

# GOVERNANCE DES SI

## En bref

Pourquoi parler de gouvernance des systèmes d'information ?

Les systèmes d'information sont devenus le socle opérationnel, décisionnel et réglementaire de toutes les organisations.

Leur gouvernance ne relève plus uniquement d'une approche purement technique. Elle constitue un levier stratégique de maîtrise des risques, de performance durable, de la pérennité ainsi que de la fiabilité de l'information tant financière que non financière.

Pour le commissaire aux comptes, comprendre et évaluer la gouvernance des SI permet :

- De s'assurer que les enjeux numériques sont intégrés à la stratégie globale de l'entreprise et donc de sa maîtrise ;
  - D'identifier des risques transverses susceptibles d'affecter la qualité de l'information (pilotage déficient de projets SI, affaiblissement du contrôle interne, cybersécurité fragile) ;
  - D'évaluer la capacité de l'organisation à maîtriser ses ressources technologiques et à gérer ses projets dans un cadre sécurisé, conforme et efficient.
- La gouvernance SI agit ainsi comme un révélateur :
- Lorsqu'elle est claire et partagée, elle contribue à réduire les incertitudes, à renforcer les contrôles, et à mieux aligner la technologie sur les besoins métier ;
  - Lorsqu'elle est absente ou défaillante, elle constitue un signal d'alerte pour l'auditeur.

Dans un contexte de transformation numérique accélérée et de pression réglementaire croissante (RGPD, DORA, CSRD...), l'analyse de la gouvernance des SI s'impose comme un élément clé de toute démarche d'audit, à la croisée du stratégique, de l'organisationnel et du technique.

## Séquence 1

# Comprendre la thématique

## Contexte et enjeux

La gouvernance des systèmes d'information constitue un enjeu central de maîtrise des risques pour toute organisation. Elle regroupe l'ensemble des dispositifs permettant :

- d'aligner les SI sur la stratégie de l'entité,
- de piloter les investissements en concordance avec les dernières technologies existantes sur le marché et/ou chez les concurrents,
- d'encadrer les risques numériques,
- et de garantir la conformité réglementaire (RGPD, DORA, NIS2...)

Pour le commissaire aux comptes, une gouvernance SI défaillante peut engendrer des conséquences directes sur la qualité de l'information financière : dérives de projets structurants, erreurs comptables, affaiblissement du contrôle interne, dépendance excessive à des prestataires.

Des signaux d'alerte tels que l'absence de comitologie SI, la mauvaise gestion des accès, ou l'insuffisance du suivi des projets structurants (ex. ERP) doivent être analysés.

Les carences de gouvernance peuvent également impacter plusieurs cycles sensibles : les immobilisations incorporelles, les provisions, ou encore les charges liées aux échecs projet, voire la continuité d'exploitation.

Dans ce contexte, intégrer une revue de la gouvernance SI dans l'évaluation des risques d'audit permet au commissaire aux comptes :

- d'adapter ses travaux aux zones les plus exposées,
- De mieux cibler les zones sensibles à forte dépendance numérique,
- et de formuler des recommandations étayées à l'organe de direction.

La maturité de la gouvernance SI devient ainsi un indicateur indirect mais révélateur de la robustesse financière et de la résilience opérationnelle de l'entité auditée.

## Conséquences pour le commissaire aux comptes

Les enjeux liés à la gouvernance des systèmes d'information influencent directement l'approche d'audit du commissaire aux comptes, car ils affectent la fiabilité des informations financières, la qualité du contrôle interne et la capacité de l'entité à gérer ses risques.

### Sur l'évaluation des risques d'audit :

- Une gouvernance SI défaillante (pilotage faible, rôles mal définis, documentation absente, non-respect des processus) accroît le risque inhérent et le risque de non-détection. Le CAC devra alors réviser son évaluation des risques, adapter sa stratégie d'audit en conséquence, et élargir l'analyse de certains cycles (achats, paie, immobilisations, etc.).

### Sur la planification des travaux :

- En présence de projets SI en cours (ERP, migration cloud, automatisation...), le CAC peut anticiper des pics de risque et planifier des revues spécifiques sur les périodes sensibles : phases de bascule, mise en production, clôture comptable...

### Sur la nature et la profondeur des tests :

- Une gouvernance SI solide autorise souvent un appui partiel sur le contrôle interne. En revanche, en cas de faiblesse, il sera nécessaire de renforcer les tests substantifs, procéder à des contrôles manuels, et élargir ses revues documentaires (traçabilité des données, qualité des livrables, validation des accès...).

