Grille d'évaluation des risques de souveraineté

Douze questions pour mesurer l'exposition de vos réunions aujourd'hui : au droit étranger, à un traitement opaque par l'IA et aux deepfakes vocaux. Comptez une dizaine de minutes. La grille s'applique aux outils que vous utilisez déjà, quels qu'ils soient.

> **Mode d'emploi.** Cochez une réponse par question et additionnez les points indiqués en violet (0, 1 ou 2). Plus le total est bas, plus le risque est faible. Répondez pour l'outil que votre organisation utilise réellement pour ses réunions sensibles : conseil, finance, juridique, RH, négociations clients. Si vous ne connaissez pas la réponse, cochez la plus risquée : ce que vous ne pouvez pas vérifier, vous ne pourrez pas le défendre devant un régulateur.

A. Juridiction

1. Où la maison mère de votre fournisseur de visio est-elle immatriculée ?

C'est le pays d'origine du fournisseur qui détermine quels gouvernements peuvent lui imposer de communiquer vos données, où que se trouvent les serveurs.

☐ Dans l'UE **0** ☐ Filiale européenne d'un groupe non européen **1** ☐ Hors de l'UE, ou je ne sais pas **2**

2. Une autorité hors UE pourrait-elle obliger votre fournisseur à livrer le contenu de vos réunions (par exemple au titre du CLOUD Act américain) ?

Une « région de données UE » règle l'endroit où sont stockées les données, pas la question de savoir qui peut être contraint de les produire.

☐ Non **0** ☐ Je ne suis pas sûr **1** ☐ Oui **2**

3. Où sont conservés les enregistrements, les transcriptions et les comptes rendus ?

Un compte rendu contient souvent plus d'informations sensibles que la réunion elle-même : décisions, montants, noms.

☐ Dans l'UE chez un fournisseur européen, ou sur nos serveurs **0**

☐ Dans une région UE d'un fournisseur non européen **1** ☐ Hors de l'UE, ou je ne sais pas **2**

B. Traitement par l'IA

4. Qui fait tourner l'IA qui transcrit, traduit et résume vos réunions ?

Des poids ouverts exécutés en Europe règlent la localisation, pas le contrôle : licence, matériel, feuille de route et recours restent étrangers. Ce qui compte, c'est qui exploite le modèle et où partent les contenus.

☐ Notre fournisseur, auto-hébergé dans l'UE ou chez nous **0** ☐ Hébergé dans l'UE mais fourni par un tiers **1**

☐ Une API externe hors UE, ou je ne sais pas **2**

5. Le contenu de vos réunions peut-il servir à entraîner des modèles d'IA ?

Une fois qu'un contenu a servi à entraîner un modèle, on ne peut plus le reprendre.

☐ Exclu par contrat **0** ☐ Exclu seulement si nous le refusons **1** ☐ Autorisé, ou je ne sais pas **2**

6. Qui détient les clés de chiffrement des données de vos réunions ?

Celui qui détient les clés peut être contraint de s'en servir.

☐ Nous-mêmes (clés gérées par le client) **0** ☐ Un fournisseur européen **1**

☐ Un fournisseur non européen, ou je ne sais pas **2**

C. Voix et identité

7. Une voix clonée pourrait-elle participer à l'une de vos réunions sans que personne ne s'en aperçoive ?

Quelques secondes d'audio public (une présentation de résultats, un podcast, une conférence) suffisent pour cloner la voix d'un dirigeant.

☐ Non : les voix sont vérifiées en direct, pendant la réunion **0** ☐ Seulement des contre-appels manuels **1**

☐ Rien n'est prévu **2**

8. Les personnes habilitées à valider un paiement, un ordre ou un contrat disposent-elles d'une identité vocale vérifiée ?

L'attaque ne vise pas votre réseau, mais la personne qui dit oui.

