COMMISSION
EUROPÉENNE

Bruxelles, le 3.6.2026
COM(2026) 502 final

ANNEXES 1 to 3

ANNEXES

du

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

établissant un cadre de mesures pour renforcer l'écosystème européen de l'informatique en nuage et de l'IA (règlement sur le développement de l'informatique en nuage et de l'IA)

{SEC(2026) 502 final} - {SWD(2026) 502 final} - {SWD(2026) 503 final}

ANNEXE I

GRANDS DEFIS

1. Grand défi nº 1: durabilité environnementale, performance et sécurité des centres de données de l'Union

Tester et déployer des technologies permettant aux centres de données dans l'ensemble de l'Union de dépasser les niveaux les plus avancés en matière d'efficacité énergétique et d'utilisation efficace des ressources.

Il s'agit notamment d'abaisser le coefficient d'efficacité de l'utilisation de l'énergie (PUE) et de permettre des taux d'utilisation des serveurs nettement plus élevés. Par exemple:

(1) ***abaisser le coefficient moyen d'efficacité de l'utilisation de l'énergie***: améliorer la durabilité environnementale et les performances des centres de données en nuage et de périphérie de l'Union pour atteindre un coefficient moyen d'efficacité de l'utilisation de l'énergie (PUE) de 1,15 dans l'ensemble de l'Union. Les principaux axes d'action consistent notamment à favoriser le développement:

   (a) de technologies avancées en matière d'efficacité énergétique des centres de données, telles que le refroidissement et la récupération de la chaleur fatale;

   (b) de technologies d'informatique quantique pour l'exploitation des infrastructures en nuage et des infrastructures de calcul;

   (c) de l'intégration au réseau et de systèmes avancés de gestion de l'énergie;

   (d) de lignes pilotes pour la validation de technologies à haut rendement énergétique de nouvelle génération à l'échelle opérationnelle;

(2) ***augmenter les taux moyens d'utilisation des serveurs dans les centres de données***: faire progresser les taux moyens d'utilisation des serveurs dans les centres de données de l'Union afin de tendre vers 50 %, en intégrant, par exemple, des technologies fondées sur l'IA pour la gestion dynamique de l'utilisation des serveurs, pour la gestion et l'ordonnancement en temps réel de la charge de travail ou pour équilibrer l'utilisation, le coût de l'énergie, les contraintes thermiques et les exigences en matière de latence;

(3) ***renforcer la sécurité et la résilience des centres de données***: renforcer la sécurité et la résilience de la chaîne de valeur et de l'approvisionnement des centres de données en y intégrant des technologies des semi-conducteurs et des technologies quantiques conçues et fabriquées dans l'Union, et en améliorant leur résistance aux menaces physiques et aux cybermenaces, y compris les attaques ciblées.

2. Grand défi nº 2: piles technologiques pour l'informatique en nuage

Mettre en place des piles technologiques matérielles et logicielles de bout en bout pour l'informatique en nuage, comprenant des couches d'outils d'IA, d'infrastructures, de services et de gestion afin de combler les lacunes critiques de l'Union en matière de capacités.

Il s'agit notamment de mettre en place des serveurs d'IA alimentés par des semi-conducteurs et des technologies quantiques conçus et fabriqués dans l'Union, destinés à l'informatique en nuage et en périphérie distribuée et décentralisée pour l'IA.

Des programmes pilotes pourraient contribuer à démontrer les capacités des piles européennes ouvertes pour l'informatique en nuage dans des secteurs d'importance stratégique.

3. Grand défi nº 3: IA d'avant-garde

Développer la nouvelle génération de modèles et de systèmes d'IA d'avant-garde multimodaux et ouvrir la voie à des capacités d'un genre nouveau.

L'accent sera mis sur la conception architecturale et le développement de modèles et systèmes multimodaux de nouvelle génération qui repoussent les limites des capacités algorithmiques actuelles afin d'obtenir des performances supérieures en matière de raisonnement avancé, de compréhension intermodale et de capacités agentiques; l'étude d'approches novatrices en matière d'efficacité des modèles, de modélisation cognitive et de structures de calcul alternatives, etc.

Les applications potentielles pourraient inclure la recherche fondamentale, notamment la découverte scientifique et l'interprétation de données complexes, ainsi que la mise au point de modèles mondiaux pour améliorer le raisonnement, la simulation automatisée de la gestion et la planification.

4. Grand défi nº 4: IA physique

Mettre au point des modèles et des systèmes d'IA physique avancés qui fonctionnent de manière autonome et sûre pour offrir des fonctions robustes de manipulation et de navigation dans des environnements non structurés.

L'accent sera mis sur la co-conception de logiciels et de leurs architectures matérielles sous-jacentes et sur la combinaison de techniques d'IA d'avant-garde avec des modèles mondiaux soutenant le raisonnement physique pour offrir des fonctions robustes de manipulation, de navigation et d'interaction avec une supervision humaine minimale.

Les applications potentielles pourraient inclure des robots autonomes, des systèmes industriels et des drones fonctionnant dans des environnements dynamiques réels.

5. Grand défi nº 5: IA industrielle

Accélérer le développement et le déploiement de l'IA industrielle européenne dans l'ensemble des secteurs stratégiques de l'Union

L'accent sera mis sur le développement de modèles et de systèmes d'IA industrielle européens capables de répondre aux besoins d'applications industrielles à forte valeur ajoutée. Ces modèles et systèmes devraient pouvoir être adaptés à des cas d'utilisation sectoriels et permettre un déploiement sécurisé.

Les initiatives lancées dans le cadre de ce grand défi devraient s'appuyer sur des ressources informatiques et des installations d'essai spécialisées nécessaires pour valider les systèmes d'IA dans des environnements réels avant de soutenir leur déploiement et leur adoption à grande échelle, y compris aux niveaux régional et local.

Dans le secteur automobile, ces initiatives peuvent faciliter le développement et le déploiement de plateformes logicielles innovantes et de modèles d'IA pour la conduite automatisée, tandis que dans le secteur manufacturier, elles peuvent permettre la création de modèles spécialisés qui optimisent les processus de production. Parmi les autres secteurs stratégiques qui pourraient bénéficier de l'IA industrielle figurent les soins de santé, l'énergie, l'agroalimentaire et la défense.

6. Grand défi nº 6: modèles industriels européens coopératifs

Mettre au point des modèles et systèmes d'IA industrielle européens coopératifs pour des secteurs stratégiques en favorisant la collaboration à l'échelle industrielle européenne sans révéler les données commercialement sensibles des participants.

L'accent sera mis sur les technologies avancées de préservation de la confidentialité. Ces mécanismes comprennent des approches d'apprentissage fédéré et distribué, dans lesquelles ce sont les algorithmes qui sont amenés vers les données, et non les données qui sont transférées de manière centralisée; des environnements d'exécution sécurisés, un traitement fondé sur le chiffrement, des techniques d'anonymisation et de pseudonymisation, une compartimentation des accès, ainsi que des mesures de protection contre l'extraction d'informations commercialement sensibles à partir des modèles entraînés.

Parmi les secteurs stratégiques qui pourraient bénéficier de modèles et de systèmes d'IA industrielle européens coopératifs figurent l'aérospatial, les produits pharmaceutiques, la cybersécurité, la mobilité, les véhicules autonomes et les drones, l'énergie et la défense.

7. Grand défi nº 7: plateforme d'agents d'IA

Élaborer un cadre européen d'orchestration des agents d'IA, fournissant les intergiciels essentiels au déploiement résilient et sécurisé d'agents autonomes à grande échelle.

L'accent sera mis sur i) l'étude de paradigmes technologiques innovants qui permettent à plusieurs agents d'IA de collaborer efficacement, dépassant les capacités des systèmes autonomes tout en maintenant des normes de sécurité rigoureuses; et ii) sur la création de plateformes en nuage ouvertes et résilientes, consacrées à la gestion d'agents d'IA à grande échelle.

Les applications potentielles pourraient inclure les soins de santé (comme les applications d'aide à la décision clinique et de coordination de la recherche), la cybersécurité (comme la détection des menaces et la réaction à celles-ci), ainsi que la recherche fondamentale.

8. Grand défi nº 8: IA dans le secteur public

Mettre au point des modèles et des systèmes d'IA à partir de données de haute qualité provenant du secteur public et ciblant des domaines critiques (tels que les soins de santé, l'administration publique, l'ordre juridique et la gestion des crises, ainsi que les services publics)

L'accent sera mis sur les solutions de service public qui devraient avoir un effet positif important sur les services publics les plus critiques et qui sont mises en œuvre à différents niveaux des organisations du secteur public.

