					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: PII18					Dokumenttitel: **Politik for PIMS-overvågning, revision og forbedring**						
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:						
X	Politik		Standard		Procedure		Formular		Register		Andet

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og regler

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 6.2	Both	Supporting	Måling af databeskyttelsesmål
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumenterede oplysninger om overvågning, revision og forbedring
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Overvågning af operationel planlægning og styring
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Overvågning, måling, analyse og evaluering
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Intern revision
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Ledelsens gennemgang
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Løbende forbedring
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Afvigelse og korrigerende handling
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Den dataansvarliges behandlingsregistre anvendt til revision
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Dokumentation for databehandleraftale og revisionssamarbejde
GDPR	Article 5(2)	Controller	Supporting	Dokumentation for ansvarlighed
GDPR	Article 24	Controller	Supporting	Den dataansvarliges foranstaltninger og gennemgang af effektivitet
GDPR	Article 28	Both	Supporting	Styring af revision og samarbejde med databehandlere
GDPR	Article 30	Both	Supporting	Fortegnelser over behandlingsaktiviteter anvendt til revision
GDPR	Article 32	Both	Supporting	Test og evaluering af sikkerhedsforanstaltninger

GDPR	Article 39	Conditional	Supporting	DPO-overvågning og revisionsrådgivning, hvor relevant
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Efterlevelse, revision og uafhængigt tilsyn vedrørende databeskyttelse
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Gennemgang af PII-beskyttelse og efterlevelseskontroller
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Overvågning og evaluering af informationssikkerhed
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	Understøttelse af intern revision af ISMS
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	Understøttelse af ISMS-ledelsens gennemgang
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	Understøttelse af løbende forbedring af ISMS
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	Understøttelse af afvigelser og korrigerende handlinger i ISMS
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Uafhængig gennemgang af informationssikkerhed
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Efterlevelsesgennemgang af politikker og standarder
ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Principper, program, gennemførelse og kompetence for ledelsessystemrevisioner

1. Omfang

1.1 Denne politik fastlægger organisationens krav til PIMS-overvågning, måling, analyse, evaluering, intern revision, ledelsens gennemgang, håndtering af afvigelser, korrigerende handling og løbende forbedring.

1.2 Denne politik gælder for følgende:

1.2.1 alle PIMS-processer, kontroller, politikker, registre, bevisobjekter, systemer, leverandører, databehandlere, underdatabehandlere og datadelingsordninger inden for PIMS-omfang;

1.2.2 organisationens kontekster som dataansvarlig, fælles dataansvarlig, databehandler og underdatabehandler;

1.2.3 den konsoliderede overvågning af PIMS-præstation, databeskyttelsesmål, status for implementering af kontroller, revisionskonstateringer, afvigelser, korrigerende handlinger, opfølgningshandlinger fra ledelsens gennemgang og forbedringshandlinger;

1.2.4 bevismateriale opbevaret i REG12 og understøttende kildebevismateriale opbevaret i REG01 til og med REG11.

1.3 Denne politik erstatter ikke driftsmæssige overvågningskrav, der er fastlagt i andre PIMS-politikker. Den fastlægger den konsoliderede cyklus for præstationsevaluering, revision, gennemgang og forbedring for PIMS.

1.4 I denne politik betyder en væsentlig PIMS-afvigelse en fejl, som væsentligt påvirker PIMS-omfang, databeskyttelsesmål, ansvarlighed for PII-behandling, risikobehandling vedrørende databeskyttelse, registreredes rettigheder, behandlingssikkerhed, styring af databehandlere eller underdatabehandlere, beredskab ved brud, integriteten af dokumenteret bevismateriale, certificeringsomfang eller gentagen manglende opfyldelse af samme krav inden for en periode på 12 måneder.

1.5 I denne politik betyder en væsentlig ændring enhver ændring, der påvirker PIMS-omfang, PII-behandlingsformål, PII-kategorier, kategorier af registrerede, behandlingslokationer, rollefordeling som dataansvarlig eller databehandler, systemarkitektur, leverandør- eller underdatabehandlerordninger, risikoprofil vedrørende databeskyttelse, gældende retlige eller kontraktlige forpligtelser, revisionsomfang, overvågningsmetode eller certificeringsomfang.

