					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: PII18					Documenttitel: **PIMS-beleid voor monitoring, audit en verbetering**							
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:							
X	Beleid		Standaard		Procedure		Formulier		Register		Overig	

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/beheersmaatregel/artikel	Toepasselijkheid	Dekkingssoort	Opmerking
ISO/IEC 27701:2025	Clause 6.2	Both	Supporting	Meting van privacydoelstellingen
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Gedocumenteerde informatie over monitoring, audit en verbetering
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Monitoring van operationele planning en beheersing
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Monitoring, meting, analyse en evaluatie
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Interne audit
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Directiebeoordeling
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Voortdurende verbetering
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Non-conformiteit en corrigerende maatregel
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Verwerkingsregistraties van de verwerkingsverantwoordelijke gebruikt voor audit
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Bewijsmateriaal voor verwerkersovereenkomst en auditsamenwerking
GDPR	Article 5(2)	Controller	Supporting	Bewijsmateriaal voor verantwoordingsplicht
GDPR	Article 24	Controller	Supporting	Maatregelen van de verwerkingsverantwoordelijke en beoordeling van de doeltreffendheid
GDPR	Article 28	Both	Supporting	Governance voor audits en samenwerking met verwerkers
GDPR	Article 30	Both	Supporting	Verwerkingsregistraties gebruikt voor audit
GDPR	Article 32	Both	Supporting	Testen en evalueren van beveiligingsmaatregelen

GDPR	Article 39	Conditional	Supporting	Monitoring en auditadvies door de DPO waar van toepassing
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Privacynaleving, audit en onafhankelijk toezicht
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Beoordeling van PII-bescherming en nalevingscontroles
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Monitoring en evaluatie van informatiebeveiliging
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	Ondersteuning voor interne ISMS-audit
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	Ondersteuning voor ISMS-directiebeoordeling
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	Ondersteuning voor voortdurende verbetering van het ISMS
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	Ondersteuning voor ISMS-non-conformiteiten en corrigerende maatregelen
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Onafhankelijke beoordeling van informatiebeveiliging
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Nalevingsbeoordeling van beleid en normen
ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Auditbeginselen, auditprogramma, uitvoering en competentie voor managementsystemen

1. Reikwijdte

1.1 Dit beleid definieert de vereisten van de organisatie voor PIMS-monitoring, meting, analyse, evaluatie, interne audit, directiebeoordeling, afhandeling van non-conformiteiten, corrigerende maatregelen en voortdurende verbetering.

1.2 Dit beleid is van toepassing op:

1.2.1 alle PIMS-processen, beheersmaatregelen, beleidslijnen, registers, bewijsobjecten, systemen, leveranciers, verwerkers, subverwerkers en regelingen voor gegevensdeling binnen het PIMS-toepassingsgebied;

1.2.2 de contexten waarin de organisatie optreedt als verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker en subverwerker;

1.2.3 de geconsolideerde monitoring van PIMS-prestaties, privacydoelstellingen, implementatiestatus van beheersmaatregelen, auditbevindingen, non-conformiteiten, corrigerende maatregelen, acties uit directiebeoordelingen en verbeteracties;

1.2.4 bewijsmateriaal dat in REG12 wordt bewaard en ondersteunend bronbewijsmateriaal dat in REG01 tot en met REG11 wordt bewaard.

1.3 Dit beleid vervangt geen operationele monitoringvereisten die in andere PIMS-beleidslijnen zijn vastgelegd. Het stelt de geconsolideerde cyclus voor prestatie-evaluatie, audit, beoordeling en verbetering voor het PIMS vast.

1.4 Voor dit beleid betekent een majeure PIMS-non-conformiteit een tekortkoming die wezenlijke gevolgen heeft voor het PIMS-toepassingsgebied, privacydoelstellingen, verantwoordingsplicht voor PII-verwerking, behandeling van privacyrisico's, rechten van betrokkenen, beveiliging van de verwerking, governance van verwerkers of subverwerkers, paraatheid voor inbreuken, integriteit van gedocumenteerd bewijsmateriaal, certificeringstoepassingsgebied, of een herhaald falen van dezelfde vereiste binnen een periode van 12 maanden.

