OUTIL 03 / CADRER VOTRE ANALYSE

Carte des risques invisibles

Rendre visibles les flux, accès et dépendances hors du périmètre apparent.

Entreprise

Projet / fournisseur / usage

Pilote de l’analyse

Date et version examinée

Périmètre de l’analyse

Comment utiliser cet outil

1. Décrivez les faits et référencez les pièces dans les champs de réponse.
2. Sélectionnez un statut pour chaque critère ; conservez les inconnues.
3. Complétez la synthèse, attribuez les actions et faites valider l’arbitrage.

Statuts : Non examiné = travail non réalisé ; Inconnu = information absente ; À vérifier = information non confirmée ; Écart identifié = problème constaté ; Documenté = constat étayé ; Sans objet = motif à préciser.

Ce support prépare une analyse contextualisée. Il ne produit pas de diagnostic juridique automatique. Un statut « Documenté » ne vaut pas validation de conformité.

À remplir puis enregistrer dans votre lecteur PDF. Une copie peut être imprimée. Privilégiez un lecteur prenant en charge les formulaires PDF pour conserver les champs.

01 Télémétrie

Quelles données de diagnostic et d'usage sont émises ?

Pièces utiles : Documentation et observation technique.
Vigilance : Destination ou contenu inconnu.

Votre constat et référence des pièces

Statut Non examiné

Suite à envisager : Faire observer les flux et documenter les finalités.

02 Journaux

Que contiennent les logs, qui les consulte et combien de temps ?

Pièces utiles : Configuration et politique de conservation.
Vigilance : Secrets ou données clients copiés dans les logs.

Votre constat et référence des pièces

Statut Non examiné

Suite à envisager : Limiter contenu, accès et conservation.

03 SDK

Quels composants embarqués contactent un tiers ?

Pièces utiles : Inventaire des SDK et connexions.
Vigilance : Composant ajouté sans examen.

Votre constat et référence des pièces

Statut Non examiné

Suite à envisager : Identifier tiers et données transmises.

04 API

Quelles interfaces exposent ou récupèrent des données ?

Pièces utiles : Schéma et droits des API.
Vigilance : Jetons surdimensionnés ou interfaces oubliées.

Votre constat et référence des pièces

Statut Non examiné

Suite à envisager : Réviser droits, périmètre et révocation.

05 Administration

Qui dispose de privilèges élevés ?

Pièces utiles : Liste des comptes et habilitations.
Vigilance : Comptes anciens, partagés ou non nominatifs.

Votre constat et référence des pièces

Statut Non examiné

Suite à envisager : Faire réviser les accès.

06 Support distant

Comment les interventions sont-elles autorisées et tracées ?

Pièces utiles : Procédure et journal d'intervention.
Vigilance : Accès prestataire permanent sans contrôle.

Votre constat et référence des pièces

Statut Non examiné

Suite à envisager : Encadrer activation et preuve d'intervention.

07 Cascade

Quels tiers interviennent pour le fournisseur principal ?

Pièces utiles : Chaîne de sous-traitance et localisation.
Vigilance : Intervenant sans rôle identifié.

Votre constat et référence des pièces

Statut Non examiné

Suite à envisager : Étendre la cartographie.

08 Open source

Quels composants, versions et licences utilisez-vous ?

Pièces utiles : Inventaire des composants et licences.
Vigilance : Licence ou maintenance non examinée.

Votre constat et référence des pièces

Statut Non examiné

Suite à envisager : Organiser revue technique et juridique.

09 Sauvegardes

Où subsistent des copies après suppression ?

Pièces utiles : Plan de sauvegarde et règles d'effacement.
Vigilance : Copies hors inventaire.

Votre constat et référence des pièces

Statut Non examiné

Suite à envisager : Documenter cycles et possibilités de suppression.

10 Responsabilités

Qui contrôle chaque flux et intervient en cas d’incident ?

Pièces utiles : Contrat et référent par flux.
Vigilance : Flux sans responsable opérationnel.

Votre constat et référence des pièces

Statut Non examiné

Suite à envisager : Attribuer contrôle et escalade.

Ce que votre analyse fait apparaître

Flux et accès encore inconnus

Dépendances critiques découvertes

Vérifications techniques à commander

Points à négocier ou à documenter

Validation : nom, qualité et date

Date ou événement de réexamen

Conservez cette synthèse avec les pièces examinées et les réserves. Les motifs et conditions de l’arbitrage doivent rester identifiables.

Passer de l’analyse aux actions

Documenter un flux ou un accès

Origine et destination ; données ; acteur et lieu ; finalité ; contrôle des accès ; preuve ; information restant à obtenir.

Votre registre (à compléter ou à joindre au dossier)

Action 1 : objet et résultat attendu

Responsable	Échéance	État / preuve de clôture

Action 2 : objet et résultat attendu

Responsable	Échéance	État / preuve de clôture

Action 3 : objet et résultat attendu

Responsable	Échéance	État / preuve de clôture

Besoin de clarifier votre situation ? Échangeons sur votre projet et les points qui appellent une analyse.