### Sur la communication avec la gouvernance :

- Des constats critiques sur la gouvernance SI peuvent justifier des observations formelles, voire un signalement au comité d'audit, notamment si les risques identifiés peuvent impacter la régularité ou la sincérité des comptes.

## Séquence 2

# Mission du CAC : objectifs, bonnes pratiques et outils

### Thématique 1

## Organisation et pilotage du Système d'information

### Objectifs

Le commissaire aux comptes doit s'assurer que l'organisation du système d'information repose sur des structures claires de gouvernance, de pilotage et de responsabilité. L'objectif est de déterminer si les instances décisionnelles IT (comité SI, comité projets, comité de sécurité...) assurent une supervision efficace, un suivi des objectifs numériques, et une traçabilité des décisions techniques et budgétaires.

Il s'agit notamment de vérifier :

- que le rôle de la DSI ou du responsable IT est clairement positionné dans l'organigramme ;
- que la stratégie SI est alignée avec la stratégie d'entreprise ;
- que les projets structurants (ERP, migration cloud, cybersécurité) font l'objet d'un pilotage formel.

### Bonnes pratiques

- **Formalisation d'une instance de gouvernance SI** clairement identifiée (comité SI, comité projets IT ou équivalent), rattachée à la direction générale, avec un rôle défini : validation des orientations, suivi des projets, arbitrage budgétaire, gestion des risques numériques.
- **Définition explicite des responsabilités SI**, avec une cartographie des acteurs clés (DSI, chefs de projets, responsables métiers, RSSI) et des fiches de fonction ou lettres de mission pour encadrer les délégations.
- **Tenue régulière de comités SI ou comités projets**, avec des ordres du jour formalisés, des procès-verbaux conservés, et une traçabilité claire des décisions prises (budgets, planning, risques...).

- **Mise en place de tableaux de bord de pilotage SI partagés**, combinant des indicateurs techniques (disponibilité, incidents, avancement des projets) et des indicateurs financiers (coûts, écarts budgétaires, ROI projet). Ces indicateurs doivent être revus périodiquement par la direction.
- **Lien établi entre la stratégie numérique et la stratégie d'entreprise**, via une feuille de route SI alignée sur les enjeux métiers (ex. : digitalisation des processus, conformité réglementaire, cybersécurité, performance).
- **Existence d'un mécanisme d'alerte et d'escalade**, permettant de remonter rapidement les incidents majeurs, les dérives projets (délais, budget, qualité) ou les non-conformités, avec un traitement documenté des décisions correctives.
- **Processus de suivi budgétaire IT**, avec une distinction claire entre dépenses d'investissement (CAPEX) et charges (OPEX), et un lien entre dépenses engagées et livrables obtenus.

## Outils & documentations

- **Organigrammes fonctionnels et techniques** précisant les rattachements hiérarchiques et opérationnels entre les directions métiers, la DSI, le RSSI, et les éventuels prestataires IT. Ces documents permettent de visualiser la structure de pilotage du SI et d'identifier les zones de responsabilité.
- **Procès-verbaux (PV) des comités SI**, comités projets ou comités risques, mentionnant : la fréquence des réunions, les décisions prises, les points de suivi des projets ou des risques et les demandes d'arbitrage ou d'escalade. Leur présence atteste d'un pilotage effectif et documenté.
- **Tableaux de bord IT** consolidés : incluant des indicateurs quantitatifs (temps d'arrêt, taux de disponibilité, avancement projet, backlog, volumétrie des tickets) et qualitatifs (niveau de satisfaction utilisateur, maturité cyber, évaluation des fournisseurs).
- **Plan stratégique IT** ou **schéma directeur informatique**, présentant la trajectoire de transformation digitale envisagée par l'entité : objectifs, jalons, priorités, alignement avec les orientations métier.
- **Budgets IT détaillés**, assortis d'un suivi régulier des engagements et des réalisations. Ce suivi doit permettre de relier les coûts engagés aux résultats produits, et de détecter les dérives ou sous-performances.
- **Documents de gouvernance interne**, tels que : Chartes informatiques, Politique de sécurité du système d'information (PSSI), politiques de pilotage des projets, cadre de priorisation des investissements SI, ou cartographie des projets actifs.

