COLLABOR-IA · FICHE-MÉMO

Quiz d'équipe : l'assistant IA et vos outils

Ce que le quiz apporte.
En une réunion, chacun dit ce qu'il croit permis avec l'assistant, et l'équipe voit où elle diverge.

Ce qu'il évite.
Des règles que chacun s'invente : un compte personnel pour un dossier client, un RIB changé sur la foi d'un résumé.

Ce que contient la fiche.
Quatorze questions en quatre parties, puis les corrigés : la source et la décision à prendre ensemble.

Pour les dirigeants et responsables d'équipe de TPE et PME qui veulent faire le point à plusieurs sur l'assistant IA

Édition du 19/11/2026 · NLQ

01 Préparez la réunion

Un quiz fait à voix haute s'aligne sur la première réponse. Ce qui compte, ce sont les écarts : ils montrent les règles que personne n'a écrites.

Une feuille par personne.
Les questions seules : les corrigés commencent sur une page à part.

Chacun répond seul.
Sans en parler, une réponse par question.

On compare avant de corriger.
Les questions qui divisent passent en premier.

On décide.
Chaque corrigé finit par une décision à adapter, avec le nom de la personne qui s'en charge.

02 Vérifiez ce que l'assistant peut faire

Branché à la messagerie ou aux dossiers, l'assistant ne se contente plus de répondre. Ce qu'il peut faire chez vous, et ce qu'on a oublié de débrancher.

N°	QUESTION	VOTRE RÉPONSE
1	Un agent IA, c'est : a) un moteur de recherche plus rapide ; b) un assistant capable de réaliser des actions sans intervention humaine ; c) un outil qui ne fait que rédiger.	a · b · c
2	Un outil branché pour un essai, puis abandonné, ne présente plus de risque.	Vrai · Faux
3	Avant que l'assistant appelle un outil, l'application devrait vous montrer : a) le nom de l'outil ; b) les données qu'il va lui envoyer ; c) rien, pour aller vite.	a · b · c
4	L'assistant peut publier seul sur la page de l'entreprise : ce n'est ni un virement ni une suppression.	Vrai · Faux

03 Fixez ce qu'on lui confie

Le service, les données et le compte se décident pour toute l'équipe. Sinon, chacun applique sa propre prudence, ou aucune.

N°	QUESTION	VOTRE RÉPONSE
5	Un salarié peut utiliser son compte d'IA personnel pour une tâche du bureau, si les données ne sont pas sensibles.	Vrai · Faux
6	Aucune règle n'est écrite. Le bon réflexe : a) tout permettre en attendant ; b) éviter d'y mettre des informations sensibles (RH, projets, contrats) ; c) demander à l'IA si c'est sensible.	a · b · c
7	Qu'est-ce qui ne doit surtout pas aller dans un service d'IA grand public ? a) un texte déjà publié sur votre site ; b) les données contractuelles ou financières de l'entreprise ; c) une question d'orthographe.	a · b · c
8	Pour le compte professionnel de l'outil d'IA, un mot de passe d'au moins 12 caractères et la double authentification sont conseillés.	Vrai · Faux

04 Contrôlez ce qu'il produit

L'assistant écrit bien, et c'est le piège : une réponse soignée inspire confiance. Et un mail qu'il lit peut l'orienter sans que personne le voie.

N°	QUESTION	VOTRE RÉPONSE
9	Quand l'IA affirme une information avec assurance, c'est qu'elle est juste.	Vrai · Faux
10	Pour l'OWASP, la confiance excessive, c'est : a) un assistant trop sûr de lui ; b) une personne qui reprend ce que produit l'IA sans le vérifier ; c) un outil qui demande trop de confirmations.	a · b · c
11	Un mail reçu d'un client connu peut déclencher seul une action de l'assistant.	Vrai · Faux

05 Prévoyez le jour où ça déraille

Un incident ne prévient pas. Ce qu'on doit avoir décidé avant : le changement de RIB, la panne, le fichier abîmé.

N°	QUESTION	VOTRE RÉPONSE
12	L'assistant résume le mail d'un fournisseur qui annonce un nouveau RIB. On fait quoi ? a) on met le RIB à jour ; b) on demande à l'assistant de vérifier ; c) on appelle le fournisseur sur son numéro habituel.	a · b · c
13	Si l'assistant tombe en panne ou répond de travers, il faut avoir prévu comment travailler sans lui.	Vrai · Faux
14	Avant de laisser l'assistant modifier des fichiers, une sauvegarde suffit, même jamais restaurée.	Vrai · Faux

Comment savoir si c'est en place

Après la réunion, cinq questions pour vérifier que les décisions tiennent.

- [ ] Chaque question a-t-elle une décision écrite, avec un nom?
- [ ] Tout le monde utilise-t-il le seul service de l'entreprise?
- [ ] Chacun sait-il travailler si l'assistant est coupé?
- [ ] La liste des outils branchés est-elle tenue, sans outil abandonné?
- [ ] Publications, changements de RIB et modifications de fichiers passent-ils par une personne nommée?

06 Corrigés

Questions 1 à 4 : ce que l'assistant peut faire

N°	RÉPONSE ET SOURCE	CE QU'ON DÉCIDE DANS L'ÉQUIPE
1	**b.** Des assistants « capables de réaliser des actions sans intervention humaine ». (Cybermalveillance, Utiliser l'IA)	On liste ce que notre assistant fait déjà sans nous.
2	**Faux.** L'OWASP cite l'outil essayé puis abandonné qui reste à la disposition de l'assistant, et recommande de limiter les outils au strict nécessaire. (OWASP, LLM06)	Un outil abandonné est débranché le jour même. Une personne tient la liste.
3	**b.** Montrer les données envoyées à l'outil, pour éviter une fuite. (MCP, Tools)	On ne valide pas ce qu'on ne voit pas (voir « Ce que l'assistant fait seul, ce qu'il vous demande »).
4	**Faux.** L'ANSSI range la production de contenu public parmi les actions critiques à ne pas automatiser. (ANSSI, R9)	Rien ne devient public sans la relecture d'une personne nommée.

