L'AUDIT INFORMATIQUE EN PRATIQUE

9
FICHES POUR SE LANCER

CRCC
COMPAGNIE REGIONALE DES COMMISSAIRES AUX COMPTES
PARIS

SOMMAIRE

GOUVERNANCE 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 maitrise 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.

FICHE 01

GOUVERNANCE DES SI

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 responsabilité**s 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 & 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 *(Chief Information Officer)*	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 *(Chief Information Security Officer)*	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 *(Database Administrator)*	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.

FICHE 01

GOUVERNANCE DES SI

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 paramétrages 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 & documentations

- **Cartographie applicative et logigrammes métier/SI** : pour comprendre le périmètre couvert, les enchaînements fonctionnels, les interfaces critiques.
- **Documentation des paramétrages 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 ?

FICHE 01

GOUVERNANCE DES SI

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.

Failles 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.

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

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.

Formations recommandées

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

CONTRÔLE DES ACCÈS

En bref

Le contrôle des accès vise à garantir que seuls les utilisateurs autorisés disposent des droits nécessaires à l'exercice de leurs fonctions. La Séparation des Tâches (Segregation of duties - SoD) est un principe fondamental de maîtrise des risques opérationnels, notamment pour prévenir les fraudes ou les erreurs.

Les risques clés incluent notamment le cumul de droits sensibles intra-applicatifs (ex. : création/modification/paiement fournisseur) et inter-applicatifs (ex. accès trésorerie - accès comptabilité), l'absence de revue périodique des droits, la gestion inadéquate des départs temporaires ou définitifs d'utilisateurs internes et externes, la non-traçabilité de la demande et de la validation des attributions des accès, la gestion inadéquate des mobilités internes.

Le commissaire aux compte doit vérifier l'existence d'une politique formalisée de gestion des accès et de SoD, un outil de gestion des identités, une matrice de séparation des tâches ainsi qu'un suivi régulier des dérogations au travers un contrôle récurent du correct respect des règles de séparation des tâches.

Les ERP (type SAP, Oracle) doivent être paramétrés pour empêcher les cumuls de fonctions à risque dès la conception des profils et des habilitations.

En cas d'incompatibilités détectées, une analyse des dérogations et des contrôles compensatoires est attendue.

Enfin, l'implication du contrôle interne et de la DSI dans le pilotage est essentielle pour fiabiliser le dispositif de gestion des accès.

Séquence 1

Comprendre la thématique

Contexte et enjeux

Le dispositif de gestion des accès constitue un maillon critique du contrôle interne, en lien direct avec la sécurité des traitements comptables et financiers. Le droit d'accès est, d'une façon générale, le droit nécessaire à un utilisateur pour accéder à des ressources : ordinateur, données, réseau etc.

La séparation des tâches (SoD) vise à prévenir les fraudes, erreurs et abus en interdisant l'accumulation de fonctions incompatibles intra-applicatifs (ex. : création + validation d'un paiement) et inter-applicatifs (ex. accès trésorerie - accès comptabilité).

Pour le commissaire aux comptes, ces éléments revêtent une importance stratégique, dans la mesure où des défaillances peuvent compromettre l'intégrité des opérations comptables et la fiabilité des états financiers. L'absence de revues périodiques des droits, la persistance de profils sensibles non justifiés, la coexistence de droits incompatibles (ex. : création et validation d'un paiement) exposent l'entité auditée à des risques accrus de fraude ou d'erreurs comptables.