## Impact dans la stratégie du CAC

Une gouvernance IT bien structurée, reposant sur des instances formalisées, une traçabilité des décisions et une transparence du pilotage, constitue un indicateur de maturité organisationnelle. Elle permet au commissaire aux comptes de :

- **Mieux apprécier l'environnement de contrôle interne**, notamment pour les cycles sensibles automatisés (achats, paie, immobilisations, ventes, etc.) ;
- **Réduire son niveau de risque initial**, et potentiellement s'appuyer (sous conditions) sur les dispositifs existants pour ses travaux.
- À l'inverse, en cas de **pilotage flou, non documenté ou insuffisamment structuré**, le CAC doit :
- **Accroître ses diligences sur la qualité des flux comptables**, en particulier ceux intégrés ou automatisés via les systèmes d'information ;
- **Étendre ses vérifications** sur les zones à fort enjeu : immobilisations incorporelles (projets IT capitalisés), provisions, engagements contractuels liés à des projets numériques ;
- **Documenter plus rigoureusement ses travaux**, y compris les limites rencontrées dans l'analyse de la gouvernance, notamment si elles affectent la capacité de l'entité à maîtriser ses projets ou assurer la continuité d'exploitation.

En somme, la qualité de l'organisation et du pilotage SI constitue un facteur déterminant dans le calibrage de l'approche d'audit, tant sur le périmètre des contrôles que sur la nature des tests à effectuer.

## Thématique 2

Répartition des responsabilités  
& gestion des acteurs IT

## Objectifs

Le commissaire aux comptes évalue si la répartition des rôles, des responsabilités et des pouvoirs au sein du dispositif IT est claire, formalisée et maîtrisée.

Cette analyse vise à s'assurer que :

- les **décisions structurantes en matière de SI** sont prises par des personnes compétentes,
- les **responsabilités sont bien réparties** entre les acteurs internes et externes,
- et que les **zones de concentration de pouvoirs ou de non-supervision** sont identifiées.

Une organisation floue ou non documentée peut compromettre la fiabilité des traitements automatisés, des projets structurants ainsi que des données comptables produites.

## Bonnes pratiques

- **Formalisation des rôles clés** de la gouvernance IT (DSI, RSSI, chefs de projet, responsables applicatifs, administrateurs...) via fiches de fonction, lettres de mission ou chartes internes.
- **Cartographie des responsabilités** sur les périmètres critiques : administration des accès, traitement des anomalies, gestion des sauvegardes, conduite de projets, relation avec les prestataires...
- **Processus de validation et délégation** clairement définis et tracés : choix d'architecture, approbation des investissements, validation des mises en production, habilitations sensibles.
- **Revue périodique des responsabilités**, notamment en cas de réorganisation, de changement d'ERP, ou de transfert d'activité vers un prestataire.
- **Mécanismes de coordination entre acteurs** internes (IT, métiers, contrôle de gestion...) et externes (infogérance, éditeurs, hébergeurs), pour éviter les zones grises.

## Outils &amp; documentations

**Organigrammes fonctionnels et techniques**

- Représentation claire des lignes hiérarchiques et opérationnelles, incluant les fonctions IT, sécurité, projets, data, et les interactions avec les directions métier.

**Fiches de poste, lettres de mission ou chartes de rôle**

- Pour chaque acteur clé identifié (DSI, RSSI, chefs de projet, administrateurs, data owner...), documentant les responsabilités, les pouvoirs délégués, et les obligations de reporting.

**Cartographie des responsabilités**

- Matrice RACI ou référentiel de répartition des tâches couvrant les processus critiques (gestion des accès, validation des livrables, conduite des projets, gestion des incidents, etc.).

**Registre des prestataires IT**

- Liste des fournisseurs externes critiques avec rattachement des responsabilités internes (qui pilote, qui valide, qui contrôle).

**Supports de coordination interne**

- PV ou reporting des réunions entre IT, métiers, contrôle interne, ou contrôle de gestion : échanges d'information, arbitrages, suivi d'actions.

