					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : PII18					Titre du document : **Politique de surveillance, d'audit et d'amélioration du PIMS**							
Version : 1.0		Date d'entrée en vigueur : 01.01.2025			Propriétaire du document :							
X	Politique		Norme		Procédure		Formulaire		Registre		Autre	

Historique des révisions				
Numéro de révision	**Date de révision**	**Modifications**	**Revu par**	**Propriétaire du processus**

Approbations			
Nom	**Fonction**	**Date**	**Signature**

Alignement sur les normes et réglementations

Norme / réglementation	Clause / contrôle / article	Applicabilité	Type de couverture	Commentaire
ISO/IEC 27701:2025	Clause 6.2	Both	Supporting	Mesure des objectifs relatifs à la vie privée
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informations documentées relatives à la surveillance, à l'audit et à l'amélioration
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Surveillance de la planification et de la maîtrise opérationnelles
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Surveillance, mesure, analyse et évaluation
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Audit interne
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Revue de direction
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Amélioration continue
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Non-conformité et action corrective
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Registres des traitements du responsable du traitement utilisés pour l'audit
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Accord avec le sous-traitant et éléments de preuve de coopération en matière d'audit
GDPR	Article 5(2)	Controller	Supporting	Éléments de preuve de responsabilité
GDPR	Article 24	Controller	Supporting	Mesures du responsable du traitement et revue de leur efficacité

GDPR	Article 28	Both	Supporting	Gouvernance de l'audit et de la coopération des sous-traitants
GDPR	Article 30	Both	Supporting	Registres des traitements utilisés pour l'audit
GDPR	Article 32	Both	Supporting	Tests et évaluation des mesures de sécurité
GDPR	Article 39	Conditional	Supporting	Surveillance par le DPO et conseils en matière d'audit, le cas échéant
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Conformité à la vie privée, audit et supervision indépendante
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Revue de la protection des PII et contrôles de conformité
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Surveillance et évaluation de la sécurité de l'information
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	Appui à l'audit interne du SMSI
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	Appui à la revue de direction du SMSI
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	Appui à l'amélioration continue du SMSI
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	Appui à la non-conformité et aux actions correctives du SMSI
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Revue indépendante de la sécurité de l'information
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Revue de conformité des politiques et normes

ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Principes, programme, conduite et compétence relatifs à l'audit des systèmes de management

1. Champ d’application

1.1 La présente politique définit les exigences de l’organisation relatives à la surveillance, à la mesure, à l’analyse, à l’évaluation, à l’audit interne, à la revue de direction, au traitement des non-conformités, aux actions correctives et à l’amélioration continue du PIMS.

1.2 La présente politique s’applique à :

1.2.1 tous les processus, contrôles, politiques, registres, éléments de preuve, systèmes, fournisseurs, sous-traitants, sous-traitants ultérieurs et dispositifs de partage de données relevant du domaine d’application du PIMS ;

1.2.2 les contextes de responsable du traitement, de responsable conjoint du traitement, de sous-traitant et de sous-traitant ultérieur de l’organisation ;

1.2.3 la surveillance consolidée de la performance du PIMS, des objectifs relatifs à la vie privée, du statut de mise en œuvre des contrôles, des constats d’audit, des non-conformités, des actions correctives, des actions issues des revues de direction et des actions d’amélioration ;

1.2.4 les éléments de preuve conservés dans REG12 et les éléments de preuve sources à l’appui conservés dans REG01 à REG11.

1.3 La présente politique ne remplace pas les exigences de surveillance opérationnelle définies dans d’autres politiques PIMS. Elle établit le cycle consolidé d’évaluation de la performance, d’audit, de revue et d’amélioration du PIMS.

1.4 Aux fins de la présente politique, une non-conformité majeure du PIMS désigne une défaillance qui affecte de manière substantielle le domaine d’application du PIMS, les objectifs relatifs à la vie privée, la responsabilité du traitement de PII, le traitement des risques relatifs à la vie privée, les droits des personnes concernées, la sécurité du traitement, la gouvernance des sous-traitants ou des sous-traitants ultérieurs, la préparation aux violations, l’intégrité des éléments de preuve documentés, le périmètre de certification ou la répétition d’un manquement à la même exigence sur une période de 12 mois.