Questions 5 à 8 : ce qu'on lui confie

N°	RÉPONSE ET SOURCE	CE QU'ON DÉCIDE DANS L'ÉQUIPE
5	**Faux.** Utiliser exclusivement le service souscrit par l'employeur, sans se servir de son accès personnel pour le travail. (Cybermalveillance, Utiliser l'IA ; 10 mesures, n° 9)	Un seul service pour le travail ; voir le « Registre des usages d'IA de l'équipe ».
6	**b.** Sans politique, éviter les informations sensibles ; s'assurer qu'une charte d'usage de l'IA existe et que tous la connaissent. (Cybermalveillance, Utiliser l'IA)	On écrit la charte, en commençant par ce qu'on n'y met jamais.
7	**b.** L'ANSSI recommande de ne pas envoyer de données sensibles aux services d'IA grand public, dont les données contractuelles, juridiques ou financières et les mots de passe. (ANSSI, R34)	Contrats, chiffres et mots de passe ne vont dans aucun service grand public.
8	**Vrai.** « Au moins 12 caractères », double authentification, et un mot de passe jamais communiqué à un tiers. (Cybermalveillance, Utiliser l'IA ; Mots de passe)	Chacun son compte, son mot de passe, sa double authentification.

Questions 9 à 11 : ce qu'il produit

N°	RÉPONSE ET SOURCE	CE QU'ON DÉCIDE DANS L'ÉQUIPE
9	**Faux.** Un résultat affirmé de manière convaincante peut être erroné ou inventé : c'est l'hallucination. (Cybermalveillance, Utiliser l'IA)	Tout chiffre, nom ou date venu de l'IA est vérifié avant de sortir.
10	**b.** Trop de confiance, pas de vérification. L'OWASP veut des relecteurs formés à l'éviter. (OWASP, LLM09)	Celui qui valide relit vraiment, et on lui en laisse le temps.
11	**Faux.** L'ANSSI recommande de limiter, voire de proscrire, les actions automatiques à partir d'entrées non maîtrisées, dont les mails, qui peuvent cacher des consignes. (ANSSI, R27 ; OWASP, LLM01)	Après un mail reçu, l'assistant prépare ; une personne décide.

Questions 12 à 14 : le jour où ça déraille

N°	RÉPONSE ET SOURCE	CE QU'ON DÉCIDE DANS L'ÉQUIPE
12	**c.** Nouveau RIB reçu par message : appeler le créancier sur son numéro habituel. (Cybermalveillance, faux RIB ; 10 mesures, n° 6)	Aucun changement de RIB sans cet appel, passé par la personne qui règle les fournisseurs.
13	**Vrai.** L'ANSSI recommande de prévoir au minimum une procédure de contournement du système d'IA. (ANSSI, R15)	On écrit comment travailler sans l'assistant, et qui peut le couper.
14	**Faux.** Une sauvegarde ne s'effectue pas toujours correctement : il faut vérifier qu'elle fonctionne. (Cybermalveillance, Sauvegardes)	On essaie une restauration avant d'ouvrir l'écriture à l'assistant.

VOTRE PROCHAINE ÉTAPE

Venez avec la feuille des décisions de votre équipe et les questions qui l'ont divisée : on les reprend ensemble, une par une.

www.collabor-ia.fr/rendez-vous/

Réserver un échange gratuit

Sources et portée

- ANSSI, guide ANSSI-PA-102, version 1.0 du 29/04/2024 : R9, R15, R27, R34. https://messervices.cyber.gouv.fr/documents-guides/Recommandations_de_s%C3%A9curit%C3%A9_pour_un_syst%C3%A8me_d_IA_g%C3%A9n%C3%A9rative.pdf, consulté le 19/11/2026.
- OWASP, *LLM01:2025*. https://genai.owasp.org/llmrisk/llm01-prompt-injection/, consulté le 19/11/2026.
- OWASP, *LLM06:2025*. https://genai.owasp.org/llmrisk/llm062025-excessive-agency/, consulté le 19/11/2026.
- OWASP, *LLM09:2025*. https://genai.owasp.org/llmrisk/llm092025-misinformation/, consulté le 19/11/2026.
- Spécification MCP 2026-07-28, *Tools*. https://modelcontextprotocol.io/specification/2026-07-28/server/tools, consulté le 19/11/2026.
- Cybermalveillance.gouv.fr, *Utiliser l'IA*. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/utiliser-ia-conseils-pour-les-particuliers-et-les-professionnels, consulté le 19/11/2026.
- Cybermalveillance.gouv.fr, *Mots de passe*. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe, consulté le 19/11/2026.
- Cybermalveillance.gouv.fr, *Sauvegardes*. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes, consulté le 19/11/2026.
- Cybermalveillance.gouv.fr, *Faux RIB*. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/que-faire-en-cas-de-fraude-au-virement-ou-au-faux-rib, consulté le 19/11/2026.
- Cybermalveillance.gouv.fr, *10 mesures essentielles*. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique, consulté le 19/11/2026.

Portée : un quiz d'équipe tiré de textes publics datés. Les décisions sont des exemples à adapter ; elles ne remplacent pas l'avis d'un spécialiste de la sécurité.

Édité par NLQ — Collabor-IA (www.collabor-ia.fr), avec le soutien d'ALMA, sponsor. Édition du 19/11/2026. Exemples fictifs ; ce qui est dit des textes cités vient des sources datées ci-dessus.