					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P06					Titre du document : **Politique de gestion des risques**							
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 6.1, 8.32, 10	Socle de l'identification et de la gestion des risques, intégration à la gestion des changements, amélioration continue
ISO/IEC 27005:2024	Méthodologie complète du cycle de vie des risques	Processus complet de gestion des risques conforme à la norme
ISO 31000:2018	Principes et cadre de gestion des risques	Principes de gestion des risques adoptés dans le cadre
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Lignes directrices et structure pour les évaluations des risques, gouvernance des risques à plusieurs niveaux
RGPD de l'UE	Articles 24, 25, 32	Processus et contrôles relatifs aux risques en matière de protection des données
NIS2 de l'UE	Article 21(2)(a–d)	Obligations en matière d'évaluation des risques et de sécurité
DORA de l'UE	Articles 5, 6	Gestion des risques liés aux TIC et résilience opérationnelle
COBIT 2019	APO12, MEA	Cadre de structuration et de supervision de la gestion des risques

1. Objet

1.1 La présente politique établit un cadre unifié et formalisé pour identifier, analyser, évaluer, traiter, surveiller et revoir les risques de sécurité de l'information dans l'ensemble de l'organisation.

1.2 Elle impose l'application cohérente de principes fondés sur les risques afin de protéger la confidentialité, l'intégrité et la disponibilité des actifs informationnels, conformément à la clause 6.1 de l'ISO/IEC 27001:2022 et à l'ISO 31000:2018.

1.3 La présente politique intègre la gestion des risques de sécurité de l'information aux processus décisionnels de l'organisation afin de répondre aux objectifs stratégiques internes et aux exigences réglementaires externes.

2. Champ d'application

2.1 La présente politique s'applique à l'ensemble des unités organisationnelles, des processus métier, des systèmes, des membres du personnel et des engagements avec des tiers intervenant dans le traitement, le développement, le stockage ou la gestion des actifs informationnels.

2.2 Le champ d'application couvre les actifs physiques, numériques et hébergés dans le cloud, y compris les données structurées et non structurées, les applications, les infrastructures, les réseaux et les services.

2.3 Elle couvre les risques de sécurité de l'information aux niveaux stratégique, opérationnel, projet et technique, et s'impose à tous les employés, prestataires et prestataires de services participant aux activités du SMSI.

2.4 La gestion des risques doit être appliquée aux scénarios suivants :

2.4.1 Mise en œuvre d'un nouveau projet ou d'un nouveau système

2.4.1.1 Changements significatifs (par ex. architecture, propriété, processus)

2.4.1.2 Intégration d'un fournisseur et accords avec des tiers

2.4.1.3 Réponse aux incidents et revues post-incident

2.4.1.4 Revues périodiques des risques organisationnels ou audits

3. Objectifs

3.1 Établir et mettre en œuvre un processus de gestion des risques reproductible à l'échelle de l'organisation, fondé sur les méthodologies ISO/IEC 27005 et ISO 31000.

3.2 Garantir que les risques sont identifiés, analysés, évalués et traités au moyen de méthodes structurées et traçables, y compris l'attribution de propriétaires de risques et l'articulation avec les mesures de sécurité.

3.3 Maintenir un registre des risques centralisé ainsi qu'un plan de traitement des risques soumis à gestion de versions, reflétant l'état actuel des risques, la couverture des mesures de sécurité et l'avancement des mesures d'atténuation.

3.4 Aligner les décisions relatives aux risques sur l'appétence au risque documentée et les niveaux de tolérance définis, et permettre des décisions de gouvernance éclairées en matière d'acceptation, d'atténuation, de transfert ou d'évitement du risque.

3.5 Surveiller en continu les tendances de risque et garantir l'efficacité des traitements des risques, tout en permettant des ajustements proactifs en fonction de l'évolution des menaces ou des changements métier.

4. Rôles et responsabilités

4.1 Haute direction / conseil d'administration

4.1.1 Approuve le cadre de gestion des risques et définit l'appétence au risque acceptable ainsi que les seuils de tolérance.

4.1.2 Autorise les stratégies de traitement des risques pour les risques résiduels dépassant la tolérance.

4.1.3 Alloue les ressources nécessaires et assure la supervision du fonctionnement efficace du programme de gestion des risques.

4.2 Responsable du SMSI / Responsable des risques

4.2.1 Est propriétaire de la présente politique et en assure l'alignement avec les normes ISO/IEC 27001 et 27005.

4.2.2 Pilote le processus d'évaluation des risques de l'organisation et tient à jour le registre des risques et le plan de traitement.

4.2.3 Garantit les revues périodiques et l'escalade des risques majeurs vers la haute direction ou le comité de pilotage du SMSI.

[... 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 et le cadre associé doivent faire l'objet d'une revue annuelle, ou :

9.1.1 Après un événement de risque majeur ou un incident de sécurité

9.1.2 À la suite d'un changement organisationnel ou technique significatif

9.1.3 En réponse à des constats d'audit ou à de nouvelles exigences réglementaires

9.2 Le Responsable du SMSI, le Responsable des risques et l'équipe Conformité sont conjointement responsables de :

9.2.1 Initier le cycle de revue

9.2.2 Recueillir les contributions des unités métier

9.2.3 Réviser les procédures et les seuils si nécessaire

9.3 Toutes les révisions doivent être :

9.3.1 Soumises à gestion de versions et consignées

9.3.2 Approuvées par la haute direction

9.3.3 Communiquées aux parties prenantes

9.3.4 Conservées dans le référentiel d'audit pendant une durée minimale de 5 ans

10. Politiques connexes et articulations

10.1 La présente politique est interdépendante avec les politiques de sécurité de l'information suivantes :

10.1.1 P1 – Politique de sécurité de l'information : définit le modèle global de gouvernance de la sécurité dans lequel s'inscrit la présente politique de gestion des risques.