1.5 Aux fins de la présente politique, une modification substantielle désigne toute modification affectant le domaine d’application du PIMS, les finalités du traitement de PII, les catégories de PII, les catégories de personnes concernées, les lieux de traitement, la répartition des rôles de responsable du traitement ou de sous-traitant, l’architecture système, les dispositifs avec les fournisseurs ou sous-traitants ultérieurs, le profil de risque relatif à la vie privée, les obligations légales ou contractuelles applicables, le périmètre d’audit, la méthode de surveillance ou le périmètre de certification.

2. Objet

2.1 La présente politique a pour objet de veiller à ce que l’organisation évalue la performance du PIMS, vérifie la conformité du PIMS, identifie les non-conformités, corrige les faiblesses de contrôle et améliore continuellement le PIMS au moyen d’éléments de preuve objectifs.

2.2 La présente politique permet à l’organisation de démontrer que les activités de surveillance, d’audit, de revue de direction et d’amélioration du PIMS sont planifiées, indépendantes lorsque requis, fondées sur des éléments de preuve, réalisées en temps utile et traçables jusqu’aux rôles responsables et aux éléments de preuve canoniques.

3. Objectifs

3.1 Les objectifs de la présente politique sont les suivants :

3.1.1 définir un processus consolidé de surveillance et de mesure du PIMS ;

3.1.2 veiller à ce que les objectifs relatifs à la vie privée et la performance des contrôles PIMS soient mesurés au moyen d’éléments de preuve documentés ;

3.1.3 établir un programme d’audit interne du PIMS fondé sur les risques ;

3.1.4 préserver l’indépendance et l’objectivité dans les activités d’audit du PIMS ;

3.1.5 veiller à ce que la revue de direction reçoive des données d’entrée complètes et à jour sur la performance du PIMS ;

3.1.6 veiller à ce que les non-conformités soient enregistrées, évaluées, corrigées et vérifiées ;

3.1.7 veiller à ce que les actions correctives soient suivies jusqu’à leur clôture et revues quant à leur efficacité ;

3.1.8 identifier les faiblesses récurrentes et les opportunités d’amélioration ;

3.1.9 soutenir la préparation à la certification et la gestion responsable des éléments de preuve ;

3.1.10 éviter de dupliquer les indicateurs opérationnels déjà définis dans les politiques PIMS associées.

4. Énoncés de politique

4.1 Cadre de surveillance et de mesure du PIMS

4.1.1 [Both] Privacy Lead / PIMS Manager doit définir le programme consolidé de surveillance du PIMS dans REG12 avant l’exploitation initiale du PIMS, puis annuellement.

4.1.2 [Both] Privacy Lead / PIMS Manager doit définir la méthode de mesure, la fréquence, la source des éléments de preuve, la cible et le rôle responsable pour chaque indicateur PIMS dans REG12 avant le début du cycle de mesure.

4.1.3 [Both] Process Owner / Business Owner doit fournir trimestriellement à Privacy Lead / PIMS Manager les données d’entrée relatives à la surveillance des activités de traitement de PII provenant de REG02.

4.1.4 [Both] Information Security Lead doit fournir trimestriellement à Privacy Lead / PIMS Manager les données d’entrée relatives au statut des contrôles de sécurité des PII provenant de REG03.

4.1.5 [Both] Vendor / Procurement Owner doit fournir trimestriellement à Privacy Lead / PIMS Manager les données d’entrée relatives au statut des sous-traitants, des sous-traitants ultérieurs, du partage avec des tiers et de l’assurance fournisseur provenant de REG08.

4.1.6 [All] Incident Response Coordinator doit fournir à Privacy Lead / PIMS Manager les données d’entrée relatives aux tendances des incidents relatifs à la vie privée et des violations à partir de REG10 mensuellement et dans les 10 jours ouvrables suivant la clôture d’un incident majeur.

4.1.7 [Both] Privacy Lead / PIMS Manager doit consolider trimestriellement les résultats de surveillance du PIMS dans REG12.

4.2 Programme d’audit interne du PIMS

4.2.1 [All] Internal Audit / Compliance Reviewer doit préparer annuellement un programme d’audit interne du PIMS fondé sur les risques dans REG12 avant le premier cycle d’audit PIMS planifié.