2. Formål

2.1 Formålet med denne politik er at sikre, at organisationen evaluerer PIMS-præstation, verificerer PIMS-overensstemmelse, identificerer afvigelser, korrigerer kontrolsvagheder og løbende forbedrer PIMS på grundlag af objektivt bevismateriale.

2.2 Denne politik gør det muligt for organisationen at dokumentere, at PIMS-overvågning, revision, ledelsens gennemgang og forbedringsaktiviteter er planlagte, uafhængige hvor det kræves, evidensbaserede, rettidige og sporbare til ansvarlige roller og kanoniske bevisobjekter.

3. Mål

3.1 Målene med denne politik er at:

3.1.1 fastlægge en konsolideret proces for PIMS-overvågning og -måling;

3.1.2 sikre, at databeskyttelsesmål og PIMS-kontroludførelse måles ved hjælp af dokumenteret bevismateriale;

3.1.3 etablere et risikobaseret program for intern revision af PIMS;

3.1.4 bevare uafhængighed og objektivitet i PIMS-revisionsaktiviteter;

3.1.5 sikre, at ledelsens gennemgang modtager fuldstændige og aktuelle input om PIMS-præstation;

3.1.6 sikre, at afvigelser registreres, vurderes, korrigeres og verificeres;

3.1.7 sikre, at korrigerende handlinger spores til lukning og gennemgås for effektivitet;

3.1.8 identificere tilbagevendende svagheder og forbedringsmuligheder;

3.1.9 understøtte revisionsberedskab til certificering og ansvarlig styring af bevismateriale;

3.1.10 undgå at duplikere driftsmæssige metrikker, der allerede er fastlagt i relaterede PIMS-politikker.

4. Politikkerklæringer

4.1 Ramme for PIMS-overvågning og -måling

4.1.1 [Both] Privacy Lead / PIMS Manager SKAL definere det konsoliderede PIMS-overvågningsprogram i REG12 før den første PIMS-drift og derefter årligt.

4.1.2 [Both] Privacy Lead / PIMS Manager SKAL fastlægge målemetode, frekvens, beviskilde, mål og ansvarlig rolle for hver PIMS-metrik i REG12, før målecyklussen begynder.

4.1.3 [Both] Process Owner / Business Owner SKAL kvartalsvist levere overvågningsinput vedrørende PII-behandlingsaktiviteter fra REG02 til Privacy Lead / PIMS Manager.

4.1.4 [Both] Information Security Lead SKAL kvartalsvist levere input om status for PII-sikkerhedskontroller fra REG03 til Privacy Lead / PIMS Manager.

4.1.5 [Both] Vendor / Procurement Owner SKAL kvartalsvist levere input om status for databehandlere, underdatabehandlere, deling med tredjeparter og leverandørassurance fra REG08 til Privacy Lead / PIMS Manager.

4.1.6 [All] Incident Response Coordinator SKAL månedligt og inden for 10 arbejdsdage efter lukning af en større hændelse levere input om tendenser for databeskyttelseshændelser og brud fra REG10 til Privacy Lead / PIMS Manager.

4.1.7 [Both] Privacy Lead / PIMS Manager SKAL kvartalsvist konsolidere PIMS-overvågningsresultater i REG12.

4.2 Program for intern PIMS-revision

4.2.1 [All] Internal Audit / Compliance Reviewer SKAL årligt udarbejde et risikobaseret program for intern PIMS-revision i REG12 før den første planlagte PIMS-revisionscyklus.

4.2.2 [All] Internal Audit / Compliance Reviewer SKAL fastlægge formål, kriterier, omfang, metode, stikprøvegrundlag og rapporteringsfrist for hver PIMS-revision i REG12, før revisionsfeltarbejdet begynder.

4.2.3 [All] Internal Audit / Compliance Reviewer SKAL registrere kontroller af revisors uafhængighed og interessekonflikter i REG12 før hver revisionsopgave.

