					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: PII18					Titlul documentului: **Politica de monitorizare, audit și îmbunătățire a PIMS**							
Versiunea: 1.0		Data intrării în vigoare: 01.01.2025			Proprietarul documentului:							
X	Politică		Standard		Procedură		Formular		Registru		Altul	

Istoricul reviziilor				
Numărul reviziei	**Data reviziei**	**Modificări**	**Revizuit de**	**Proprietarul procesului**

Aprobări			
Nume	**Funcție**	**Data**	**Semnătură**

Aliniată la standardele și reglementările aplicabile

Standard/reglementare	Clauză/control/articol	Aplicabilitate	Tip de acoperire	Comentariu
ISO/IEC 27701:2025	Clause 6.2	Both	Supporting	Măsurarea obiectivelor privind confidențialitatea
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informații documentate privind monitorizarea, auditul și îmbunătățirea
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Monitorizarea planificării și controlului operațional
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Monitorizare, măsurare, analiză și evaluare
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Audit intern
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Revizuire de management
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Îmbunătățire continuă
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Neconformitate și acțiune corectivă
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Evidențele de prelucrare ale operatorului utilizate pentru audit
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Dovezi privind acordurile cu persoana împuternicită și cooperarea la audit
GDPR	Article 5(2)	Controller	Supporting	Dovezi privind responsabilitatea
GDPR	Article 24	Controller	Supporting	Măsuri ale operatorului și revizuirea eficacității

GDPR	Article 28	Both	Supporting	Guvernanța auditului și cooperării cu persoanele împuternicite
GDPR	Article 30	Both	Supporting	Evidențe ale prelucrării utilizate pentru audit
GDPR	Article 32	Both	Supporting	Testarea și evaluarea măsurilor de securitate
GDPR	Article 39	Conditional	Supporting	Monitorizare de către DPO și consiliere privind auditul, după caz
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Conformitate privind confidențialitatea, audit și supraveghere independentă
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Revizuirea protecției PII și verificări de conformitate
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Monitorizarea și evaluarea securității informației
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	Suport pentru auditul intern ISMS
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	Suport pentru revizuirea de management ISMS
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	Suport pentru îmbunătățirea continuă ISMS
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	Suport pentru neconformități și acțiuni corective ISMS
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Revizuire independentă a

				securității informației
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Revizuirea conformității politicilor și standardelor
ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Principii, program, desfășurare și competență pentru auditul sistemelor de management

1. Domeniu de aplicare

1.1 Această politică definește cerințele organizației pentru monitorizarea, măsurarea, analiza, evaluarea, auditul intern, revizuirea de management, gestionarea neconformităților, acțiunea corectivă și îmbunătățirea continuă a PIMS.

1.2 Această politică se aplică următoarelor:

1.2.1 tuturor proceselor, controalelor, politicilor, registrelor, obiectelor de dovezi, sistemelor, furnizorilor, persoanelor împuternicite, persoanelor subîmputernicite și aranjamentelor de partajare a datelor din domeniul de aplicare al PIMS;

1.2.2 contextelor organizației de operator, operator asociat, persoană împuternicită și persoană subîmputernicită;

1.2.3 monitorizării consolidate a performanței PIMS, obiectivelor privind confidențialitatea, stadiului implementării controalelor, constatărilor de audit, neconformităților, acțiunilor corective, acțiunilor rezultate din revizuirea de management și acțiunilor de îmbunătățire;

1.2.4 dovezilor păstrate în REG12 și dovezilor-sursă suport păstrate în REG01 până la REG11.

1.3 Această politică nu înlocuiește cerințele de monitorizare operațională definite în alte politici PIMS. Ea stabilește ciclul consolidat de evaluare a performanței, audit, revizuire și îmbunătățire pentru PIMS.

1.4 În sensul acestei politici, o neconformitate majoră PIMS înseamnă un eșec care afectează în mod semnificativ domeniul de aplicare al PIMS, obiectivele privind confidențialitatea, responsabilitatea pentru prelucrarea PII, tratamentul riscurilor privind confidențialitatea, drepturile persoanei vizate, securitatea prelucrării, guvernanța persoanelor împuternicite sau subîmputernicite, pregătirea pentru încălcări ale securității datelor, integritatea dovezilor documentate, domeniul de certificare sau eșecul repetat al aceleiași cerințe într-o perioadă de 12 luni.