## Récapitulatif synthétique « Qui fait quoi ? »

Fonction	Acronyme (FR / EN)	Rôle principal dans la gouvernance IT
Directeur des systèmes d'information	DSI / CIO ( <i>Chief Information Officer</i> )	Définit et met en œuvre la stratégie SI, pilote les projets structurants, gère le budget IT, rend compte à la DG ou au comité SI.
Directeur de la sécurité des SI	RSSI / CISO ( <i>Chief Information Security Officer</i> )	Supervise la politique de cybersécurité, gère les risques IT, pilote les audits de sécurité et la réponse aux incidents.
Responsable de la gouvernance IT (le cas échéant)	RGI / IT Governance Officer	Veille à l'alignement du SI avec la stratégie d'entreprise, anime la gouvernance et les comités SI, suit les indicateurs de pilotage.
Responsable de la conformité IT	RCI / IT Compliance Officer	Supervise la conformité du SI avec les réglementations (ex. : RGPD, DORA, LPM), et les politiques internes.
Responsable de la production informatique	RPI / IT Operations Manager	Garantit le fonctionnement continu des infrastructures, le traitement des flux, la supervision et les sauvegardes.
Responsable de projet SI	Chef de projet / IT Project Manager	Conduit les projets (ERP, cloud, GED, etc.), gère les plannings, les risques, le budget, et le lien entre MOA/MOE.
Responsable applicatif	Responsable fonctionnel / Product Owner	Gère une application métier spécifique (ex. : paie, compta), suit les anomalies, valide les évolutions fonctionnelles.
Administrateur systèmes et réseaux	Admin. Systèmes / Sysadmin	Gère les serveurs, les droits d'accès, les environnements techniques, les mises à jour, la sécurité technique.
Administrateur base de données	DBA ( <i>Database Administrator</i> )	Responsable de l'intégrité, de la performance et de la sécurité des bases de données de production.
Utilisateur clé métier	Key User	Fait le lien entre la DSI et les utilisateurs métier, participe aux tests, à la formation, au support et à la validation des évolutions.
Responsable de la donnée / Propriétaire de donnée	Data Owner	Définit les règles de gestion et de qualité des données, valide les référentiels, gère les droits d'usage métier.
Prestataire IT externe	Infogérant / Third-party provider	Exécute des prestations déléguées (hébergement, support, maintenance), sous pilotage de la DSI ou du responsable de contrat.

## Impact dans la stratégie du CAC

Une répartition claire et bien encadrée des responsabilités IT constitue un facteur de confiance pour le CAC dans l'évaluation de l'efficacité du contrôle interne informatisé, la qualité des livrables SI et la conformité des opérations critiques.

À l'inverse, une confusion des responsabilités, une superposition des rôles ou une délégation non tracée peut conduire à

- renforcer les tests substantifs sur les cycles sensibles,
- réinterroger la fiabilité des traitements informatiques,
- formuler des observations à la gouvernance sur les dispositifs de pilotage IT.

## Thématique 3

Cohérence fonctionnelle  
& contrôle interne IT

## Objectifs

Le commissaire aux comptes doit s'assurer que le système d'information permet une gestion fluide, fiable et maîtrisée de l'information financière et non financière. Cela suppose que les outils couvrent l'ensemble des processus critiques, que les flux inter-applicatifs soient cohérents et automatisés, et que les traitements informatisés soient intégrés dans un contrôle interne structuré.

Il s'agit de vérifier que les applications utilisées sont bien alignées avec les processus métiers, que les interfaces fonctionnent correctement sans rupture de chaîne, et que la donnée qui alimente les comptes est produite et contrôlée dans un environnement sécurisé, traçable et documenté.

## Bonnes pratiques

- **Cartographie complète du système d'information**, représentant de manière lisible les applications, les interfaces et leur lien avec les processus de gestion (ex. : commande → livraison → facturation → comptabilisation).
- **Documentation des contrôles automatisés** intégrés dans les outils : règles de validation, blocages sur seuils, contrôles de cohérence ou d'exhaustivité, alertes sur écarts.
- **Mécanismes de traçabilité efficaces**, via des fichiers de logs, des pistes d'audit intégrées ou des historiques de modifications : indispensables pour vérifier les opérations sensibles.
- **Contrôle formalisé des droits d'accès aux outils**, avec une séparation claire des rôles (création, validation, mise en production) et des revues régulières des profils sensibles (ex. : admin ERP, superviseurs paie).  
(Cf. Fiche 02 - Contrôle des accès)
- **Fiabilisation des interfaces inter-systèmes** : automatisation des échanges (API, ETL, transferts sécurisés), documentation des flux, et suivi des erreurs d'intégration.
- **Alignement régulier entre les processus réels et les paramètres du SI** : la documentation doit refléter les pratiques réelles ; les ajustements manuels ou les outils « Hors SI » (Excel, saisie parallèle) doivent être maîtrisés.
- **Tests réguliers de robustesse** : simulations de bascule, tests de continuité d'activité, campagnes de tests sur les traitements comptables automatisés.