4.2.4 [All] Privacy Lead / PIMS Manager SKAL gøre anmodede kontrollerede PIMS-dokumenterede oplysninger og registerbevismateriale tilgængelige via REG12 inden for 10 arbejdsdage efter en godkendt revisionsanmodning.

4.2.5 [Both] Internal Audit / Compliance Reviewer SKAL under hver PIMS-revision teste status for implementering af relevante PIMS-kontroller op mod REG03.

4.2.6 [Both] Internal Audit / Compliance Reviewer SKAL under hver PIMS-revision registrere den valgte stikprøve af PII-bevismateriale for behandling i REG12.

4.2.7 [All] Internal Audit / Compliance Reviewer SKAL registrere PIMS-revisionsresultater i REG12 inden for 15 arbejdsdage efter revisionens afslutning.

4.2.8 [All] Privacy Lead / PIMS Manager SKAL tildele ejere af korrigerende handlinger for accepterede PIMS-revisionskonstateringer i REG12 inden for 10 arbejdsdage efter accept af revisionsresultaterne.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Undtagelser

9.1 Undtagelser vedrørende overvågning, revision og forbedring

9.1.1 [All] Process Owner / Business Owner SKAL anmode om enhver undtagelse fra denne politik i REG12, før afvigelsen finder sted.

9.1.2 [All] Privacy Lead / PIMS Manager SKAL vurdere påvirkningen af hver anmodet undtagelse på databeskyttelse, certificering, revision og korrigerende handling i REG12 inden for 10 arbejdsdage efter anmodningen.

9.1.3 [All] Data Protection Officer / Privacy Advisor SKAL registrere rådgivning i REG12 før godkendelse af enhver undtagelse, der påvirker retlige forpligtelser, registreredes rettigheder, DPIA-forpligtelser, kunderevisionsforpligtelser eller højrisikobehandling.

9.1.4 [All] Top Management SKAL godkende undtagelser, der påvirker gennemførelse af revisionsplan, ledelsens gennemgang, væsentlige afvigelser, certificeringsomfang eller højrisikobehandling, i REG12, før undtagelsen får virkning.

9.1.5 [All] Privacy Lead / PIMS Manager SKAL fastsætte en udløbsdato på højst 90 dage i REG12 for hver godkendt undtagelse vedrørende overvågning, revision eller forbedring.

9.1.6 [All] Privacy Lead / PIMS Manager SKAL lukke eller revurdere hver undtagelse vedrørende overvågning, revision eller forbedring i REG12 inden for fem arbejdsdage efter udløb.

10. Håndhævelse

10.1 Håndhævelse af krav til overvågning, revision og forbedring

10.1.1 [All] Privacy Lead / PIMS Manager SKAL registrere en manglende overvågningscyklus, manglende PIMS-revision, forfalden ledelsesgennemgang, manglende revisionsbevismateriale, forfalden korrigerende handling eller forfalden forbedringshandling som en afvigelse i REG12 inden for fem arbejdsdage efter identifikation.

10.1.2 [All] Internal Audit / Compliance Reviewer SKAL registrere alvorligheden af revisionskonstateringer i REG12, før revisionsrapporten udstedes.

10.1.3 [All] Top Management SKAL kræve korrigerende handling for hver væsentlig PIMS-afvigelse i REG12 inden for 10 arbejdsdage efter eskalering.

10.1.4 [All] Process Owner / Business Owner SKAL forhindre idriftsættelse i produktionsmiljøet eller indsendelse af ekstern assurance for højrisikobehandling, hvor krævet bevismateriale for korrigerende handling mangler i REG12 før idriftsættelse eller indsendelse.

10.1.5 [All] Privacy Lead / PIMS Manager SKAL eskalere gentagne overskredne frister for overvågning eller korrigerende handlinger til Top Management i REG12 inden for fem arbejdsdage efter anden forekomst i en periode på 12 måneder.

10.1.6 [All] Internal Audit / Compliance Reviewer SKAL verificere lukning af håndhævelseshandlinger i REG12 ved næste planlagte revision eller inden for 60 dage efter rapporteret lukning, alt efter hvad der indtræffer først.