4.2.2 [All] Internal Audit / Compliance Reviewer doit définir l’objectif, les critères, le périmètre, la méthode, la base d’échantillonnage et l’échéance de rapport pour chaque audit PIMS dans REG12 avant le début des travaux d’audit sur le terrain.

4.2.3 [All] Internal Audit / Compliance Reviewer doit enregistrer dans REG12 les vérifications d’indépendance de l’auditeur et de conflit d’intérêts avant chaque affectation d’audit.

4.2.4 [All] Privacy Lead / PIMS Manager doit mettre à disposition les informations documentées PIMS contrôlées et les éléments de preuve de registre demandés via REG12 dans les 10 jours ouvrables suivant une demande d’audit approuvée.

4.2.5 [Both] Internal Audit / Compliance Reviewer doit tester le statut de mise en œuvre des contrôles PIMS applicables par rapport à REG03 lors de chaque audit PIMS.

4.2.6 [Both] Internal Audit / Compliance Reviewer doit enregistrer dans REG12 l'échantillon sélectionné d'éléments de preuve relatifs au traitement de PII lors de chaque audit PIMS.

4.2.7 [All] Internal Audit / Compliance Reviewer doit enregistrer les résultats d'audit PIMS dans REG12 dans les 15 jours ouvrables suivant l'achèvement de l'audit.

4.2.8 [All] Privacy Lead / PIMS Manager doit désigner les propriétaires des actions correctives pour les constats d'audit PIMS acceptés dans REG12 dans les 10 jours ouvrables suivant l'acceptation des résultats d'audit.

[... Les sections 4.3–8 ne sont pas incluses dans cet aperçu. Achetez le document complet pour accéder à l'intégralité du contenu. ...]

9. Exceptions

9.1 Exceptions relatives à la surveillance, à l'audit et à l'amélioration

9.1.1 [All] Process Owner / Business Owner doit demander toute exception à la présente politique dans REG12 avant que l'écart ne se produise.

9.1.2 [All] Privacy Lead / PIMS Manager doit évaluer dans REG12 l'impact de chaque exception demandée sur la vie privée, la certification, l'audit et les actions correctives dans les 10 jours ouvrables suivant la demande.

9.1.3 [All] Data Protection Officer / Privacy Advisor doit enregistrer ses conseils dans REG12 avant l'approbation de toute exception affectant les obligations légales, les droits des personnes concernées, les engagements de DPIA, les obligations d'audit client ou les traitements à haut risque.

9.1.4 [All] Top Management doit approuver dans REG12 les exceptions affectant l'achèvement du calendrier d'audit, la revue de direction, les non-conformités majeures, le périmètre de certification ou les traitements à haut risque avant que l'exception ne prenne effet.

9.1.5 [All] Privacy Lead / PIMS Manager doit fixer dans REG12 une date d'expiration n'excédant pas 90 jours pour chaque exception approuvée relative à la surveillance, à l'audit ou à l'amélioration.

9.1.6 [All] Privacy Lead / PIMS Manager doit clôturer ou réévaluer chaque exception relative à la surveillance, à l'audit ou à l'amélioration dans REG12 dans les cinq jours ouvrables suivant son expiration.

10. Mise en application

10.1 Mise en application des exigences de surveillance, d'audit et d'amélioration

10.1.1 [All] Privacy Lead / PIMS Manager doit enregistrer tout cycle de surveillance manqué, audit PIMS manqué, revue de direction en retard, élément de preuve d'audit manquant, action corrective en retard ou action d'amélioration en retard comme une non-conformité dans REG12 dans les cinq jours ouvrables suivant son identification.

10.1.2 [All] Internal Audit / Compliance Reviewer doit enregistrer le niveau de gravité des constats d'audit dans REG12 avant l'émission du rapport d'audit.

10.1.3 [All] Top Management doit exiger une action corrective pour chaque non-conformité majeure du PIMS dans REG12 dans les 10 jours ouvrables suivant l'escalade.

10.1.4 [All] Process Owner / Business Owner doit empêcher la mise en production ou la soumission d'une assurance externe pour les traitements à haut risque lorsque les éléments de preuve requis d'action corrective sont absents de REG12 avant la mise en production ou la soumission.