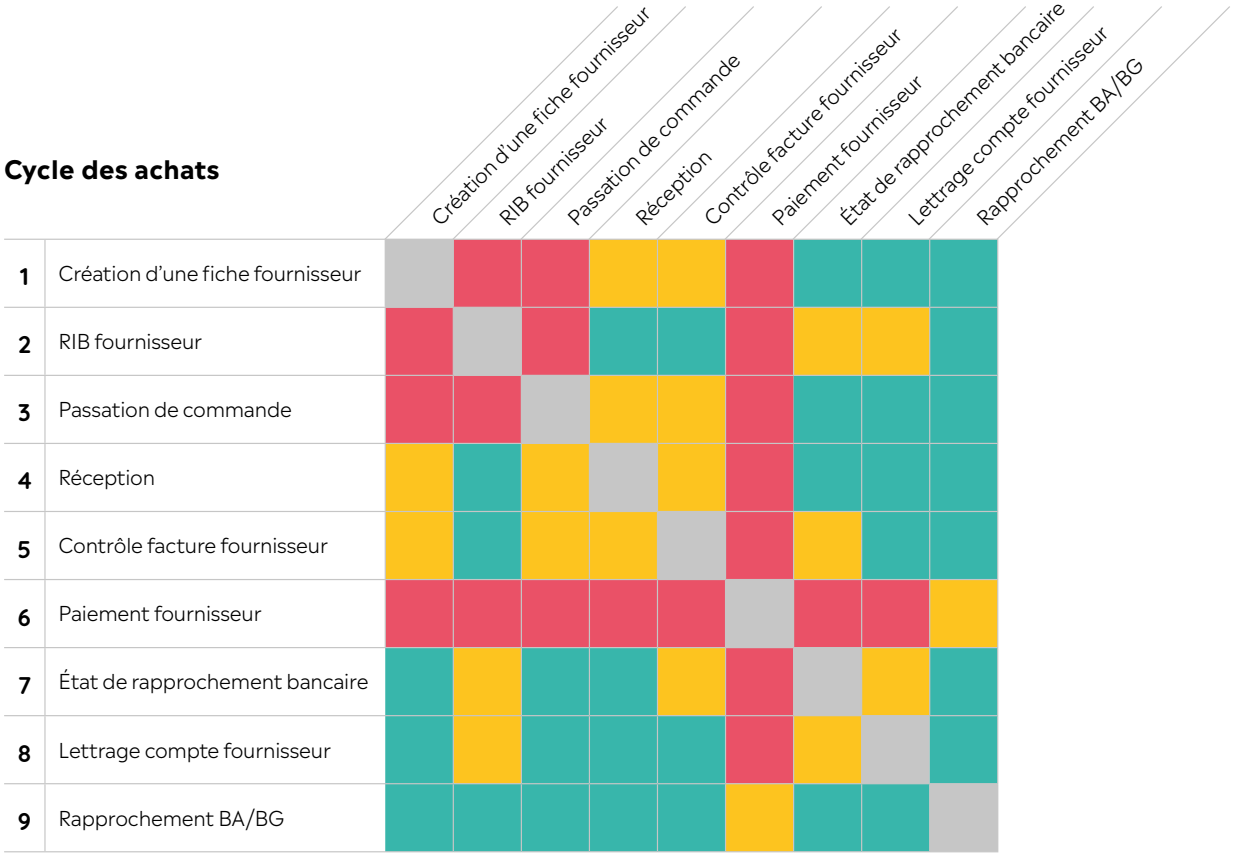
Ces faiblesses peuvent remettre en cause la maîtrise des processus clés (achats, ventes, paie, trésorerie, comptabilité) et avoir un impact direct sur la certification des comptes.

Il est donc essentiel pour l'auditeur de s'assurer que l'entité dispose d'un dispositif robuste de gestion des accès, d'un processus défini de gestion et de contrôle des règles de SoD et de contrôles compensatoires documentés en cas de dérogation.