## Outils &amp; documentations

- **Cartographie applicative et logigrammes métier/SI** : pour comprendre le périmètre couvert, les enchaînements fonctionnels, les interfaces critiques.
- **Documentation des paramètres applicatifs**, notamment sur les cycles comptables : règles d'imputation automatique, journaux de clôture, seuils de déclenchement des contrôles.
- **Matrice des droits d'accès et profils utilisateurs**, avec documentation des principes de séparation des tâches, notamment sur les cycles à risque.
- **Fichiers de logs, rapports de supervision ou outils de traçabilité**, permettant de reconstituer les opérations critiques (modification de données, suppression d'écritures, création de fournisseurs...).
- **Dossiers d'interfaces** : documentation technique des flux automatisés entre applications (formats, fréquence, gestion des erreurs, points de réconciliation).
- **Rapports d'audit IT et plans d'action associés**, notamment en cas d'audit interne, de contrôle réglementaire (CNIL, ACPR), ou d'évaluation RGPD/DORA.

## Impact dans la stratégie du CAC

Un système d'information cohérent, automatisé et bien contrôlé permet au commissaire aux comptes d'accroître sa confiance dans les données produites et, sous conditions, de réduire la profondeur de certains tests substantifs.

À l'inverse, toute rupture dans la chaîne d'information, toute absence de supervision des interfaces, ou tout accès inapproprié peut générer des anomalies significatives, voire des risques de fraude ou d'erreurs non détectées.

Le CAC doit alors élargir son périmètre de tests, renforcer ses investigations sur les traitements manuels ou les systèmes en silo, et, si nécessaire, adresser des recommandations formelles à la gouvernance sur la robustesse du SI.



## Thématique 4

# Divers

*Sujets complémentaires à considérer selon le contexte*

Tous les environnements SI ne présentent pas le même niveau de complexité ou de maturité. Certains sujets peuvent ne pas justifier une revue systématique, mais doivent être pris en compte par le CAC lorsqu'ils représentent un enjeu pour la fiabilité de l'information financière, la maîtrise des risques ou la continuité d'exploitation.

### Gouvernance des projets informatiques

*(Cf. Fiche 03 – Conduite de projet)*

Dans le cadre d'un projet structurant (mise en place ou migration d'un ERP, digitalisation des processus, migration cloud...), le CAC évalue l'existence d'un cadrage clair, d'une gouvernance projet, d'un dispositif de suivi des risques et d'une formalisation des livrables (recette, PV de mise en production, documentation fonctionnelle). Des projets mal pilotés ou en dérive peuvent impacter directement la production des états financiers.

### Gouvernance des données (data governance)

Le CAC peut s'intéresser à la gestion de la qualité des données, notamment si les comptes sont alimentés par des référentiels complexes ou des chaînes d'intégration multiples. La fiabilisation des rôles dédiés (data owner, data steward), de règles de qualité, ou d'un dispositif de revue des référentiels peut constituer un facteur de fiabilisation.

### Continuité d'activité et PRA/PCA

*(Cf. Fiche 07 – PCA & PRI)*

En cas de dépendance forte au SI, ou dans les secteurs sensibles (santé, transport, finance...), l'existence d'un plan de continuité d'activité (PCA) ou d'un plan de reprise informatique (PRI) documenté et testé peut constituer un critère de robustesse opérationnelle. Le CAC peut interroger la direction sur les dispositifs en place, sans nécessairement en évaluer le détail technique.

### Cybersécurité et gestion des incidents

*(Cf. Fiche 08 – CyberSécurité)*

Même si le CAC ne mène pas un audit de sécurité, il peut être amené à interroger l'entité sur les incidents significatifs (cyberattaques, ransomware, pertes de données...) survenus sur l'exercice, et les mesures correctrices mises en place. La cybersécurité devient un enjeu transversal, dont la maturité peut impacter la confiance du CAC dans la maîtrise des systèmes.

### Relation avec les prestataires externes

*(Cf. Fiche 09 – Sous traitance & Cloud)*

Lorsque des fonctions SI critiques sont externalisées (infogérance, hébergement cloud, TMA, éditeurs SaaS), il est important d'identifier la gouvernance en place, les clauses contractuelles (SLA, sécurité, continuité), et le niveau de supervision interne. Une absence de pilotage peut constituer une zone de risque.