11. Gennemgang og vedligeholdelse

11.1 Gennemgang og vedligeholdelse af politikken

11.1.1 [All] Privacy Lead / PIMS Manager SKAL gennemgå denne politik i REG12 årligt og inden for 30 dage efter væsentlig ændring af krav til PIMS-overvågning, revision, ledelsens gennemgang, korrigerende handling eller certificering.

11.1.2 [All] Internal Audit / Compliance Reviewer SKAL årligt gennemgå effektiviteten af PIMS-revisionsprogrammet i REG12 efter den sidste planlagte revision for PIMS-driftsåret.

11.1.3 [All] Data Protection Officer / Privacy Advisor SKAL gennemgå ændringer af denne politik med væsentlig betydning for databeskyttelse i REG12 før godkendelse.

11.1.4 [All] Top Management SKAL godkende væsentlige ændringer af denne politik i REG12 før offentliggørelse.

11.1.5 [All] Privacy Lead / PIMS Manager SKAL opdatere REG01 og REG03 inden for 15 arbejdsdage efter godkendte ændringer af denne politik, der ændrer PIMS-omfang eller kontrollers anvendelighed.

11.1.6 [All] Privacy Lead / PIMS Manager SKAL registrere kommunikation af godkendte ændringer af denne politik i REG11 inden for 30 dage efter offentliggørelse.