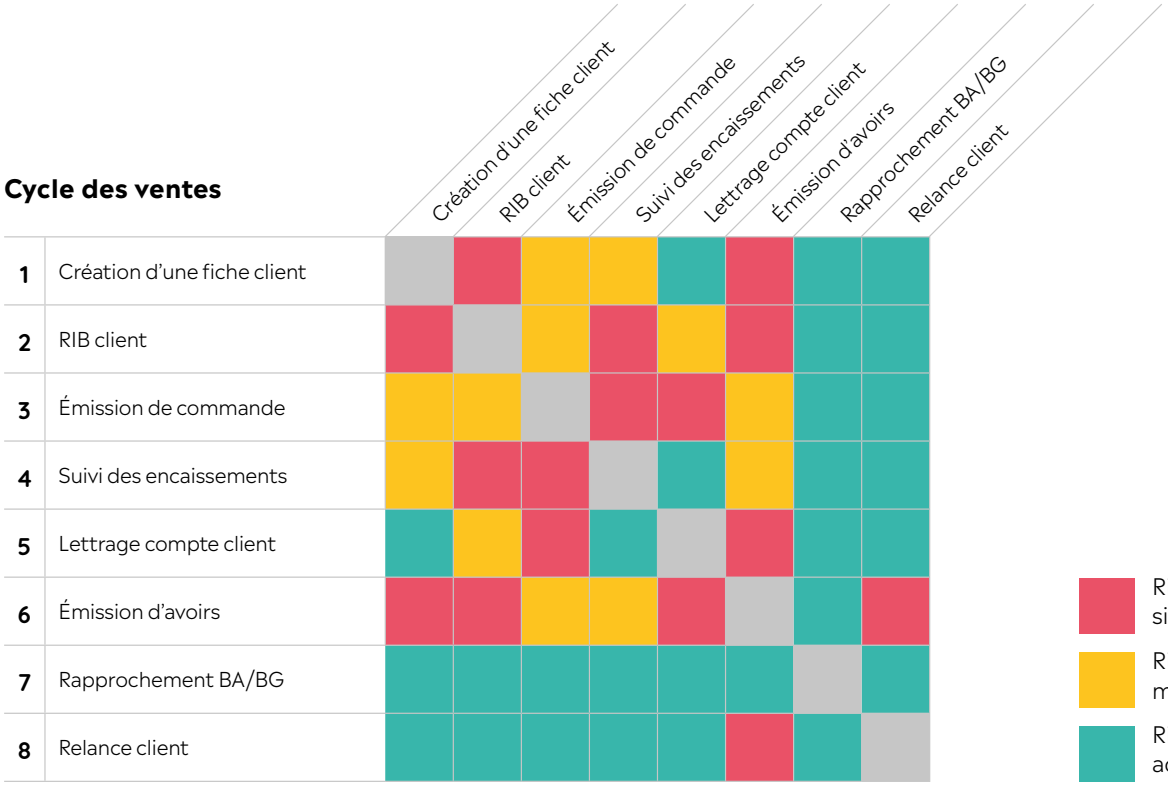
FICHE 02

CONTRÔLE DES ACCÈS

Cycle des achats



Cycle des ventes



Les enjeux et risques spécifiques liés au contrôle des accès et à la séparation des tâches à couvrir par les commissaires aux comptes afin d'évaluer leur impact potentiel sur les comptes annuels et la fiabilité des traitements comptables sont les suivants :

- Absence de procédure de gestion et de validation des accès qui couvre création, modification, suppression des droits avec une vérification des règles SoD avec une attention particulière,
- Le cas échéant, la formalisation des règles de SoD dans une matrice de séparation des tâches détaillant les combinaisons incompatibles des habilitations basées sur l'analyse des fonctions incompatibles sur les processus critiques (achats, paie, comptabilité générale),
- Persistance de profils sensibles non justifiés,
- Absence de piste d'audit pour les actions critiques,
- Absence de contrôles compensatoires en cas de dérogation aux règles SoD,
- Absence de revue périodique des accès.

Ces lacunes peuvent affecter la traçabilité, l'intégrité et la fiabilité des écritures comptables. Elles sont susceptibles d'entraîner des anomalies non détectées ou des erreurs significatives, avec incidence potentielle sur l'opinion d'audit.

Le droit d'accès à une ressource ou un système d'information doit être aligné au poste occupé par le collaborateur. Il doit par ailleurs prendre en compte l'aspect relatif à la séparation des tâches, pour éviter une situation d'auto-approbation, contraire aux principes élémentaires du contrôle interne quel que soit le niveau de droit d'accès autorise. Les règles de séparation des tâches et le principe du moindre privilège doivent s'appliquer également aux accès en lecteur seule. Les avantages liés à la correcte séparation des tâches résident dans la facilitation de la détection des erreurs (involontaires ou frauduleuses). Les deux matrices ci-contre illustrent les tâches incompatibles entre elles pour le cycle des achats et le cycle des ventes. Elles sont un exemple concret des tâches qui ne doivent pas être réalisées par les mêmes personnes. Toutefois, l'organisation de l'entité et le jugement professionnel du commissaire aux comptes doit être pris en considération pour adapter ces matrices à l'environnement applicable (NEP 315).