L'un des objectifs sera de permettre le partage de données et le développement de modèles d'avant-garde dans les services publics nationaux afin d'accroître l'incidence sur l'ensemble du secteur public de l'Union, y compris dans les domaines traitant des données sensibles. Des cadres de préservation de la vie privée (tels que l'apprentissage fédéré et la production de données synthétiques haute fidélité), qui permettent d'entraîner des modèles sans compromettre la confidentialité des ensembles de données sous-jacents, ainsi que des mesures visant à accélérer l'adoption à grande échelle de ces modèles, y compris aux niveaux régional et local, contribueront également à la réalisation de cet objectif.

ANNEXE II

CRITERES APPLICABLES AUX NIVEAUX D'ASSURANCE DE L'UNION

La présente annexe définit les critères auxquels doivent satisfaire les fournisseurs de services d'informatique en nuage et leurs services d'informatique en nuage pour être reconnus comme proposant des services correspondant aux niveaux d'assurance de l'Union 1, 2, 3 et 4. Aux fins des critères applicables aux niveaux d'assurance de l'Union 1, 2, 3 et 4, les «logiciels» au sens de l'article 3, point 4), du règlement (UE) 2024/2847, relèvent du champ d'application de la présente annexe et de l'annexe III du présent règlement. Le «matériel informatique» au sens de l'article 3, point 5), du règlement (UE) 2024/2847 ne relève pas du champ d'application.

1. Niveau d'assurance de l'Union 1

1.1. Pour le niveau d'assurance de l'Union 1, les fournisseurs de services d'informatique en nuage doivent remplir les critères cumulatifs suivants:

(a) le fournisseur de services d'informatique en nuage est établi dans l'Union;

(b) l'infrastructure et les actifs du fournisseur de services d'informatique en nuage, y compris ceux de ses sous-traitants qui participent à la fourniture du service, sont situés dans l'Union, sauf si l'organisme du secteur public en dispose autrement de manière explicite;

(c) les données client, y compris les métadonnées et les données de télémétrie, qui sont traitées, stockées et transférées par le fournisseur de services d'informatique en nuage et par les sous-traitants participant à la fourniture du service, restent exclusivement au sein de l'Union, sauf si l'organisme du secteur public en dispose autrement de manière explicite et à tout moment, y compris avant, pendant ou après la configuration ou l'utilisation du service;

(d) lorsque le fournisseur de services d'informatique en nuage externalise le soutien ou l'assistance technique et opérationnelle, y compris dans le cadre de tout accord ultérieur de sous-externalisation, à des fournisseurs de services tiers situés en dehors de l'Union, les mesures juridiques, techniques et organisationnelles nécessaires sont mises en œuvre pour garantir la traçabilité, la sécurité et la gouvernance de ces opérations et ces opérations ne compromettent en aucune manière l'autonomie opérationnelle du fournisseur de services d'informatique en nuage;

(e) le fournisseur de services d'informatique en nuage démontre que le service respecte les normes de cybersécurité les plus récentes;

(f) le fournisseur de services d'informatique en nuage garantit une transparence totale quant au recours à des sous-traitants. Le fournisseur de services d'informatique en nuage soumet les sous-traitants à des obligations de diligence raisonnable, à des obligations contractuelles et à une surveillance continue afin de respecter les obligations légales de l'Union;

(g) lorsque le fournisseur de services d'informatique en nuage est soumis au contrôle d'un pays tiers ou d'une entité juridique établie dans un pays tiers, le fournisseur de services d'informatique en nuage garantit qu'il n'existe aucune législation ou pratique en vigueur dans ce pays tiers, démontrée par des sources indépendantes, exigeant du fournisseur de services d'informatique en nuage qu'il communique des informations sur les vulnérabilités logicielles aux autorités de ce pays tiers avant qu'il ne soit établi que ces vulnérabilités ont été exploitées.

1.2. Pour le niveau d'assurance de l'Union 1, les sous-traitants visés au premier alinéa doivent être des sous-traitants qui sont des tiers ayant une relation contractuelle directe avec le fournisseur de services d'informatique en nuage et contribuant à la fourniture du service d'informatique en nuage.

2. Niveau d'assurance de l'Union 2

2.1. Pour le niveau d'assurance de l'Union 2, les fournisseurs de services d'informatique en nuage doivent remplir les critères cumulatifs suivants:

(a) le fournisseur audité et les sous-traitants qui participent à la fourniture du service audité sont établis dans l'Union;

(b) l'infrastructure, les actifs et le personnel du fournisseur audité, y compris ceux de ses sous-traitants qui participent à la fourniture du service, sont situés dans l'Union;

(c) les données client, y compris les métadonnées et les données de télémétrie, qui sont traitées, stockées et transférées par le fournisseur audité et par les sous-traitants participant à la fourniture du service, restent exclusivement au sein de l'Union, sauf si l'organisme du secteur public en dispose autrement de manière explicite et à tout moment, y compris avant, pendant ou après la configuration ou l'utilisation du service;

(d) si l'organisme du secteur public détermine qu'il est nécessaire d'imposer des exigences supplémentaires en matière de sélection du personnel et de citoyenneté de l'Union, le fournisseur audité devrait veiller à ce que le personnel satisfaisant à ces exigences soit disponible;

(e) le service audité obtient un certificat de cybersécurité européen d'un niveau d'assurance au moins «substantiel» dans le cadre d'un schéma européen de certification de cybersécurité couvrant les services d'informatique en nuage qui doit être établi en vertu du règlement (UE) 2019/881, à condition qu'un tel schéma ait été établi en vertu dudit règlement et soit mis à la disposition des fournisseurs de services d'informatique en nuage. Jusqu'à la mise en place d'un tel schéma, les schémas nationaux de certification de cybersécurité s'appliquent, lorsqu'ils existent. En l'absence de schémas de certification de cybersécurité nationaux ou de l'Union, le fournisseur audité doit démontrer que le service respecte les normes de cybersécurité les plus élevées en vertu du droit de l'Union applicable;

(f) les données générées par l'utilisation du service audité ne sont pas utilisées pour entraîner ou affiner un système d'IA exploité par un pays tiers ou une entité juridique établie dans un pays tiers, et ne sont en aucun cas transférées en dehors de l'Union;

(g) si le fournisseur audité et les sous-traitants qui participent à la fourniture du service audité sont soumis au contrôle d'un pays tiers ou d'une entité juridique établie dans un pays tiers, ils démontrent que les mesures juridiques, techniques et organisationnelles nécessaires ont été mises en œuvre pour garantir que:

i. le contrôle du pays tiers ou de l'entité juridique établie dans un pays tiers sur le fournisseur audité n'est pas exercé d'une manière qui limite ou restreint la capacité du fournisseur à exécuter et à fournir le service, impose des limitations à l'infrastructure, aux actifs et au personnel nécessaires à la fourniture du service, ou compromet les capacités et les normes nécessaires à la fourniture du service audité;

ii. l'accès d'un pays tiers ou d'une entité juridique établie dans un pays tiers aux données client est empêché;

iii. la possibilité d'une interruption de la continuité du service et/ou d'une dégradation de la qualité du service par un pays tiers ou une entité juridique établie dans un pays tiers est empêchée;

iv. le contrôle exercé par le pays tiers ou l'entité juridique établie dans un pays tiers sur le fournisseur audité ne l'est pas de manière à obliger ce dernier à mettre en œuvre, à appliquer, à faire respecter ou à se conformer à des mesures restrictives telles que des régimes de sanctions, des embargos ou toute mesure juridique ou administrative équivalente adoptée par un pays tiers, à moins que ces mesures ne soient légitimes au regard du droit national des États membres ou du droit de l'Union;

(h) le soutien ou l'assistance technique et opérationnelle liés au service audité, y compris les accords de sous-traitance ultérieurs, sont mis en place et exécutés exclusivement au sein de l'Union;

