					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P33S					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	Clauses 9.2, 10	Audits internes, amélioration continue et remédiation des non-conformités
ISO/IEC 27002:2022	Mesures 5.35, 5.37	Revues internes planifiées, revues indépendantes des processus externalisés
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	Évaluations de sécurité, surveillance continue, revue, analyse et reporting d'audit
RGPD de l'UE	Articles 24 et 32	Audit des mesures techniques et organisationnelles, éléments probants de l'efficacité des contrôles
NIS2 de l'UE	Article 21(2)(f)	Revue proactive et conformité fondée sur des éléments probants
DORA de l'UE	Article 10	Gestion des risques liés aux TIC, surveillance et reporting
COBIT 2019	MEA01, MEA03	Surveillance et évaluation de la conformité, préparation aux revues par des tiers

1. Objet

1.1 La présente politique définit l'approche de l'organisation en matière d'audits internes, de vérification des mesures de sécurité et de surveillance de la conformité réglementaire. Elle impose que l'ensemble des contrôles, politiques, systèmes et prestataires de services fasse l'objet d'une revue régulière et structurée.

1.2 Elle vise à détecter les défaillances des contrôles, à prévenir toute non-conformité et à démontrer la diligence raisonnable au regard de l'ISO/IEC 27001, du RGPD et des référentiels associés.

1.3 Elle permet aux PME de maintenir la maîtrise opérationnelle et la préparation à la certification, même en l'absence d'une fonction conformité dédiée, en s'appuyant sur des listes de contrôle simples et reproductibles, ainsi que sur des constats priorisés selon les risques.

2. Champ d'application

2.1 La présente politique s'applique à :

2.1.1 Tous les départements internes et prestataires externes ayant des responsabilités relatives aux systèmes d'information, aux données à caractère personnel et aux services critiques pour l'activité

2.1.2 Tous les contrôles et systèmes relevant du champ d'application du SMSI

2.1.3 Tous les audits internes, revues des mesures de sécurité et contrôles de conformité, qu'ils soient réalisés en interne ou par un consultant externe, un client ou une autorité de régulation

2.2 La présente politique s'applique également à la collecte d'éléments probants et au reporting pour :

2.2.1 Les audits de certification et de renouvellement de certification ISO/IEC 27001

2.2.2 Les audits de protection des données au titre du RGPD ou d'obligations contractuelles

2.2.3 Les questionnaires de sécurité émis par les clients ou les revues de diligence raisonnable

2.2.4 Toute revue réglementaire ou indépendante au titre de NIS2 ou de DORA, le cas échéant

3. Objectifs

3.1 Veiller à ce que tous les contrôles clés et toutes les politiques fassent régulièrement l'objet d'une revue de leur efficacité et de leur conformité.

3.2 Maintenir une piste d'audit et des enregistrements des actions correctives permettant de démontrer la responsabilité et l'amélioration continue.

3.3 Se préparer à la certification, au renouvellement de certification et aux programmes d'assurance demandés par les clients (par exemple ISO 27001, intégration des fournisseurs).

3.4 Identifier rapidement les lacunes afin de permettre une remédiation rapide avant l'aggravation des problèmes ou le non-respect d'obligations.

3.5 Permettre au Directeur général et au prestataire informatique de coordonner les revues avec un niveau minimal de complexité, tout en garantissant des résultats défendables.

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 Supervise le programme d'audit

4.1.2 Approuve les plans de revue interne et les constats

4.1.3 Attribue les actions correctives et en assure le suivi

4.1.4 Autorise le recours à des auditeurs ou consultants externes

4.2 Prestataire informatique / Administrateur système

4.2.1 Fournit les éléments probants lors des audits internes et externes (par exemple journaux, configurations, enregistrements de contrôle d'accès)

4.2.2 Assiste aux vérifications techniques (par exemple état des sauvegardes, conformité des correctifs)

4.2.3 Tient à jour le référentiel des éléments probants 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. Exigences de revue et de mise à jour

