

# SOUS-TRAITANCE ET CLOUD

## En bref

Le recours généralisé à la sous-traitance et aux solutions cloud (SaaS, PaaS, IaaS) apporte agilité, expertise et maîtrise des coûts, mais fait peser sur l'entité des risques majeurs : sécurité des données, disponibilité et intégrité des traitements, dépendance au fournisseur et conformité réglementaire.

Pour le commissaire aux comptes, la perte de contrôle sur les systèmes hébergeant des données personnelles ou sensibles peut, de fait, être de nature à compromettre la fiabilité de l'information financière.

Il devra en conséquence se positionner sur :

- La cartographie du SI et l'identification des dits services externalisés,
- L'appréciation de la criticité des applications (faible pour la messagerie SaaS, élevée pour un ERP ou logiciel de paie),
- L'usage de rapports d'audit ad hoc (ISAE 3402/SOC, ISAE 3000), certifications (ISO 27001, SecNumCloud, HDS...) et de contrôles contractuels (clauses de réversibilité, SLA, droits d'audit) pour ajuster son approche d'audit (ITGC, ITAC, tests substantifs, etc.),
- L'anticipation des délais et la coopération variable des prestataires, tout en sensibilisant son client sur la nécessité de contractualiser l'accès aux informations nécessaires à l'audit.

Par ailleurs, la montée en puissance de NIS2, DORA et du RGPD renforce la responsabilité du client final et exige du CAC une vigilance accrue quant à la supervision effective des fournisseurs externes (Statuts des tiers – Sous-traitants/Responsable de traitement).

Enfin, l'entrée en vigueur du RIA au premier trimestre 2025, renforce encore un peu plus le poids des enjeux juridiques quant à l'externalisation du traitement des données, concernant l'usage de technologies à base d'IA (Intelligence Artificielle).

## Séquence 1

# Comprendre la thématique

## Contexte et enjeux

Le recours à des prestataires externes pour la gestion des systèmes d'information est aujourd'hui généralisé. Il peut prendre la forme de sous-traitance traditionnelle (infogérance, maintenance, hébergement) ou de solutions cloud (SaaS, PaaS, IaaS), portées par des éditeurs ou opérateurs spécialisés.

Ces modèles apportent de réels atouts (agilité, expertise, maîtrise des coûts), mais introduisent également des risques critiques pour l'entité, en matière de :

- Sécurité des données,
- Disponibilité et intégrité des traitements,
- Dépendance vis-à-vis du fournisseur,
- Et conformité réglementaire, notamment dans les secteurs sensibles.

Pour le commissaire aux comptes, la perte de contrôle direct sur des systèmes hébergeant des données comptables, financières ou opérationnelles sensibles peut compromettre la fiabilité de l'information financière.

Ce risque est accentué si l'entreprise ne dispose pas d'un cadre de gouvernance robuste ou d'une supervision suffisante des services externalisés.

Les principaux risques identifiés sont :

- Disponibilité du service : interruption chez le prestataire, affectant les clôtures ou la continuité des opérations; pertes de données éventuelles,
- Sécurité et confidentialité : accès inapproprié à des données sensibles, erreurs de traitement, failles techniques non corrigées,

- Réversibilité : incapacité à récupérer les données ou à redémarrer l'activité en cas de rupture contractuelle ou de défaillance du prestataire,
- Conformité réglementaire : non-respect des obligations issues du RGPD, de NIS2, de DORA ou des référentiels sectoriels (HDS, SecNumCloud...),
- Traçabilité et auditabilité : absence de journaux d'activité, de reporting individualisé ou de rapport de contrôle type ISAE 3402/SOC.