(i) le fournisseur audité démontre que les mesures suivantes relatives à la chaîne d'approvisionnement des logiciels sont en place:

i. une nomenclature des logiciels complète et à jour, telle que définie à l'article 3, point 39), du règlement (UE) 2024/2847, et une liste des dépendances recensées pertinentes pour la fourniture du service sont documentées et mises à la disposition de l'organisme d'audit;

ii. lorsque des composants logiciels, tels que définis à l'article 3, point 6), du règlement (UE) 2024/2847, ou des produits sont fournis, détenus et concédés sous licence par une entité juridique établie dans un pays tiers, des contrôles sont mis en œuvre et documentés afin de bloquer toute fonctionnalité à distance susceptible d'altérer ou de perturber de manière substantielle un appareil, un système ou un logiciel (y compris lors des mises à jour) et de veiller à ce que les composants pertinents pour la sécurité provenant de fabricants de logiciels de pays tiers, tels que définis à l'article 3, point 13), du règlement (UE) 2024/2847, fassent l'objet d'audits du code source et disposent d'un plan de migration documenté en cas de défaillance du fournisseur ou d'imposition de restrictions par un pays tiers;

iii. lorsque le fournisseur de services d'informatique en nuage est soumis au contrôle d'un pays tiers ou d'une entité juridique établie dans un pays tiers, le fournisseur de services d'informatique en nuage garantit qu'il n'existe aucune législation ou pratique en vigueur dans ce pays tiers, démontrée par des sources indépendantes, exigeant du fournisseur de services d'informatique en nuage qu'il communique des informations sur les vulnérabilités logicielles aux autorités de ce pays tiers avant qu'il ne soit établi que ces vulnérabilités ont été exploitées;

(j) lorsqu'un logiciel mis en service dans le cadre d'une licence open source est utilisé pour la fourniture du service, le fournisseur audité démontre qu'il a mis en œuvre et documenté les contrôles appropriés pour empêcher l'utilisation de toute fonctionnalité ou de tout mécanisme à distance susceptible d'être utilisé pour altérer ou perturber de manière substantielle un appareil, un système ou un logiciel;

(k) dans la mesure où le fournisseur audité fournit ses services à l'échelle mondiale et dispose d'une filiale dans un pays tiers, il a mis en œuvre les mesures nécessaires pour garantir et assurer la séparation juridique, technique et organisationnelle effective entre la société mère dans l'Union et toute filiale située dans un pays tiers.

2.2. Pour le niveau d'assurance de l'Union 2, les sous-traitants visés au premier alinéa doivent être des sous-traitants qui sont des tiers ayant une relation contractuelle directe avec le fournisseur de services d'informatique en nuage et contribuant à la fourniture du service d'informatique en nuage.

3. Niveau d'assurance de l'Union 3

3.1. Pour le niveau d'assurance de l'Union 3, les fournisseurs de services d'informatique en nuage doivent remplir les critères cumulatifs suivants:

(a) le fournisseur audité et les sous-traitants qui participent à la fourniture du service audité sont établis dans l'Union;

(b) l'infrastructure, les actifs et le personnel du fournisseur audité, y compris ceux des sous-traitants qui participent à la fourniture du service, sont situés dans l'Union;

(c) les données client, y compris les métadonnées et les données de télémétrie, qui sont traitées, stockées et transférées par le fournisseur audité et par les sous-traitants participant à la fourniture du service, restent exclusivement au sein de l'Union, sauf si l'organisme du secteur public en dispose autrement de manière explicite et à tout moment, y compris avant, pendant ou après la configuration ou l'utilisation du service;

(d) le personnel, y compris le personnel des sous-traitants participant à la fourniture du service audité, possède la citoyenneté de l'Union et, le cas échéant, doit également disposer de l'habilitation de sécurité nationale nécessaire délivrée par un État membre lorsqu'il traite des informations classifiées, telles que définies à l'article 2, point 21), du règlement (UE) 2021/697;

(e) le service audité obtient un certificat de cybersécurité européen d'un niveau d'assurance au moins «substantiel» dans le cadre d'un schéma européen de certification de cybersécurité couvrant les services d'informatique en nuage qui doit être établi en vertu du règlement (UE) 2019/881, à condition qu'un tel schéma ait été établi en vertu dudit règlement et soit mis à la disposition des fournisseurs de services d'informatique en nuage. Jusqu'à la mise en place d'un tel schéma, les schémas nationaux de certification de cybersécurité s'appliquent, lorsqu'ils existent. En l'absence de schémas de certification de cybersécurité nationaux ou de l'Union, le fournisseur audité doit démontrer que le service respecte les normes de cybersécurité les plus élevées en vertu du droit de l'Union applicable;

(f) les données générées par l'utilisation du service audité ne sont pas utilisées pour entraîner ou affiner un système d'IA exploité par un pays tiers ou une entité juridique établie dans un pays tiers, et ne sont en aucun cas transférées en dehors de l'Union;

(g) le fournisseur audité et les sous-traitants qui participent à la fourniture du service audité ne sont pas soumis au contrôle d'un pays tiers ou d'une entité juridique établie dans un pays tiers. Par dérogation à ce critère, un fournisseur de services d'informatique en nuage et ses sous-traitants qui participent à la fourniture du service audité et qui sont soumis au contrôle d'un pays tiers ou d'une entité juridique établie dans un pays tiers peuvent faire l'objet d'un audit pour le niveau d'assurance de l'Union 3 lorsque la Commission a adopté un acte d'exécution en vertu de l'article 19. Lorsque la Commission a adopté un acte d'exécution en vertu de l'article 19, le fournisseur audité et les sous-traitants qui participent à la fourniture du service audité doivent également démontrer que les mesures juridiques, techniques et organisationnelles nécessaires ont été mises en œuvre pour garantir que:

i. le contrôle du pays tiers ou de l'entité juridique établie dans un pays tiers sur le fournisseur audité n'est pas exercé d'une manière qui limite ou restreint la capacité du fournisseur à exécuter et à fournir le service, impose des limitations à l'infrastructure, aux actifs et au personnel nécessaires à la fourniture du service, ou compromet les capacités et les normes nécessaires à la fourniture du service audité. Le fournisseur audité devrait permettre un accès raisonnable au code;

ii. l'accès d'un pays tiers ou d'une entité juridique établie dans un pays tiers aux données client est empêché;

iii. la possibilité d'une interruption de la continuité du service et/ou d'une dégradation de la qualité du service par un pays tiers ou une entité juridique établie dans un pays tiers est empêchée;

iv. le contrôle exercé par le pays tiers ou l'entité juridique établie dans un pays tiers sur le fournisseur audité ne l'est pas de manière à obliger ce dernier à mettre en œuvre, à appliquer, à faire respecter ou à se conformer à des mesures restrictives telles que des régimes de sanctions, des embargos ou toute mesure juridique ou administrative équivalente adoptée par un pays tiers, à moins que ces mesures ne soient légitimes au regard du droit national des États membres ou du droit de l'Union;

(h) le soutien ou l'assistance technique et opérationnelle liés au service audité, y compris les accords de sous-traitance ultérieurs, sont mis en place et exécutés exclusivement au sein de l'Union, par du personnel résidant dans l'Union et par des tiers qui ne sont pas soumis au contrôle d'un pays tiers ou d'une entité juridique établie dans un pays tiers;

(i) le fournisseur audité démontre que les mesures suivantes relatives à la chaîne d'approvisionnement des logiciels sont en place:

i. une nomenclature des logiciels complète et à jour et une liste des dépendances recensées pertinentes pour la fourniture du service sont documentées et mises à la disposition de l'organisme d'audit;

ii. lorsque des composants logiciels ou des produits sont fournis, détenus et concédés sous licence par une entité juridique établie dans un pays tiers, des contrôles sont mis en œuvre et documentés afin de bloquer toute fonctionnalité à distance susceptible d'altérer ou de perturber de manière substantielle un appareil, un système ou un logiciel (y compris lors des mises à jour) et de veiller à ce que les composants pertinents pour la sécurité provenant de fabricants de pays tiers fassent l'objet d'audits du code source et disposent d'un plan de migration documenté en cas de défaillance du fournisseur ou d'imposition de restrictions par un pays tiers;

iii. lorsque le fournisseur de services d'informatique en nuage est soumis au contrôle d'un pays tiers ou d'une entité juridique établie dans un pays tiers, le fournisseur de services d'informatique en nuage garantit qu'il n'existe aucune législation ou pratique en vigueur dans ce pays tiers, démontrée par des sources indépendantes, exigeant du fournisseur de services d'informatique en nuage qu'il communique des informations sur les vulnérabilités logicielles aux autorités de ce pays tiers avant qu'il ne soit établi que ces vulnérabilités ont été exploitées;

(j) lorsqu'un logiciel mis en service dans le cadre d'une licence open source est utilisé pour la fourniture du service, le fournisseur audité démontre qu'il a mis en œuvre et documenté les contrôles appropriés pour empêcher l'utilisation de toute fonctionnalité ou de tout mécanisme à distance susceptible d'être utilisé pour altérer ou perturber de manière substantielle un appareil, un système ou un logiciel;

(k) dans la mesure où le fournisseur audité fournit ses services en dehors de l'Union et dispose d'une filiale dans un pays tiers, il démontre qu'il a mis en œuvre les mesures nécessaires pour garantir et assurer la séparation juridique, technique et organisationnelle effective entre la société mère dans l'Union et toute filiale située dans un pays tiers.