Conséquences pour le commissaire aux comptes

Les enjeux liés au contrôle des accès et à la séparation des tâches (SoD) influencent directement l'approche d'audit du commissaire aux comptes. En présence de faiblesses identifiées dans ces dispositifs, celui-ci devra adapter sa planification en intensifiant les tests sur les cycles sensibles (achats, paie, trésorerie), vérifier la traçabilité des opérations critiques, et étendre la portée de ses contrôles substantifs. L'absence de SoD effective ou de revue périodique des habilitations constitue un facteur de risque majeur qui peut conduire à une évaluation plus faible du contrôle interne et justifier une approche d'audit plus substantielle. Dans certains cas, ces constats peuvent également alimenter le jugement professionnel du CAC sur la fiabilité du dispositif global de gouvernance, voire impacter la formulation de son opinion.

En conséquence, les accès et leurs contrôles constituent un élément du dispositif de contrôle interne de l'entité. Le pilotage des accès au patrimoine applicatif de l'entité dépend à la fois du service des ressources humaines (connaissance du profil et du niveau de responsabilité) et de la DSI (connaissance des outils et de leurs fonctionnalités), ce qui suppose une communication permanente pour une mise à jour des profils utilisateurs et droits d'accès correspondant en fonction de l'évolution des effectifs (entrées / mouvements/sorties) au sein de l'entité.

FICHE 02

CONTRÔLE DES ACCÈS

Séquence 2

Mission du CAC : objectifs, bonnes pratiques et outils

Thématique 1

Gestion des accès

Objectifs

Dans le cadre de sa mission et conformément à la NEP 315 (compréhension de l'entité et de son environnement), le commissaire aux comptes doit vérifier que l'entité dispose d'un dispositif formalisé de gestion des accès. Il s'attache à valider l'existence d'une politique d'attribution des droits fondée sur le principe du moindre privilège (accès juste nécessaire), la traçabilité et la validation des créations, modifications et suppressions de comptes utilisateurs, ainsi que la mise en œuvre de revues périodiques des accès. Il vérifie que les droits sont systématiquement révoqués en cas de départ, de changement de fonction ou d'inactivité prolongée.

Il est également essentiel de s'assurer que les contrôles soient effectués non seulement au niveau du réseau si existant, mais aussi au niveau applicatif. Les comptes à droits étendus, sont des comptes utilisateurs auxquels sont associés des droits ou permissions élargis, leur permettant d'accéder à des fonctionnalités, services ou ressources supplémentaires par rapport à des comptes standards. Ils doivent être restreints et justifiés. Ils doivent également faire l'objet d'un contrôle renforcé, notamment d'une revue périodique et d'une supervision d'activité. Ces travaux visent à garantir l'intégrité des données, la sécurité des systèmes et la fiabilité des traitements comptables et financiers.

Bonnes pratiques

- Définir, formaliser et mettre en place processus formalisé de gestion des accès (entrée/mouvement/sortie) en lien avec les processus RH et en intégrant les principes de moindre privilège (accès juste nécessaire) et de SoD,
- Identifier, dans une cartographie fonctionnelle et applicative, les principaux systèmes d'information qui concourent à la construction des états financiers (logiciels comptables, logiciels de gestion, logiciels métier) et veiller à définir les profils et les droits associés aux différents cas d'usage, en respectant les principes du moindre privilège et les règles SoD,
- Mettre en place un processus de revue périodique des accès (de toute nature),
- Sécuriser les comptes à droits étendus (administrateurs) par une supervision renforcée, une journalisation des actions et, idéalement, l'usage de coffres-forts pour les mots de passe,
- Définir et mettre en place un contrôle permettant de désactiver les comptes inactifs automatiquement après un délai défini (ex. 90 jours).