10.1.2 P2 – Politique relative aux rôles et responsabilités de gouvernance : définit les responsables désignés et les niveaux de gouvernance référencés dans la matrice d'escalade des risques.

10.1.3 P5 – Politique de gestion des changements : déclenche la réévaluation des risques pour les changements d'infrastructure et les changements organisationnels.

10.1.4 P13 – Politique de classification et d'étiquetage des données : soutient l'évaluation de l'impact lors de l'identification des risques.

10.1.5 P33 – Politique de surveillance de l'audit et de la conformité : valide le respect de la politique, y compris l'exhaustivité du registre des risques et les éléments probants des traitements.

11. Normes et référentiels de référence

11.1 La présente politique est explicitement alignée sur les normes et référentiels suivants afin de satisfaire aux bonnes pratiques internationales et aux attentes réglementaires en matière de gestion des risques de sécurité de l'information :

11.2 ISO/IEC 27001 :

11.2.1 Clause 6.1 : établit les exigences relatives à l'identification des risques et des opportunités, y compris l'ensemble du cycle de vie des évaluations et des traitements des risques de sécurité de l'information. La présente politique met en œuvre les clauses 6.1.2 et 6.1 au moyen d'un cadre structuré imposant des protocoles documentés pour l'identification, l'analyse, l'évaluation, le traitement et l'acceptation du risque résiduel.

11.2.2 Clause 8.32 : l'intégration d'une approche fondée sur les risques dans les processus de gestion des changements garantit que tout changement organisationnel significatif déclenche une réévaluation formelle des risques.

11.2.3 Clause 10 : l'amélioration continue est intégrée au moyen de revues régulières de la politique, de l'analyse des tendances de risque et de mises à jour de la SoA guidées par les enseignements tirés de l'analyse des risques.

11.3 ISO/IEC 27005 :

11.3.1 Fournit des orientations spécialisées et détaillées sur la gestion des risques de sécurité de l'information. La présente politique met en œuvre l'ensemble du modèle de processus de risque ISO/IEC 27005 : établissement du contexte, identification des risques, analyse des risques,

évaluation des risques, traitement des risques, acceptation du risque, communication sur les risques, surveillance et revue des risques.

11.4 ISO 31000 :

11.4.1 La présente politique intègre les principes de l'ISO 31000, notamment l'engagement de la direction, l'intégration à la prise de décision et l'amélioration continue. Elle garantit que la gestion des risques est intégrée à la culture et aux opérations de l'organisation.

11.5 NIST SP 800-30 Rev.1 :

11.5.1 S'aligne sur le guide du NIST relatif à la conduite des évaluations des risques, y compris l'identification des menaces, l'analyse des vulnérabilités, l'estimation de la vraisemblance et la détermination de l'impact. La structure de la présente politique reflète les étapes d'évaluation des risques définies par le NIST et les adapte aux processus techniques et métier.

11.6 NIST SP 800-39 :

11.6.1 Soutient la gouvernance des risques au niveau de l'entreprise, en mettant l'accent sur une gestion des risques à plusieurs niveaux aux échelons de l'organisation, de la mission/du processus métier et du système d'information. La politique garantit que la propriété des risques est clairement définie à tous les niveaux et inclut des stratégies de traitement au niveau organisationnel.

11.7 RGPD de l'UE :

11.7.1 Article 24 : exige la mise en œuvre de mesures techniques et organisationnelles appropriées afin de garantir une gestion adéquate des risques liés à la protection des données, ce qui est traité par le processus de risque structuré défini dans la présente politique.

11.7.2 Article 25 : la « protection des données dès la conception et par défaut » s'aligne avec l'intégration du traitement des risques dans la conception des systèmes et des processus.

11.7.3 Article 32 : impose une approche fondée sur les risques pour les mesures de sécurité, satisfaite au moyen d'évaluations des risques fondées sur l'impact et de la sélection des mesures de sécurité fondée sur les risques.

11.8 Directive NIS2 de l'UE :

11.8.1 Article 21(2)(a–d) : exige des entités qu'elles réalisent des évaluations des risques, mettent en œuvre des politiques d'analyse des risques et assurent des mesures de sécurité proportionnées. La présente politique répond à ces obligations par l'application continue du cycle de vie des risques et une gouvernance documentée.

11.9 DORA de l'UE :

11.9.1 Article 5 : impose un cadre documenté de gestion des risques liés aux TIC, entièrement couvert par l'architecture de la présente politique, y compris l'articulation avec la SoA et les KRI.

11.9.2 Article 6 : exige l'intégration de la gestion des risques dans les stratégies de résilience opérationnelle, ce qui est traité au moyen de matrices d'escalade et du suivi des actifs critiques.

11.10 COBIT 2019 :

11.10.1 APO12 – Manage Risk : correspond directement à la mise en place par l'organisation d'une approche structurée de gestion des risques, avec attribution des rôles, suivi des traitements et responsabilité au niveau du conseil d'administration.

11.10.2 MEA01 – Monitor, Evaluate and Assess Performance and Conformance : se reflète dans l'accent mis par la présente politique sur l'analyse des tendances, la surveillance des KRI et l'intégration des retours d'audit dans les boucles d'amélioration continue.