3.2. Pour le niveau d'assurance de l'Union 3, les sous-traitants visés au premier alinéa doivent être des sous-traitants qui sont des tiers ayant une relation contractuelle directe avec le fournisseur de services d'informatique en nuage, contribuant à la fourniture du service d'informatique en nuage et pouvant avoir besoin d'accéder à des informations classifiées ou sensibles, telles que définies à l'article 2, point 22), du règlement (UE) 2021/697.

4. Niveau d'assurance de l'Union 4

4.1. Pour le niveau d'assurance de l'Union 4, les fournisseurs de services d'informatique en nuage doivent remplir les critères cumulatifs suivants:

(a) le fournisseur audité et les sous-traitants qui participent à la fourniture du service audité sont établis dans l'Union;

(b) l'infrastructure, les actifs et le personnel du fournisseur audité, y compris ceux des sous-traitants qui participent à la fourniture du service, sont situés dans l'Union;

(c) les données client, y compris les métadonnées et les données de télémétrie qui, selon une évaluation des risques, sont considérées comme sensibles, et qui sont traitées, stockées et transférées par le fournisseur audité et par les sous-traitants participant à la fourniture du service, restent exclusivement au sein de l'Union et à tout moment, y compris avant, pendant ou après la configuration ou l'utilisation du service;

(d) le personnel, y compris le personnel des sous-traitants participant à la fourniture du service audité, possède la citoyenneté de l'Union et, le cas échéant, doit également disposer de l'habilitation de sécurité nationale nécessaire délivrée par un État membre lorsqu'il traite des informations classifiées;

(e) le service audité obtient un certificat de cybersécurité européen d'un niveau d'assurance au moins «élevé» dans le cadre d'un schéma européen de certification de cybersécurité couvrant les services d'informatique en nuage qui doit être établi en vertu du règlement (UE) 2019/881, à condition qu'un tel schéma ait été établi en vertu dudit règlement et soit mis à la disposition des fournisseurs de services d'informatique en nuage. Jusqu'à la mise en place d'un tel schéma, les schémas nationaux de certification de cybersécurité s'appliquent, lorsqu'ils existent. En l'absence de schémas de certification de cybersécurité nationaux ou de l'Union, le fournisseur audité doit démontrer que le service respecte les normes de cybersécurité les plus élevées en vertu du droit de l'Union applicable;

(f) les données générées par l'utilisation du service audité ne sont pas utilisées pour entraîner ou affiner un système d'IA exploité par un pays tiers ou une entité juridique établie dans un pays tiers, et ne sont en aucun cas transférées en dehors de l'Union;

(g) le fournisseur audité et les sous-traitants qui participent à la fourniture du service audité ne sont pas soumis au contrôle d'un pays tiers ou d'une entité juridique établie dans un pays tiers;

(h) le soutien ou l'assistance technique et opérationnelle liés au service audité, y compris les accords de sous-traitance ultérieurs, sont mis en place et exécutés exclusivement au sein de l'Union, par du personnel résidant dans l'Union et par des tiers qui ne sont pas soumis au contrôle d'un pays tiers ou d'une entité juridique établie dans un pays tiers;

(i) le fournisseur audité démontre que les mesures suivantes relatives à la chaîne d'approvisionnement des logiciels sont en place:

i. une nomenclature des logiciels complète et à jour et une liste des dépendances recensées pertinentes pour la fourniture du service sont documentées et mises à la disposition de l'organisme d'audit;

ii. les mesures en place pour conserver un contrôle effectif sur les composants logiciels ou les produits en démontrant qu'un pays tiers ou une entité juridique établie dans un pays tiers n'exerce pas de contrôle effectif sur la conception, le développement, la maintenance et l'évolution de ces composants ou produits. Un contrôle efficace implique la capacité d'influer de manière substantielle sur l'évolution technique, les priorités en matière de maintenance, les mesures correctives en matière de sécurité et la continuité à long terme du composant;

(j) lorsqu'un logiciel mis en service dans le cadre d'une licence open source est utilisé, le fournisseur audité démontre qu'il a mis en œuvre et documenté les contrôles appropriés pour empêcher l'utilisation de toute fonctionnalité ou de tout mécanisme à distance susceptible d'être utilisé pour altérer ou perturber de manière substantielle un appareil, un système ou un logiciel;

(k) dans la mesure où le fournisseur audité fournit ses services en dehors de l'Union et dispose d'une filiale dans un pays tiers, il démontre qu'il a mis en œuvre les mesures nécessaires pour garantir et assurer la séparation juridique, technique et organisationnelle effective entre la société mère dans l'Union et toute filiale située dans un pays tiers.

4.2. Pour le niveau d'assurance de l'Union 4, les sous-traitants visés au premier alinéa doivent être des sous-traitants qui sont des tiers ayant une relation contractuelle directe avec le fournisseur de services d'informatique en nuage, contribuant à la fourniture du service d'informatique en nuage et pouvant avoir besoin d'accéder à des informations classifiées ou sensibles afin d'assurer la fourniture du service.

ANNEXE III

ÉLEMENTS PROBANTS AUX FINS DE LA PROCEDURE D'AUDIT

Les organismes d'audit devraient demander au fournisseur audité les éléments probants énumérés dans la présente annexe lorsqu'ils évaluent la conformité du service audité au regard des critères d'audit applicables en vertu de l'annexe II.

La présente annexe est indicative et ne limite pas les éléments probants susceptibles d'être demandés ou pris en considération par les organismes d'audit. Les auditeurs peuvent solliciter toute information supplémentaire nécessaire pour garantir une évaluation complète et précise de la conformité aux fins de la réalisation des audits. Si les éléments probants demandés peuvent être les mêmes, les aspects à analyser varient en fonction des critères propres à chaque niveau d'assurance et de leur degré de rigueur.

1. Critère d'audit A – Établissement dans l'Union

L'organisme d'audit évalue le critère d'audit énoncé au point a) de l'annexe II pour les niveaux d'assurance de l'Union 2, 3 et 4 sur la base des éléments probants suivants:

(1) tout élément probant démontrant que le fournisseur audité est constitué en société conformément au droit d'un État membre de l'Union ou autrement constitué conformément au droit des sociétés d'un État membre de l'Union;

(2) tout élément probant attestant que le siège statutaire, l'administration centrale et l'établissement principal du fournisseur audité sont établis dans l'Union;

(3) l'organisme d'audit devrait vérifier le cadre juridique de l'Union applicable au fournisseur audité et déterminer si son établissement est réel et stable, ou si le fournisseur audité peut uniquement être considéré comme un fournisseur de pays tiers proposant des services dans l'Union;

(4) l'organisme d'audit devrait vérifier si le fournisseur est légalement constitué dans un État membre de l'Union. Les éléments probants à cet égard peuvent inclure, sans s'y limiter, les extraits du registre national des sociétés, les documents attestant de la résidence fiscale, les licences d'exploitation, l'immatriculation à la TVA, la vérification de l'enregistrement du fournisseur dans le système d'interconnexion des registres du commerce (BRIS) et le système d'échange d'informations sur la TVA (VIES);

(5) l'organisme d'audit devrait vérifier la présence stable et effective du fournisseur audité dans l'Union. L'organisme d'audit devrait donc vérifier que:

  (a) des bureaux physiques ou des locaux d'exploitation existent dans l'UE (par exemple, au moyen de contrats de bail, de factures de consommation courante ou d'actes de propriété);

  (b) du personnel permanent est situé dans l'Union et que les activités d'assistance à la clientèle sont exercées dans l'Union (par exemple, au moyen de contrats de travail, de fiches de paie, de feuilles de présence du personnel);

  (c) les opérations contractuelles sont gérées dans l'Union (par exemple, au moyen de registres de gestion des activités, de registres de signalement des incidents);

  (d) les fonctions bancaires et comptables sont exercées exclusivement dans l'Union (par exemple, au moyen d'états financiers et de rapports d'audit).

