



Inciter l'innovation Sécuriser l'essentiel

Kezber, votre partenaire de confiance
en innovation TI

**Grille
d'autoévaluation**
cybersécurité

Faites le point sur ce qui protège réellement votre organisation aujourd'hui.

Pourquoi cette évaluation est essentielle?

La cybersécurité et l'IA ne sont plus des enjeux techniques. Ce sont des enjeux stratégiques.

Chaque nouvelle technologie, chaque automatisation, chaque intégration d'IA amplifie la maturité réelle de votre organisation. Si les bases sont solides, elle accélère la performance. Si elles sont fragiles, elle amplifie le risque.

Prendre 5 minutes pour faire le point permet d'identifier les angles morts avant qu'un incident ne le fasse pour vous. Cette grille ne vise pas la perfection. Elle vise la lucidité.

La grille d'évaluation cybersécurité de Kezber, un outil d'évaluation en 15 points, simple et efficace.

Clarifier les angles morts

Identifiez rapidement ce qui est réellement en place et ce qui repose sur des perceptions. Mettez en lumière les zones grises avant qu'elles ne deviennent des vulnérabilités.

Aligner la direction

Positionnez la cybersécurité et l'IA comme des enjeux de gouvernance. Favorisez une discussion au niveau décisionnel, et non uniquement opérationnel.

Prioriser les actions

Distinguez les urgences des améliorations progressives. L'objectif n'est pas de tout faire, mais de savoir par où commencer avec impact.

Cochez chaque affirmation qui est VRAIE dans votre organisation aujourd'hui.

Si vous hésitez ou que vous n'êtes pas certain, considérez que c'est NON et ne cochez pas. Additionnez ensuite le nombre de cases cochées.

Gouvernance et responsabilité

- ☐ Quelqu'un est clairement imputable de la cybersécurité dans l'organisation
- ☐ La direction connaît les systèmes critiques et les données stratégiques
- ☐ La cybersécurité est discutée au niveau de la direction, pas seulement par les TI

Accès et identités

- ☐ Tous les accès aux systèmes sont justifiés, documentés et révisés régulièrement
- ☐ L'authentification multifacteur est activée pour les accès critiques
- ☐ Les accès sont retirés immédiatement lors d'un départ ou d'un changement de rôle

Sauvegardes et continuité

- ☐ Des sauvegardes automatiques protègent les données critiques
- ☐ Les sauvegardes sont testées régulièrement et restaurables
- ☐ L'organisation connaît son seuil de tolérance à l'arrêt, combien de temps elle peut fonctionner sans ses systèmes

L'IA ne fera qu'amplifier votre niveau de maturité. Si les bases sont faibles, elle amplifie le risque. Si les bases sont solides, elle amplifie la performance.

Cybersécurité et IA

Grille d'autoévaluation (suite)

Courriels et utilisateurs

- ☐ Les employés savent reconnaître un courriel suspect
- ☐ Ils savent exactement quoi faire en cas de clic accidentel
- ☐ La direction applique elle-même les bonnes pratiques numériques

Visibilité et gestion d'incident

- ☐ Un incident de sécurité serait détecté rapidement
- ☐ Un plan d'intervention existe et a déjà été réfléchi
- ☐ Les rôles sont clairs en cas d'incident majeur, qui décide, qui communique, qui agit

Interprétation de vos résultats

✓ 0 à 5 cases cochées

Bases très fragiles. L'organisation est fortement exposée et dépend davantage de la chance que d'une structure.

✓ 6 à 10 cases cochées

Bases partielles. Des éléments sont en place, mais des angles morts importants subsistent.

✓ 11 à 15 cases cochées

La posture est saine, mais la vigilance et l'amélioration continue demeurent essentielles.



**L'IA AMPLIFIE VOTRE
NIVEAU DE MATURITÉ.**

**Si les bases sont faibles,
elle amplifie le risque.**

**Si les bases sont solides,
elle amplifie la performance.**



Passez à l'action dès maintenant!

Les résultats de cet outil vous donnent un premier aperçu des vulnérabilités potentielles de votre entreprise. Pour aller plus loin, une évaluation approfondie par un expert de Kezber est essentielle. Nos spécialistes vous aideront à analyser en détail vos besoins, à identifier les solutions adaptées et à mettre en place des actions concrètes pour garantir la sécurité et la conformité de vos outils.

Ne laissez pas les failles de sécurité mettre votre entreprise à risque.

**Contactez-nous
dès aujourd'hui
pour une consultation
personnalisée.**

« La cybersécurité n'est plus un luxe, c'est une responsabilité. Identifier les vulnérabilités est la première étape pour protéger votre entreprise et vos utilisateurs. »

Jared Warnholtz
Directeur du département TI
chez Kezber