### Conséquences pour le commissaire aux comptes

Face à ces enjeux, le CAC doit adapter son approche pour :

- Cartographier le SI du client, afin d'identifier les services externalisés, les applications hébergées en cloud (SaaS notamment), et les processus impactés,
- Apprécier la criticité des applications concernées : une application SaaS utilisée pour la messagerie ou le marketing aura un impact faible sur les comptes, tandis qu'un ERP ou un logiciel de paie externalisé peut affecter directement les états financiers,
- Adapter ses travaux sur les ITGC : dans un environnement SaaS, l'analyse du contrôle interne repose en partie sur l'étude du cadre contractuel, et sur la revue de rapports d'audit de tiers (ISAE 3402, SOC 1 & 2), que le CAC doit savoir lire et interpréter.

**À noter :** certains éditeurs ou hébergeurs peuvent se montrer peu coopératifs ou ne pas fournir les données attendues sans délai ni développement spécifique. Le CAC doit anticiper ces délais et sensibiliser son client à l'importance de contractualiser les engagements d'accès à l'information utile à l'audit.

Enfin, la réglementation se durcit :

- La directive NIS2 impose aux entités critiques un encadrement strict de leur chaîne de sous-traitance numérique,
- Le règlement DORA (secteur financier) renforce les exigences de résilience opérationnelle vis-à-vis des prestataires IT,
- Le RGPD, toujours en vigueur, impose une formalisation contractuelle (article 28) et une traçabilité des traitements.

Ces cadres réglementaires renforcent la responsabilité du client final, mais nécessitent également une vigilance accrue du CAC sur la supervision réelle exercée sur les fournisseurs externes...

### Séquence 2

## Mission du CAC : objectifs, bonnes pratiques et outils

#### Thématique 1

### Garantie sur les contrôles et la conformité du prestataire (rapports ISAE/SOC/audits, SECNumcloud)

#### Objectifs

Le CAC doit évaluer si les prestataires externes sur lesquels l'entité s'appuie (hébergement, SaaS, infogérance) apportent des garanties suffisantes sur la sécurité, la qualité et la traçabilité des traitements.

Ces garanties peuvent être formalisées à travers :

- Des rapports d'audit tiers (ISAE 3402, SOC 1 & 2, ISAE 3000),
- Des certifications de référence (ISO 27001, ISO 22301, SecNumCloud, HDS...),
- Ou des démarches internes de contrôle (questionnaires, reporting, tableaux de bord).

Le CAC doit s'assurer que :

- Le périmètre couvert est bien celui du service utilisé,
- Les risques comptables et financiers sont effectivement adressés,
- Et que ces garanties ne couvrent pas seulement le prestataire, mais sont intégrées dans le dispositif global du client.

## Bonnes pratiques

### Analyser la portée réelle et le type des rapports fournis

Vérifier que les documents couvrent bien l'environnement utilisé par l'entité (ex. module comptable d'un ERP en SaaS), ainsi que les bonnes périodes (exercice en cours). Type I = design du contrôle / Type II = test opérationnel sur la durée.

### Identifier les contrôles restant sous la responsabilité du client

Exemples : création de comptes utilisateurs, paramétrages d'interfaces, processus de rapprochement.

### Demander les livrables clés :

Rapports annuels, plans d'action à la suite des audits, extraits de logs, attestations d'audit afin de vérifier si les écarts identifiés ont été traités par le client.

### Anticiper les limites de coopération de certains prestataires

Certains éditeurs SaaS refusent de transmettre des extractions ou imposent des formats fermés.

Il convient donc de prévoir un délai de négociation, voire une clause contractuelle pour encadrer ces points.