## Séquence 3

# Cas d'usage

## Contexte de l'entité

La société **SERVINOVA** est une entreprise de services spécialisée dans la gestion externalisée de prestations RH pour les collectivités locales. Elle emploie 60 collaborateurs, dispose de trois sites, et génère un chiffre d'affaires de 65 M€.

Son système d'information repose sur plusieurs briques fonctionnelles : un logiciel métier SaaS, un ERP comptable interne, une solution de paie infogérée, et divers outils bureautiques. L'activité étant soumise à de fortes contraintes réglementaires, la direction a entrepris une transformation numérique partielle en 2023, avec des changements organisationnels non finalisés.

## Travaux à réaliser

### Organisation SI et alignement stratégique

Le CAC doit évaluer si la gouvernance SI permet un alignement effectif entre stratégie d'entreprise, besoins métiers et fonctionnement des systèmes.

- Existe-t-il une gouvernance SI formalisée (comité, feuille de route, suivi des projets) ?
- Le SI est-il intégré dans les arbitrages stratégiques ou budgétaires ?
- Une analyse de risques SI ou de dépendances critiques est-elle disponible ?
- Les rôles clés (DSI, RSSI, responsables applicatifs) sont-ils désignés et documentés ?
- La DSI rend-elle compte régulièrement à la direction ? Des indicateurs sont-ils suivis ?

**Répartition des responsabilités et dispositifs de supervision**

Le CAC s'assure de la clarté des responsabilités, de la supervision des acteurs SI et de la maîtrise des délégations internes.

- Les fonctions critiques (administrateurs, référents IT, key users) sont-elles identifiées et formalisées ?
- Une matrice RACI existe-t-elle pour les processus clés ?
- Les délégations de pouvoir sont-elles à jour et opposables ?
- Des relais sont-ils prévus en cas d'indisponibilité de personnes clés ?
- Des procédures de suivi (revue de performance, reporting IT) sont-ils en place ?

**Cohérence fonctionnelle et couverture applicative**

Le CAC vérifie que le système d'information couvre bien l'ensemble des processus métier, sans rupture ou doublon de traitement.

- Les processus critiques (ventes, achats, paie, stock, immobilisations) sont-ils intégralement couverts par les outils ?
- Les flux entre applications sont-ils automatisés ? Documentés ? Traçables ?
- Des écarts ou anomalies d'intégration ont-ils été identifiés et suivis ?
- Les outils sont-ils alignés sur les processus métiers réellement appliqués ?
- Un référentiel d'architecture ou une cartographie applicative existe-t-il ?

**Contrôle interne informatisé et fiabilité des traitements**

Le CAC évalue l'efficacité des contrôles intégrés dans les systèmes (automatisations, paramétrages, séparation des tâches...).

- Existe-t-il une matrice des habilitations et une revue périodique des accès ?
- Les paramétrages comptables (comptes par défaut, TVA, analytique) sont-ils validés et restreints ?
- Les contrôles automatisés (alertes, blocages, double validation) sont-ils actifs ?
- Les logs de connexion et d'opérations sont-ils activés, stockés et revus ?
- Des tests périodiques de fonctionnement du contrôle interne IT sont-ils réalisés ?

**Sécurité, sauvegardes et continuité informatique**

Le CAC doit apprécier le niveau de résilience du SI face aux risques techniques, humains ou cyber.

- Une politique de sauvegarde est-elle en place, testée et externalisée ?

- Un Plan de Reprise Informatique (PRI) existe-t-il ? A-t-il été testé ?
- Les procédures de redémarrage sont-elles accessibles, documentées, à jour ?
- Des incidents (cyber, pannes) ont-ils été recensés ? Comment ont-ils été traités ?
- Une sensibilisation à la sécurité a-t-elle été réalisée (phishing, MFA, etc.) ?
- Quels sont les moyens utilisés pour sécuriser les systèmes d'information ?

**Sous-traitance, infogérance et outils SaaS**

Le CAC évalue la maîtrise des tiers techniques et la robustesse contractuelle associée aux prestataires.