(6) L’organisme d’audit devrait vérifier la présence d’unités d’établissement ou de succursales dans les États membres de l’UE (par exemple, au moyen de contrats de bail, de factures de consommation courante, d’actes de propriété, de contrats de travail, de feuilles de présence, de fiches de paie ou de bons de commande).

2. Critère d’audit B – Localisation de l’infrastructure, des actifs et du personnel

L’organisme d’audit évalue le critère d’audit énoncé au point b) de l’annexe II pour les niveaux d’assurance de l’Union 2, 3 et 4 sur la base des éléments probants suivants:

(1) Localisation de l’infrastructure

(a) Une liste comportant les informations pertinentes sur la localisation de l’infrastructure et des lieux de stockage de données utilisés pour la fourniture du service audité. Cette liste devrait inclure la localisation précise (numéro, rue, ville, code postal et pays) de l’infrastructure démontrant que tous les éléments restent situés dans l’Union pour la fourniture du service audité. Cela comprend la localisation du stockage principal, du stockage de sauvegarde, du stockage de rétablissement après sinistre et du stockage des journaux.

(b) Tout autre élément probant attestant que l’infrastructure informatique est située dans l’Union, tel que les contrats de bail, les actes de propriété, les contrats de maintenance, les contrats de service et les journaux d’accès aux installations.

(c) Des schémas de réseau et des documents d’architecture illustrant l’utilisation exclusive d’une infrastructure située dans l’Union pour le stockage et le traitement des données, y compris les données de sauvegarde et les données reproduites.

(2) Localisation des actifs

(a) Une liste et les informations pertinentes relatives aux actifs utilisés pour la fourniture du service audité, telles qu’un registre des actifs.

(b) Les éléments probants démontrant que les serveurs, les équipements et les actifs opérationnels sont situés dans l’Union, tels que des registres identifiant le serveur et sa localisation, des factures d’achat, des bons de livraison, des contrats de licence, des contrats d’abonnement ou des factures d’achat ou d’abonnement de logiciels, des factures accompagnées de preuves de livraison du matériel informatique.

(c) Les éléments probants démontrant que les capacités de fourniture du service se trouvent dans l’Union, tels que des registres de déploiement, des registres d’installation, des rapports d’état du service, des rapports de configuration, des résultats de surveillance, des registres administratifs attestant l’utilisation du service.

(3) Localisation du personnel

(a) Une liste et les informations pertinentes relatives au personnel participant à la fourniture du service audité.

(b) Des éléments probants démontrant que le personnel participant à la fourniture du service audité est situé dans l’Union, y compris les contrats de travail, les fiches de paie, les feuilles de présence, les relevés d’activité et les organigrammes démontrant que le personnel situé dans l’Union exerce des responsabilités opérationnelles.

(4) Considérations relatives à l'infrastructure, aux actifs et au personnel

(a) L'organisme d'audit devrait également évaluer si cette infrastructure, ces actifs ou ce personnel:

i. stockent, transmettent, consultent, traitent ou gèrent d'une autre manière les données clients;

ii. fournissent, permettent ou pourraient permettre l'accès administratif aux données client, le contrôle ou la configuration de ces données ou une visibilité sur celles-ci;

iii. pourraient raisonnablement, en cas de compromission, de mauvaise configuration, d'indisponibilité ou de perturbation, entraîner la perturbation ou l'indisponibilité du service audité.

***Remarque**: «Infrastructure» désigne l'infrastructure physique, y compris, sans s'y limiter, l'infrastructure des centres de données ou l'infrastructure de colocalisation, le réseau, les systèmes de refroidissement et les systèmes informatiques permettant la gestion du centre de données.*

«Actifs» désigne le matériel et les logiciels, y compris, sans s'y limiter, les bibliothèques, le réseau interne nécessaire à la communication entre les composants logiciels, le matériel cryptographique permettant la fourniture du service d'informatique en nuage.

«Personnel», y compris le personnel géré par des sous-traitants, désigne les personnes qui contribuent à la fourniture, l'administration, la sécurité, la disponibilité ou le fonctionnement du service audité.

3. Critère d'audit C – Localisation des données dans l'Union

L'organisme d'audit évalue le critère d'audit énoncé au point c) de l'annexe II pour les niveaux d'assurance de l'Union 2, 3 et 4 sur la base des éléments probants suivants:

(1) les éléments probants démontrant que les données client sont stockées et traitées exclusivement dans l'Union et que les tiers ou les sous-traitants qui ne remplissent pas les conditions prévues par la présente annexe ne sont en aucun cas en mesure, sur le plan technique ou opérationnel, d'accéder aux données client, de les obtenir, de les rendre indisponibles, de les détruire ou, plus généralement, de les traiter sans autorisation préalable. Il s'agit, par exemple, des journaux d'accès, des politiques d'accès à l'assistance, des registres d'accès privilégié, de la politique de conservation des sauvegardes, du schéma des flux de données indiquant où les données client sont stockées, traitées, reproduites et sauvegardées. En cas de traitement de données à caractère personnel, les contrats conclus avec les sous-traitants démontrant le respect du règlement (UE) 2016/679;

(2) les éléments probants, sous forme de journaux et de registres de surveillance, démontrant que toutes les données sont stockées et traitées exclusivement au sein de l'Union. Il peut s'agir, par exemple, d'accords-cadres de services, d'accords de traitement de données, d'accords contractuels relatifs à la localisation des données ou de toute limite de l'UE en matière de données;

(3) les éléments probants (tels que des accords contractuels, des journaux et des procédures proposées aux organismes du secteur public) démontrant que le fournisseur audité et les sous-traitants participant à la fourniture du service audité ont mis en place les mesures nécessaires pour garantir:

(a) qu'aucune donnée client, y compris les données chiffrées, n'est transférée en dehors de l'Union sans l'approbation d'un organisme du secteur public;

(b) qu'aucune donnée n'est transférée à un tiers autre que les sous-traitants participant à la fourniture du service ou les destinataires expressément autorisés par l'organisme du secteur public;

(4) un schéma des flux de données montrant les flux de données entre le fournisseur de services d'informatique en nuage et les données clients, ainsi qu'avec les services tiers et les sous-traitants. Le schéma doit clairement indiquer la source et la destination des données et démontrer que celles-ci ne quittent pas l'Union.

Remarque: aux fins de la présente annexe, on entend par «client» un organisme du secteur public ayant conclu un accord contractuel ou un autre accord juridiquement contraignant avec le fournisseur de services d'informatique en nuage afin d'accéder au service d'informatique en nuage ou de l'utiliser.

Les «données client» peuvent désigner toutes les données sous le contrôle du client du service d'informatique en nuage, que ce soit par des moyens juridiques, contractuels ou autres, qui sont:

(a) saisies dans le service d'informatique en nuage par le client ou en son nom, y compris les identifiants d'authentification;

(b) produites par l'utilisation du service d'informatique en nuage par le client.

Les données client peuvent également inclure les données sous le contrôle des fournisseurs audités qui sont obtenues à la suite de l'interaction du client du service d'informatique en nuage avec le service audité. Cela comprend les données clients et toutes les données résultant de l'utilisation des services d'informatique en nuage (c'est-à-dire les données de télémétrie et les métadonnées).

Les «données dérivées du service d'informatique en nuage» comprennent la partie des données de journal contenant des enregistrements relatifs à l'identité des utilisateurs du service, aux heures d'utilisation, aux fonctions utilisées, aux types de données concernés, etc. Elles peuvent également inclure des informations sur le nombre d'utilisateurs autorisés et leur identité, ainsi que toute donnée de configuration ou de personnalisation, lorsque le service d'informatique en nuage dispose de telles fonctionnalités.

