Corrigé de l'exercice — Sécurisation d'un workflow

3 failles identifiées

Faille	Risque	Action corrective
Compte personnel du fondateur	Si le fondateur part, le workflow est coupé ; l'accès n'est pas maîtrisé par l'entreprise	Créer un compte email professionnel dédié
Absence de contrôle sur les destinataires	Un email groupé avec des données commerciales peut être transféré ou envoyé par erreur	Limiter la liste à un groupe validé par le dirigeant
Lien direct vers un tableau de bord	Sans vérification des droits, le lien peut circuler hors de l'entreprise	Vérifier les permissions Notion, désactiver le partage public, activer les logs

3 actions correctives immédiates

1. Créer un compte email professionnel dédié (ex. automation@monentreprise.fr) et transférer l'envoi depuis ce compte.
2. Limiter la liste des destinataires à un petit groupe validé, avec une procédure d'ajout/retour manuel.
3. Vérifier les permissions du tableau de bord Notion : accès restreint, pas de partage public, activation des logs d'accès.

Règle de diffusion

> *Les emails récapitulatifs hebdomadaires ne peuvent être envoyés qu'aux personnes identifiées dans la liste de diffusion validée par le dirigeant. Toute demande d'ajout doit faire l'objet d'une validation écrite. Les données chiffrées sensibles (CA détaillé, marges, données clients nominatives) ne sont pas incluses dans le corps de l'email.*

Fréquence de maintenance

- **Mensuelle** : vérification des logs d'envoi et de la liste des destinataires.
- **Trimestrielle** : révision des permissions, test du workflow avec une donnée fictive, mise à jour de la documentation.

Donnée à surveiller dans les logs

Le nombre d'emails envoyés avec succès et le nombre d'erreurs/bounces. Une baisse inattendue du nombre d'envois peut indiquer une panne silencieuse.

Grille d'évaluation du livrable

Critère	1 point	2 points	3 points
Failles identifiées	Moins de 3 failles	3 failles mais peu priorisées	3 failles claires avec risques associés

Actions correctives	Actions imprécises	Actions pertinentes mais mal détaillées	3 actions concrètes avec responsable et délai
Règle de diffusion	Règle absente ou floue	Règle présente mais incomplète	Règle claire sur destinataires et données sensibles
Fréquence de maintenance	Aucune fréquence	Fréquence unique non justifiée	Fréquence mensuelle et trimestrielle adaptée
Donnée à surveiller	Donnée peu pertinente	Donnée pertinente mais mal justifiée	Donnée pertinente avec explication de la panne silencieuse