## Outils & documentations mises à disposition

### Tableau récapitulatif des rapports et certifications couramment rencontrés

Type	Acronyme	Description	Périmètre couvert	Points d'attention pour le CAC
Rapport d'attestation	ISAE 3402 / SOC 1	Contrôle interne sur processus liés aux états financiers	Prestations comptables / paie / ERP / SI	Type I ou II / adéquation du périmètre / période / sous-traitance
	SOC 2	Sécurité, confidentialité, disponibilité, etc.	Cloud, hébergement, SaaS	Complémentaire à ISAE 3402
	ISAE 3000	Données non financières (RGPD, ESG, etc.)	Activités diverses	Norme ouverte, vigilance sur le référentiel utilisé
	SOC 3	Version publique de SOC 2	Communication synthétique	Peu détaillé / ne se suffit pas à lui seul
Normes de certification	ISO 27001	Management de la sécurité de l'information	Entité, site, solution ou datacenter	Vérifier que le SMSI couvre bien le service utilisé
	ISO 22301	Management de la continuité d'activité	SI critique, PCA	À croiser avec l'analyse PRA/PCA
	ISO 27701	Extension ISO 27001 sur les données personnelles	Données personnelles	Intéressant pour les environnements RGPD
	HDS	Hébergement de données de santé (France)	Données de santé	Certification obligatoire en santé
	SecNumCloud	Certification ANSSI sur les prestataires cloud souverains	IaaS, PaaS, SaaS	Requis pour certaines entités régulées

## Impact dans la stratégie du commissaire aux comptes

Ces éléments peuvent :

- Réduire les travaux de test s'ils sont suffisamment probants et couvrent les bons risques,
- Mettre en évidence des zones non couvertes à compenser (ex : flux interapplicatifs, paramètres côté client),
- Être utilisés comme éléments probants indirects (NEP 500).

Le CAC doit alors :

- Vérifier l'actualité et la pertinence des documents,
- Sensibiliser le client à leur bonne lecture et exploitation,
- Et documenter les limites dans le dossier d'audit, notamment en cas de non-fourniture.

### Thématique 2

## Contrats, SLA et clauses critiques (réversibilité, sécurité, auditabilité ; sous-traitance ou responsable de traitement ?)

### Objectifs

Le CAC doit s'assurer que les relations contractuelles avec les prestataires couvrent les engagements essentiels liés à la continuité, à la sécurité, à la conformité et à l'accès aux informations nécessaires à l'audit. Il s'agit notamment de s'assurer que l'entreprise :

- Dispose de garanties suffisantes pour récupérer ses données en cas de rupture ou de sinistre,
- Peut auditer ou superviser les prestations externalisées,
- Et a clarifié les responsabilités juridiques, notamment au regard du RGPD.

Le CAC ne valide pas juridiquement les contrats, mais il doit alerter en cas d'absence de clauses critiques, susceptibles d'affecter la fiabilité de l'information financière ou la continuité d'exploitation.

## Bonnes pratiques

### Revue des clauses de réversibilité

Les contrats doivent prévoir les conditions de restitution des données, les coûts, leur format, les délais de migration et les responsabilités en fin de contrat.

**Astuce :** demander à voir la clause de réversibilité et vérifier si un plan de sortie est documenté.

### Revue des autres clauses de sécurité / confidentialité/ RGPD

Le contrat doit inclure des engagements concrets du prestataire sur :

- La protection des données,
- La gestion des incidents,
- Les contrôles d'accès.

Il est crucial de formaliser qui est le responsable de traitement et qui est le sous-traitant.

**Astuce :** interroger sur les obligations de notification en cas d'incident de sécurité et vérifier que les articles 28 et suivants du RGPD sont bien traités contractuellement.

### Vérifier la présence de SLA (Service Level Agreements) formalisés

Des niveaux de service doivent être définis (disponibilité, délais de rétablissement, support), avec des pénalités si les seuils ne sont pas respectés.

**Astuce :** contrôler les SLA pour les applications critiques (compta, paie, facturation...).

### S'assurer de la possibilité d'auditer ou d'obtenir des rapports de contrôle

Le contrat doit prévoir :

- Un droit d'audit formel accordé à l'entité (ou à ses auditeurs) sur les environnements externalisés,
- Ou, à défaut, la remise régulière de rapports de contrôle produits par des tiers indépendants (ex. rapports ISAE 3402, SOC 1 ou 2).