4. Critère d'audit D – Citoyenneté de l'Union

L'organisme d'audit évalue le critère d'audit énoncé au point d) de l'annexe II pour les niveaux d'assurance de l'Union 2, 3 et 4 sur la base des éléments probants suivants:

(1) le fournisseur audité devrait fournir à l'organisme d'audit les éléments probants attestant qu'il a mis en œuvre les mesures permettant de garantir que, si un organisme du secteur public devait exiger la citoyenneté de l'Union, le personnel participant à la fourniture du service audité possède la citoyenneté de l'Union. Cela peut être démontré au moyen de documents officiels en cours de validité délivrés par les pouvoirs publics (par exemple, un passeport et une carte d'identité nationale en cours de validité);

(2) le fournisseur audité devrait fournir des organigrammes et des descriptions de postes confirmant qu'il peut garantir, sur demande, que seul le personnel possédant la citoyenneté de l'Union a accès à l'exploitation, à la gestion, à la maintenance et à l'assistance du service audité;

(3) le fournisseur audité devrait fournir des documents démontrant les politiques de contrôle d'accès et les pistes d'audit montrant que seul le personnel autorisé possédant la citoyenneté de l'Union peut accéder aux systèmes et aux données du service;

(4) le fournisseur audité devrait démontrer qu'il a mis en place des procédures décrivant la manière dont la citoyenneté est vérifiée avant l'affectation et dont le respect de ce critère d'audit est maintenu tout au long de l'emploi.

Remarque: *le personnel participant à la fourniture du service audité pourrait comprendre le personnel disposant d'un accès logique ou physique à l'infrastructure et aux actifs utilisés pour l'exploitation du service d'informatique en nuage, ainsi que celui chargé de l'assistance à la clientèle, et l'ensemble du personnel exerçant un contrôle de gestion sur le fournisseur de services d'informatique en nuage.*

5. Critère d'audit E – Schéma européen de certification de cybersécurité adopté en vertu du règlement (UE) 2019/881

L'organisme d'audit évalue le critère d'audit énoncé au point e) de l'annexe II pour les niveaux d'assurance de l'Union 2, 3 et 4 sur la base des éléments probants suivants:

(1) un certificat de cybersécurité européen valide délivré par un organisme d'évaluation de la conformité compétent démontrant que le service audité a été évalué et jugé conforme aux exigences correspondant aux niveaux d'assurance «élémentaire», «substantiel» ou «élevé» dans le cadre d'un schéma européen de certification de cybersécurité adopté en vertu du règlement (UE) 2019/881, pour autant qu'un tel schéma ait été établi;

(2) un rapport de certification comprenant une description des principaux composants utilisés pour le développement et l'exploitation du service d'informatique en nuage couvert par le certificat d'audit;

(3) tant que le schéma européen de certification de cybersécurité couvrant les services d'informatique en nuage n'a pas été établi, le fournisseur audité peut démontrer sa conformité au moyen de certifications de cybersécurité valides. Cela peut inclure, sans s'y limiter:

  (a) un certificat valide délivré par un organisme d'évaluation de la conformité compétent (conformément au CEN/CLC/TS 18072:2025) démontrant que le service d'informatique en nuage a été évalué et jugé conforme aux exigences correspondant aux niveaux d'assurance «élémentaire», «substantiel» ou «élevé» définis dans la norme CEN/TS 18026:2024;

  (b) un certificat valide délivré par l'autorité nationale compétente concernée démontrant que le service d'informatique en nuage a été évalué et jugé conforme aux exigences du schéma national de cybersécurité actuellement en place dans l'État membre;

  (c) en l'absence d'un schéma national, des éléments probants démontrant le respect du niveau le plus élevé de normes de cybersécurité disponibles sur le marché.

6. Critère d'audit F – Systèmes d'IA exploités par un pays tiers ou une entité juridique d'un pays tiers

L'organisme d'audit évalue le critère d'audit énoncé au point f) de l'annexe II pour les niveaux d'assurance de l'Union 2, 3 et 4 sur la base des éléments probants suivants:

(1) des clauses contractuelles stipulant que les données traitées ou générées à l'aide du service audité, y compris les données dérivées du client, les journaux et les données de télémétrie, ne seront pas utilisées pour entraîner ou affiner un modèle ou un système d'IA exploité par un pays tiers ou une entité juridique d'un pays tiers, et ne sont en aucun cas transférées en dehors de l'Union;

(2) des clauses contractuelles précisant que les données sont traitées uniquement aux fins de la fourniture du service audité et non pour des améliorations du service, du modèle ou du système ou pour toute autre finalité secondaire;

(3) des schémas de flux de données documentant le flux de données de bout en bout, couvrant l'ingestion, le stockage, le traitement et la suppression des données. Les diagrammes devraient également montrer les points de connexion entre les pipelines d'IA ou les opérations d'apprentissage automatique (MLOps) et les données des clients;

(4) des MLOps ou des registres de déploiement démontrant que les lieux de construction, d'essai et de mise en service sont situés dans l'UE;

(5) des fiches de modèle ou de système précisant le nom du modèle ou du système, sa version, ainsi que les sources d'entraînement et de validation, y compris des déclarations attestant que les données générées par l'utilisation du service audité ne quittent pas l'Union;

(6) des politiques de traçabilité des données et la documentation de mise en œuvre associée démontrant que le fournisseur exploite des outils de traçabilité et de provenance des données et qu'il peut démontrer (par enregistrement) à quelles fins les données ont été utilisées;

(7) une liste des sous-traitants (indiquant leur pays d'établissement) ayant accès aux données générées par l'utilisation du service audité.

7. Critère d'audit G – Absence de contrôle par un pays tiers ou une entité d'un pays tiers

L'organisme d'audit évalue le critère d'audit énoncé au point g) de l'annexe II pour les niveaux d'assurance de l'Union 2, 3 et 4 sur la base des éléments probants suivants:

(1) l'organisme d'audit devrait recenser et analyser:

(a) l'ensemble des actionnaires directs et indirects, jusqu'aux propriétaires ultimes;

(b) le tableau de capitalisation documentant la structure de propriété de la société;

(c) le ou les organes habilités à prendre des décisions stratégiques (assemblée générale des actionnaires, conseil de surveillance, conseil d'administration, etc.);

(d) les règles de nomination/d'élection/de révocation des organes directeurs et la composition effective de ces organes (par exemple, pour déterminer si un actionnaire a le droit de désigner un représentant au conseil d'administration ou dispose de sièges majoritaires au conseil d'administration);

(e) les quorums et la majorité requis pour adopter des décisions stratégiques, afin de déterminer si un actionnaire peut prendre une décision stratégique (soit parce qu'il dispose de la majorité requise pour approuver une telle décision, soit parce qu'il peut bloquer une telle décision au moyen d'un veto ou d'autres droits spécifiques, même s'il ne peut imposer une telle décision à lui seul, etc.);

(f) l'influence possible sur les décisions stratégiques via des liens commerciaux, des liens financiers ou d'autres moyens, etc.;

(2) le fournisseur audité devrait demander toutes les informations susmentionnées à ses sous-traitants et les mettre à la disposition de l'organisme d'audit.

7.1. Évaluation de la propriété et du contrôle:

(1) Le fournisseur audité devrait fournir à l'organisme d'audit les éléments probants suivants relatifs au siège:

(a) le lieu et l'adresse complète du siège mondial et/ou du siège social;

(b) les lieux d'implantation des structures exécutives de gestion.

(2) Le fournisseur audité devrait fournir à l'organisme d'audit les éléments probants suivants relatifs à la structure de propriété et aux droits spécifiques:

(a) une liste détaillée décrivant les propriétaires qui:

i. détiennent, directement ou indirectement, au moins 5 % du capital ou au moins 5 % des droits de vote, y compris via tout accord, entente, relation ou intermédiaire. Cela inclut les accords de vote entre actionnaires qui, ensemble, détiendraient plus de 5 % des droits de vote ou 5 % du capital;

ii. détiennent un ou plusieurs des droits spécifiques suivants en lien avec leur propriété: a) le droit de s'opposer à un transfert d'actions; b) des droits de préemption; c) le droit d'acheter des actions ou des investissements supplémentaires sous certaines conditions;

(b) l'organisme d'audit devrait demander les pièces justificatives suivantes afin d'évaluer les éléments visés au point 2 a):

i. des extraits du registre du commerce et des registres des actionnaires de l'organisation, ainsi que tout autre document pertinent indiquant clairement les actionnaires et leurs droits de vote ou leur pourcentage de participation;

ii. le pacte d'actionnaires, le protocole d'accord entre actionnaires, les statuts ou autres documents pertinents concernant les procédures décisionnelles au sein de l'entité juridique, les accords d'investissement entre actionnaires, etc.;

iii. pour tout actionnaire qui est une personne morale détenant au moins 5 % du capital ou au moins 5 % des droits de vote:

(1) un schéma décrivant les différents niveaux de propriété/la chaîne de contrôle jusqu'aux propriétaires ultimes;

(2) les statuts, le règlement intérieur ou les actes constitutifs équivalents;

(3) un registre des administrateurs, dirigeants et signataires.

