SAKIRA

TUTORIEL 24

Préparer un audit : les preuves à chercher pour chaque exigence

© SAKIRA

© SAKIRA. Reproduction et diffusion interdites sans accord écrit.
SAKIRA SAS · 6 rue d'Armaille, 75017 Paris · SIREN 108 493 933

TUTORIEL 24 · DU DÉBUTANT AU CONFIRMÉ

Préparer un audit : les preuves à chercher pour chaque exigence

Un auditeur ne demande pas si vous respectez une exigence : il demande à voir de quoi le montrer. Savoir à l'avance quelles preuves il attend permet de les chercher une par une, au lieu de les découvrir le jour de l'audit.

La règle à respecter

L'IA liste les preuves qu'un auditeur attend, elle ne dit jamais qu'elles existent. Elle n'a vu aucun de vos documents : « vous disposez sans doute d'une procédure de départ » est une supposition, pas un constat. Une preuve n'existe pour l'audit que si vous avez ouvert le document, noté où il se trouve et lu sa date. Un document trouvé n'est pas pour autant suffisant : une procédure qui dit « rapidement » ne prouve pas un retrait en cinq jours. Ne collez que des exigences, jamais vos documents internes.

AVANT DE COMMENCER

Il vous faut

La liste des exigences du référentiel qui sera audité (le texte des exigences, pas vos documents), Excel, et un assistant d'IA comme Claude.

Résultat

Un tableau Excel avec les preuves attendues pour chaque exigence, une colonne où vous notez ce que vous avez trouvé, et le nombre de preuves encore introuvables.

01 Préparer les exigences

Recopiez les exigences dans un fichier texte, une par ligne, avec leur numéro. Collez le texte de l'exigence telle qu'elle est écrite dans le référentiel : l'IA n'a pas besoin de vos documents, et vous n'avez pas à les lui montrer. Dans l'exemple de ce guide, un audit interne porte sur cinq exigences, par exemple « Les droits d'accès d'une personne qui quitte l'entreprise sont supprimés dans les cinq jours ouvrés. ». Les cinq sujets sont : suppression des accès au départ d'une personne, test de restauration des sauvegardes, évaluation annuelle des fournisseurs qui hébergent des données, traitement des incidents de sécurité, sensibilisation des personnes qui entrent dans les locaux de production.

02 Donner la consigne à l'assistant

Dans un Projet Claude, ou collée au début d'une conversation, avec vos exigences à la fin :

© SAKIRA. Reproduction et diffusion interdites sans accord écrit. · sakira.fr
SAKIRA SAS · 6 rue d'Armaille, 75017 Paris · SIREN 108 493 933

À COPIER

```
Tu aides un responsable qualité à préparer un audit. Je te donne des exigences, une par ligne, avec leur numéro. Pour chaque exigence, liste les preuves qu'un auditeur demandera : documents, enregistrements, observations sur le terrain, entretiens. Tu n'as vu aucun document de mon entreprise : tu ne dis jamais qu'une preuve existe, qu'elle est probablement disponible ni qu'elle est conforme. Tu écris seulement ce que l'auditeur attendra de voir.

Si tu ne le sais pas encore, demande en une seule question quel audit est visé (interne, client ou certification) et sur quel périmètre.

Rends un tableau dont les colonnes sont séparées par des points-virgules, pour que je le colle dans Excel, sans ligne d'introduction. Colonnes : Numéro ; Exigence ; Preuve attendue (une seule preuve par ligne) ; Type (document, enregistrement, observation ou entretien) ; Fonction qui la détient d'habitude. Une ligne par preuve, donc plusieurs lignes pour une même exigence, entre deux et quatre. Si une exigence est trop vague pour savoir quelle preuve attendre, écris « exigence à préciser » à la place de la preuve et pose ta question sous le tableau. Aucun compliment, aucune phrase de conclusion.

Exigences : [coller ici vos exigences]
```

L'assistant demande d'abord le type d'audit et le périmètre. Répondez par exemple : « Audit interne, site de production principal. »