9.1 Revue annuelle de la politique et du plan d'audit

9.1.1 Le Directeur général (DG) doit revoir la présente politique et le calendrier des audits au moins une fois par an.

9.1.2 La revue doit évaluer :

9.1.2.1 L'efficacité des audits dans l'identification des lacunes

9.1.2.2 Le taux de réalisation des audits et des actions correctives

9.1.2.3 Les évolutions des exigences légales, réglementaires ou de certification applicables

9.2 Mises à jour déclenchées par un événement

9.2.1 La politique doit être revue et mise à jour lorsque :

9.2.2 Un audit de certification ou de surveillance aboutit à une non-conformité majeure

9.2.3 Les cadres juridiques ou réglementaires évoluent (par exemple nouvelles orientations RGPD, transposition nationale de NIS2)

9.2.4 Des changements d'activité affectent les systèmes, processus ou fournisseurs inclus dans le champ d'application de l'audit

9.2.5 Un incident critique ou une violation révèle des lacunes de contrôle jusque-là non détectées

9.3 Documentation des mises à jour

9.3.1 Toutes les révisions doivent être consignées dans un journal de gestion des versions de la politique.

9.3.2 Les mises à jour doivent être diffusées à tous les membres d'équipe impliqués dans les audits.

9.3.3 Un résumé des changements doit accompagner la politique mise à jour afin d'en assurer la bonne compréhension.

10. Politiques associées et articulations

10.1 La présente politique est soutenue par plusieurs autres politiques de la PME et les renforce :

10.1.1 P1S – Politique de sécurité de l'information : définit le référentiel de base pour l'ensemble des exigences de contrôle et impose leur vérification par audit.

10.1.2 P2S – Politique relative aux rôles et responsabilités de gouvernance : établit la responsabilité en matière de planification des audits, d'exécution et de prise en charge des actions correctives.

10.1.3 P6S – Politique de gestion des risques : identifie les faiblesses de contrôle révélées par les audits et impose la documentation des constats dans le registre des risques.

10.1.4 P17S – Politique de protection des données et de la vie privée : définit les contrôles RGPD devant être audités, y compris le traitement des données, la réponse aux violations et les notices d'information sur la vie privée.

10.1.5 P22S – Politique de journalisation et de surveillance : fournit les journaux d'audit et les données forensiques utilisés lors des revues de conformité et de contrôle.

10.1.6 P30S – Politique de réponse aux incidents : exige un audit périodique des enregistrements d'incident et des revues post-événement afin de vérifier l'efficacité de la réponse.

10.1.7 P31S – Politique d'investigation forensique et de collecte des éléments probants : fournit les procédures de collecte, pendant les audits, d'éléments probants vérifiables respectant la chaîne de conservation.

10.2 Ensemble, ces politiques constituent un environnement de contrôle en boucle fermée permettant la vérification interne, l'assurance externe et une gouvernance alignée sur les normes.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001 :

11.1.1 Clause 9.2 – Exige des audits internes pour évaluer la performance du SMSI et son alignement sur les exigences.

11.1.2 Clause 10.1 – Implique l'amélioration continue à partir des résultats d'audit et de la remédiation des non-conformités.

11.2 ISO/IEC 27002 :

11.2.1 Mesure 5.35 – Exige des revues internes planifiées des contrôles et des processus.

11.2.2 Mesure 5.37 – Met l'accent sur les revues indépendantes, en particulier pour les processus externalisés.

11.3 NIST SP 800-53 Rev.5 :

11.3.1 CA-2 – Évaluations de sécurité : exige des audits des contrôles mis en œuvre afin de vérifier leur efficacité.

11.3.2 CA-7 – Surveillance continue : met l'accent sur la détection proactive et la revue des faiblesses de contrôle.

11.3.3 AU-6 – Revue, analyse et reporting d'audit : exige l'analyse régulière et le traitement des journaux d'audit et des constats.

11.4 RGPD de l'UE :

11.4.1 Articles 24 et 32 – Exigent la mise en œuvre et l'audit de mesures techniques et organisationnelles, y compris des éléments probants de l'efficacité des contrôles et de leur amélioration dans le temps.

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

11.5.1 Articles 20–21 – Imposent une revue proactive des contrôles, une conformité fondée sur des éléments probants et l'auditabilité pour les entités essentielles et importantes.

11.6 COBIT 2019 :

11.6.1 MEA01 – Surveiller, évaluer et apprécier la performance et la conformité : exige une évaluation périodique de la performance des processus et des contrôles au regard des normes et objectifs.

11.6.2 MEA03 – Assurer la conformité aux exigences externes : met l'accent sur la surveillance interne et la préparation aux audits de tiers et aux revues réglementaires.