☐ Oui **0** ☐ Certaines d'entre elles **1** ☐ Non **2**

9. Quand vous traduisez la parole, quelle voix est utilisée, et qui en détient un modèle ?

Confier la voix de vos dirigeants à un service vocal extérieur crée un modèle de leur voix que vous ne maîtrisez pas.

☐ Aucune voix de synthèse, ou la propre voix du locuteur, traitée par notre fournisseur **0**

☐ Un service vocal tiers dans l'UE **1** ☐ Un service vocal tiers hors UE, ou je ne sais pas **2**

D. Conformité et maîtrise

10. Les sons générés ou modifiés par l'IA pendant vos réunions sont-ils signalés aux participants et marqués de façon lisible par machine ?

L'article 50 du règlement européen sur l'IA s'applique depuis le 2 août 2026, avec des amendes pouvant atteindre 15 millions d'euros ou 3 % du chiffre d'affaires mondial. Il impose de marquer les contenus synthétiques ; il n'impose pas de détecter les deepfakes, une protection qui relève d'une décision distincte.

☐ Oui **0** ☐ En partie **1** ☐ Non, ou je ne sais pas **2**

11. Si nécessaire, pourriez-vous faire tourner votre plateforme de réunion sur vos propres serveurs, y compris en réseau isolé (air-gap) ?

Certaines réunions (défense, enquêtes, fusions-acquisitions) ne devraient jamais passer par un cloud partagé.

☐ Oui **0** ☐ Seulement en instance de cloud privée **1** ☐ Non **2**

12. Pourriez-vous présenter dès aujourd'hui à un auditeur ou à un régulateur chaque sous-traitant qui traite les données de vos réunions, et le lieu où il les traite ?

Le RGPD, NIS2 et DORA attendent que vous connaissiez votre chaîne d'approvisionnement, pas seulement votre fournisseur principal.

☐ Oui **0** ☐ En partie **1** ☐ Non **2**

Votre total : _____ / 24

Ce que signifie votre score

0 à 6 · Exposition faible
Vos réunions sont bien protégées. Gardez la preuve de chaque réponse à disposition de vos auditeurs.

7 à 14 · Exposition modérée
Il reste des failles, souvent sur l'IA, les clés ou l'identité vocale. Commencez par les questions où vous avez coché 2.

15 à 24 · Exposition élevée
Vos décisions sensibles sont exposées au droit étranger, à une IA opaque ou à la fraude vocale. À traiter en priorité.

Trois actions pour la suite

1. **Recensez vos réunions sensibles.** Listez celles où une décision, un paiement ou une information confidentielle est en jeu, et l'outil utilisé pour chacune.
2. **Demandez des preuves à votre fournisseur** pour chaque question où vous avez coché 2 : maison mère, sous-traitants, modèles d'IA, gestion des clés, politique d'entraînement.
3. **Protégez les personnes qui disent oui.** Ajoutez une vérification de l'identité vocale pour toute personne qui peut valider un paiement ou un ordre au téléphone ou en visio.

À propos de Kizwork. Kizwork est une entreprise française (Sophia Antipolis, avec un établissement à Lisbonne). Sa plateforme de réunion fonctionne dans l'UE (Scaleway : Paris, Amsterdam, Varsovie), sur vos propres serveurs (y compris en réseau isolé) ou dans votre propre cloud. Elle signale en direct les voix clonées pendant la réunion (99,1 % de précision sur un jeu de test équilibré, alerte en 2 à 3 secondes ; validation indépendante commanditée), et propose une identité vocale certifiée ainsi que la traduction voix-à-voix dans la propre voix de chaque locuteur, en 47 langues, sans aucune voix IA tierce. Envoyez-nous votre grille remplie à **contact@kizwork.com** : nous la passerons en revue avec vous.

Cette grille est un outil d'auto-évaluation, pas un avis juridique. Kizwork S.A.S., RCS Grasse 891 606 519 · www.kizwork.com