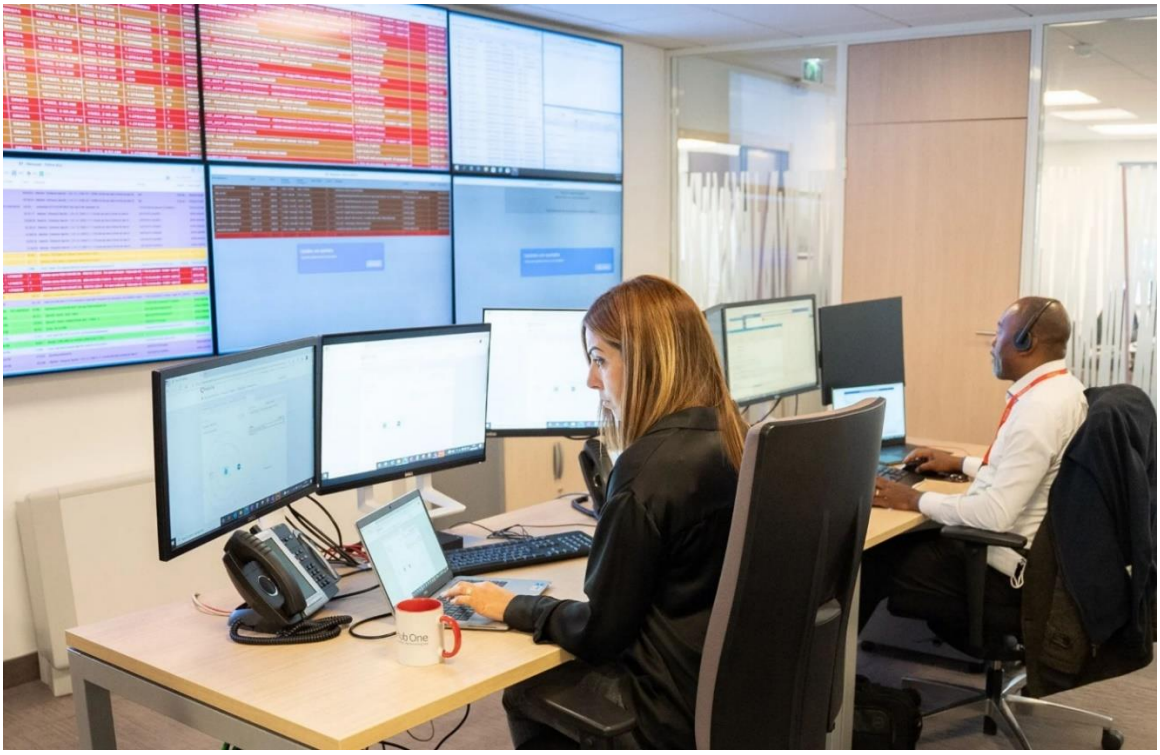
La visite sur site

d'un Prestataire de Services Externalisés



Centre d'exploitation -©VO

Temps de lecture : 4 mn

La revue sur site est un élément important dans le choix ou la confirmation d'un Prestataires de Services Externalisés, surtout s'il agit de services Essentiels.

Si la revue sur site n'est pas une obligation règlementaire, il est important de savoir quand elle est recommandée et pourquoi elle est réalisée.
En effet, si les rapports sur les contrôles, type ISAE 3402, et le contrat de niveau de service sont importants, ils ne suffisent pas pour justifier d'une diligence raisonnable.
Et **la visite sur site fait partie des moyens de diligence** sur les Prestataires.

Intérêt d'une visite sur site

Un **examen approfondi de la documentation disponible**, qu'elle soit fournie par le Prestataire de Services Externalisés, donnée par d'autres clients du Prestataire, par des associations professionnelles, ou juste disponible dans diverses bases de données, **est le prérequis** d'une diligence raisonnable.

Les visites sur site sont **nécessaires** lorsqu'il y a des informations importantes qui ne peuvent pas être obtenues à distance, ou lorsqu'il existe des informations discordantes, tout spécialement lorsqu'il s'agit de services critiques ou de données sensibles pour l'entreprise.
Ainsi, la visite sur site va souvent permettre d'**accéder à certains documents confidentiels** pour le Prestataire, comme l'encadrement des relations avec ses propres fournisseurs ou ses rapports de test de Plan de Continuité d'Activités.

La visite sur site d'un fournisseur va s'avérer particulièrement utile quand :

- **un Prestataire de Services Externalisés n'est pas soumis à une règlementation équivalente à celle qui régit l'entreprise** ;
- lors d'une entrée en relation, un Prestataire de Services Externalisés Essentiels ne peut donner suffisamment de **références** sur le marché local ;
- **les performances de niveau de service d'un Prestataire de Services Externalisés ne sont pas conformes aux engagements qu'il avait pris**.

