					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P33					Titre du document : **Politique d'audit et de surveillance de la conformité**							
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/Article	Commentaire
ISO/IEC 27001:2022	Articles 9.2, 9.3, 10	
ISO/IEC 27002:2022	Mesures 5.35–5.37	
NIST SP 800-53 Rév. 5	CA-2, CA-5, CA-7	
RGPD de l'UE	Articles 24, 32, 33	
NIS2 de l'UE	Article 21(2)(g), 27	
DORA de l'UE	Articles 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

1. Objet

1.1 La présente politique a pour objet d'établir et d'encadrer le programme d'audit et de surveillance de la conformité de l'organisation afin de :

1.1.1 valider l'efficacité des contrôles de sécurité et de protection des données

1.1.2 garantir l'alignement sur les normes applicables, les cadres juridiques et les obligations contractuelles

1.1.3 détecter en temps utile les non-conformités, les inefficacités et les risques de conformité

1.1.4 soutenir l'amélioration continue et la préparation aux certifications, aux évaluations et aux revues réglementaires

1.2 La présente politique contribue à l'intégrité et à la maturité du système de management de la sécurité de l'information (SMSI) en y intégrant des pratiques d'audit et de surveillance structurées, fondées sur les risques et étayées par des éléments probants.

2. Champ d'application

2.1 La présente politique s'applique à l'ensemble des éléments suivants :

2.1.1 les unités opérationnelles internes, fonctions et départements

2.1.2 les sites physiques, environnements cloud, environnements SaaS et services externalisés

2.1.3 les systèmes d'information, applications, infrastructures et actifs de données relevant du périmètre du SMSI

2.1.4 les employés, prestataires et fournisseurs tiers ayant des obligations d'audit ou de conformité

2.2 La politique couvre :

2.2.1 l'audit interne

2.2.2 les audits externes et de certification

2.2.3 la surveillance technique de la conformité

2.2.4 les audits des fournisseurs et des tiers

2.2.5 les actions correctives et préventives (CAPA)

2.2.6 les indicateurs, tableaux de bord et processus de reporting

2.3 Elle s'applique à tous les référentiels pertinents auxquels l'organisation est soumise, notamment ISO/IEC 27001, le RGPD, NIS2, DORA et SOC 2.

3. Objectifs

3.1 Vérifier l'adéquation et l'efficacité des contrôles, politiques et procédures mis en œuvre dans l'ensemble du SMSI et des environnements associés.

3.2 Identifier et corriger toute défaillance, non-conformité ou lacune avant qu'elle ne se transforme en incident ou en manquement.

3.3 Maintenir un niveau durable de préparation aux revues de gouvernance internes, aux audits externes et aux certifications indépendantes.

3.4 Produire des éléments probants opposables et une piste d'audit à l'appui des demandes des autorités de régulation, des procédures judiciaires ou des demandes d'assurance des clients.

3.5 Intégrer les résultats d'audit dans la gestion globale des risques de l'organisation, les indicateurs de sécurité et les activités d'amélioration continue.

4. Rôles et responsabilités

4.1 Responsable de l'audit interne / Responsable conformité

4.1.1 Planifie, programme et exécute les audits internes selon les priorités de risque.

4.1.2 Tient le registre des audits, coordonne les activités d'audit et assure le suivi des actions correctives.

4.2 Responsable de la sécurité des systèmes d'information (RSSI)

4.2.1 Veille à ce que le périmètre d'audit couvre tous les éléments pertinents du SMSI et les mesures de l'Annexe A.

4.2.2 Supervise la vérification des CAPA et intègre les résultats d'audit au programme de sécurité.

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

9. Exigences de revue et de mise à jour

9.1 La présente politique doit faire l'objet d'une revue au moins annuelle par le Responsable conformité et le RSSI, ou plus tôt en cas de :

9.1.1 changements dans les référentiels réglementaires, contractuels ou de certification

9.1.2 constats d'audit significatifs ou défaillances de contrôle répétées

9.1.3 restructuration organisationnelle ou changements du système GRC

9.1.4 recommandations d'auditeurs externes ou retours d'autorités de régulation

9.2 Le processus de revue doit évaluer :

9.2.1 la méthodologie et la fréquence de planification des audits

9.2.2 les changements du périmètre du SMSI ou de l'infrastructure

9.2.3 les mises à jour du catalogue des contrôles ou du registre juridique

9.2.4 la cohérence et la qualité des éléments probants d'audit et des processus CAPA

9.3 Toute modification de la politique doit être :

9.3.1 documentée dans un référentiel soumis à la gestion des versions

9.3.2 approuvée par la haute direction

9.3.3 communiquée à l'ensemble du personnel concerné et intégrée dans les procédures mises à jour et les programmes de sensibilisation

9.4 La validation après revue doit confirmer que les exigences mises à jour sont répercutées dans le registre des audits, les outils de conformité et les tableaux de bord internes de surveillance.

