					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: PII18					Názov dokumentu: **Politika monitorovania, auditu a zlepšovania PIMS**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

Súlad s normami a predpismi

Norma / predpis	Kapitola / kontrola / článok	Uplatniteľnosť	Typ pokrytia	Poznámka
ISO/IEC 27701:2025	Clause 6.2	Both	Supporting	Meranie cieľov ochrany súkromia
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Zdokumentované informácie o monitorovaní, audite a zlepšovaní
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Monitorovanie prevádzkového plánovania a riadenia
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Monitorovanie, meranie, analýza a hodnotenie
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Vnútorný audit
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Preskúmanie manažmentom
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Neustále zlepšovanie
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Nezhoda a nápravné opatrenie
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Záznamy prevádzkovateľa o spracúvaní používané na audit
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Dôkazy o dohode sprostredkovateľa a súčinnosti pri audite
GDPR	Article 5(2)	Controller	Supporting	Dôkazy preukázateľnej zodpovednosti
GDPR	Article 24	Controller	Supporting	Opatrenia prevádzkovateľa a preskúmanie ich účinnosti
GDPR	Article 28	Both	Supporting	Správa auditu sprostredkovateľa a súčinnosti
GDPR	Article 30	Both	Supporting	Záznamy o spracúvaní používané na audit

GDPR	Article 32	Both	Supporting	Testovanie a hodnotenie bezpečnostných opatrení
GDPR	Article 39	Conditional	Supporting	Monitorovanie a poradenstvo DPO k auditu, ak sa uplatňuje
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Súlad v oblasti ochrany súkromia, audit a nezávislý dohľad
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Preskúmanie ochrany PII a kontroly súladu
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Monitorovanie a hodnotenie informačnej bezpečnosti
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	Podpora vnútorného auditu ISMS
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	Podpora preskúmania ISMS manažmentom
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	Podpora neustáleho zlepšovania ISMS
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	Podpora riešenia nezhôd a nápravných opatrení v ISMS
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Nezávislé preskúmanie informačnej bezpečnosti
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Preskúmanie súladu politík a noriem
ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Zásady auditov systémov manažérstva, program, vykonávanie a kompetentnosť

1. Rozsah

1.1 Táto politika vymedzuje požiadavky organizácie na monitorovanie, meranie, analýzu, hodnotenie, vnútorný audit, preskúmanie manažmentom, riešenie nezhôd, nápravné opatrenia a neustále zlepšovanie PIMS.

1.2 Táto politika sa vzťahuje na:

1.2.1 všetky procesy, kontroly, politiky, registre, dôkazové objekty, systémy, dodávateľov, sprostredkovateľov, ďalších sprostredkovateľov a dojednania o zdieľaní údajov v rozsahu PIMS;

1.2.2 kontexty organizácie ako prevádzkovateľa, spoločného prevádzkovateľa, sprostredkovateľa a ďalšieho sprostredkovateľa;

1.2.3 konsolidované monitorovanie výkonnosti PIMS, cieľov ochrany súkromia, stavu implementácie kontrol, auditných zistení, nezhôd, nápravných opatrení, opatrení z preskúmania manažmentom a zlepšovacích opatrení;

1.2.4 dôkazy uchovávané v REG12 a podporné zdrojové dôkazy uchovávané v REG01 až REG11.

1.3 Táto politika nenahrádza požiadavky na prevádzkové monitorovanie vymedzené v iných politikách PIMS. Ustanovuje konsolidovaný cyklus hodnotenia výkonnosti, auditu, preskúmania a zlepšovania PIMS.

1.4 Na účely tejto politiky závažná nezhoda PIMS znamená zlyhanie, ktoré podstatne ovplyvňuje rozsah PIMS, ciele ochrany súkromia, preukázateľnú zodpovednosť pri spracúvaní PII, ošetrenie rizík ochrany súkromia, práva dotknutých osôb, bezpečnosť spracúvania, správu sprostredkovateľov alebo ďalších sprostredkovateľov, pripravenosť na porušenie ochrany osobných údajov, integritu zdokumentovaných dôkazov, rozsah certifikácie alebo opakované zlyhanie tej istej požiadavky v období 12 mesiacov.