**Astuce :** interroger l'entité sur l'existence de rapports déjà transmis par le prestataire (rapport d'audit, synthèse de conformité, certification annuelle).

Si aucun document n'est disponible ou si la couverture est insuffisante, vous pouvez recommander la réalisation d'un audit du prestataire, dans le cadre d'un SACC (Service Autres que de Certification des Comptes), sous réserve de respecter les règles d'indépendance.

## Outils & documentations mises à disposition

Le CAC peut s'appuyer sur :

- Les contrats cadres et annexes avec les prestataires (hébergeur, SaaS, infogérant...),
- Les SLA et leurs rapports de suivi,
- Les clauses de réversibilité, de sécurité, et les annexes RGPD,
- Les rapports de contrôle interne fournis par les tiers (ISAE 3402 / SOC),
- Les grilles d'analyse contractuelle ou checklists fournies par les CRCC, CNIL ou l'ANSSI,
- Les guides sectoriels (ex. SecNumCloud, HDS...).

## Impact dans la stratégie du commissaire aux comptes

Un contrat mal rédigé ou incomplet peut exposer l'entreprise à :

- Une indisponibilité prolongée des données sans recours,
- Une impossibilité de récupérer ses systèmes ou fichiers en cas de rupture,
- Une perte de traçabilité sur les traitements externalisés,
- Ou encore une non-conformité réglementaire, notamment au regard du RGPD.

Le CAC devra alors :

- Adapter sa cartographie des risques (NEP 315),
- Renforcer ses tests sur les cycles supportés par des prestataires externes,
- Évaluer l'impact d'un défaut contractuel sur la fiabilité de l'information financière,
- Et, le cas échéant, communiquer ses observations à la gouvernance, voire les intégrer à sa lettre d'affirmation ou de recommandations.

## Divers

**Définition des acronymes les plus couramment rencontrés :**

Acronyme	Signification	Définition / Utilité
<b>SaaS</b>	Software as a Service	Application accessible en ligne, sans installation locale. Exemple : Salesforce, Silae.
<b>PaaS</b>	Platform as a Service	Environnement technique pour développer et exécuter des applications.
<b>IaaS</b>	Infrastructure as a Service	Mise à disposition d'infrastructure (serveurs, réseau, stockage) à la demande.
<b>On Premise</b>	—	Solution hébergée et exploitée en interne par l'entité, sur ses propres serveurs.
<b>BYOD</b>	Bring Your Own Device	Utilisation d'équipements personnels pour accéder au SI de l'entreprise.
<b>IDaaS</b>	Identity as a Service	Gestion des identités et des accès externalisée (authentification, MFA...).
<b>MFA</b>	Multi-Factor Authentication	Authentification renforcée par plusieurs facteurs (ex. mot de passe + code SMS).
<b>DLP</b>	Data Loss Prevention	Outils ou politiques visant à prévenir les fuites de données sensibles.
<b>SIEM</b>	Security Information and Event Management	Plateforme centralisée de journalisation et de détection d'incidents de sécurité.
<b>EDR</b>	Endpoint Detection and Response	Outil de détection de menaces sur les postes de travail et serveurs

### Sécurité des données externalisées

Lorsque des données sont traitées ou hébergées en dehors de l'entreprise, l'entité conserve l'entière responsabilité de leur protection — notamment en cas de traitement de données à caractère personnel. Le CAC doit donc s'interroger sur plusieurs points :

- Où sont physiquement stockées les données (UE / hors UE / cloud souverain) ?
- Quelles sont les mesures mises en place pour garantir la confidentialité, l'intégrité et l'accès restreint ?
- L'entité est-elle en conformité avec le RGPD, notamment l'article 28 sur les sous-traitants ?

*Cf. Fiche 05 - Conformité réglementaire pour une évaluation détaillée des enjeux de protection des données.*

### Accès des prestataires externes aux systèmes de l'entreprise

Les prestataires techniques (éditeurs, infogérants, hébergeurs...) disposent parfois de droits d'administration ou d'intervention à distance, avec des niveaux d'autorisation élevés (comptes à privilèges).