1.5 În sensul acestei politici, o modificare semnificativă înseamnă orice modificare care afectează domeniul de aplicare al PIMS, scopurile prelucrării PII, categoriile de PII, categoriile de persoane vizate, locațiile de prelucrare, alocarea rolului de operator sau persoană împuternicită, arhitectura sistemului, aranjamentele cu furnizorii sau persoanele subîmputernicite, profilul de risc privind confidențialitatea, obligațiile legale sau contractuale aplicabile, domeniul auditului, metoda de monitorizare sau domeniul de certificare.

2. Scop

2.1 Scopul acestei politici este să asigure că organizația evaluează performanța PIMS, verifică conformitatea PIMS, identifică neconformitățile, corectează punctele slabe ale controalelor și îmbunătățește continuu PIMS pe baza dovezilor obiective.

2.2 Această politică permite organizației să demonstreze că activitățile de monitorizare, audit, revizuire de management și îmbunătățire ale PIMS sunt planificate, independente acolo unde este necesar, bazate pe dovezi, realizate la timp și trasabile către roluri responsabile și obiecte de dovezi canonice.

3. Obiective

3.1 Obiectivele acestei politici sunt să:

3.1.1 definească un proces consolidat de monitorizare și măsurare PIMS;

3.1.2 asigure că obiectivele privind confidențialitatea și performanța controalelor PIMS sunt măsurate folosind dovezi documentate;

3.1.3 stabilească un program de audit intern bazat pe risc pentru PIMS;

3.1.4 păstreze independența și obiectivitatea în activitățile de audit PIMS;

3.1.5 asigure că revizuirea de management primește date complete și actuale privind performanța PIMS;

3.1.6 asigure că neconformitățile sunt înregistrate, evaluate, corectate și verificate;

3.1.7 asigure că acțiunile corective sunt urmărite până la închidere și revizuite din perspectiva eficacității;

3.1.8 identifice punctele slabe recurente și oportunitățile de îmbunătățire;

3.1.9 sprijine pregătirea pentru certificare și gestionarea responsabilă a dovezilor;

3.1.10 evite duplicarea metricilor operaționale deja definite în politicile PIMS conexe.

4. Declarații de politică

4.1 Cadrul de monitorizare și măsurare PIMS

4.1.1 [Both] Privacy Lead / PIMS Manager TREBUIE să definească programul consolidat de monitorizare PIMS în REG12 înainte de operarea inițială a PIMS și ulterior anual.

4.1.2 [Both] Privacy Lead / PIMS Manager TREBUIE să definească metoda de măsurare, frecvența, sursa dovezilor, ținta și rolul responsabil pentru fiecare metrică PIMS în REG12 înainte de începerea ciclului de măsurare.

4.1.3 [Both] Process Owner / Business Owner TREBUIE să furnizeze trimestrial către Privacy Lead / PIMS Manager date de monitorizare a activităților de prelucrare PII din REG02.

4.1.4 [Both] Information Security Lead TREBUIE să furnizeze trimestrial către Privacy Lead / PIMS Manager date privind stadiul controalelor de securitate PII din REG03.

4.1.5 [Both] Vendor / Procurement Owner TREBUIE să furnizeze trimestrial către Privacy Lead / PIMS Manager date privind stadiul asigurării pentru persoanele împuternicite, persoanele subîmputernicite, partajarea cu terți și furnizorii, din REG08.

4.1.6 [All] Incident Response Coordinator TREBUIE să furnizeze către Privacy Lead / PIMS Manager date privind tendințele incidentelor de confidențialitate și ale încălcărilor securității datelor, din REG10, lunar și în termen de 10 zile lucrătoare după închiderea unui incident major.

4.1.7 [Both] Privacy Lead / PIMS Manager TREBUIE să consolideze trimestrial rezultatele monitorizării PIMS în REG12.

4.2 Programul de audit intern PIMS

4.2.1 [All] Internal Audit / Compliance Reviewer TREBUIE să pregătească anual, în REG12, un program de audit intern PIMS bazat pe risc, înainte de primul ciclu planificat de audit PIMS.

4.2.2 [All] Internal Audit / Compliance Reviewer TREBUIE să definească obiectivul, criteriile, domeniul, metoda, baza de eșantionare și termenul de raportare pentru fiecare audit PIMS în REG12 înainte de începerea activităților de audit pe teren.

4.2.3 [All] Internal Audit / Compliance Reviewer TREBUIE să înregistreze verificările privind independența auditorului și conflictele de interese în REG12 înainte de fiecare misiune de audit.

4.2.4 [All] Privacy Lead / PIMS Manager TREBUIE să pună la dispoziție informațiile documentate ale PIMS controlate și dovezile din registre solicitate, prin REG12, în termen de 10 zile lucrătoare de la o cerere de audit aprobată.