1.5 Na účely tejto politiky podstatná zmena znamená akúkoľvek zmenu ovplyvňujúcu rozsah PIMS, účely spracúvania PII, kategórie PII, kategórie dotknutých osôb, miesta spracúvania, rozdelenie rolí prevádzkovateľa alebo sprostredkovateľa, architektúru systému, dojednania s dodávateľmi alebo ďalšími sprostredkovateľmi, profil rizík ochrany súkromia, uplatniteľné právne alebo zmluvné povinnosti, rozsah auditu, metódu monitorovania alebo rozsah certifikácie.

2. Účel

2.1 Účelom tejto politiky je zabezpečiť, aby organizácia hodnotila výkonnosť PIMS, overovala zhodu PIMS, identifikovala nezhody, odstraňovala slabiny kontrol a neustále zlepšovala PIMS na základe objektívnych dôkazov.

2.2 Táto politika umožňuje organizácii preukázať, že činnosti monitorovania PIMS, auditu, preskúmania manažmentom a zlepšovania sú plánované, nezávislé tam, kde sa to vyžaduje, založené na dôkazoch, včasné a sledovateľné k zodpovedným rolám a kanonickým dôkazovým objektom.

3. Ciele

3.1 Cieľmi tejto politiky je:

3.1.1 vymedziť konsolidovaný proces monitorovania a merania PIMS;

3.1.2 zabezpečiť, aby sa ciele ochrany súkromia a výkonnosť kontrol PIMS merali pomocou zdokumentovaných dôkazov;

3.1.3 ustanoviť rizikovo orientovaný program vnútorného auditu PIMS;

3.1.4 zachovať nezávislosť a objektívnosť pri auditných činnostiach PIMS;

3.1.5 zabezpečiť, aby preskúmanie manažmentom dostávalo úplné a aktuálne vstupy o výkonnosti PIMS;

3.1.6 zabezpečiť, aby sa nezhody zaznamenávali, posudzovali, opravovali a overovali;

3.1.7 zabezpečiť, aby sa nápravné opatrenia sledovali až do uzavretia a preskúmavala sa ich účinnosť;

3.1.8 identifikovať opakujúce sa slabiny a príležitosti na zlepšenie;

3.1.9 podporovať pripravenosť na certifikáciu a zodpovednú správu dôkazov;

3.1.10 zabrániť duplicite prevádzkových metrík, ktoré sú už vymedzené v súvisiacich politikách PIMS.

4. Vyhlásenia politiky

4.1 Rámec monitorovania a merania PIMS

4.1.1 [Both] Privacy Lead / PIMS Manager musí v REG12 vymedziť konsolidovaný program monitorovania PIMS pred prvou prevádzkou PIMS a následne každoročne.

4.1.2 [Both] Privacy Lead / PIMS Manager musí v REG12 vymedziť metódu merania, frekvenciu, zdroj dôkazov, cieľovú hodnotu a zodpovednú rolu pre každú metriku PIMS pred začiatkom meracieho cyklu.

4.1.3 [Both] Process Owner / Business Owner musí štvrťročne poskytovať Privacy Lead / PIMS Manager vstupy z monitorovania činností spracúvania PII z REG02.

4.1.4 [Both] Information Security Lead musí štvrťročne poskytovať Privacy Lead / PIMS Manager vstupy o stave bezpečnostných kontrol PII z REG03.

4.1.5 [Both] Vendor / Procurement Owner musí štvrťročne poskytovať Privacy Lead / PIMS Manager vstupy o stave sprostredkovateľov, ďalších sprostredkovateľov, zdieľania s tretími stranami a uistenia dodávateľov z REG08.

4.1.6 [All] Incident Response Coordinator musí mesačne a do 10 pracovných dní po uzavretí závažného incidentu poskytovať Privacy Lead / PIMS Manager vstupy o trendoch incidentov ochrany súkromia a porušení ochrany osobných údajov z REG10.

4.1.7 [Both] Privacy Lead / PIMS Manager musí štvrťročne konsolidovať výsledky monitorovania PIMS v REG12.

4.2 Program vnútorného auditu PIMS

4.2.1 [All] Internal Audit / Compliance Reviewer musí každoročne pred prvým plánovaným auditným cyklom PIMS pripraviť v REG12 rizikovo orientovaný program vnútorného auditu PIMS.

