					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: PII18					Naziv dokumenta: **Politika praćenja, revizije i poboljšanja PIMS-a**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i propisima

Standard/propis	Točka/kontrola/članak	Primjenjivost	Vrsta pokrivenosti	Napomena
ISO/IEC 27701:2025	Clause 6.2	Both	Supporting	Mjerenje ciljeva privatnosti
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentirane informacije o praćenju, reviziji i poboljšanju
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Praćenje operativnog planiranja i kontrole
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Praćenje, mjerenje, analiza i vrednovanje
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Interna revizija
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Preispitivanje od strane uprave
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Kontinuirano poboljšanje
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Nesukladnost i korektivna radnja
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Evidencije obrade voditelja obrade koje se koriste za reviziju
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Dokazi o ugovoru izvršitelja obrade i suradnji u reviziji
GDPR	Article 5(2)	Controller	Supporting	Dokazi o odgovornosti
GDPR	Article 24	Controller	Supporting	Mjere voditelja obrade i pregled njihove djelotvornosti
GDPR	Article 28	Both	Supporting	Upravljanje revizijom i suradnjom izvršitelja obrade
GDPR	Article 30	Both	Supporting	Evidencije obrade koje se koriste za reviziju

GDPR	Article 32	Both	Supporting	Testiranje i vrednovanje sigurnosnih mjera
GDPR	Article 39	Conditional	Supporting	DPO praćenje i savjeti u vezi s revizijom, kada je primjenjivo
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Usklađenost privatnosti, revizija i neovisni nadzor
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Pregled zaštite PII i provjere usklađenosti
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Praćenje i vrednovanje informacijske sigurnosti
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	Podrška internoj reviziji ISMS-a
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	Podrška preispitivanju ISMS-a od strane uprave
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	Podrška kontinuiranom poboljšanju ISMS-a
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	Podrška nesukladnostima i korektivnim radnjama ISMS-a
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Neovisni pregled informacijske sigurnosti
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Pregled usklađenosti politika i standarda
ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Načela revizije sustava upravljanja, program, provedba i kompetencije

1. Opseg

1.1 Ova politika definira zahtjeve organizacije za praćenje, mjerenje, analizu, vrednovanje, internu reviziju, preispitivanje od strane uprave, postupanje s nesukladnostima, korektivne radnje i kontinuirano poboljšanje PIMS-a.

1.2 Ova se politika primjenjuje na:

1.2.1 sve PIMS procese, kontrole, politike, registre, objekte dokaza, sustave, dobavljače, izvršitelje obrade, podizvršitelje obrade i aranžmane dijeljenja podataka unutar opsega PIMS-a;

1.2.2 kontekste organizacije kao voditelja obrade, zajedničkog voditelja obrade, izvršitelja obrade i podizvršitelja obrade;

1.2.3 objedinjeno praćenje učinkovitosti PIMS-a, ciljeva privatnosti, statusa implementacije kontrola, nalaza revizije, nesukladnosti, korektivnih radnji, radnji iz preispitivanja od strane uprave i radnji poboljšanja;

1.2.4 dokaze zadržane u REG12 i pripadajuće izvorne dokaze zadržane u REG01 do REG11.

1.3 Ova politika ne zamjenjuje zahtjeve operativnog praćenja definirane u drugim PIMS politikama. Njome se uspostavlja objedinjeni ciklus vrednovanja učinkovitosti, revizije, pregleda i poboljšanja za PIMS.

1.4 Za potrebe ove politike, velika PIMS nesukladnost znači propust koji bitno utječe na opseg PIMS-a, ciljeve privatnosti, odgovornost za obradu PII, obradu rizika za privatnost, prava ispitanika, sigurnost obrade, upravljanje izvršiteljem obrade ili podizvršiteljem obrade, spremnost za povredu, cjelovitost dokumentiranih dokaza, opseg certifikacije ili ponovljeni propust istog zahtjeva unutar razdoblja od 12 mjeseci.

