesar mai mult timp pentru tranziție?	Da	Evaluarea trebuie să includă cel puțin 0,5 zi de evaluare suplimentar pentru a confirma tranziția OEC atunci când tranziția se efectuează ca o evaluare separată.
Altele	Da	1) OA poate defini în programul evaluării în vederea tranziției termenul pentru depunerea solicitării de tranziție de către OEC. 2) OA trebuie să ia decizia de tranziție pe baza rezultatului evaluării/evaluărilor în vederea tranziției. 3) Dacă este aplicabil, OA trebuie să actualizeze informațiile privind acreditarea pentru OEC acreditate (de exemplu, certificatul de acreditare) dacă a fost demonstrată competența lor pentru ISO/IEC 27001:2022. 4) Dacă OEC acreditat nu finalizează cu succes evaluarea în vederea tranziției înainte de data limită aferentă menționată la Clauza 3, data expirării acreditării acestora pentru ISO/IEC 27001:2013 nu trebuie să depășească sfârșitul perioadei de tranziție.

4.2 Acțiuni ale OEC

Activitate	**Da/ Nu**	**Note**
Aranjamente ale OEC	Da	1) OEC trebuie să stabilească aranjamentul de tranziție la ISO/IEC 27001:2022 având în vedere cerințele acestui document și aranjamentul de tranziție al OA respectiv. 2) Aranjamentul de tranziție trebuie să abordeze ceea ce trebuie să facă OEC și clientul. OEC poate avea mai multe documente separate privind aranjamentul de tranziție. 3) Aranjamentul de tranziție trebuie să includă cel puțin luarea în considerare a următoarelor: • Schimbările din ISO/IEC 27001 și analiza

		GAP. • Necesitatea de a modifica procesele, documentele de certificare conexe și, dacă este aplicabil, sistemele IT pentru gestionarea activităților de certificare. • Personalul relevant este competent pentru ISO/IEC 27001:2022 și procesul de tranziție. • Echipa de audit, în ansamblu, trebuie să aibă cunoștințe privind toate controalele de securitate a informațiilor conținute în ISO/IEC 27002:2022 și implementarea acestora (a se vedea ISO/IEC 27006:2015, 7.1.2.1.3 b)). • Programul de audit în vederea tranziției. • Există o comunicare în timp util către clienți referitoare la programul de tranziție, cum ar fi cronologia și abordarea auditului privind tranziția și consecinţele dacă clientul nu finalizează tranziţia până la sfârșitul perioadei de tranziție. 4) OEC sunt încurajate să planifice și să înceapă acțiunile necesare cât mai curând posibil.
Auditul în vederea traziției	Da	1) OEC poate efectua auditul în vederea tranziției împreună cu auditul de supraveghere, auditul de recertificare sau printr-un audit separat. 2) Auditul în vederea tranziției nu trebuie să se bazeze doar pe analiza documentelor, în special pentru revizuirea controalelor de securitate în tehnologia informațiilor. 3) Auditul în vederea tranziției trebuie să includă, dar nu se va limita la următoarele: • Analiza GAP a ISO/IEC 27001:2022, precum și nevoia de modificare a SMSI al clientului. • Actualizarea declarației de aplicabilitate (SoA). • Dacă este aplicabil, actualizarea planului

		de tratare a riscurilor. • Implementarea și eficacitatea controalelor de securitate a informațiilor noi sau modificate, alese de clienți. 4) OEC poate efectua auditul în vederea tranziției de la distanță dacă se asigură că obiectivele auditului în vederea tranziției sunt îndeplinite.
Este posibil să fie necesar mai mult timp pentru tranziție?	Da	1) Minim 0,5 zile-auditor pentru auditul în vederea tranziției, atunci când este efectuat împreună cu un audit de recertificare. 2) Minim 1,0 zi-auditor pentru auditul în vederea tranziției atunci când acesta este efectuat împreună cu un audit de supraveghere sau ca un audit separat.
Altele	Da	1) OEC poate defini în programul auditului în vederea tranziției termenul pentru depunerea solicitării de tranziție de către clienții certificați. 2) OEC trebuie să ia decizia de tranziție pe baza rezultatului auditului efectuat în vederea tranziției. 3) OEC trebuie să actualizeze documentele de certificare pentru clientul certificat dacă SMSI-ul acestuia îndeplinește cerințele ISO/IEC 27001:2022. Notă: Atunci când documentul de certificare este actualizat deoarece clientul a finalizat cu succes doar auditul în vederea tranziției, termenul de expirare al ciclului său de certificare actual nu va fi modificat. 4) Toate certificările bazate pe ISO/IEC 27001:2013 trebuie să expire sau să fie retrase la sfârșitul perioadei de tranziție.

4.3 Altele

4.3.1 Evaluarea sediului OEC ca urmare a deciziei de tranziție trebuie să se concentreze pe verificarea implementării aranjamentului de tranziție înainte ca aranjamentul de tranziție al OEC să fie finalizat în totalitate. Această evaluare a sediului trebuie să includă cel puțin următoarele:

- Implementarea proceselor și procedurilor revizuite ale OEC.
- Competența personalului implicat este demonstrată înainte ca acesta să fie implicat în activitățile de certificare ISO/IEC 27001:2022.

- Progresul tranziției pentru clienții certificați pentru ISO/IEC 27001:2022.

4.3.2 Toate evaluările prin asistare selectate în urma deciziei de tranziție trebuie să se bazeze pe ISO/IEC 27001:2022 și să se concentreze pe competența OEC de a efectua un audit bazat pe ISO/IEC 27001:2022.

Sfarșitul Documentului Obligatoriu IAF privind Cerințele de Tranziție la ISO/IEC 27001:2022

Informații suplimentare:

Pentru informații suplimentare privind acest document sau alte documente IAF, contactați orice membru IAF sau Secretariatul IAF.

Pentru detaliile de contact ale membrilor IAF – a se vedea pagina de internet a IAF: http://www.iaf.nu.

Secretariat:

Elva Nilsen
IAF Corporate Secretary
Telephone: +1 (613) 454-8159
Email: secretary@iaf.nu