



La gestion moderne du risque fournisseurs
par l'IA



Resources

Au programme



L'objectif : partager 5 bonnes pratiques observées sur plus de 250 programmes TPRM :

1. Quel type de questionnaire ?
2. Comment bien poser des questions ?
3. Faut il des preuves ?
4. Quelle valeur apporte un score ?
5. Comment l'IA peut aider ?

Avant de commencer

Philosophie sur le process

- **Process** : S'inscrit dans un processus plus large (Criticité du fournisseur notamment)
- **Finalité** : Le résultat c'est savoir si le fournisseur répond à vos exigences ou non
- **Etat d'esprit** : Le fournisseur par défaut est de bonne foi. Si vous pouvez l'ajouter en preuve contractuelle, je vous le recommande.

Type de questionnaire

Taille moyenne de questionnaire

- > 100 questions
- $50 < x < 100$ questions
- < 50 questions

Type de questions / réponses

- Réponse de type commentaire
- Réponse de type Conforme / Pas conforme (auto-évaluation)
- Réponse choix simple / multiple entre différentes options

Type de questions / réponses

- Réponse de type commentaire
- Réponse de type Conforme / Pas conforme (auto-évaluation)
- Réponse choix simple / multiple entre différentes options



A proscrire si possible



**Simple mais peu fiable
et exploitable**



Simple et exploitable

Formulation des questions

Recommendations

Questions

1. **Une question = Un sujet** : Scinder en plusieurs questions distinctes si plusieurs points doivent être évalués.
2. La question doit être **courte** et éviter les jargons trop techniques

Format des Réponses

3. **Clarté** : Les options proposées doivent être courtes et faciles à comprendre.
4. **Exclusivité** : Les options doivent être mutuellement exclusives, sans ambiguïté possible.
5. **Orientation décisionnelle** : Chaque option doit clairement indiquer si la réponse est conforme ou non conforme.

Exemple de question à éviter

"L'organisation doit définir, approuver, publier et réviser régulièrement une politique de sécurité de l'information.

Les responsabilités concernant la sécurité de l'information doivent être identifiées et documentées dans les fiches de poste.

L'application des mesures de sécurité est de la responsabilité de l'ensemble du personnel. Cela est communiqué à tout le personnel."

Choix :

- Conforme
- Partiellement conforme
- Pas conforme

Exemple de question à éviter

“Votre entreprise a-t-elle une politique et un programme de formation et de mise à l’essai en matière de sensibilisation à la cybersécurité permettant la formation des utilisateurs contre les attaques cyber telles que le malware, ransomware, phishing, etc.?”

Exemple de questions claires

- Avez vous une politique de gestion d'incidents ?
- Utilisez vous un EDR pour protéger vos points de terminaison ?
- Avez vous des audits réalisés par des organismes indépendants ?
- Faites vous des pentest annuels sur l'application ?

Preuves dans le questionnaire

Notre conseil

- Demandez quelques preuves clés :
 - Certificat ISO/SOC2...
 - Politique de sécurité de l'information
 - Process et politique de gestion d'incidents
 - Pentest
- Trop de preuves tue la preuve : concentrez-vous sur celles qui démontrent réellement la maturité

Score dans votre
questionnaire

Exemple 2 fournisseurs



Entreprise A

Score 86/100



Entreprise B

Score 78/100

Exemple 2 fournisseurs



Entreprise A

Score 86/100



!!! Données en Chine



Entreprise B

Score 78/100

Conseil sur le score dans un questionnaire

- Essayer de le coupler à une liste des écarts importants ou critiques repérés
- Construisez votre score en fonction de votre politique de risque : chaque fournisseur part de 100, puis perd des points selon la criticité des écarts constatés