1.5 Za potrebe ove politike, značajna promjena znači svaku promjenu koja utječe na opseg PIMS-a, svrhe obrade PII, kategorije PII, kategorije ispitanika, lokacije obrade, raspodjelu uloga voditelja obrade ili izvršitelja obrade, arhitekturu sustava, aranžmane s dobavljačima ili podizvršiteljima obrade, profil rizika za privatnost, primjenjive pravne ili ugovorne obveze, opseg revizije, metodu praćenja ili opseg certifikacije.

2. Svrha

2.1 Svrha ove politike jest osigurati da organizacija vrednuje učinkovitost PIMS-a, provjerava usklađenost PIMS-a, utvrđuje nesukladnosti, ispravlja slabosti kontrola i kontinuirano poboljšava PIMS na temelju objektivnih dokaza.

2.2 Ova politika omogućuje organizaciji da dokaže kako su aktivnosti praćenja, revizije, preispitivanja od strane uprave i poboljšanja PIMS-a planirane, neovisne gdje je to potrebno, utemeljene na dokazima, pravodobne i sljedive do odgovornih uloga i kanonskih objekata dokaza.

3. Ciljevi

3.1 Ciljevi ove politike jesu:

3.1.1 definirati objedinjeni postupak praćenja i mjerenja PIMS-a;

3.1.2 osigurati da se ciljevi privatnosti i učinkovitost PIMS kontrola mjere uporabom dokumentiranih dokaza;

3.1.3 uspostaviti program interne revizije PIMS-a temeljen na riziku;

3.1.4 očuvati neovisnost i objektivnost u aktivnostima revizije PIMS-a;

3.1.5 osigurati da preispitivanje od strane uprave dobije potpune i aktualne ulazne podatke o učinkovitosti PIMS-a;

3.1.6 osigurati da se nesukladnosti evidentiraju, procjenjuju, ispravljaju i provjeravaju;

3.1.7 osigurati da se korektivne radnje prate do zatvaranja i pregledavaju u pogledu djelotvornosti;

3.1.8 utvrditi ponavljajuće slabosti i prilike za poboljšanje;

3.1.9 podržati spremnost za certifikaciju i odgovorno upravljanje dokazima;

3.1.10 izbjeći dupliciranje operativnih metrika koje su već definirane u povezanim PIMS politikama.

4. Izjave politike

4.1 Okvir praćenja i mjerenja PIMS-a

4.1.1 [Both] Privacy Lead / PIMS Manager mora definirati objedinjeni program praćenja PIMS-a u REG12 prije početnog rada PIMS-a i nakon toga jednom godišnje.

4.1.2 [Both] Privacy Lead / PIMS Manager mora definirati metodu mjerenja, učestalost, izvor dokaza, cilj i odgovornu ulogu za svaku PIMS metriku u REG12 prije početka mjernog ciklusa.

4.1.3 [Both] Process Owner / Business Owner mora tromjesečno dostavljati Privacy Lead / PIMS Manager ulazne podatke o praćenju aktivnosti obrade PII iz REG02.

4.1.4 [Both] Information Security Lead mora tromjesečno dostavljati Privacy Lead / PIMS Manager ulazne podatke o statusu sigurnosnih kontrola PII iz REG03.

4.1.5 [Both] Vendor / Procurement Owner mora tromjesečno dostavljati Privacy Lead / PIMS Manager ulazne podatke o statusu izvršitelja obrade, podizvršitelja obrade, dijeljenja s trećim stranama i osiguranja dobavljača iz REG08.

4.1.6 [All] Incident Response Coordinator mora mjesečno te unutar 10 radnih dana nakon zatvaranja većeg incidenta dostavljati Privacy Lead / PIMS Manager ulazne podatke o trendovima incidenata u vezi s privatnošću i povreda iz REG10.

4.1.7 [Both] Privacy Lead / PIMS Manager mora tromjesečno objediniti rezultate praćenja PIMS-a u REG12.

4.2 Program internog audita PIMS-a

4.2.1 [All] Internal Audit / Compliance Reviewer mora jednom godišnje, prije prvog planiranog ciklusa revizije PIMS-a, pripremiti program internog audita PIMS-a temeljen na riziku u REG12.