Outils & documentations mises à disposition

- Politique de gestion des accès et procédures et workflows associés en identifiant les outils, les acteurs, les rôles et responsabilités et les contrôles mis en place,
- Extractions détaillées des accès associés aux principaux systèmes d'information qui concourent à la construction des états financiers (logiciels comptables, logiciels de gestion, logiciels métier),
- Rapport ISAE 3402
- Registres des comptes utilisateurs (création, modification, suppression)
- Listes de mouvements RH (entrée, sortie, mobilité) et listes des effectifs RH (internes, externes, stagiaires, etc.),
- Compte-rendu des revues périodiques des droits incluant les extractions avant et après des utilisateurs et accompagnés de la liste des actions correctives,
- Cartographie des applications critiques qui concourent à la construction des états financiers et dictionnaires des profils associés en identifiants les accès à droits étendus,
- Plans d'actions issus d'audits internes ou de contrôles précédents

Impact dans la stratégie du commissaire aux comptes

Ces éléments analysés permettent au CAC d'évaluer la robustesse du contrôle général sur l'intégrité des systèmes d'information. Une faiblesse dans la gestion des accès pourrait élever le niveau de risque d'audit, notamment sur la fiabilité des données comptables et financières. Cela peut justifier un élargissement du périmètre de contrôle IT, une intensification des tests substantifs, et la formulation de recommandations fermes dans la lettre d'observations. Une analyse d'impact doit être menée par les commissaires aux comptes afin d'identifier si des mesures compensatoires (procédures, contrôles etc.) permettent de mitiger le risque résiduel associé à des éventuelles faiblesses identifiées dans la gestion des accès. Par exemple un compte utilisateur appartenant à un ancien collaborateur n'a pas été désactivé plusieurs mois après son départ.

Le CAC devra analyser si une connexion post-départ est effectuée. Dans le cas ou, il n'y a pas de connexion post-départ.

Le risque résiduel est faible. Il doit également vérifier s'il existe un contrôle compensatoire, tel qu'un monitoring des connexions ou analyse des journaux d'accès sensible, permettant de réduire le risque d'utilisation frauduleuse. En l'absence de tels dispositifs, le risque résiduel est élevé et doit être considéré dans l'évaluation du risque d'audit global.

Thématique 2

SoD

Objectifs

Le commissaire aux comptes, dans le cadre de l'évaluation du contrôle interne (NEP 265 et NEP 330), doit analyser l'existence d'une séparation effective des tâches dans les processus critiques (achats, ventes, paie, trésorerie, comptabilité). Il identifie les combinaisons de droits ou de rôles pouvant générer un risque de fraude ou d'anomalie (ex. : création et validation d'un paiement, saisie et approbation d'écritures).

Il vérifie l'existence d'une cartographie des risques SoD, de contrôles préventifs dans les outils (paramétrage), et, en cas d'exceptions, de contrôles compensatoires documentés et actifs. L'objectif est de s'assurer que les flux comptables ne peuvent être manipulés, que les anomalies soient détectées en amont, et que les processus soient suffisamment robustes pour garantir la régularité, la sincérité et la fidélité des comptes annuels.

Bonnes pratiques

- Élaborer une matrice de séparation des tâches alignée sur les profils métiers pour les processus clés incluant les règles de SoD intra- applicatifs et inter-applicatifs pour tous les droits applicatifs y compris les droits en consultation, validée par la direction financière et la DSI,
- Mettre en place un contrôle de vérification de la correcte mise à jour des règles SoD suite aux évolutions applicatives impactant les profils utilisateurs et les fonctionnalités,
- Mettre en place un processus permettant d'identifier les règles de séparation des tâches dans la définition et l'implémentation des profils applicatifs,
- Intégrer des contrôles SoD dans les applications, via des profils types ou des alertes en cas de cumul de fonctions lors de la création ou modification d'accès.
- Mettre en place un contrôle de monitoring et d'analyse régulière des dérogations et des violations SoD en documentant systématiquement les justifications et contrôles compensatoires associés,
- Formaliser les justifications et plans de remédiation associés aux cas de non-respect des règles SoD,
- Sensibiliser les utilisateurs clés aux enjeux de la séparation des tâches à travers des sessions de formation ou des communications internes.