4.2.5 [Both] Internal Audit / Compliance Reviewer TREBUIE să testeze stadiul implementării controalelor PIMS aplicabile în raport cu REG03 în cadrul fiecărui audit PIMS.

4.2.6 [Both] Internal Audit / Compliance Reviewer TREBUIE să înregistreze în REG12, în cadrul fiecărui audit PIMS, eșantionul selectat de dovezi privind prelucrarea PII.

4.2.7 [All] Internal Audit / Compliance Reviewer TREBUIE să înregistreze rezultatele auditului PIMS în REG12 în termen de 15 zile lucrătoare după finalizarea auditului.

4.2.8 [All] Privacy Lead / PIMS Manager TREBUIE să desemneze proprietari ai acțiunilor corective pentru constatările acceptate ale auditului PIMS în REG12, în termen de 10 zile lucrătoare de la acceptarea rezultatelor auditului.

[... Secțiunile 4.3–8 nu sunt incluse în această previzualizare. Achiziționați documentul complet pentru a accesa conținutul integral. ...]

9. Excepții

9.1 Excepții privind monitorizarea, auditul și îmbunătățirea

9.1.1 [All] Process Owner / Business Owner TREBUIE să solicite orice excepție de la această politică în REG12 înainte ca abaterea să aibă loc.

9.1.2 [All] Privacy Lead / PIMS Manager TREBUIE să evalueze impactul fiecărei excepții solicitate asupra confidențialității, certificării, auditului și acțiunilor corective în REG12 în termen de 10 zile lucrătoare de la solicitare.

9.1.3 [All] Data Protection Officer / Privacy Advisor TREBUIE să înregistreze consilierea în REG12 înainte de aprobarea oricărei excepții care afectează obligațiile legale, drepturile persoanei vizate, angajamentele DPIA, obligațiile de audit față de clienți sau prelucrările cu risc ridicat.

9.1.4 [All] Top Management TREBUIE să aprobe în REG12 excepțiile care afectează finalizarea calendarului de audit, revizuirea de management, neconformitățile majore, domeniul de certificare sau prelucrările cu risc ridicat înainte ca excepția să producă efecte.

9.1.5 [All] Privacy Lead / PIMS Manager TREBUIE să stabilească în REG12 o dată de expirare care să nu depășească 90 de zile pentru fiecare excepție aprobată privind monitorizarea, auditul sau îmbunătățirea.

9.1.6 [All] Privacy Lead / PIMS Manager TREBUIE să închidă sau să reevalueze fiecare excepție privind monitorizarea, auditul sau îmbunătățirea în REG12 în termen de cinci zile lucrătoare de la expirare.

10. Aplicare

10.1 Aplicarea cerințelor privind monitorizarea, auditul și îmbunătățirea

10.1.1 [All] Privacy Lead / PIMS Manager TREBUIE să înregistreze un ciclu de monitorizare omis, un audit PIMS omis, o revizuire de management restantă, dovezi de audit lipsă, o acțiune corectivă restantă sau o acțiune de îmbunătățire restantă ca neconformitate în REG12 în termen de cinci zile lucrătoare de la identificare.

10.1.2 [All] Internal Audit / Compliance Reviewer TREBUIE să înregistreze severitatea constatării de audit în REG12 înainte de emiterea raportului de audit.

10.1.3 [All] Top Management TREBUIE să solicite acțiune corectivă pentru fiecare neconformitate majoră PIMS în REG12 în termen de 10 zile lucrătoare de la escaladare.

10.1.4 [All] Process Owner / Business Owner TREBUIE să împiedice intrarea în producție sau transmiterea asigurării externe pentru prelucrări cu risc ridicat atunci când dovezile obligatorii privind acțiunea corectivă lipsesc din REG12 înainte de intrarea în producție sau transmitere.

10.1.5 [All] Privacy Lead / PIMS Manager TREBUIE să escaladeze către Top Management termenele de monitorizare sau de acțiuni corective omise în mod repetat în REG12 în termen de cinci zile lucrătoare după a doua apariție într-o perioadă de 12 luni.

10.1.6 [All] Internal Audit / Compliance Reviewer TREBUIE să verifice închiderea măsurilor de aplicare în REG12 la următorul audit programat sau în termen de 60 de zile de la închiderea raportată, oricare dintre acestea survine mai întâi.