4.2.2 [All] Internal Audit / Compliance Reviewer mora u REG12 definirati cilj, kriterije, opseg, metodu, osnovu uzorkovanja i rok izvješćivanja za svaku reviziju PIMS-a prije početka terenskog dijela revizije.

4.2.3 [All] Internal Audit / Compliance Reviewer mora u REG12 evidentirati provjere neovisnosti revizora i sukoba interesa prije svake dodjele revizijskog zadatka.

4.2.4 [All] Privacy Lead / PIMS Manager mora zatražene kontrolirane PIMS dokumentirane informacije i dokaze iz registara učiniti dostupnima putem REG12 unutar 10 radnih dana od odobrenog zahtjeva za reviziju.

4.2.5 [Both] Internal Audit / Compliance Reviewer mora tijekom svake revizije PIMS-a testirati status implementacije primjenjivih PIMS kontrola u odnosu na REG03.

4.2.6 [Both] Internal Audit / Compliance Reviewer mora tijekom svake revizije PIMS-a evidentirati odabrani uzorak dokaza o obradi PII u REG12.

4.2.7 [All] Internal Audit / Compliance Reviewer mora evidentirati rezultate revizije PIMS-a u REG12 unutar 15 radnih dana nakon završetka revizije.

4.2.8 [All] Privacy Lead / PIMS Manager mora dodijeliti vlasnike korektivnih radnji za prihvaćene nalaze revizije PIMS-a u REG12 unutar 10 radnih dana od prihvaćanja rezultata revizije.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Iznimke

9.1 Iznimke od praćenja, revizije i poboljšanja

9.1.1 [All] Process Owner / Business Owner mora zatražiti svaku iznimku od ove politike u REG12 prije nastanka odstupanja.

9.1.2 [All] Privacy Lead / PIMS Manager mora procijeniti utjecaj svake zatražene iznimke na privatnost, certifikaciju, reviziju i korektivnu radnju u REG12 unutar 10 radnih dana od zahtjeva.

9.1.3 [All] Data Protection Officer / Privacy Advisor mora evidentirati savjet u REG12 prije odobrenja svake iznimke koja utječe na pravne obveze, prava ispitanika, obveze iz DPIA-e, obveze revizije klijenata ili visokorizičnu obradu.

9.1.4 [All] Top Management mora odobriti iznimke koje utječu na dovršetak revizijskog rasporeda, preispitivanje od strane uprave, velike nesukladnosti, opseg certifikacije ili visokorizičnu obradu u REG12 prije stupanja iznimke na snagu.

9.1.5 [All] Privacy Lead / PIMS Manager mora u REG12 odrediti datum isteka koji ne premašuje 90 dana za svaku odobrenu iznimku od praćenja, revizije ili poboljšanja.

9.1.6 [All] Privacy Lead / PIMS Manager mora zatvoriti ili ponovno procijeniti svaku iznimku od praćenja, revizije ili poboljšanja u REG12 unutar pet radnih dana od isteka.

10. Provedba

10.1 Provedba zahtjeva za praćenje, reviziju i poboljšanje

10.1.1 [All] Privacy Lead / PIMS Manager mora evidentirati propušteni ciklus praćenja, propuštenu reviziju PIMS-a, preispitivanje od strane uprave s prekoračenim rokom, nedostajuće revizijske dokaze, korektivnu radnju s prekoračenim rokom ili radnju poboljšanja s prekoračenim rokom kao nesukladnost u REG12 unutar pet radnih dana od utvrđivanja.

10.1.2 [All] Internal Audit / Compliance Reviewer mora evidentirati ozbiljnost nalaza revizije u REG12 prije izdavanja izvješća o reviziji.

10.1.3 [All] Top Management mora zahtijevati korektivnu radnju za svaku veliku PIMS nesukladnost u REG12 unutar 10 radnih dana od eskalacije.

10.1.4 [All] Process Owner / Business Owner mora spriječiti puštanje u produkcijski rad ili podnošenje za vanjsko osiguranje za visokorizičnu obradu kada potrebni dokazi o korektivnoj radnji nedostaju iz REG12 prije puštanja u produkcijski rad ili podnošenja.