1.5 Voor dit beleid betekent een wezenlijke wijziging iedere wijziging die gevolgen heeft voor het PIMS-toepassingsgebied, PII-verwerkingsdoelen, PII-categorieën, categorieën betrokkenen, verwerkingslocaties, rolverdeling tussen verwerkingsverantwoordelijke en verwerker, systeemarchitectuur, leveranciers- of subverwerkersregelingen, privacyrisicoprofiel, toepasselijke wettelijke of contractuele verplichtingen, audittoepassingsgebied, monitoringmethode of certificeringstoepassingsgebied.

2. Doel

2.1 Het doel van dit beleid is te waarborgen dat de organisatie PIMS-prestaties evalueert, PIMS-conformiteit verifieert, non-conformiteiten identificeert, zwaktes in beheersmaatregelen corrigeert en het PIMS voortdurend verbetert op basis van objectief bewijsmateriaal.

2.2 Dit beleid stelt de organisatie in staat aan te tonen dat PIMS-monitoring, audit, directiebeoordeling en verbeteractiviteiten gepland, waar vereist onafhankelijk, op bewijsmateriaal gebaseerd, tijdig en herleidbaar zijn naar verantwoordelijke rollen en canonieke bewijsobjecten.

3. Doelstellingen

3.1 De doelstellingen van dit beleid zijn:

3.1.1 een geconsolideerd proces voor PIMS-monitoring en -meting definiëren;

3.1.2 waarborgen dat privacydoelstellingen en prestaties van PIMS-beheersmaatregelen worden gemeten met behulp van gedocumenteerd bewijsmateriaal;

3.1.3 een risicogebaseerd intern auditprogramma voor het PIMS vaststellen;

3.1.4 onafhankelijkheid en objectiviteit in PIMS-auditactiviteiten behouden;

3.1.5 waarborgen dat de directiebeoordeling volledige en actuele input over PIMS-prestaties ontvangt;

3.1.6 waarborgen dat non-conformiteiten worden geregistreerd, beoordeeld, gecorrigeerd en geverifieerd;

3.1.7 waarborgen dat corrigerende maatregelen tot afsluiting worden gevolgd en op doeltreffendheid worden beoordeeld;

3.1.8 terugkerende zwaktes en verbeterkansen identificeren;

3.1.9 gereedheid voor certificering en verantwoord beheer van bewijsmateriaal ondersteunen;

3.1.10 voorkomen dat operationele metrieken die al in gerelateerde PIMS-beleidslijnen zijn gedefinieerd, worden gedupliceerd.

4. Beleidsverklaringen

4.1 Kader voor PIMS-monitoring en -meting

4.1.1 [Both] The Privacy Lead / PIMS Manager moet het geconsolideerde PIMS-monitoringprogramma vóór de initiële PIMS-operatie en daarna jaarlijks definiëren in REG12.

4.1.2 [Both] The Privacy Lead / PIMS Manager moet de meetmethode, frequentie, bron van bewijsmateriaal, doelstelling en verantwoordelijke rol voor elke PIMS-metriek in REG12 definiëren voordat de meetcyclus begint.

4.1.3 [Both] The Process Owner / Business Owner moet per kwartaal monitoringinput over PII-verwerkingsactiviteiten uit REG02 aan The Privacy Lead / PIMS Manager verstrekken.

4.1.4 [Both] The Information Security Lead moet per kwartaal input over de status van PII-beveiligingsmaatregelen uit REG03 aan The Privacy Lead / PIMS Manager verstrekken.

4.1.5 [Both] The Vendor / Procurement Owner moet per kwartaal input over de status van verwerkers, subverwerkers, gegevensdeling met derden en leveranciersassurance uit REG08 aan The Privacy Lead / PIMS Manager verstrekken.

4.1.6 [All] The Incident Response Coordinator moet maandelijks en binnen 10 werkdagen na afsluiting van een majeur incident input over trends in privacy-incidenten en inbreuken uit REG10 aan The Privacy Lead / PIMS Manager verstrekken.

4.1.7 [Both] The Privacy Lead / PIMS Manager moet PIMS-monitoringresultaten per kwartaal consolideren in REG12.

4.2 Intern PIMS-auditprogramma

4.2.1 [All] The Internal Audit / Compliance Reviewer moet jaarlijks, vóór de eerste geplande PIMS-auditcyclus, een risicogebaseerd intern PIMS-auditprogramma opstellen in REG12.

4.2.2 [All] The Internal Audit / Compliance Reviewer moet de doelstelling, criteria, reikwijdte, methode, steekproefbasis en rapportagedeadline voor elke PIMS-audit in REG12 definiëren voordat het auditveldwerk begint.