- Les prestataires critiques sont-ils identifiés (ERP, hébergeur, infogérant, éditeurs SaaS) ?
- Des contrats-cadres (SLA, clause de continuité, portabilité des données) sont-ils signés ?
- Des audits externes (ISAE 3402, SOC 1/2) sont-ils disponibles ?
- Une gouvernance des prestataires (comité, revues, pénalités) est-elle en place ?
- En cas de rupture de service, des alternatives sont-elles prévues ? Testées ?

**Principaux constats du commissaire aux comptes****Gouvernance et pilotage insuffisants**

Aucune instance dédiée à la gouvernance des SI n'est identifiée. Les décisions IT sont prises au fil de l'eau, sans cadrage formalisé. L'alignement entre les priorités métiers, les investissements SI et la gestion des risques n'est pas assuré.

**Répartition des responsabilités peu claire**

La DSI est rattachée à la direction financière, mais sans lettre de mission ni délégation explicite. Les rôles entre le contrôle interne, la DAF, l'IT et les opérationnels sont confus. Aucun référentiel de responsabilités (RACI) n'est formalisé.

**Contrôle interne informatique partiellement maîtrisé**

Les droits d'accès à l'ERP et à la paie ne sont pas revus régulièrement. Certains comptes sont partagés. Les paramètres comptables (comptes automatiques, TVA, analytique) sont modifiés directement par les utilisateurs métiers, sans double validation.



### SI fragmenté et interfaces manuelles

Le CRM, le logiciel métier et l'ERP ne sont pas interfacés. La facturation et les écritures comptables sont saisies à la main. Les erreurs d'intégration sont corrigées a posteriori, sans traçabilité complète.

### Faibles de sécurité et continuité

Aucune revue de sécurité n'a été réalisée depuis 2 ans. Les sauvegardes sont locales, sans test de restauration. Aucun plan de reprise informatique (PRA) n'est formalisé. Un incident de ransomware a été signalé fin 2023, sans analyse de cause complète.

### Dépendance à des prestataires critiques

Le logiciel métier est opéré en SaaS par un éditeur qui ne fournit ni indicateur de disponibilité, ni rapport d'audit externe (type ISAE 3402). La société n'a pas formalisé de clause de réversibilité en cas de rupture de contrat.

## Impact pour l'approche d'audit :

- Abandon d'un appui sur les contrôles automatisés ;
- Renforcement des tests substantifs, notamment sur les ventes, la paie et des charges ;
- Contrôles de cohérence entre outils métiers et comptables ;
- Entretien approfondi avec les organes de gouvernance pour une sensibilisation.

## Séquence 4

# Allez plus loin

## Missions complémentaires possibles (SACC)

- Le commissaire aux comptes peut proposer, sous réserve des règles d'indépendance, des missions de services autres que la certification des comptes (SACC) à forte valeur ajoutée, notamment dans le domaine de la gouvernance des systèmes d'information.

## Exemples d'interventions possibles

### → Avis sur les rôles et responsabilités SI

Cartographie des fonctions, clarté des délégations, supervision et reporting.

### → Appréciation de la gouvernance des données

Revue de la qualité, de la traçabilité, de la propriété et de la documentation des données.

### → Examen de la couverture et de la cohérence du SI

Diagnostic des interfaces, du périmètre applicatif, de l'alignement SI/métier.

### → Avis sur la gestion de l'évolution du SI et la gouvernance des projets

Analyse de la structuration de la fonction projets (portefeuille, comitologie, méthodes), du pilotage des projets

Les avis peuvent être assortis de recommandations qui visent à contribuer à l'amélioration des traitements de l'information tant financière qu'extra-financière et qui portent sur des éléments du contrôle interne.

La prestation décrite dans le présent document est un Service autre que la certification des comptes (SACC) : il ne s'agit pas d'une mission de certification des comptes.

## Ressources pratiques

### NEP et référentiels

- NEP 315 : Connaissance de l'entité et de son environnement et évaluation du risque d'anomalies significatives
- NEP 330 : Procédures d'audit mises en œuvre par le commissaire aux comptes à l'issue de son évaluation des risques

### Documentation technique

- Doctrine de la CNCC relative aux prestations entrant dans le cadre des Services Autres que la Certification des Comptes (SACC)
- COBIT (Common Objectives for Business Information Technology) qui a pour but l'alignement des objectifs et la stratégie de l'organisation avec les technologies de l'information

## Formations recommandées

- Executive master Audit et conseil en SI
- <https://executive-education.dauphine.psl.eu/formations/executive-master-diplome-universite/audit-conseil-systemes-information>