11. Revizuire și menținere

11.1 Revizuirea și menținerea politicii

11.1.1 [All] Privacy Lead / PIMS Manager TREBUIE să revizuiască această politică în REG12 anual și în termen de 30 de zile de la o modificare semnificativă a cerințelor privind monitorizarea, auditul, revizuirea de management, acțiunea corectivă sau certificarea PIMS.

11.1.2 [All] Internal Audit / Compliance Reviewer TREBUIE să revizuiască anual eficacitatea programului de audit PIMS în REG12 după auditul final programat pentru anul operațional PIMS.

11.1.3 [All] Data Protection Officer / Privacy Advisor TREBUIE să revizuiască în REG12 modificările semnificative din perspectiva confidențialității ale acestei politici înainte de aprobare.

11.1.4 [All] Top Management TREBUIE să aprobe modificările semnificative ale acestei politici în REG12 înainte de publicare.

11.1.5 [All] Privacy Lead / PIMS Manager TREBUIE să actualizeze REG01 și REG03 în termen de 15 zile lucrătoare după modificările aprobate ale acestei politici care schimbă domeniul de aplicare al PIMS sau aplicabilitatea controalelor.

11.1.6 [All] Privacy Lead / PIMS Manager TREBUIE să înregistreze comunicarea modificărilor aprobate ale acestei politici în REG11 în termen de 30 de zile de la publicare.

12. Politici conexe

12.1 Această politică este susținută de următoarele politici conexe:

12.1.1 PII01 - Politica Sistemului de management al informațiilor privind confidențialitatea

12.1.2 PII02 - Politica privind rolurile, responsabilitățile și responsabilitatea în domeniul confidențialității

12.1.3 PII03 - Politica privind inventarul prelucrării PII și temeiul juridic

12.1.4 PII04 - Politica privind nota de informare și transparența

12.1.5 PII05 - Politica de gestionare a consimțământului și preferințelor

12.1.6 PII06 - Politica de gestionare a drepturilor persoanei vizate

12.1.7 PII07 - Politica privind evaluarea riscurilor privind confidențialitatea și DPIA

12.1.8 PII08 - Politica privind protecția datelor încă din faza de proiectare și în mod implicit

12.1.9 PII09 - Politica privind colectarea, utilizarea, divulgarea și partajarea PII

12.1.10 PII10 - Politica privind retenția, ștergerea și eliminarea PII

12.1.11 PII11 - Politica privind exactitatea și calitatea PII

12.1.12 PII12 - Politica de management al confidențialității pentru persoanele împuternicite, persoanele subîmputernicite și terți

12.1.13 PII13 - Politica privind transferul internațional al PII

12.1.14 PII14 - Politica privind securitatea PII și controlul accesului

12.1.15 PII15 - Politica de management al incidentelor PII și al încălcărilor securității datelor

12.1.16 PII16 - Politica privind instruirea, conștientizarea și competența în domeniul confidențialității

12.1.17 PII17 - Politica de management al informațiilor documentate și dovezilor PIMS

13. Standarde și cadre de referință

13.1 Această politică este mapată la următoarele standarde și reglementări. Maparea explică modul în care politica sprijină cerințele citate și identifică clauzele interne care le implementează sau le susțin.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.2** - Mapată la definirea, măsurarea, raportarea și revizuirea obiectivelor PIMS și a metricilor de performanță PIMS. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Mapată la menținerea informațiilor documentate pentru rezultatele monitorizării, programele de audit, rezultatele auditului, dovezile revizuirii de management, neconformități, acțiuni corective și acțiuni de îmbunătățire. Addressed by clauses [4.1.7; 4.2.4; 4.2.7; 4.3.1; 4.4.1; 7.1.8; 11.1.1].

13.2.3 **Clause 8.1** - Mapată la operarea ciclului planificat de monitorizare PIMS, audit, acțiune corectivă și îmbunătățire ca parte a controlului operațional PIMS. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Mapată la definirea elementelor monitorizate și măsurate, consolidarea rezultatelor monitorizării, evaluarea performanței PIMS și menținerea dovezilor de măsurare. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.1.7; 8.1.1; 8.1.2; 8.1.4; 8.1.7].

13.2.5 **Clause 9.2** - Mapată la menținerea programului de audit intern, planificarea auditului, verificările privind independența auditorului, eșantionarea dovezilor, rezultatele auditului și urmărirea constatărilor de audit. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 8.1.3; 10.1.2].

13.2.6 **Clause 9.3** - Mapată la planificarea revizuirii de management, revizuirea performanței PIMS, revizuirea tendințelor de audit și acțiuni corective, aprobarea rezultatelor și deciziile privind resursele. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 6.1.7].