Le CAC doit vérifier :

- Que ces accès sont encadrés contractuellement (clause de responsabilité, conditions d'utilisation),
- Qu'ils sont techniquement tracés et contrôlés (journalisation, durée d'activation, double authentification),
- Qu'une revue régulière de ces accès est réalisée par l'entité.

*Cf. Fiche 03 - Contrôle des accès pour les bonnes pratiques de gestion des droits et des comptes à privilèges.*

### Type d'hébergement : dédié ou mutualisé ?

Le type d'hébergement a une incidence directe sur le niveau d'isolement des données, la sécurité et la réversibilité.

- En environnement mutualisé, les ressources sont partagées entre plusieurs clients, ce qui peut rendre plus difficile : le cloisonnement strict des données, la traçabilité des flux, ou la mise en œuvre d'audits individuels.

Le CAC devra donc s'assurer que :

- Des mesures de séparation logique sont effectivement en place,
- Le prestataire bénéficie de certifications adaptées (ex. SecNumCloud, HDS),
- Et que les modalités de restitution des données sont bien prévues.

### Flux de données externalisés

L'externalisation ne concerne pas seulement le stockage ou l'exécution : elle implique souvent des **flux d'échange de données** entre l'entreprise et ses prestataires (ex. : envoi de fichiers de paie, extraction comptable, retour de justificatifs...).

Le CAC doit vérifier que :

- Ces flux sont **cartographiés et documentés**,
- Ils sont **chiffrés ou sécurisés** lors des transferts,
- Leur **intégration dans les systèmes internes** ne pose pas de risque d'altération ou de perte,
- La conformité des **traitements réalisés** sur les données cibles (**données personnelles - RGPD, traitement par IA - RIA**).

Conséquence de quoi aujourd'hui l'approche du CAC, en matière d'**externalisation de la donnée**, doit être la plus holistique possible en intégrant les aspects technique (Système d'Information) et juridique (RGPD, RIA, etc.) dans l'approche d'audit déployée

*Cf. Fiche 07 - Exploitation informatique sur la gestion des flux applicatifs, la supervision, l'ordonnancement et la surveillance.*

## Séquence 3

# Cas d'usage

### Contexte de l'entité :

La société ABSOLUMENT SAAS est une PME de prestations de services, disposant d'un ERP en hébergement SaaS (solution cloud accessible via navigateur) et ayant externalisé son infogérance (maintenance, support et gestion de l'environnement utilisateur).

L'appréciation du risque par le commissaire aux comptes se limite à la comptabilité, la facturation vente et la paie, tous supportés par l'ERP.

### Problématiques rencontrées

Le CAC souhaite évaluer la fiabilité des traitements comptables, de paie et de facturation réalisés dans un environnement 100 % externalisé. Aucun accès direct n'est possible aux serveurs.

L'entreprise s'appuie sur un contrat standardisé avec l'éditeur de l'ERP et n'a pas mené d'audit formel de ses prestataires.

### Travaux réalisés

#### Cartographie des systèmes

Avec une identification des applicatifs externalisés (incluant l'hébergement) et des flux de données.

#### Revue documentaire

- Obtention du contrat de prestation,
- Identification d'éventuelle certification ou rapport ISAE 3402 et SOC2 fourni par l'éditeur de l'ERP, couvrant l'exercice audité, (Cf. onglet ITGC x Référentiels de l'outil fourni)
- Vérification que le rapport couvre bien le périmètre utilisé par l'entité (comptabilité, paie), et que les tests opérationnels soient concluants.