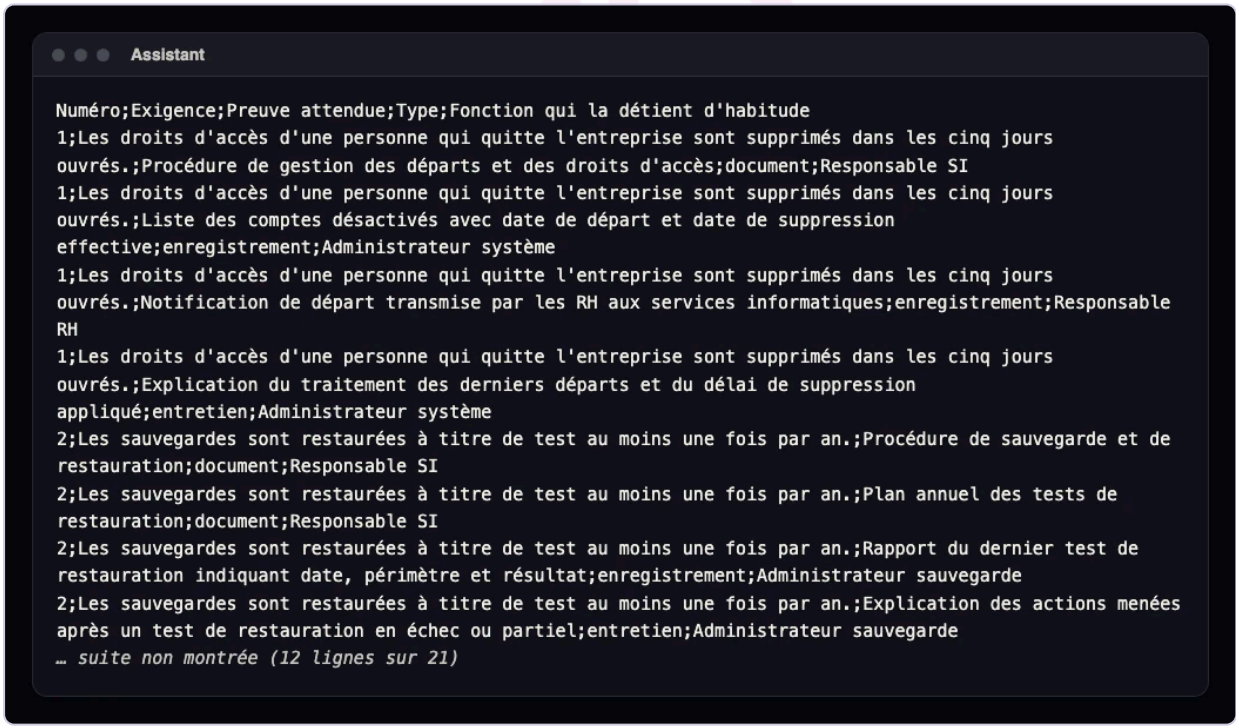


Figure 1. Les premières lignes du tableau obtenu : plusieurs preuves par exigence, chacune avec son type et la fonction qui la détient d'habitude.

© SAKIRA. Reproduction et diffusion interdites sans accord écrit. · sakira.fr
SAKIRA SAS · 6 rue d'Armaille, 75017 Paris · SIREN 108 493 933

> **GARDE-FOU**
> La colonne « Fonction qui la détient d'habitude » est une habitude générale, pas votre organisation. Chez vous, la preuve de suppression des accès peut se trouver ailleurs que chez le « responsable SI » (responsable des systèmes informatiques). Cherchez-la là où elle est vraiment.

03 Coller dans Excel

Copiez le tableau et collez-le dans la cellule A1. Si tout reste dans la colonne A, sélectionnez-la, puis ouvrez l'outil de conversion du texte en colonnes (onglet Données), choisissez « Délimité », puis « Point-virgule ». Chaque colonne se range dans sa cellule.

Ajoutez trois colonnes à droite, avec ces titres : F « Où je l'ai trouvée », G « Date de la preuve », H « Statut ». Les formules ci-dessous supposent la ligne 1 pour les titres et les preuves en lignes 2 à 30 : adaptez les numéros à votre tableau.

- Colonne F : vous y écrivez l'emplacement de la preuve (dossier, nom du fichier, outil), jamais « oui ».
- Colonne G : la date écrite sur la preuve elle-même, au format Date.
- Colonne H, à recopier vers le bas, sur chaque ligne qui porte une preuve : `=SI(F2="";"Non trouvée";"Trouvée")`
- Nombre de preuves attendues, dans une cellule libre (J1) : `=NBVAL(C2:C30)`
- Nombre de preuves introuvables (J2) : `=NB.SI(H2:H30;"Non trouvée")`

Ces formules sont écrites pour Excel en français. Dans la version anglaise, les points-virgules deviennent des virgules et les fonctions s'appellent IF, COUNTA et COUNTIF.

04 Chercher les preuves une par une

Prenez les lignes dans l'ordre, ouvrez le document, et notez en F où il se trouve, en G sa date. Une preuve que vous ne trouvez pas reste « Non trouvée » : c'est une information utile, elle vous dit quoi chercher avant la date de l'audit.

> **GARDE-FOU**
> « Trouvée » veut dire qu'il y a quelque chose à montrer, pas que cela suffit. L'IA et la formule ne jugent pas si la preuve satisfait l'exigence. C'est l'auditeur qui le fait.