10.1.5 [All] Privacy Lead / PIMS Manager mora eskalirati ponovljeno propuštanje rokova praćenja ili korektivnih radnji Top Management u REG12 unutar pet radnih dana nakon drugog pojavljivanja u razdoblju od 12 mjeseci.

10.1.6 [All] Internal Audit / Compliance Reviewer mora provjeriti zatvaranje provedbene radnje u REG12 pri sljedećoj zakazanoj reviziji ili unutar 60 dana od prijavljenog zatvaranja, ovisno o tome što nastupi prije.

11. Pregled i održavanje

11.1 Pregled i održavanje politike

11.1.1 [All] Privacy Lead / PIMS Manager mora pregledati ovu politiku u REG12 jednom godišnje i unutar 30 dana od značajne promjene zahtjeva za praćenje PIMS-a, reviziju, preispitivanje od strane uprave, korektivnu radnju ili certifikaciju.

11.1.2 [All] Internal Audit / Compliance Reviewer mora jednom godišnje nakon završne zakazane revizije za PIMS operativnu godinu pregledati djelotvornost programa audita PIMS-a u REG12.

11.1.3 [All] Data Protection Officer / Privacy Advisor mora pregledati promjene ove politike značajne za privatnost u REG12 prije odobrenja.

11.1.4 [All] Top Management mora odobriti značajne promjene ove politike u REG12 prije objave.

11.1.5 [All] Privacy Lead / PIMS Manager mora ažurirati REG01 i REG03 unutar 15 radnih dana nakon odobrenih promjena ove politike koje mijenjaju opseg PIMS-a ili primjenjivost kontrola.

11.1.6 [All] Privacy Lead / PIMS Manager mora evidentirati komunikaciju odobrenih promjena ove politike u REG11 unutar 30 dana od objave.