4.2.2 [All] Internal Audit / Compliance Reviewer musí pred začiatkom auditorských prác vymedziť v REG12 cieľ, kritériá, rozsah, metódu, základ vzorkovania a termín vykázania pre každý audit PIMS.

4.2.3 [All] Internal Audit / Compliance Reviewer musí pred každým auditným pridelením zaznamenať v REG12 kontroly nezávislosti audítora a konfliktu záujmov.

4.2.4 [All] Privacy Lead / PIMS Manager musí do 10 pracovných dní od schválenej žiadosti o audit sprístupniť požadované riadené zdokumentované informácie PIMS a dôkazy z registrov prostredníctvom REG12.

4.2.5 [Both] Internal Audit / Compliance Reviewer musí počas každého auditu PIMS otestovať stav implementácie uplatniteľných kontrol PIMS voči REG03.

4.2.6 [Both] Internal Audit / Compliance Reviewer musí počas každého auditu PIMS zaznamenať v REG12 vybranú vzorku dôkazov o spracúvaní PII.

4.2.7 [All] Internal Audit / Compliance Reviewer musí zaznamenať výsledky auditu PIMS v REG12 do 15 pracovných dní po dokončení auditu.

4.2.8 [All] Privacy Lead / PIMS Manager musí do 10 pracovných dní od akceptácie výsledkov auditu priradiť v REG12 vlastníkov nápravných opatrení pre akceptované auditné zistenia PIMS.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Výnimky

9.1 Výnimky z monitorovania, auditu a zlepšovania

9.1.1 [All] Process Owner / Business Owner musí požiadať o akúkoľvek výnimku z tejto politiky v REG12 pred tým, ako nastane odchýlka.

9.1.2 [All] Privacy Lead / PIMS Manager musí posúdiť dopad každej požadovanej výnimky na ochranu súkromia, certifikáciu, audit a nápravné opatrenia v REG12 do 10 pracovných dní od žiadosti.

9.1.3 [All] Data Protection Officer / Privacy Advisor musí zaznamenať poradenstvo v REG12 pred schválením akejkoľvek výnimky ovplyvňujúcej právne povinnosti, práva dotknutých osôb, záväzky DPIA, povinnosti auditu zákazníka alebo vysokorizikové spracúvanie.

9.1.4 [All] Top Management musí schváliť výnimky ovplyvňujúce dokončenie harmonogramu auditov, preskúmanie manažmentom, závažné nezhody, rozsah certifikácie alebo vysokorizikové spracúvanie v REG12 pred nadobudnutím účinnosti výnimky.

9.1.5 [All] Privacy Lead / PIMS Manager musí v REG12 stanoviť dátum uplynutia platnosti nepresahujúci 90 dní pre každú schválenú výnimku z monitorovania, auditu alebo zlepšovania.

9.1.6 [All] Privacy Lead / PIMS Manager musí uzavrieť alebo prehodnotiť každú výnimku z monitorovania, auditu alebo zlepšovania v REG12 do piatich pracovných dní od uplynutia platnosti.

10. Uplatňovanie

10.1 Uplatňovanie požiadaviek na monitorovanie, audit a zlepšovanie

10.1.1 [All] Privacy Lead / PIMS Manager musí zaznamenať vynechaný monitorovací cyklus, vynechaný audit PIMS, omeškané preskúmanie manažmentom, chýbajúce auditné dôkazy, omeškané nápravné opatrenie alebo omeškané zlepšovacie opatrenie ako nezhodu v REG12 do piatich pracovných dní od identifikácie.

10.1.2 [All] Internal Audit / Compliance Reviewer musí zaznamenať závažnosť auditného zistenia v REG12 pred vydaním auditnej správy.

10.1.3 [All] Top Management musí vyžadovať nápravné opatrenie pre každú závažnú nezhodu PIMS v REG12 do 10 pracovných dní od eskalácie.

10.1.4 [All] Process Owner / Business Owner musí zabrániť spusteniu do produkčného prostredia alebo predloženiu externého uistenia pri vysokorizikovom spracúvaní, ak v REG12 chýbajú požadované dôkazy o nápravnom opatrení pred spustením alebo predložením.