Exemple 2 fournisseurs



!!! Données en Chine

Entreprise A

Score 50/100



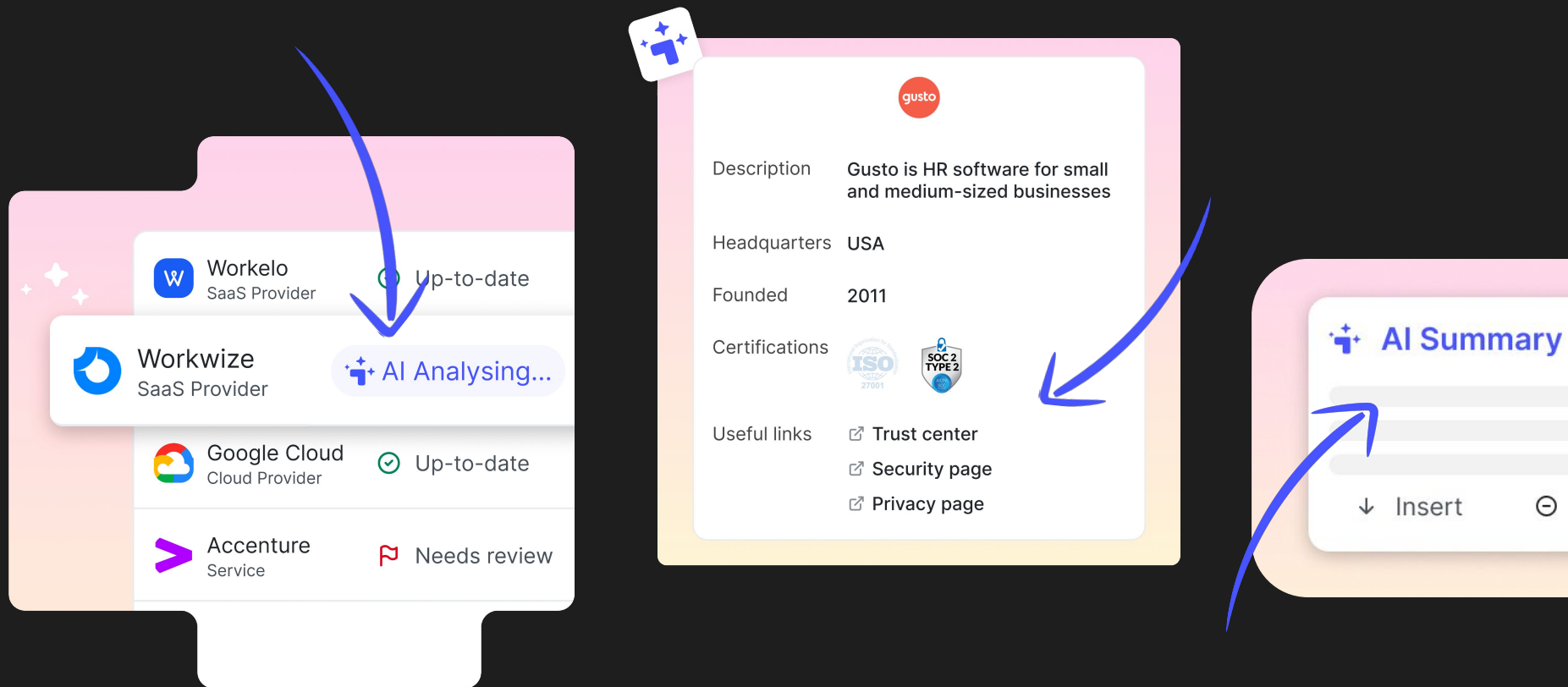
! Incident response
procedure does not
include a data breach
scenario

Entreprise B

Score 95/100

Usage de l'IA

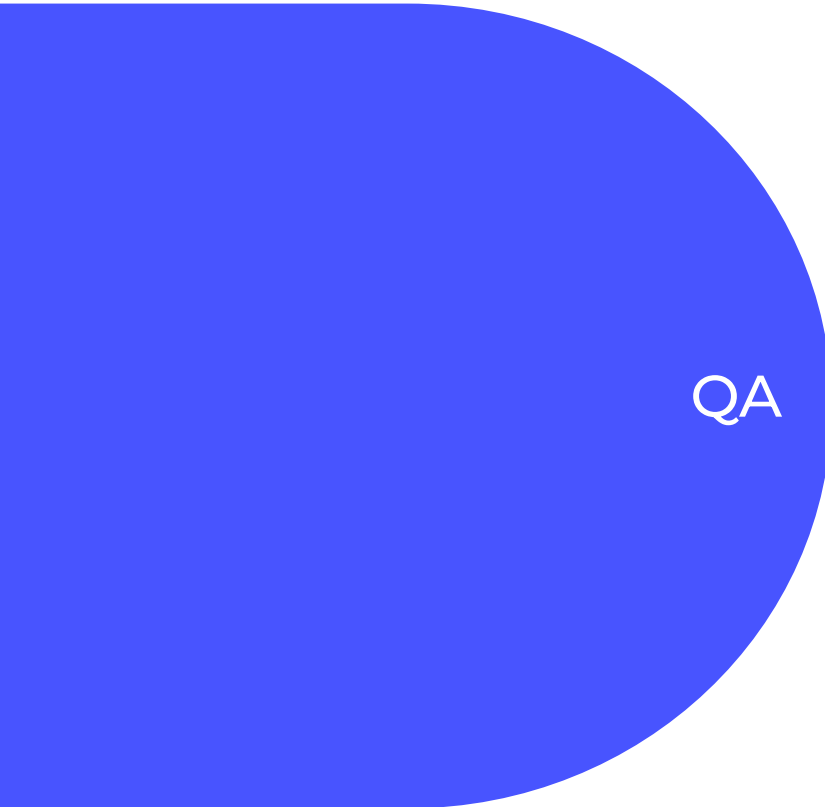
L'IA est une opportunité pour répondre aux défis des questionnaires



Conclusion

En conclusion

- Pourquoi fait on cela ? Pour optimiser **votre temps**, celui du **fournisseur** (donc le vôtre) tout en élevant votre niveau de sécurité
- Le questionnaire est un outil à votre disposition qui est “malheureusement” le plus fiable pour estimer la maturité cyber du fournisseur et de la prestation
- Enfin, le questionnaire a l’avantage que vous pouvez l’ajouter en annexe du contrat



QA

Liens utiles :

- Blog Galink

Prochains Webinars :

- Dans 2 jours sur l'IA et gestion du risque cyber fournisseurs avec Galink



Merci beaucoup !

etienne.retout@galink.com



 galink