#### Analyse contractuelle

- Revue du contrat et des SLA (Service Level Agreement),
  - Le contrat couvre-t-il le périmètre et l'exercice audité ?
  - Quelles sont les clauses existantes ? (Réversibilité, RGPD, Disponibilité de la donnée, etc...),
  - Comment sont gérées les sauvegardes chez l'éditeur ? Ou sont physiquement stockées vos données ?
  - Un test de restauration a-t-il été réalisé au cours de la période ? Respecte-t-il les engagements contractuelles ?
  - Des tests de cyber-résilience ont-ils été réalisés ? Ont-ils mis en exergue un risque pour la société audité ?
  - Existe-t-il des rapports de suivi réguliers des SLA ? Ces rapports sont-ils conservés et exploitables pour contrôle ?
- Revue des accès étendus attribués à l'éditeur ainsi que de leur supervision.

#### Contrôles internes côté client

- Revue des rapports de type ISAE 3402 et identification des contrôles restants à la charge du client : création/suppression des utilisateurs, paramétrage des plans comptables, suivi des exports et/ou des interfaçages,
- Revue des accès utilisateurs et des logs d'administration fournis par le support,
- Revue des incidents (Cf. Fiche 06. Exploitation des SI).

### Impact pour l'approche d'audit

- Limitation des tests sur les cycles non couverts par le rapport ISAE, avec un complément ciblé sur les interfaces et les contrôles utilisateurs,
- Documentation des limites d'accès et des risques contractuels dans le dossier d'audit,
- Communication des recommandations formelles à la gouvernance sur la gestion des risques liés à l'externalisation (y compris RGPD et continuité d'activité).

En cas de violation des données, le commissaire aux comptes devra adapter sa stratégie en intégrant une analyse de l'impact de l'incident sur la fiabilité et l'intégrité des données financières.



## Séquence 4

# Allez plus loin

## Missions complémentaires possibles (SACC)

Le CAC peut, sous réserve du respect des règles d'indépendance, proposer des prestations de services autres que de certification des comptes (SACC) en lien avec la sous-traitance ou les projets de migration IT. Exemples :

### Audit d'un projet de migration / transformation SI :

- Revue des risques associés (perte de données, cut-off),
- Vérification de la trajectoire projet, des livrables et des tests,
- Anticipation des impacts sur les comptes.

### Revue contractuelle ciblée :

- Sur les contrats cloud ou d'infogérance critiques,
- Sur les clauses d'assurance, de réversibilité, de continuité ou de disponibilité,
- En lien avec un changement d'environnement applicatif.

### Diagnostic de conformité RGPD :

- Sur le traitement des données personnelles au sein de l'entreprise,
- Sur les enjeux spécifiques relatifs aux données dites « sensibles »,
- En lien avec la réalisation d'une analyse d'impact.

## Ressources pratiques

### Outils CNCC/CRCC

- RGPD'AUDIT
- Cyber'AUDIT

### Documentation technique

- **COBIT** (ISACA) – Référentiel de gouvernance IT (notamment le domaine DSS et EDM)
- **SecNumCloud** – Guide ANSSI pour l'évaluation des prestataires cloud souverains
- **Guide de contractualisation CNIL** – Points de vigilance et modèle de clauses
- **ISO 27036** – Lignes directrices pour la sécurité dans les relations avec les fournisseurs

### NEP et référentiels

- NEP-250. Prise en compte du risque d'anomalies significatives dans les comptes résultant du non-respect des textes légaux et réglementaires
- NEP-315. Connaissance de l'entité et de son environnement et évaluation du risque d'anomalies significatives dans les comptes

## Formations recommandées

- CISA (Certified Information Systems Auditor) – ISACA
- CRISC (Certified in Risk and Information Systems Control) – ISACA
- Formations CNCC / CRCC

## Organismes spécialisés

- CNIL – Autorité française pour les questions de traitement des données personnelles
- ANSSI – Autorité nationale en cybersécurité (SecNumCloud, guides pratiques)
- ISACA – Organisation internationale de référence en audit et gouvernance IT
- ENISA – Agence européenne pour la cybersécurité (guides DORA, NIS2)