10.1.5 [All] Privacy Lead / PIMS Manager musí eskalovať opakované zmeškanie termínov monitorovania alebo nápravných opatrení na Top Management v REG12 do piatich pracovných dní po druhom výskyte v období 12 mesiacov.

10.1.6 [All] Internal Audit / Compliance Reviewer musí overiť uzavretie opatrení na uplatnenie požiadaviek v REG12 pri najbližšom plánovanom audite alebo do 60 dní od nahláseného uzavretia, podľa toho, čo nastane skôr.

11. Preskúmanie a údržba

11.1 Preskúmanie a údržba politiky

11.1.1 [All] Privacy Lead / PIMS Manager musí preskúmať túto politiku v REG12 každoročne a do 30 dní od podstatnej zmeny požiadaviek na monitorovanie PIMS, audit, preskúmanie manažmentom, nápravné opatrenia alebo certifikáciu.

11.1.2 [All] Internal Audit / Compliance Reviewer musí každoročne po poslednom plánovanom audite za prevádzkový rok PIMS preskúmať účinnosť programu auditu PIMS v REG12.

11.1.3 [All] Data Protection Officer / Privacy Advisor musí pred schválením preskúmať v REG12 zmeny tejto politiky, ktoré sú významné z hľadiska ochrany súkromia.

11.1.4 [All] Top Management musí schváliť podstatné zmeny tejto politiky v REG12 pred zverejnením.

11.1.5 [All] Privacy Lead / PIMS Manager musí aktualizovať REG01 a REG03 do 15 pracovných dní po schválených zmenách tejto politiky, ktoré menia rozsah PIMS alebo uplatniteľnosť kontrol.

11.1.6 [All] Privacy Lead / PIMS Manager musí zaznamenať komunikáciu schválených zmien tejto politiky v REG11 do 30 dní od zverejnenia.

12. Súvisiace politiky

12.1 Túto politiku podporujú tieto súvisiace politiky:

12.2 PII01 - Politika systému manažérstva informácií o súkromí

12.3 PII02 - Politika rolí, zodpovedností a preukázateľnej zodpovednosti v oblasti ochrany súkromia

12.4 PII03 - Politika evidencie spracúvania PII a právneho základu

12.5 PII04 - Politika oznámenia o ochrane údajov a transparentnosti

12.6 PII05 - Politika správy súhlasov a preferencií

12.7 PII06 - Politika riadenia práv dotknutých osôb

12.8 PII07 - Politika posudzovania rizík ochrany súkromia a DPIA

12.9 PII08 - Politika ochrany súkromia už od návrhu a štandardne

12.10 PII09 - Politika zhromažďovania, používania, poskytovania a zdieľania PII

12.11 PII10 - Politika uchovávania, výmazu a likvidácie PII

12.12 PII11 - Politika presnosti a kvality PII

12.13 PII12 - Politika riadenia ochrany súkromia sprostredkovateľov, ďalších sprostredkovateľov a tretích strán

12.14 PII13 - Politika medzinárodného prenosu PII

12.15 PII14 - Politika bezpečnosti PII a riadenia prístupu

12.16 PII15 - Politika riadenia incidentov a porušení ochrany PII

12.17 PII16 - Politika školení, povedomia a kompetentnosti v oblasti ochrany súkromia

12.18 PII17 - Politika zdokumentovaných informácií a správy dôkazov PIMS

13. Referenčné normy a rámce

13.1 Táto politika je namapovaná na tieto normy a predpisy. Mapovanie vysvetľuje, ako politika podporuje citované požiadavky, a identifikuje interné body, ktoré ich implementujú alebo podporujú.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.2** - Mapované na vymedzenie, meranie, vykazovanie a preskúmanie cieľov PIMS a metrík výkonnosti PIMS. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Mapované na udržiavanie zdokumentovaných informácií o výsledkoch monitorovania, programoch auditov, výsledkoch auditov, dôkazoch pre preskúmanie