FICHE 02

CONTRÔLE DES ACCÈS

Outils & documentations mises à disposition

- Matrice des fonctions incompatibles par processus (achats, paie, compta…)
- Fiches de poste et rôles dans les systèmes
- Paramétrages des droits dans l'ERP ou autres outils (profil utilisateur)
- Preuves des contrôles de monitoring des règles SoD,
- Relevés et justification des dérogations SoD,
- Relevés d'anomalies SoD issues d'audits internes ou outils GRC
- Justifications et plans de remédiation en cas de violation des règles SoD
- Description des contrôles compensateurs et preuves d'exécution

Impact dans la stratégie du commissaire aux comptes

Une matrice SoD incomplète ou non suivie génère un risque de manipulation ou de fraude interne, avec une incidence directe sur les cycles sensibles.

Le CAC adaptera alors sa stratégie en renforçant les travaux sur les processus impactés, en approfondissant les tests sur les écritures comptables et en questionnant la gouvernance de contrôle interne. La lettre de recommandations pourra inclure une exigence de mise en conformité rapide.

Par ailleurs, dans les environnements traitant des données à caractère personnel, une mauvaise séparation des tâches peut entraîner des traitements inappropriés ou non conformes aux exigences du Règlement Général sur la Protection des Données (RGPD).

Le commissaire aux comptes, bien que n'étant pas chargé de certifier la conformité au RGPD, peut relever que l'absence de SoD effective compromet également la sécurité des données personnelles (ex. : accès non justifié à des données RH ou clients).

Ces constats peuvent justifier l'émission de recommandations visant la mise en œuvre rapide d'un référentiel de droits cohérent, la formalisation des contrôles compensatoires, et une meilleure articulation entre gestion des risques opérationnels et exigences de conformité réglementaire.

Séquence 3

Cas d'usage

Usage 1

SoD

Contexte

Dans le cadre de notre mission légale de l'entité « Best in Class », nous avons pris connaissance de l'environnement informatique qui repose sur l'ERP SAP couvrant notamment les modules Finance (FI), Gestion des articles (MM), Vente & Distribution (SD) et Comptabilité des immobilisations (FI-AA).

Une procédure interne encadre la désactivation des comptes utilisateurs SAP. Elle prévoit :

- une clôture des comptes dans un délai de 31 jours suivant le départ d'un collaborateur,
- une obligation pour les managers de notifier par e-mail le service support le jour du départ.

Travaux à réaliser

À la demande de la direction et en amont de nos propres investigations, un audit flash a été diligenté sur la thématique des accès SAP, avec un focus sur la désactivation systématique des comptes des collaborateurs sortants.

L'objectif de cette analyse est de vérifier le respect effectif de la procédure en place et de détecter d'éventuelles failles exposant l'entité à des risques de :

- Maintien d'accès pour des utilisateurs non autorisés,
- Usage inapproprié ou détourné des droits d'accès résiduels,
- Altération ou perte de confidentialité des données sensibles.

Impact pour notre stratégie d'audit

Les constats issus de cette analyse influenceront directement :
- → Notre évaluation du risque d'audit IT, notamment sur le cycle achats et finances,
- → La détermination du périmètre des contrôles applicables à SAP et la fiabilité du paramétrage des autorisations,
- → La nature et l'étendue des tests à mener sur les flux traités via les comptes SAP (journaux, écritures, affectations…).

En cas de lacunes constatées, des recommandations spécifiques seront émises à l'attention de la gouvernance, et nous pourrions être amenés à renforcer notre approche substantielle sur les zones exposées.