12. Povezane politike

12.1 Ovu politiku podržavaju sljedeće povezane politike:

12.2 PII01 - Politika sustava upravljanja informacijama o privatnosti

12.3 PII02 - Politika uloga, odgovornosti i odgovornosti za privatnost

12.4 PII03 - Politika popisa obrade PII i pravne osnove

12.5 PII04 - Politika obavijesti o privatnosti i transparentnosti

12.6 PII05 - Politika upravljanja privolama i preferencijama

12.7 PII06 - Politika upravljanja pravima ispitanika

12.8 PII07 - Politika procjene rizika za privatnost i DPIA-e

12.9 PII08 - Politika ugrađene zaštite privatnosti i zaštite privatnosti prema zadanim postavkama

12.10 PII09 - Politika prikupljanja, uporabe, otkrivanja i dijeljenja PII

12.11 PII10 - Politika zadržavanja, brisanja i zbrinjavanja PII

12.12 PII11 - Politika točnosti i kvalitete PII

12.13 PII12 - Politika upravljanja privatnošću izvršitelja obrade, podizvršitelja obrade i trećih strana

12.14 PII13 - Politika međunarodnog prijenosa PII

12.15 PII14 - Politika sigurnosti PII i kontrole pristupa

12.16 PII15 - Politika upravljanja incidentima i povredama PII

12.17 PII16 - Politika obuke, podizanja svijesti i kompetencija u području privatnosti

12.18 PII17 - Politika dokumentiranih informacija i upravljanja dokazima PIMS-a

13. Referentni standardi i okviri

13.1 Ova je politika mapirana na sljedeće standarde i propise. Mapiranje objašnjava kako politika podržava navedene zahtjeve i utvrđuje interne točke koje ih provode ili podržavaju.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.2** - Mapirano na definiranje, mjerenje, izvješćivanje i pregled ciljeva PIMS-a i metrika učinkovitosti PIMS-a. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Mapirano na održavanje dokumentiranih informacija za rezultate praćenja, programe audita, rezultate revizije, dokaze za preispitivanje od strane uprave, nesukladnosti, korektivne radnje i radnje poboljšanja. 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** - Mapirano na provedbu planiranog ciklusa praćenja PIMS-a, revizije, korektivnih radnji i poboljšanja kao dijela operativne kontrole PIMS-a. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Mapirano na definiranje onoga što se prati i mjeri, objedinjavanje rezultata praćenja, vrednovanje učinkovitosti PIMS-a i održavanje dokaza o mjerenju. 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** - Mapirano na održavanje programa internog audita, planiranje revizije, provjere neovisnosti revizora, uzorkovanje dokaza, rezultate revizije i praćenje nalaza revizije. 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** - Mapirano na planiranje preispitivanja od strane uprave, pregled učinkovitosti PIMS-a, pregled trendova revizije i korektivnih radnji, odobrenje izlaznih rezultata i odluke o resursima. 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** - Mapirano na utvrđivanje, odobravanje, provedbu i praćenje prilika za kontinuirano poboljšanje prikladnosti, primjerenosti i djelotvornosti PIMS-a. 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** - Mapirano na evidentiranje nesukladnosti, analizu temeljnog uzroka, planiranje korektivnih radnji, provedbu korektivnih radnji, provjeru djelotvornosti, eskalaciju i provedbu. 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** - Mapirano na evidencije obrade voditelja obrade koje se koriste kao izvori dokaza za praćenje, revizijsko uzorkovanje i metrike ažurnosti popisa obrade. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Mapirano na dokaze o ugovoru izvršitelja obrade, reviziji klijenta, odgovoru na zahtjev za osiguranje i suradnji izvršitelja obrade, koji se prate kroz postupke osiguranja dobavljača i klijenata. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapirano na dokaze o odgovornosti za praćenje, reviziju, preispitivanje od strane uprave, korektivne radnje i kontinuirano poboljšanje. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Mapirano na upravljačke mjere voditelja obrade, pregled djelotvornosti, preispitivanje od strane uprave, korektivne radnje i dokumentirane dokaze o poboljšanju. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Mapirano na dokaze o izvršitelju obrade, podizvršitelju obrade, reviziji klijenta, osiguranju trećih strana i suradnji dobavljača. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Mapirano na evidencije obrade koje se koriste kao dokazi za praćenje, revizijsko uzorkovanje, potpunost objekata dokaza i ažurnost popisa obrade. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Mapirano na praćenje i vrednovanje statusa sigurnosnih kontrola PII, dokaze o tehničkim kontrolama i dokaze o djelotvornosti povezane sa sigurnošću. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Mapirano na savjete o privatnosti, opažanja praćenja, podršku reviziji i pregled trendova usklađenosti privatnosti koje provodi Data Protection Officer / Privacy Advisor, kada je primjenjivo. 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** - Mapirano na provjeru usklađenosti privatnosti, interne ili neovisne revizije, interne kontrole, nadzorne mehanizme i dokaze o procjeni rizika za privatnost. 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** - Mapirano na neovisni pregled informacijske sigurnosti povezane s PII, usklađenost s politikama i standardima te tehnički pregled usklađenosti za zaštitu 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** - Mapirano na ulazne podatke o praćenju i vrednovanju informacijske sigurnosti koji podržavaju mjerenje učinkovitosti PIMS-a i status sigurnosnih kontrola PII. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Mapirano na podršku interne revizije ISMS-a za planiranje revizije PIMS-a, revizijske dokaze, rezultate revizije i dovršetak programa audita. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Mapirano na ulazne i izlazne podatke preispitivanja od strane uprave za integrirani nadzor učinkovitosti PIMS-a i informacijske sigurnosti. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Mapirano na kontinuirano poboljšanje PIMS-a i podržavajućeg okruženja kontrola informacijske sigurnosti. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Mapirano na postupanje s nesukladnostima, planiranje korektivnih radnji, provedbu korektivnih radnji i provjeru djelotvornosti. 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 - Mapirano na neovisni pregled, provjere neovisnosti revizora, testiranje revizijskih dokaza i neovisnu provjeru djelotvornosti korektivnih radnji. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Mapirano na pregled usklađenosti PIMS-a i politika informacijske sigurnosti, status implementacije kontrola i dokaze o usklađenosti sa standardima. 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** - Mapirano na načela revizije, upravljanje programom audita, provedbu revizije, izvješćivanje o reviziji temeljeno na dokazima, praćenje nakon revizije i očekivanja u pogledu kompetencija revizora za revizije PIMS-a. 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].