10.1.5 [All] Privacy Lead / PIMS Manager doit escalader à Top Management les échéances de surveillance ou d'action corrective manquées de façon répétée dans REG12 dans les cinq jours ouvrables suivant la seconde occurrence sur une période de 12 mois.

10.1.6 [All] Internal Audit / Compliance Reviewer doit vérifier la clôture de l'action de mise en application dans REG12 lors du prochain audit planifié ou dans les 60 jours suivant la clôture déclarée, selon la première échéance atteinte.

11. Revue et maintenance

11.1 Revue et maintenance de la politique

11.1.1 [All] Privacy Lead / PIMS Manager doit revoir la présente politique dans REG12 annuellement et dans les 30 jours suivant toute modification substantielle des exigences relatives à la surveillance, à l'audit, à la revue de direction, aux actions correctives ou à la certification du PIMS.

11.1.2 [All] Internal Audit / Compliance Reviewer doit revoir annuellement l'efficacité du programme d'audit PIMS dans REG12 après le dernier audit planifié de l'année d'exploitation du PIMS.

11.1.3 [All] Data Protection Officer / Privacy Advisor doit examiner dans REG12 les changements à enjeu significatif pour la vie privée apportés à la présente politique avant approbation.

11.1.4 [All] Top Management doit approuver les modifications substantielles apportées à la présente politique dans REG12 avant publication.

11.1.5 [All] Privacy Lead / PIMS Manager doit mettre à jour REG01 et REG03 dans les 15 jours ouvrables suivant les changements approuvés de la présente politique qui modifient le domaine d'application du PIMS ou l'applicabilité des contrôles.

11.1.6 [All] Privacy Lead / PIMS Manager doit enregistrer dans REG11 la communication des changements approuvés de la présente politique dans les 30 jours suivant la publication.