Le droit d'audit, avec la visite sur site, par l'entreprise et aussi par les régulateurs, en intégrant le PCA, doit être **formalisé dans les contrats** avec le Prestataire, tout comme la clause de réversibilité.

Rapports sur les contrôles

Pour faire face aux demandes d'audit de leurs clients, les Prestataires de Services Externalisés établis établissent un guide décrivant leurs processus et les contrôles associés. Ils font ensuite vérifier ces documents et leur mise en œuvre par un tiers selon une méthodologie.

Pour les services financiers, le rapport **ISAE 3402** est un rapport sur **les contrôles qui ont un impact sur les états financiers des clients**.
Le Type I atteste de l'existence du contrôle interne, et **le type II de son efficacité**.
Les américains utilisent plutôt les rapports SOC 1 (« Systems and Organisation Control 1»), avec les deux mêmes types. Le rapports SOC 2 sont utilisés pour évaluer la sécurité du système d'information.

Ces rapports sont donc plus orientés sur l'impact financiers que sur la qualité des processus et le contrôle du changement. De plus, **le périmètre du rapport est parfois différent du périmètre des services externalisés par le client**.

Objectifs de la visite sur site

L'objectif sur site est de s'assurer de la cohérence entre les services tels qu'ils ont attendus et connus du client et de ceux qui sont effectivement opérés par le prestataire.

Si la visite n'est pas suffisamment préparée, la valeur de la visite sur place va être limitée à la confirmation de l'existence de l'entreprise et de certains de ses moyens, et éventuellement le respect de certaines politiques ou procédures.
La bonne pratique consiste à établir un guide d'audit pour les prestations externalisées, qui aidera aux préparations des visites.

Cartographie et encadrement des processus

L'existence et la qualité de la documentation des processus par le Prestataire est le premier point de la visite sur site.
Cette documentation doit absolument inclure les **processus de contrôle du changement** et les **méthodes de décision et de diffusion de ces changements**.
Tous les écarts observés doivent être consignés dans le rapport de visite et intégrés au plan d'action.

Vérification de points de contrôle

Les Prestataires sont chargés des contrôles de niveau 1, et parfois aussi de niveau 2.
Une vérification globale du **registre des contrôles** est réalisée, avec une vérification détaillée de quelques **contrôles par échantillonnage**.

Remontée et traitement des anomalies

Les anomalies doivent être remontées aux clients dans **des délais correspondant à leur criticité**.
Il convient de vérifier que les délais sont respectés et des anomalies ne restent pas en **déshérence**, soit parce qu'elles ont été affectées à un autre client, ou parce qu'elles ne sont pas affectées. La visite peut être l'occasion de créer une anomalie fictive pour observer son traitement.

Qualification des problèmes

Les anomalies récurrentes doivent l'objet d'un traitement spécifique par le Prestataire : **un plan d'action du Prestataire** doit être mis en place pour y remédier.

Identification des dépendances et atténuation des risques

La **dépendance du Prestataire à ses propres fournisseurs** pour réaliser les services ne doit pas être négligée.
Dans le cas d'une Prestation de Service Externalisé Essentielle (PSEE), c'est **la responsabilité du client d'exiger que le Prestataire lui déclare l'ensemble de la chaine de sous-traitance**.

Il est impératif de s'assurer que le Prestataire a bien évalué **la criticité des services qu'il a lui-même sous-traités et des solutions d'atténuation** qu'il a étudiées ou mises en place.
La bonne pratique, qui peut aussi être une exigence règlementaire, est de tenir à jour un registre des prestations externalisées.

Revue du Plan de Continuité d'Activités

Les résultats des tests d'activation des plans de continuité d'activités du Prestataire sont généralement confidentiels, mais ils peuvent souvent être consultés lors de visite sur site.
En général, le plan de continuité des activités du Prestataire (PCA) ne concerne que ses propres opérations. Il convient de s'assurer que ses sous-traitants ont eux aussi leur propre plan de continuité à jour et testé en coordination avec le Prestataire.

Adéquation des moyens

Le Prestataire doit **disposer des moyens techniques et humains suffisants** pour assurer sa mission.
S'il peut être difficile pour un Prestataire d'accueillir tous ses clients individuellement pour des visites sur site, l'incapacité d'accueillir un client important peut être révélateur d'un manque de moyens.

Rapport de visite

Le rapport de la visite sur site doit comporter des **analyses** sur les éléments quantitatifs sur les processus et leurs contrôles et des **avis** sur l'encadrement des risques et l'adéquation des moyens.

Ce rapport peut être une simple confirmation du prestataire, faire l'objet d'un plan d'actions spécifiques ou encore recommander la remise en concurrence du prestataire. Evidemment, il est souvent judicieux de partager les plans d'actions avec le Prestataire de Service Externalisés.

Synthèse

Même si la visite sur site n'est pas une obligation règlementaire, **la bonne pratique consiste à fixer une fréquence de visites régulières selon la criticité des services et la sensibilité des données**.