					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P41					Titre du document : **Politique de gestion des risques de dépendance aux fournisseurs**							
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 la réglementation

Norme/Réglementation	Clause/Article	Commentaire
ISO/IEC 27001:2022	6.1.3, 8.1, 9.1	
ISO/IEC 27002:2022	5.20, 5.21, 5.22, 5.23, 5.30	
NIST SP 800-53 Rev.5	SR-2, SR-3, SR-5, SR-6, SR-11, RA-3	
RGPD de l'UE	Art. 28, Art. 32(1)(d)	
NIS2 de l'UE	Art. 21(2)(d), Art. 21(3), Art. 22	
DORA de l'UE	Art. 28–30	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. Objet

1.1 Renforcer les pratiques de sécurité de la chaîne d'approvisionnement de l'organisation en mettant en place un processus d'identification et de gestion des dépendances critiques vis-à-vis des fournisseurs et des prestataires de services, conformément à l'article 21(3) de NIS2 et aux évaluations des risques de la chaîne d'approvisionnement menées au niveau de l'Union.

1.2 Veiller à ce que les risques résultant d'une concentration ou d'une dépendance à un fournisseur unique soient compris et atténués, et à ce que tout risque sectoriel propre à la chaîne d'approvisionnement (tel que signalé par les autorités au titre de l'article 22 de NIS2) soit intégré à notre gestion des risques de sécurité de l'information et à notre planification de la continuité d'activité.

2. Champ d'application

2.1 La présente politique s'applique à l'ensemble des fournisseurs critiques et des prestataires de services sur lesquels l'organisation s'appuie pour ses opérations critiques, en particulier au sein de la chaîne d'approvisionnement TIC (matériel, logiciels, cloud, télécommunications, services managés).

2.2 Elle couvre les fonctions internes, notamment les Achats, la gestion des fournisseurs, la gestion des risques et les départements opérationnels concernés. Elle implique également ces fournisseurs eux-mêmes dans la mesure nécessaire à la collecte d'informations sur les risques. Les « fournisseurs critiques » sont ceux dont la défaillance ou la compromission pourrait affecter de manière significative notre capacité à fournir des services ou à respecter nos obligations légales.

3. Objectifs

3.1 Obtenir une visibilité sur les dépendances de la chaîne d'approvisionnement, en particulier afin d'identifier les points de défaillance uniques ou les risques de concentration élevés dans notre panel de fournisseurs (par exemple, une dépendance à un seul fournisseur cloud pour l'ensemble des services).

3.2 Mettre en œuvre des mesures visant à réduire et à maîtriser les risques liés aux fournisseurs, telles que la diversification, les plans de contingence ou l'exigence d'un renforcement des contrôles chez les fournisseurs, afin d'accroître la résilience face aux défaillances de fournisseurs ou aux attaques provenant de la chaîne d'approvisionnement.

3.3 Se conformer aux exigences de NIS2 en intégrant, dans les décisions de risque de l'organisation, les résultats de toute évaluation coordonnée des risques de sécurité portant sur des chaînes

d’approvisionnement critiques (au titre de l’article 22), et en veillant à ce que notre propre démarche de gestion des risques de la chaîne d’approvisionnement soit documentée et démontrable.

4. Rôles et responsabilités

4.1 Bureau de gestion des fournisseurs (Vendor Management Office - VMO) : tient le registre des dépendances fournisseurs et coordonne les évaluations des risques. Veille à ce que, lors de l’intégration puis périodiquement par la suite, chaque fournisseur clé fasse l’objet d’une évaluation de criticité et du niveau de dépendance.

4.2 Gestion des risques (Comité des risques de l’entreprise) : effectue la revue des analyses de risque de concentration et de dépendance, valide les stratégies de traitement des risques (par exemple, approuver l’ajout d’un fournisseur alternatif ou le maintien d’un stock supplémentaire de composants critiques). Intègre le risque lié à la chaîne d’approvisionnement dans le registre global des risques et en rend compte à la haute direction.

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

9. Surveillance et audit

9.1 Le registre des dépendances et les évaluations des risques feront l’objet d’un audit interne sur une base annuelle. L’audit interne vérifiera que tous les fournisseurs critiques sont répertoriés, que leurs niveaux de risque sont à jour et que des plans d’atténuation sont en place et progressent. Il vérifiera également que les apports externes en matière d’évaluation des risques (rapports au titre de l’article 22, etc.) ont bien été pris en compte.