13.2.7 **Clause 10.1** - Mapată la identificarea, aprobarea, implementarea și urmărirea oportunităților de îmbunătățire continuă pentru adecvarea, caracterul corespunzător și eficacitatea PIMS. Addressed by clauses [4.3.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 7.1.6].

13.2.8 **Clause 10.2** - Mapată la înregistrarea neconformităților, analiza cauzei principale, planificarea acțiunilor corective, implementarea acțiunilor corective, verificarea eficacității, escaladare și aplicare. Addressed by clauses [4.2.8; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 10.1.1; 10.1.3; 10.1.6].

13.2.9 **Annex A.1.2.9** - Mapată la evidențele de prelucrare ale operatorului utilizate ca surse de dovezi pentru monitorizare, eșantionare de audit și metrici privind actualitatea inventarului prelucrărilor. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Mapată la acordurile cu persoanele împuternicite, auditul clientului, răspunsul de asigurare și dovezile de cooperare ale persoanei împuternicite, urmărite prin procesele de asigurare a furnizorilor și clienților. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapată la dovezile privind responsabilitatea pentru monitorizare, audit, revizuire de management, acțiune corectivă și îmbunătățire continuă. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Mapată la măsurile de guvernanță ale operatorului, revizuirea eficacității, revizuirea de management, acțiunea corectivă și dovezile documentate privind îmbunătățirea. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Mapată la dovezile privind persoanele împuternicite, persoanele subîmputernicite, auditul clientului, asigurarea terților și cooperarea furnizorilor. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Mapată la evidențele de prelucrare utilizate ca dovezi pentru monitorizare, eșantionare de audit, caracterul complet al obiectelor de dovezi și actualitatea inventarului prelucrărilor. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32 -** Mapată la monitorizarea și evaluarea stadiului controalelor de securitate PII, a dovezilor privind controalele tehnice și a dovezilor de eficacitate legate de securitate. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Mapată la consilierea privind confidențialitatea, observațiile de monitorizare, suportul pentru audit și revizuirea tendințelor de conformitate privind confidențialitatea de către Data Protection Officer / Privacy Advisor, după caz. Addressed by clauses [5.1.3; 6.1.6; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Mapată la verificarea conformității privind confidențialitatea, audituri interne sau independente, controale interne, mecanisme de supraveghere și dovezi privind evaluarea riscurilor privind confidențialitatea. Addressed by clauses [4.2.1; 4.2.3; 4.2.7; 4.5.1; 6.1.6; 8.1.7].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.2.2; Clause 18.2.3; Clause 18.2.4** - Mapată la revizuirea independentă a securității informațiilor legate de PII, conformitatea cu politicile și standardele și revizuirea tehnică a conformității pentru protecția PII. Addressed by clauses [4.2.3; 4.2.5; 7.1.4; 8.1.2; 10.1.6].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 9.1** - Mapată la datele de monitorizare și evaluare a securității informației care sprijină măsurarea performanței PIMS și stadiul controalelor de securitate PII. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Mapată la suportul de audit intern ISMS pentru planificarea auditului PIMS, dovezile de audit, rezultatele auditului și finalizarea programului de audit. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Mapată la datele de intrare și rezultatele revizuirii de management pentru supravegherea integrată a performanței PIMS și a securității informației. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Mapată la îmbunătățirea continuă a PIMS și a mediului suport al controalelor de securitate a informației. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Mapată la gestionarea neconformităților, planificarea acțiunilor corective, implementarea acțiunilor corective și verificarea eficacității. Addressed by clauses [4.4.2; 4.4.4; 4.4.6; 4.4.7; 10.1.1].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.35 - Mapată la revizuirea independentă, verificările privind independența auditorului, testarea dovezilor de audit și verificarea independentă a eficacității acțiunilor corective. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Mapată la revizuirea conformității politicilor PIMS și de securitate a informației, a stadiului implementării controalelor și a dovezilor de conformitate cu standardele. Addressed by clauses [4.1.4; 4.2.5; 4.5.3; 8.1.2].

13.8 ISO 19011:2018

13.8.1 **Clause 4; Clause 5; Clause 6; Clause 7** - Mapată la principiile de audit, managementul programului de audit, desfășurarea auditului, raportarea auditului pe bază de dovezi, urmărirea auditului și așteptările privind competența auditorilor pentru auditurile PIMS. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.6; 4.2.7; 4.4.7; 5.1.9; 11.1.2].