manažmentom, nezhodách, nápravných opatreniach a zlepšovacích opatreniach. 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** - Mapované na prevádzkovanie plánovaného cyklu monitorovania PIMS, auditu, nápravných opatrení a zlepšovania ako súčasti prevádzkového riadenia PIMS. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Mapované na vymedzenie toho, čo sa monitoruje a meria, konsolidáciu výsledkov monitorovania, hodnotenie výkonnosti PIMS a udržiavanie dôkazov o meraní. 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** - Mapované na udržiavanie programu vnútorného auditu, plánovanie auditu, kontroly nezávislosti audítora, vzorkovanie dôkazov, výsledky auditu a následné riešenie auditných zistení. 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** - Mapované na plánovanie preskúmania manažmentom, preskúmanie výkonnosti PIMS, preskúmanie trendov auditov a nápravných opatrení, schvaľovanie výstupov a rozhodnutia o zdrojoch. 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** - Mapované na identifikáciu, schvaľovanie, implementáciu a sledovanie príležitostí na neustále zlepšovanie vhodnosti, primeranosti a účinnosti 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** - Mapované na zaznamenávanie nezhôd, analýzu koreňovej príčiny, plánovanie nápravných opatrení, implementáciu nápravných opatrení, overenie účinnosti, eskaláciu a uplatňovanie požiadaviek. 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** - Mapované na záznamy prevádzkovateľa o spracúvaní používané ako zdroje dôkazov pre monitorovanie, auditné vzorkovanie a metriky aktuálnosti evidencie spracúvania. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Mapované na dohodu sprostredkovateľa, audit zákazníka, odpoveď v rámci uistenia a dôkazy o súčinnosti sprostredkovateľa sledované prostredníctvom procesov uistenia dodávateľov a zákazníkov. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapované na dôkazy preukázateľnej zodpovednosti pri monitorovaní, audite, preskúmaní manažmentom, nápravných opatreniach a neustálom zlepšovaní. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Mapované na opatrenia správy prevádzkovateľa, preskúmanie účinnosti, preskúmanie manažmentom, nápravné opatrenia a zdokumentované dôkazy o zlepšovaní. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Mapované na dôkazy o sprostredkovateľoch, ďalších sprostredkovateľoch, audite zákazníka, uistení tretích strán a súčinnosti dodávateľov. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Mapované na záznamy o spracúvaní používané ako dôkazy pre monitorovanie, auditné vzorkovanie, úplnosť dôkazových objektov a aktuálnosť evidencie spracúvania. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Mapované na monitorovanie a hodnotenie stavu bezpečnostných kontrol PII, dôkazy o technických kontrolách a dôkazy o účinnosti súvisiacej s bezpečnosťou. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Mapované na poradenstvo v oblasti ochrany súkromia, pozorovania z monitorovania, podporu auditu a preskúmanie trendov súladu v oblasti ochrany súkromia zo

strany Data Protection Officer / Privacy Advisor, ak sa uplatňuje. 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** - Mapované na overovanie súladu v oblasti ochrany súkromia, interné alebo nezávislé audity, interné kontroly, mechanizmy dohľadu a dôkazy z posúdenia rizík ochrany súkromia. 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** - Mapované na nezávislé preskúmanie informačnej bezpečnosti súvisiacej s PII, súlad s politikami a normami a preskúmanie technického súladu pri ochrane 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** - Mapované na vstupy z monitorovania a hodnotenia informačnej bezpečnosti, ktoré podporujú meranie výkonnosti PIMS a stav bezpečnostných kontrol PII. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Mapované na podporu vnútorného auditu ISMS pri plánovaní auditu PIMS, auditných dôkazoch, výsledkoch auditu a dokončení programu auditu. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Mapované na vstupy a výstupy preskúmania manažmentom pre integrovaný dohľad nad výkonnosťou PIMS a informačnej bezpečnosti. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Mapované na neustále zlepšovanie PIMS a podporného prostredia kontrol informačnej bezpečnosti. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Mapované na riešenie nezhôd, plánovanie nápravných opatrení, implementáciu nápravných opatrení a overenie účinnosti. 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 - Mapované na nezávislé preskúmanie, kontroly nezávislosti audítora, testovanie auditných dôkazov a nezávislé overenie účinnosti nápravného opatrenia. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Mapované na preskúmanie súladu politík PIMS a informačnej bezpečnosti, stavu implementácie kontrol a dôkazov o zhode s normami. 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** - Mapované na zásady auditu, riadenie programu auditov, vykonávanie auditu, auditné vykazovanie založené na dôkazoch, následné opatrenia po audite a očakávania týkajúce sa kompetentnosti audítorov pre audity 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].