12. Relaterede politikker

12.1 Denne politik understøttes af følgende relaterede politikker:

12.2 PII01 - Politik for Privacy Information Management System

12.3 PII02 - Politik for roller, ansvar og ansvarlighed vedrørende databeskyttelse

12.4 PII03 - Politik for fortegnelse over PII-behandlingsaktiviteter og behandlingsgrundlag

12.5 PII04 - Politik for privatlivsmeddelelse og gennemsigtighed

12.6 PII05 - Politik for samtykke- og præferencestyring

12.7 PII06 - Politik for håndtering af registreredes rettigheder

12.8 PII07 - Politik for risikovurdering vedrørende databeskyttelse og DPIA

12.9 PII08 - Politik for databeskyttelse gennem design og standardindstillinger

12.10 PII09 - Politik for indsamling, brug, videregivelse og deling af PII

12.11 PII10 - Politik for opbevaring, sletning og bortskaffelse af PII

12.12 PII11 - Politik for PII-nøjagtighed og -kvalitet

12.13 PII12 - Politik for privatlivsstyring af databehandlere, underdatabehandlere og tredjeparter

12.14 PII13 - Politik for international overførsel af personhenførbare oplysninger (PII)

12.15 PII14 - Politik for PII-sikkerhed og adgangsstyring

12.16 PII15 - Politik for PII-hændelser og brud

12.17 PII16 - Politik for databeskyttelsestræning, bevidstgørelse og kompetence

12.18 PII17 - Politik for PIMS-dokumenterede oplysninger og styring af bevismateriale

13. Referencestandarder og rammeværker

13.1 Denne politik er kortlagt til følgende standarder og regler. Kortlægningen forklarer, hvordan politikken understøtter de citerede krav, og identificerer de interne klausuler, der implementerer eller understøtter dem.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.2** - Kortlagt til fastlæggelse, måling, rapportering og gennemgang af PIMS-mål og PIMS-præstationsmetrikker. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Kortlagt til vedligeholdelse af dokumenterede oplysninger om overvågningsresultater, revisionsprogrammer, revisionsresultater, bevismateriale til ledelsens gennemgang, afvigelser, korrigerende handlinger og forbedringshandlinger. 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** - Kortlagt til drift af den planlagte cyklus for PIMS-overvågning, revision, korrigerende handling og forbedring som led i PIMS' operationelle styring. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Kortlagt til fastlæggelse af, hvad der overvåges og måles, konsolidering af overvågningsresultater, evaluering af PIMS-præstation og vedligeholdelse af målebevismateriale. 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** - Kortlagt til vedligeholdelse af programmet for intern revision, revisionsplanlægning, kontroller af revisors uafhængighed, stikprøver af bevismateriale, revisionsresultater og opfølgning på revisionskonstateringer. 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** - Kortlagt til planlægning af ledelsens gennemgang, gennemgang af PIMS-præstation, gennemgang af tendenser i revision og korrigerende handlinger, godkendelse af output og ressourcebeslutninger. 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** - Kortlagt til identifikation, godkendelse, implementering og sporing af muligheder for løbende forbedring af PIMS' egnethed, tilstrækkelighed og effektivitet. 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** - Kortlagt til registrering af afvigelser, rodårsagsanalyse, planlægning af korrigerende handlinger, implementering af korrigerende handlinger, verifikation af effektivitet, eskalering og håndhævelse. 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** - Kortlagt til den dataansvarliges behandlingsregistre, der anvendes som beviskilder til overvågning, revisionsstikprøver og metrikker for behandlingsfortegnelsens aktualitet. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Kortlagt til bevismateriale for databehandleraftale, kunderevision, assurancerespons og databehandlersamarbejde, der spores gennem leverandør- og kundeassuranceprocesser. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Kortlagt til dokumentation for ansvarlighed vedrørende overvågning, revision, ledelsens gennemgang, korrigerende handling og løbende forbedring. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Kortlagt til den dataansvarliges styringsforanstaltninger, gennemgang af effektivitet, ledelsens gennemgang, korrigerende handling og dokumenteret forbedringsbevismateriale. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Kortlagt til bevismateriale for databehandlere, underdatabehandlere, kunderevision, tredjepartsassurance og leverandørsamarbejde. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Kortlagt til behandlingsregistre, der anvendes som bevismateriale for overvågning, revisionsstikprøver, fuldstændighed af bevisobjekter og behandlingsfortegnelsens aktualitet. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Kortlagt til overvågning og evaluering af status for PII-sikkerhedskontroller, bevismateriale for tekniske kontroller og sikkerhedsrelateret bevismateriale for effektivitet. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Kortlagt til databeskyttelsesrådgivning, overvågningsobservationer, revisionsstøtte og gennemgang af tendenser for efterlevelse af databeskyttelse udført af Data Protection Officer / Privacy Advisor, hvor relevant. 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** - Kortlagt til verifikation af efterlevelse vedrørende databeskyttelse, interne eller uafhængige revisioner, interne kontroller, tilsynsmekanismer og bevismateriale for risikovurdering vedrørende databeskyttelse. 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** - Kortlagt til uafhængig gennemgang af PII-relateret informationssikkerhed, overholdelse af politikker og standarder samt teknisk efterlevelsesgennemgang af PII-beskyttelse. 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** - Kortlagt til input om overvågning og evaluering af informationssikkerhed, der understøtter måling af PIMS-præstation og status for PII-sikkerhedskontroller. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Kortlagt til understøttelse fra intern revision af ISMS til PIMS-revisionsplanlægning, revisionsbevismateriale, revisionsresultater og gennemførelse af revisionsprogrammet. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Kortlagt til input og output fra ledelsens gennemgang for integreret tilsyn med PIMS- og informationssikkerhedspræstation. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Kortlagt til løbende forbedring af PIMS og det understøttende kontrolmiljø for informationssikkerhed. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Kortlagt til håndtering af afvigelser, planlægning af korrigerende handlinger, implementering af korrigerende handlinger og verifikation af effektivitet. 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 - Kortlagt til uafhængig gennemgang, kontroller af revisors uafhængighed, test af revisionsbevismateriale og uafhængig verifikation af effektiviteten af korrigerende handlinger. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Kortlagt til efterlevelsesgennemgang af PIMS- og informationssikkerhedspolitikker, status for implementering af kontroller og bevismateriale for overensstemmelse med standarder. 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** - Kortlagt til revisionsprincipper, styring af revisionsprogram, gennemførelse af revision, evidensbaseret revisionsrapportering, revisionsopfølgning og forventninger til revisorkompetence for PIMS-revisioner. 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].