05 Faire relire la description de ce que vous avez trouvé

Pour une preuve qui vous semble fragile, décrivez-la en deux lignes à l'assistant (sans coller le document) et demandez-lui ce qu'un auditeur ne pourrait pas vérifier :

© SAKIRA. Reproduction et diffusion interdites sans accord écrit. · sakira.fr
SAKIRA SAS · 6 rue d'Armaille, 75017 Paris · SIREN 108 493 933

À COPIER

```
Voici une exigence d'audit et la description de la preuve que j'ai trouvée. Tu n'as pas vu le document : tu ne dis pas s'il est suffisant ni conforme. Liste seulement ce qu'un auditeur ne pourrait pas vérifier d'après ma description : date, signataire, périmètre couvert, lien avec le délai ou la fréquence de l'exigence. Une puce par élément manquant. Si rien ne manque dans la description, écris-le sans dire que la preuve est valable. Aucun compliment. Écris en texte simple, sans astérisques ni dièses, avec des tirets pour les listes.

Exigence : [coller l'exigence]

Ma description : [décrire la preuve en deux lignes : titre, version, qui l'a rédigée, où elle est rangée, ce qu'elle dit du délai ou de la fréquence]
```

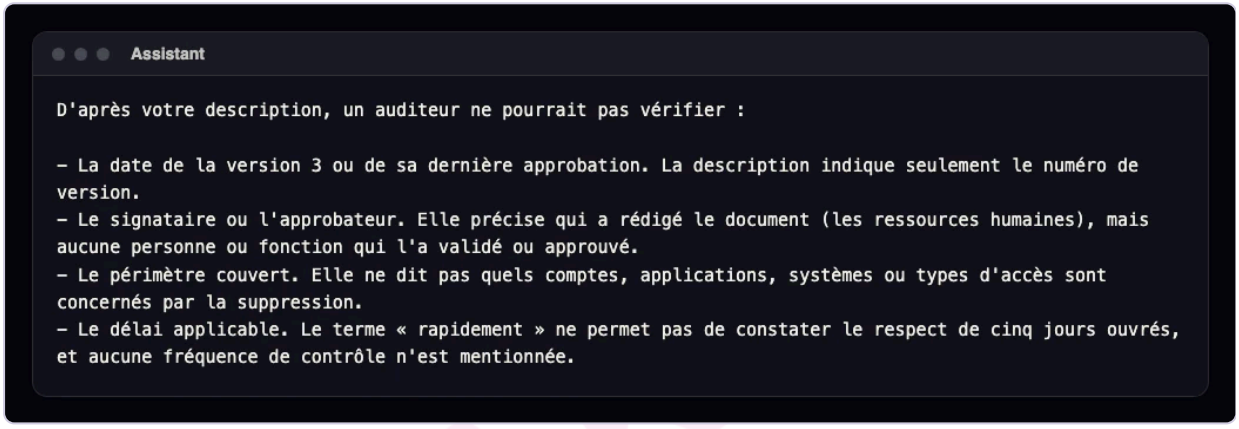


Figure 2. Sur une procédure de départ qui dit que les accès sont retirés « rapidement » : l'IA relève qu'aucune date, aucun approbateur et aucun délai chiffré ne figurent dans la description.

Chaque puce est une question à poser au propriétaire du document, ou une pièce à aller chercher : l'enregistrement des retraits d'accès réels, par exemple, prouve le délai mieux que la procédure.

Qui fait quoi

L'IA fait	Vous faites
Liste les preuves qu'un auditeur attend	Cherchez chaque preuve dans vos dossiers et notez où elle est
Dit ce qui manque dans votre description	Retrouvez la date et le signataire sur le document lui-même
Ne dit jamais qu'une preuve existe	Écrivez « Non trouvée » tant que vous n'avez pas ouvert le document
Ne juge pas si la preuve suffit	Faites relire par un auditeur avant l'audit

© SAKIRA. Reproduction et diffusion interdites sans accord écrit. · sakira.fr
SAKIRA SAS · 6 rue d'Armaille, 75017 Paris · SIREN 108 493 933

Ce que ce guide ne fait pas

Il ne dit pas si votre organisation est conforme, et il ne remplace pas la lecture du référentiel : l'IA liste les preuves usuelles, un auditeur peut en demander d'autres. Pour un audit de certification ou un audit client, demandez à un auditeur interne ou externe de relire votre tableau avant la date : lui seul dit si une preuve suffit.

© SAKIRA

© SAKIRA. Reproduction et diffusion interdites sans accord écrit. · sakira.fr
SAKIRA SAS · 6 rue d'Armaille, 75017 Paris · SIREN 108 493 933