12. Politiques associées

12.1 La présente politique est soutenue par les politiques associées suivantes :

12.2 PII01 - Politique du système de management des informations relatives à la vie privée

12.3 PII02 - Politique relative aux rôles, responsabilités et à la responsabilité en matière de vie privée

12.4 PII03 - Politique d'inventaire des traitements de PII et de base légale

12.5 PII04 - Politique relative aux mentions d'information et à la transparence

12.6 PII05 - Politique de gestion du consentement et des préférences

12.7 PII06 - Politique de gestion des droits des personnes concernées

12.8 PII07 - Politique d'appréciation des risques relatifs à la vie privée et de DPIA

12.9 PII08 - Politique de protection de la vie privée dès la conception et par défaut

12.10 PII09 - Politique de collecte, d'utilisation, de divulgation et de partage des PII

12.11 PII10 - Politique de conservation, de suppression et d'élimination des PII

12.12 PII11 - Politique d'exactitude et de qualité des PII

12.13 PII12 - Politique de gestion de la vie privée des sous-traitants, des sous-traitants ultérieurs et des tiers

12.14 PII13 - Politique relative aux transferts internationaux de PII

12.15 PII14 - Politique de sécurité et de contrôle d'accès des PII

12.16 PII15 - Politique de gestion des incidents et violations de PII

12.17 PII16 - Politique de formation, de sensibilisation et de compétence en matière de vie privée

12.18 PII17 - Politique de gestion des informations documentées et des éléments de preuve du PIMS

13. Normes et référentiels de référence

13.1 La présente politique est mise en correspondance avec les normes et réglementations suivantes. Cette cartographie explique comment la politique soutient les exigences citées et identifie les clauses internes qui les mettent en œuvre ou les appuient.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.2** - Mise en correspondance avec la définition, la mesure, la communication et la revue des objectifs du PIMS et des indicateurs de performance du PIMS. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Mise en correspondance avec la tenue d'informations documentées relatives aux résultats de surveillance, aux programmes d'audit, aux résultats d'audit, aux éléments de preuve de revue de direction, aux non-conformités, aux actions correctives et aux actions d'amélioration. 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** - Mise en correspondance avec l'exploitation du cycle planifié de surveillance, d'audit, d'action corrective et d'amélioration du PIMS dans le cadre de la maîtrise opérationnelle du PIMS. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Mise en correspondance avec la définition de ce qui est surveillé et mesuré, la consolidation des résultats de surveillance, l'évaluation de la performance du PIMS et la conservation des éléments de preuve de mesure. 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** - Mise en correspondance avec la tenue du programme d'audit interne, la planification de l'audit, les vérifications d'indépendance des auditeurs, l'échantillonnage des éléments de preuve, les résultats d'audit et le suivi des constats d'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** - Mise en correspondance avec la planification de la revue de direction, la revue de la performance du PIMS, la revue des tendances d'audit et d'actions correctives, l'approbation des éléments de sortie et les décisions relatives aux ressources. 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** - Mise en correspondance avec l'identification, l'approbation, la mise en œuvre et le suivi des opportunités d'amélioration continue de la pertinence, de l'adéquation et de l'efficacité du 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** - Mise en correspondance avec l'enregistrement des non-conformités, l'analyse de la cause racine, la planification des actions correctives, la mise en œuvre des actions correctives, la vérification de l'efficacité, l'escalade et la mise en application. 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** - Mise en correspondance avec les registres des traitements du responsable du traitement utilisés comme sources d'éléments de preuve pour la surveillance, l'échantillonnage d'audit et les indicateurs d'actualité de l'inventaire des traitements. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Mise en correspondance avec les accords avec les sous-traitants, les audits clients, les réponses d'assurance et les éléments de preuve de coopération des sous-traitants suivis au moyen des processus d'assurance fournisseur et client. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Mise en correspondance avec les éléments de preuve de responsabilité pour la surveillance, l'audit, la revue de direction, les actions correctives et l'amélioration continue. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Mise en correspondance avec les mesures de gouvernance du responsable du traitement, la revue de l'efficacité, la revue de direction, les actions correctives et les éléments de preuve documentés d'amélioration. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Mise en correspondance avec les éléments de preuve relatifs aux sous-traitants, aux sous-traitants ultérieurs, aux audits clients, à l'assurance des tiers et à la coopération des fournisseurs. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Mise en correspondance avec les registres des traitements utilisés comme éléments de preuve de surveillance, d'échantillonnage d'audit, d'exhaustivité des éléments de preuve et d'actualité de l'inventaire des traitements. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Mise en correspondance avec la surveillance et l'évaluation du statut des contrôles de sécurité des PII, des éléments de preuve de contrôles techniques et des éléments de preuve d'efficacité liés à la sécurité. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Mise en correspondance avec les conseils en matière de vie privée, les observations de surveillance, l'appui à l'audit et la revue des tendances de conformité relatives à la vie privée par Data Protection Officer / Privacy Advisor, le cas échéant. 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** - Mise en correspondance avec la vérification de la conformité à la vie privée, les audits internes ou indépendants, les contrôles internes, les mécanismes de supervision et les éléments de preuve d'appréciation des risques relatifs à la vie privée. 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** - Mise en correspondance avec la revue indépendante de la sécurité de l'information relative aux PII, la conformité aux politiques et normes, et la revue de conformité technique pour la protection des 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** - Mise en correspondance avec les données d'entrée de surveillance et d'évaluation de la sécurité de l'information qui soutiennent la mesure de la performance du PIMS et le statut des contrôles de sécurité des PII. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Mise en correspondance avec l'appui de l'audit interne du SMSI à la planification des audits PIMS, aux éléments de preuve d'audit, aux résultats d'audit et à l'achèvement du programme d'audit. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Mise en correspondance avec les données d'entrée et de sortie de la revue de direction pour la supervision intégrée de la performance du PIMS et de la sécurité de l'information. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Mise en correspondance avec l'amélioration continue du PIMS et de l'environnement de contrôles de sécurité de l'information à l'appui. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Mise en correspondance avec le traitement des non-conformités, la planification des actions correctives, la mise en œuvre des actions correctives et la vérification de l'efficacité. 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 - Mise en correspondance avec la revue indépendante, les vérifications d'indépendance des auditeurs, les tests des éléments de preuve d'audit et la vérification indépendante de l'efficacité des actions correctives. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Mise en correspondance avec la revue de conformité des politiques PIMS et de sécurité de l'information, du statut de mise en œuvre des contrôles et des éléments de preuve de conformité aux normes. 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** - Mise en correspondance avec les principes d'audit, la gestion du programme d'audit, la conduite de l'audit, le rapport d'audit fondé sur des éléments de preuve, le suivi d'audit et les attentes en matière de compétence des auditeurs pour les audits 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].