(3) Le fournisseur audité devrait fournir à l'organisme d'audit les éléments probants suivants relatifs à la gouvernance d'entreprise:

(a) le fournisseur audité devrait fournir à l'organisme d'audit une description:

i. des organes de décision, de leur composition ainsi que des nationalités ou lieux d'établissement de leurs membres (le cas échéant);

ii. des règles relatives à l'élection, à la nomination, à la désignation ou au mandat des membres des organes de décision ou d'autres postes d'encadrement;

iii. des procédures décisionnelles, y compris des informations sur la majorité et/ou le quorum requis pour les décisions;

iv. des politiques de gouvernance interne décrivant la manière dont les décisions en matière de propriété et de contrôle sont enregistrées et approuvées;

des décisions du conseil d'administration et de la direction reflétant la structure de contrôle déclarée;

des procès-verbaux et résolutions du conseil d'administration relatifs aux changements de contrôle;

(b) le fournisseur audité devrait fournir à l'organisme d'audit des pièces justificatives présentant ou décrivant: les organes de décision et les règles relatives à leur élection, nomination, désignation ou mandat, les procédures décisionnelles, les droits de vote, les droits de veto, les droits de nomination, les droits d'approbation au sein de l'entité juridique (par exemple, statuts, règlement intérieur, rapports sur la gouvernance d'entreprise, etc.). Les pièces justificatives et les informations devraient être fournies pour chaque entité juridique intermédiaire qui détient directement ou indirectement 5 % ou plus du capital ou des droits de vote, jusqu'aux propriétaires ultimes de l'ensemble des niveaux concernés.

(4) Le fournisseur audité devrait fournir à l'organisme d'audit les éléments probants suivants relatifs au contrôle:

(a) le fournisseur audité devrait fournir à l'organisme d'audit les éléments probants relatifs aux liens commerciaux conférant le contrôle. Cela comprend, sans s'y limiter, une liste de personnes physiques ou morales avec lesquelles le fournisseur audité (ou les propriétaires du fournisseur audité, y compris les niveaux intermédiaires jusqu'aux propriétaires ultimes) entretient une relation commerciale qui a) confère un niveau de contrôle sur la gestion et les ressources semblable à celui conféré par la détention d'actions ou d'actifs; et b) est de très longue durée (par exemple, des accords d'approvisionnement à long terme très importants ou des crédits accordés par des fabricants de logiciels/clients, associés à des liens structurels);

(b) les pièces justificatives devraient inclure les accords de coopération conclus avec l'organisme du secteur public ou les fabricants de logiciels, etc.

(5) Le fournisseur audité devrait fournir à l'organisme d'audit les éléments probants suivants relatifs aux liens financiers conférant un contrôle:

(a) le fournisseur audité devrait dresser la liste des personnes physiques ou morales (y compris les actionnaires ou propriétaires majoritaires) dont le fournisseur audité (ou les propriétaires) dépend financièrement d'une manière qui pourrait leur permettre d'obtenir des concessions dans des domaines d'activité stratégiques;

(b) les pièces justificatives devraient inclure les documents de prêt, les règlements intérieurs, les documents démontrant le lien financier, etc.

(6) Le fournisseur audité devrait fournir à l'organisme d'audit les éléments probants suivants relatifs aux autres sources de contrôle:

(a) les fournisseurs audités devraient indiquer à l'organisme d'audit s'il existe d'autres moyens, processus ou liens conférant en définitive le contrôle à un autre pays tiers ou à une entité juridique établie dans un pays tiers (niveau de contrôle sur la gestion et les ressources semblable à celui conféré par la détention d'actions ou d'actifs de longue durée);

(b) les pièces justificatives devraient apporter la preuve d'un tel contrôle ou une déclaration attestant l'absence d'un tel contrôle (cette déclaration pouvant émaner du conseil d'administration du fournisseur de services).

Remarque: *les éléments à prendre en considération pour l'évaluation du contrôle sont les structures de propriété et les droits spécifiques, la gouvernance d'entreprise, les liens commerciaux conférant un contrôle, les liens financiers conférant un contrôle et toute autre source de contrôle.*

7.2. Étapes supplémentaires fondées sur la conclusion de l'évaluation de propriété et de contrôle

Si l'organisme d'audit détermine que le fournisseur audité est soumis au contrôle d'un pays tiers ou d'une entité juridique d'un pays tiers, il devrait demander les éléments probants supplémentaires suivants:

(c) la démonstration que la Commission a adopté une décision en vertu de l'article 19 concernant le pays tiers au contrôle duquel est soumis le fournisseur de services d'informatique en nuage;

(d) l'ensemble des éléments probants démontrant que le fournisseur audité et les éventuels sous-traitants participant à la fourniture du service audité ont mis en œuvre les mesures nécessaires pour assurer la séparation juridique, technique et organisationnelle effective entre le fournisseur de services d'informatique en nuage et tout pays tiers ou toute entité juridique établie dans un pays tiers, en veillant à ce que le fournisseur de services d'informatique en nuage ne soit pas en mesure, sur les plans juridique, technique et opérationnel, de donner suite à toute demande d'accès aux données client, y compris aux données chiffrées, ou de perturber la continuité du service ou de dégrader la qualité du service;

(e) l'ensemble des éléments probants démontrant que l'organisme du secteur public sera informé d'une telle demande et une confirmation que la demande a été rejetée;

(f) l'ensemble des éléments probants démontrant la tenue à jour d'un registre de toute demande d'accès aux données client, de perturbation de la continuité du service ou de dégradation de la qualité du service émanant d'un pays tiers ou d'une entité juridique établie dans un pays tiers, contenant au moins la demande et la réponse qui y a été apportée.

8. Critère d'audit H – Absence de soutien technique et opérationnel en dehors de l'Union

L'organisme d'audit évalue le critère d'audit énoncé au point h) de l'annexe II pour les niveaux d'assurance de l'Union 2, 3 et 4 sur la base des éléments probants suivants:

(1) les éléments probants démontrant que le fournisseur audité a mis en œuvre des clauses contractuelles contraignantes stipulant que toutes les activités de soutien, d'administration, de maintenance, de suivi, de réponse aux incidents et d'exploitation doivent être lancées et exécutées exclusivement dans l'Union. Cela peut inclure des clauses contractuelles exigeant la divulgation préalable de l'ensemble des sous-traitants et des lieux d'assistance, l'approbation écrite préalable à l'engagement de tout nouveau sous-traitant et le droit de rejeter tout sous-traitant situé en dehors de l'Union;

(2) les éléments probants démontrant que le fournisseur audité tient à jour un registre des sous-traitants;

(3) les éléments probants démontrant que le fournisseur audité ne sous-traite ni ne transfère ces activités en dehors de l'Union;

(4) les éléments probants démontrant que le fournisseur audité a mis en œuvre les mesures juridiques, techniques et organisationnelles nécessaires pour garantir qu'aucun accès à distance n'est possible depuis l'extérieur de l'Union aux fins du soutien technique et opérationnel pour le service audité;

(5) les éléments probants démontrant que les services d'assistance/de soutien du fournisseur audité, la gestion de l'infrastructure, le fonctionnement de son centre d'opérations de sécurité ou de son centre d'opérations du réseau, l'accès privilégié, la gestion des sauvegardes et les opérations de rétablissement après sinistre du service audité sont assurés exclusivement depuis l'Union, y compris la voie d'accès permettant d'exploiter le service;

(6) les éléments probants démontrant que le fournisseur audité veille à ce que le personnel, au départ de l'entreprise, n'ait plus accès au service audité et révoque toutes les politiques d'accès;

(7) les éléments probants démontrant que le fournisseur audité a mis en œuvre les mesures techniques et organisationnelles nécessaires pour garantir que l'accès administratif aux systèmes utilisés pour exploiter le service audité est fourni par des voies d'accès situées dans l'Union. Cela peut être démontré par la mise en œuvre de contrôles de réseau géographiquement limités, d'infrastructures administratives basées dans l'Union, de contrôles de gestion des accès privilégiés et de mécanismes de suivi;

(8) les éléments probants démontrant que le fournisseur audité a mis en place des procédures garantissant l'absence de contrôle effectif d'un pays tiers ou d'une entité juridique établie dans un pays tiers, y compris pour toute sous-traitance ultérieure.