4.2.3 [All] The Internal Audit / Compliance Reviewer moet controles op auditoronafhankelijkheid en belangenconflicten in REG12 registreren vóór elke auditopdracht.

4.2.4 [All] The Privacy Lead / PIMS Manager moet gevraagde beheerde PIMS-gedocumenteerde informatie en registerbewijsmateriaal via REG12 beschikbaar stellen binnen 10 werkdagen na een goedgekeurd auditverzoek.

4.2.5 [Both] The Internal Audit / Compliance Reviewer moet tijdens elke PIMS-audit de implementatiestatus van toepasselijke PIMS-beheersmaatregelen toetsen aan REG03.

4.2.6 [Both] The Internal Audit / Compliance Reviewer moet tijdens elke PIMS-audit de geselecteerde steekproef van PII-verwerkingsbewijsmateriaal registreren in REG12.

4.2.7 [All] The Internal Audit / Compliance Reviewer moet PIMS-auditresultaten binnen 15 werkdagen na voltooiing van de audit registreren in REG12.

4.2.8 [All] The Privacy Lead / PIMS Manager moet eigenaren van corrigerende maatregelen voor geaccepteerde PIMS-auditbevindingen binnen 10 werkdagen na acceptatie van de auditresultaten toewijzen in REG12.

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Uitzonderingen

9.1 Uitzonderingen voor monitoring, audit en verbetering

9.1.1 [All] The Process Owner / Business Owner moet elke uitzondering op dit beleid aanvragen in REG12 voordat de afwijking plaatsvindt.

9.1.2 [All] The Privacy Lead / PIMS Manager moet binnen 10 werkdagen na het verzoek de impact van elke aangevraagde uitzondering op privacy, certificering, audit en corrigerende maatregelen beoordelen in REG12.

9.1.3 [All] The Data Protection Officer / Privacy Advisor moet advies registreren in REG12 vóór goedkeuring van enige uitzondering die gevolgen heeft voor wettelijke verplichtingen, rechten van betrokkenen, DPIA-toezeggingen, verplichtingen inzake klantenaudits of verwerking met hoog risico.

9.1.4 [All] Top Management moet uitzonderingen die gevolgen hebben voor voltooiing van de auditplanning, directiebeoordeling, majeure non-conformiteiten, certificeringstoepassingsgebied of verwerking met hoog risico goedkeuren in REG12 voordat de uitzondering van kracht wordt.

9.1.5 [All] The Privacy Lead / PIMS Manager moet voor elke goedgekeurde uitzondering op monitoring, audit of verbetering een vervaldatum van maximaal 90 dagen vaststellen in REG12.

9.1.6 [All] The Privacy Lead / PIMS Manager moet elke uitzondering op monitoring, audit of verbetering binnen vijf werkdagen na afloop sluiten of opnieuw beoordelen in REG12.

10. Handhaving

10.1 Handhaving van vereisten voor monitoring, audit en verbetering

10.1.1 [All] The Privacy Lead / PIMS Manager moet een gemiste monitoringcyclus, gemiste PIMS-audit, achterstallige directiebeoordeling, ontbrekend auditbewijsmateriaal, achterstallige corrigerende maatregel of achterstallige verbeteractie binnen vijf werkdagen na identificatie registreren als non-conformiteit in REG12.

10.1.2 [All] The Internal Audit / Compliance Reviewer moet de ernst van auditbevindingen registreren in REG12 voordat het auditrapport wordt uitgegeven.

10.1.3 [All] Top Management moet binnen 10 werkdagen na escalatie in REG12 een corrigerende maatregel vereisen voor elke majeure PIMS-non-conformiteit.

10.1.4 [All] The Process Owner / Business Owner moet livegang of indiening van externe assurance voor verwerking met hoog risico voorkomen wanneer vereist bewijsmateriaal voor corrigerende maatregelen ontbreekt in REG12 vóór livegang of indiening.

10.1.5 [All] The Privacy Lead / PIMS Manager moet herhaaldelijk gemiste deadlines voor monitoring of corrigerende maatregelen binnen vijf werkdagen na de tweede gebeurtenis in een periode van 12 maanden escaleren naar Top Management in REG12.