9.2 L’efficacité des mesures de diversification et de contingence doit être testée périodiquement. Par exemple, une simulation planifiée peut être menée en supposant la défaillance d’un fournisseur majeur, afin de tester nos plans de continuité et nos dispositifs alternatifs (à l’instar d’un exercice de reprise après sinistre, mais appliqué à l’indisponibilité d’un fournisseur). Les résultats de ces tests doivent être documentés et toute défaillance corrigée.

9.3 Indicateurs : la fonction de gestion des risques suivra des indicateurs tels que « % des services critiques disposant d’au moins un fournisseur ou d’une solution alternative » ou « Top 5 des dépendances fournisseurs et leur tendance de risque ». Ces indicateurs doivent être intégrés dans les tableaux de bord des risques destinés à la direction. Une tendance à la baisse du risque de dépendance dans le temps constitue un objectif ; si les indicateurs montrent une dépendance croissante, cela doit déclencher une revue de direction.

10. Revue et maintenance

10.1 La présente politique fera l’objet d’une revue au moins annuelle par les équipes de gestion des fournisseurs et de gestion des risques. Cette revue prendra en compte toute évolution du paysage fournisseurs (par exemple, si un nouveau fournisseur devient critique ou si un ancien fournisseur est progressivement retiré) ainsi que toute nouvelle exigence réglementaire relative à l’externalisation ou au risque lié aux tiers.

10.2 Si les autorités sectorielles publient des orientations mises à jour ou si un incident révèle des lacunes (par exemple, si l’indisponibilité d’un fournisseur a eu un impact plus important que prévu, indiquant que notre évaluation des risques a sous-estimé la dépendance), la politique doit être mise à jour afin d’affiner les critères ou les stratégies d’atténuation.

10.3 Les versions révisées de la politique doivent être approuvées par la haute direction. Les changements significatifs doivent être communiqués à tous les départements concernés, et les supports de formation doivent être mis à jour en conséquence afin de refléter les nouvelles procédures ou normes.

11. Politiques associées et articulations

11.1 P01 – Politique de sécurité de l'information. Attribue la responsabilité de la gouvernance des dépendances fournisseurs.

11.2 P02 – Politique relative aux rôles et responsabilités de gouvernance. Clarifie l'attribution des responsabilités pour les décisions relatives au risque fournisseur.

11.3 P06 – Politique de gestion des risques. Intègre le risque de concentration dans les registres des risques de l'organisation.

11.4 P26 – Politique de sécurité des fournisseurs. Définit le référentiel minimal de sécurité ; la P41 ajoute des contrôles relatifs à la dépendance et à la concentration.

11.5 P27 – Politique d'utilisation du cloud. Applique les critères de dépendance à l'adoption des services cloud et aux plans de sortie.

11.6 P28 – Politique de développement externalisé. Couvre les risques de dépendance liés à l'ingénierie externalisée.

11.7 P32 – Politique de continuité d'activité et de reprise après sinistre. Prévoit les scénarios d'indisponibilité ou de substitution de fournisseurs.

11.8 P37 – Politique de conformité juridique et réglementaire. Garantit que les contrats et obligations intègrent les contrôles relatifs à la dépendance.

12. Références

12.1 Directive NIS2 (UE 2022/2555), article 21(3) (imposant la prise en compte des vulnérabilités propres à chaque fournisseur direct/prestataire de services direct ainsi que de la qualité de leur cybersécurité, y compris les résultats des évaluations coordonnées des risques de la chaîne d'approvisionnement)

12.2 Directive NIS2, article 22(1) (évaluations coordonnées des risques de sécurité au niveau de l'Union portant sur les chaînes d'approvisionnement critiques — informe les entités des risques fournisseurs à l'échelle sectorielle)

12.3 Règlement d'exécution (UE) 2024/2690 de la Commission, section 5 de l'annexe (exigences de sécurité de la chaîne d'approvisionnement applicables aux entités, y compris les critères de sélection des fournisseurs, la diversification et les obligations contractuelles)

12.4 ENISA Good Practices for Supply Chain Cybersecurity (2022) – recommandations relatives à l'identification des fournisseurs critiques et à la gestion des risques associés

12.5 ISO/IEC 27001:2022 / ISO/IEC 27002:2022