9. Critère d'audit I – Garantir la transparence de la chaîne d'approvisionnement des logiciels

L'organisme d'audit évalue le critère d'audit énoncé au point i) de l'annexe II pour les niveaux d'assurance de l'Union 2, 3 et 4 sur la base des éléments probants suivants:

(1) le fournisseur audité devrait mettre à la disposition de l'organisme d'audit une nomenclature des logiciels complète et à jour pour tous les composants logiciels, y compris les logiciels libres et ouverts;

(2) le fournisseur audité devrait mettre à la disposition de l'organisme d'audit une liste des dépendances. Celle-ci devrait inclure:

(a) l'ensemble des modules logiciels, bibliothèques ou interfaces de programmation d'applications (API) utilisés, ainsi que les outils de développement;

(b) l'origine du logiciel: où (pays d'origine) et par qui le logiciel est conçu, développé et entretenu, le lieu et la juridiction régissant la distribution du logiciel, et les mises à jour;

(c) le degré de dépendance à l'égard de fournisseurs, d'installations ou de technologies propriétaires de pays tiers; pour le niveau 3, les éléments probants démontrant que, dans le cas où la pile logicielle est fournie par une entité de pays tiers, aucune restriction injustifiée à l'octroi de licences n'est en place;

(d) le degré de dépendance à l'égard des logiciels libres et ouverts;

(e) la visibilité sur l'ensemble de la chaîne du fabricant et du sous-fabricant du logiciel, y compris les droits d'audit;

Remarque: *les exigences ci-dessus impliquent que les coentreprises constituées, par exemple, d'une entité de l'Union et d'une entité juridique établie dans un pays tiers peuvent bénéficier de ce niveau.*

(3) le fournisseur audité devrait fournir:

(a) les éléments probants attestant d'un processus fondé sur les risques pour recenser et atténuer les dépendances à l'égard de fabricants de logiciels externes pertinents pour l'exploitation du service d'informatique en nuage;

(b) les éléments probants attestant qu'il a trouvé une ou plusieurs autres solutions logicielles, y compris des logiciels libres et ouverts. Si aucun logiciel équivalent ne peut être trouvé, il convient de trouver une solution garantissant une fonctionnalité viable minimale. Des tests doivent être mis en œuvre, ainsi qu'un plan de bascule permettant la migration vers ces autres solutions;

(c) les éléments probants attestant qu'il peut migrer vers une autre solution en cas de défaillance du fournisseur ou de restrictions imposées par un pays tiers ou une entité juridique établie dans un pays tiers;

(d) une liste des normes ouvertes suivies dans le cadre des politiques du fournisseur audité relatives au service audité;

(4) le fournisseur audité devrait garantir la transparence par un accès à distance et la vérifiabilité du code source:

(a) en mettant à la disposition de l'organisme d'audit une liste d'éléments probants démontrant qu'aucune fonctionnalité ou aucun mécanisme à distance susceptible d'être utilisé pour altérer ou perturber de manière substantielle un appareil, un système ou un logiciel n'est utilisé. Cela devrait inclure:

i. les éléments probants relatifs aux tests du composant logiciel visant à empêcher l'utilisation de toute fonctionnalité ou de tout mécanisme à distance susceptible d'être utilisé pour altérer ou perturber de manière substantielle un appareil, un système ou un logiciel (procédure de test, rapports de test, plan de test, etc.);

ii. les éléments probants démontrant que les procédures de gestion des changements de l'organisation couvrent toute modification des micrologiciels, du BIOS et des mises à jour logicielles, ainsi que

l'intégration de nouveaux composants afin d'empêcher l'utilisation de toute fonctionnalité ou de tout mécanisme à distance;

iii. les éléments probants démontrant que la procédure de maintenance a été mise à jour afin d'empêcher l'utilisation de toute fonctionnalité ou de tout mécanisme à distance susceptible d'être utilisé pour altérer ou perturber de manière substantielle un appareil, un système ou un logiciel;

(b) le fournisseur audité doit veiller à ce que l'auditeur indépendant tiers se voie accorder le droit d'accéder au code source de ces logiciels et de l'auditer. Le fournisseur audité doit également veiller à ce que l'ensemble de la documentation, du matériel technique et des informations nécessaires à l'évaluation et à l'audit du code source soient mis à la disposition de l'organisme d'audit dans un format complet, exact et accessible.

10. Critère d'audit J – Logiciels libres et ouverts

L'organisme d'audit évalue le critère d'audit énoncé au point j) de l'annexe II pour les niveaux d'assurance de l'Union 2, 3 et 4 sur la base des éléments probants suivants:

(1) le fournisseur audité devrait garantir la transparence par un accès à distance et la vérifiabilité du code source:

(a) en mettant à la disposition de l'organisme d'audit une liste d'éléments probants démontrant qu'aucune fonctionnalité ou aucun mécanisme à distance susceptible d'être utilisé pour altérer ou perturber de manière substantielle un appareil, un système ou un logiciel n'est utilisé. Cela devrait inclure:

i. les éléments probants relatifs aux tests du composant logiciel visant à empêcher l'utilisation de toute fonctionnalité ou de tout mécanisme à distance susceptible d'être utilisé pour altérer ou perturber de manière substantielle un appareil, un système ou un logiciel (procédure de test, rapports de test, plan de test, etc.);

ii. les éléments probants démontrant que les procédures de gestion des changements de l'organisation couvrent toute modification des micrologiciels, du BIOS et des mises à jour logicielles, ainsi que l'intégration de nouveaux composants afin d'empêcher l'utilisation de toute fonctionnalité ou de tout mécanisme à distance;

iii. les éléments probants démontrant que la procédure de maintenance a été mise à jour afin d'empêcher l'utilisation de toute fonctionnalité ou de tout mécanisme à distance susceptible d'être utilisé pour altérer ou perturber de manière substantielle un appareil, un système ou un logiciel;

(2) le fournisseur audité devrait fournir:

(a) les éléments probants attestant d'un processus fondé sur les risques permettant de recenser et d'atténuer: i) la faiblesse de l'écosystème et du soutien communautaire du logiciel libre et ouvert; ii) l'absence de surveillance continue des mises à jour publiées; iii) les cas où le logiciel libre et ouvert est obsolète ou n'est plus entretenu;

(b) les éléments probants démontrant que le fournisseur audité a appliqué les mises à jour du logiciel libre et ouvert sans retard indu;

(c) les éléments probants démontrant que le fournisseur audité a trouvé une ou plusieurs autres solutions open source. Si le fournisseur audité n'est pas en mesure de trouver un logiciel équivalent, il doit trouver une solution garantissant une fonctionnalité viable minimale. Le fournisseur audité doit mettre en œuvre des tests et un plan de bascule permettant la migration vers les autres solutions;

(3) lorsque le fournisseur audité utilise un logiciel mis en service dans le cadre d'une licence open source, il devrait mettre en œuvre des mécanismes permettant de détecter et de notifier en temps utile à l'organisme du secteur public si le logiciel a été acquis par un pays tiers ou une entité juridique ou une fondation établie dans un pays tiers, ou s'il est contrôlé par un pays tiers ou une entité juridique ou une fondation établie dans un pays tiers.

11. Critère d'audit K – Services mondiaux et filiales dans des pays tiers

L'organisme d'audit évalue le critère d'audit énoncé au point k) de l'annexe II pour les niveaux d'assurance de l'Union 2, 3 et 4 sur la base des éléments probants suivants:

(1) l'organisme d'audit devrait vérifier que la filiale est indépendante, sur les plans juridique et opérationnel, du fournisseur audité;

(2) le fournisseur audité doit démontrer que la filiale n'a pas accès aux systèmes de traitement ou de stockage des données client;

(3) le fournisseur audité doit démontrer que la filiale ne dispose d'aucun compte à privilèges au sein des environnements de production de l'Union, notamment des privilèges en matière d'administration du nuage, de gestion des identités et des accès (IAM), de gestion des accès privilégiés (PAM), de surveillance ou d'administration de bases de données;

(4) l'organisme d'audit devrait vérifier que le personnel de la filiale ne peut obtenir l'accès aux données des clients de l'Union;

(5) l'organisme d'audit devrait vérifier que la filiale n'a pas le pouvoir de donner pour instruction au personnel opérationnel de l'Union de divulguer les données clients ou de contourner les procédures de sécurité;

(6) l'organisme d'audit devrait vérifier que toutes les demandes émanant de pouvoirs publics étrangers reçues par la filiale sont officiellement redirigées vers l'entité compétente de l'Union aux fins d'une évaluation juridique en vertu du droit de l'Union et du droit des États membres.