10.1.6 [All] The Internal Audit / Compliance Reviewer moet afsluiting van handhavingsmaatregelen verifiëren in REG12 tijdens de eerstvolgende geplande audit of binnen 60 dagen na gemelde afsluiting, afhankelijk van wat zich het eerst voordoet.

11. Beoordeling en onderhoud

11.1 Beleidsbeoordeling en onderhoud

11.1.1 [All] The Privacy Lead / PIMS Manager moet dit beleid jaarlijks en binnen 30 dagen na een wezenlijke wijziging in vereisten voor PIMS-monitoring, audit, directiebeoordeling, corrigerende maatregelen of certificering beoordelen in REG12.

11.1.2 [All] The Internal Audit / Compliance Reviewer moet jaarlijks na de laatste geplande audit voor het PIMS-operationeel jaar de doeltreffendheid van het PIMS-auditprogramma beoordelen in REG12.

11.1.3 [All] The Data Protection Officer / Privacy Advisor moet wijzigingen aan dit beleid die significant zijn voor privacy vóór goedkeuring beoordelen in REG12.

11.1.4 [All] Top Management moet wezenlijke wijzigingen aan dit beleid vóór publicatie goedkeuren in REG12.

11.1.5 [All] The Privacy Lead / PIMS Manager moet REG01 en REG03 binnen 15 werkdagen bijwerken na goedgekeurde wijzigingen aan dit beleid die het PIMS-toepassingsgebied of de toepasselijkheid van beheersmaatregelen wijzigen.

11.1.6 [All] The Privacy Lead / PIMS Manager moet communicatie over goedgekeurde wijzigingen aan dit beleid binnen 30 dagen na publicatie registreren in REG11.

12. Gerelateerde beleidslijnen

12.1 Dit beleid wordt ondersteund door de volgende gerelateerde beleidslijnen:

12.2 PII01 - Beleid voor het privacy-informatiemanagementsysteem

12.3 PII02 - Beleid voor privacyrollen, verantwoordelijkheden en verantwoordingsplicht

12.4 PII03 - Beleid voor PII-verwerkingsinventaris en rechtsgrondslag

12.5 PII04 - Beleid voor privacyverklaring en transparantie

12.6 PII05 - Beleid voor toestemming en voorkeurenbeheer

12.7 PII06 - Beleid voor beheer van rechten van betrokkenen

12.8 PII07 - Beleid voor privacyrisicobeoordeling en DPIA

12.9 PII08 - Beleid voor privacy by design en privacy by default

12.10 PII09 - Beleid voor verzameling, gebruik, verstrekking en delen van PII

12.11 PII10 - Beleid voor bewaring, verwijdering en vernietiging van PII

12.12 PII11 - Beleid voor juistheid en kwaliteit van PII

12.13 PII12 - Beleid voor privacybeheer van verwerkers, subverwerkers en derde partijen

12.14 PII13 - Beleid voor internationale PII-doorgifte

12.15 PII14 - Beleid voor PII-beveiliging en toegangscontrole

12.16 PII15 - Beleid voor beheer van PII-incidenten en inbreuken

12.17 PII16 - Beleid voor privacytraining, bewustwording en competentie

12.18 PII17 - Beleid voor PIMS-gedocumenteerde informatie en beheer van bewijsmateriaal

13. Referentienormen en -raamwerken

13.1 Dit beleid is gekoppeld aan de volgende normen en regelgeving. De koppeling licht toe hoe het beleid de aangehaalde vereisten ondersteunt en identificeert de interne clausules die deze implementeren of ondersteunen.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.2** - Gekoppeld aan het definiëren, meten, rapporteren en beoordelen van PIMS-doelstellingen en PIMS-prestatiemetrieken. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Gekoppeld aan het onderhouden van gedocumenteerde informatie voor monitoringresultaten, auditprogramma's, auditresultaten, bewijsmateriaal voor