10. Politiques associées et articulations

10.1 La présente politique s'aligne sur les politiques organisationnelles connexes suivantes :

10.1.1 P1 – Politique de sécurité de l'information : définit le SMSI et établit la responsabilité en matière de conformité et d'amélioration continue

10.1.2 P5 – Politique de gestion des changements : garantit la visibilité de l'audit sur les changements d'infrastructure et de configuration affectant les environnements de contrôle

10.1.3 P6 – Politique de gestion des risques : intègre les résultats d'audit aux activités d'évaluation et de traitement des risques de l'organisation

10.1.4 P14 – Politique de conservation et d'élimination des données : encadre la conservation des éléments probants d'audit, des journaux et des enregistrements de conformité

10.1.5 P18 – Politique relative aux contrôles cryptographiques : soutient le stockage et le transfert sécurisés des données d'audit sensibles

10.1.6 P26 – Politique relative à la sécurité des tiers et des fournisseurs : couvre les droits d'audit, la documentation d'assurance et la supervision de la conformité des fournisseurs

10.1.7 P30 – Politique de réponse aux incidents : aligne les audits des processus de gestion des incidents sur les objectifs d'assurance du SMSI

10.1.8 P32 – Politique de continuité d'activité et de reprise après sinistre : impose la vérification des tests de continuité et de la conformité au plan de reprise après sinistre au cours des cycles d'audit

11. Normes et référentiels de référence

11.1 La présente politique est alignée sur les normes internationales et les exigences juridiques applicables en matière d'audit et de validation continue de la conformité.

11.2 ISO/IEC 27001 :

11.2.1 Article 9.2 – Audit interne : impose des audits réguliers du SMSI, fondés sur les risques, afin d'évaluer l'efficacité et la conformité.

11.2.2 Article 9.3 – Revue de direction : les résultats d'audit doivent alimenter la revue stratégique et l'amélioration.

11.2.3 Article 10.1 – Non-conformité et action corrective : les constats d'audit doivent être traités au moyen de procédures CAPA documentées.

11.3 ISO/IEC 27002:2022 – Mesures 5.35–5.37 :

11.3.1 Mesures de l'Annexe A 5.35–5.37 : couvrent la revue indépendante, la conformité aux exigences juridiques et contractuelles, ainsi que la journalisation d'audit.

11.3.2 Fournissent des orientations de mise en œuvre pour la planification, l'exécution et l'amélioration des programmes d'audit et de conformité.

11.4 NIST SP 800-53 Rév. 5 :

11.4.1 CA-2 – Évaluation des contrôles : impose la revue régulière des contrôles de sécurité mis en œuvre.

11.4.2 CA-5 – Plan of Action and Milestones (POA&M) : s'aligne sur le suivi et la remédiation des constats d'audit.

11.4.3 CA-7 – Surveillance continue : soutient des évaluations proactives et automatisées de la conformité.

11.5 RGPD de l'UE (2016/679) :

11.5.1 Articles 24 et 32 : imposent de pouvoir démontrer la mise en œuvre et l'efficacité des contrôles de sécurité au moyen de structures de gouvernance appropriées.

11.5.2 Article 33 : justifie la nécessité de pistes d'audit vérifiées pour la réponse aux violations et la notification.

11.6 Directive NIS2 de l'UE (2022/2555) :

11.6.1 Article 21(2)(g) : impose l'audit des politiques et procédures dans le cadre des mesures minimales de gestion des risques de cybersécurité.

11.6.2 Article 27 : les autorités nationales peuvent réaliser ou exiger des audits pour les entités essentielles et importantes.

11.7 DORA de l'UE (2022/2554) :

11.7.1 Article 10(2)(e) : les entités doivent réaliser des audits internes et externes des pratiques de gestion des risques liés aux TIC.

11.7.2 Article 25 – Exigences d'audit : impose des audits périodiques réalisés par des auditeurs internes ou des auditeurs externes indépendants avec visibilité réglementaire.

11.8 COBIT 2019 :

11.8.1 MEA01 – Surveiller, évaluer et apprécier la performance et la conformité : garantit que l'efficacité des contrôles est vérifiée et communiquée aux organes de gouvernance.

11.8.2 MEA03 – Surveiller, évaluer et apprécier la conformité : impose l'alignement des pratiques de l'organisation sur les exigences juridiques, contractuelles et normatives.