directiebeoordelingen, non-conformiteiten, corrigerende maatregelen en verbeteracties. 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** - Gekoppeld aan het uitvoeren van de geplande PIMS-cyclus voor monitoring, audit, corrigerende maatregelen en verbetering als onderdeel van operationele PIMS-beheersing. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Gekoppeld aan het definiëren wat wordt gemonitord en gemeten, het consolideren van monitoringresultaten, het evalueren van PIMS-prestaties en het onderhouden van meetbewijsmateriaal. 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** - Gekoppeld aan het onderhouden van het interne auditprogramma, auditplanning, controles op auditoronafhankelijkheid, steekproeven van bewijsmateriaal, auditresultaten en opvolging van auditbevindingen. 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** - Gekoppeld aan planning van directiebeoordelingen, beoordeling van PIMS-prestaties, beoordeling van audit- en corrigerende-maatregeltrends, goedkeuring van output en resourcebesluiten. 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** - Gekoppeld aan het identificeren, goedkeuren, implementeren en volgen van kansen voor voortdurende verbetering van de geschiktheid, toereikendheid en doeltreffendheid van het 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** - Gekoppeld aan het registreren van non-conformiteiten, oorzaakanalyse, planning van corrigerende maatregelen, implementatie van corrigerende maatregelen, verificatie van doeltreffendheid, escalatie en handhaving. 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** - Gekoppeld aan verwerkingsregistraties van de verwerkingsverantwoordelijke die worden gebruikt als bronnen van bewijsmateriaal voor monitoring, auditsteekproeven en metrieken voor actualiteit van de verwerkingsinventaris. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Gekoppeld aan verwerkersovereenkomst, klantenaudit, assuranceresponsen en bewijsmateriaal voor samenwerking door verwerkers dat via leveranciers- en klantassuranceprocessen wordt gevolgd. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Gekoppeld aan bewijsmateriaal voor verantwoordingsplicht inzake monitoring, audit, directiebeoordeling, corrigerende maatregelen en voortdurende verbetering. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Gekoppeld aan governancemaatregelen van de verwerkingsverantwoordelijke, beoordeling van doeltreffendheid, directiebeoordeling, corrigerende maatregelen en gedocumenteerd verbeterbewijsmateriaal. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Gekoppeld aan bewijsmateriaal voor verwerkers, subverwerkers, klantenaudits, assurance door derden en samenwerking met leveranciers. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Gekoppeld aan verwerkingsregistraties die worden gebruikt als monitoring-, auditsteekproef-, bewijsobjectvolledigheids- en verwerkingsinventarisactualiteitsbewijsmateriaal. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Gekoppeld aan het monitoren en evalueren van de status van PII-beveiligingsmaatregelen, technisch bewijsmateriaal voor beheersmaatregelen en

beveiligingsgerelateerd doeltreffendheidsbewijsmateriaal. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Gekoppeld aan privacyadvies, monitoringobservaties, auditondersteuning en beoordeling van trends in privacynaleving door The Data Protection Officer / Privacy Advisor waar van toepassing. 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** - Gekoppeld aan verificatie van privacynaleving, interne of onafhankelijke audits, interne beheersmaatregelen, toezichtmechanismen en bewijsmateriaal voor privacyrisicobeoordelingen. 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** - Gekoppeld aan onafhankelijke beoordeling van PII-gerelateerde informatiebeveiliging, naleving van beleid en normen, en technische nalevingsbeoordeling voor PII-bescherming. 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** - Gekoppeld aan input voor monitoring en evaluatie van informatiebeveiliging ter ondersteuning van PIMS-prestatiemeting en de status van PII-beveiligingsmaatregelen. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Gekoppeld aan ondersteuning vanuit interne ISMS-audits voor PIMS-auditplanning, auditbewijsmateriaal, auditresultaten en voltooiing van auditprogramma's. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Gekoppeld aan input en output van directiebeoordelingen voor geïntegreerd toezicht op PIMS- en informatiebeveiligingsprestaties. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Gekoppeld aan voortdurende verbetering van het PIMS en de ondersteunende omgeving van informatiebeveiligingsmaatregelen. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Gekoppeld aan afhandeling van non-conformiteiten, planning van corrigerende maatregelen, implementatie van corrigerende maatregelen en verificatie van doeltreffendheid. 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 - Gekoppeld aan onafhankelijke beoordeling, controles op auditoronafhankelijkheid, toetsing van auditbewijsmateriaal en onafhankelijke verificatie van de doeltreffendheid van corrigerende maatregelen. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Gekoppeld aan nalevingsbeoordeling van PIMS- en informatiebeveiligingsbeleid, implementatiestatus van beheersmaatregelen en bewijsmateriaal voor conformiteit aan normen. 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** - Gekoppeld aan auditbeginselen, beheer van auditprogramma's, adituitvoering, op bewijsmateriaal gebaseerde auditrapportage, auditopvolging en competentieverwachtingen voor PIMS-audits. 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].