Démarche

L'audit se déroule en deux étapes :
1. **Évaluation de la conception du contrôle** (*Design effectiveness*). L'objectif est d'évaluer si la procédure de désactivation des comptes couvre bien les risques identifiés et si elle est bien implémentée.
   Question clé : La procédure existante garantit-elle un niveau de contrôle suffisant ?
2. **Évaluation de l'efficacité opérationnelle du contrôle** (*Operating effectiveness*). Il s'agit d'analyser si la procédure est effectivement appliquée.
   Méthodologie : Comparaison entre les **utilisateurs SAP** actifs et les **collaborateurs présents sur la période auditée** :
   Données nécessaires :
   - → Liste des utilisateurs SAP
   - → Liste des collaborateurs durant la période auditée (internes et externes).

Séquences de tests détaillées

Évaluation de la conception du contrôle :
- → Analyse de la cohérence du délai de 31 jours : ce délai est-il justifié par des contraintes opérationnelles (délai RH, process IT) ou défini arbitrairement ?
- → Vérification de l'absence de mécanisme d'alerte automatique à l'approche ou au dépassement du délai.
- → Question à poser : un délai plus court ou un contrôle automatisé limiterait-il mieux l'exposition au risque ?
- → Constat 1 : Si la justification du délai est faible ou si aucun contrôle de suivi n'existe, la conception du contrôle est perfectible.

Identification des comptes utilisateurs SAP des collaborateurs sortants
- → Clé de rapprochement :
  - Colonne « Utilisateur » dans la liste SAP.
  - Colonne « LOGIN USER » dans les données RH.
- → Outil utilisé : Fonction Excel RECHERCHEV.
- → Constat 2 : Si les comptes des collaborateurs sortants ne sont pas désactivés, la procédure n'est pas respectée

Analyse du délai de désactivation
- → Calcul du nombre de jours entre la date de sortie et la date de désactivation.
- → Formule Excel : Soustraction simple.
- → Constat 3 : Si l'écart dépasse 31 jours, la procédure n'a pas été respectée.

Identification des connexions après départ
- → Vérification des comptes non désactivés ayant une dernière connexion postérieure à la date de sortie.
- → Formule Excel : Soustraction simple.
- → Constat 4 : Si un nombre de jours positif est constaté, cela signifie qu'un accès a eu lieu après le départ.

Observations attendues

Sur la conception du contrôle :
- → La procédure de désactivation est-elle claire, complète et réaliste ?
- → Existe-t-il des écarts possibles non couverts par la procédure ?

Sur l'application du contrôle :
- → La désactivation est-elle effective ?
- → Les délais de désactivation sont-ils respectés ?
- → Y a-t-il des connexions suspectes après départ ?
- → Des actions correctives sont-elles nécessaires pour renforcer la sécurité ?

FICHE 02

CONTRÔLE DES ACCÈS

Conclusion

L'analyse de la procédure de désactivation des comptes utilisateurs SAP au sein de l'entité « Best in Class » met en évidence plusieurs points d'attention, tant sur la conception que sur l'application du contrôle.

La procédure actuelle couvre les risques majeurs liés à la gestion des accès, notamment via la définition d'un délai de désactivation et l'implication des managers.

Toutefois, elle présente certaines limites : elle repose sur une notification manuelle, sujette à des oublis ou retards, et aucun mécanisme de vérification a posteriori systématique n'est prévu pour s'assurer de la bonne exécution de la procédure.

Les tests réalisés ont permis de relever plusieurs cas de non-conformité, notamment des comptes non désactivés dans les délais impartis, voire toujours actifs après le départ de certains collaborateurs.

Dans certains cas, des connexions postérieures à la date de sortie ont été observées, ce qui constitue un risque pour la sécurité du système d'information.

Pour améliorer ce dispositif, il est recommandé de mettre en place un processus automatisé de désactivation basé sur les données RH, de réaliser des contrôles réguliers de cohérence entre les comptes SAP et les effectifs RH, d'archiver systématiquement les preuves de désactivation via un outil de ticketing, et de renforcer la sensibilisation des managers sur leurs responsabilités dans le processus de départ.

Usage 2

SoD

Contexte

Dans le cadre de notre mission légale auprès de l'entité « Smart Supply », nous avons pris connaissance de l'environnement informatique structuré autour d'un ERP SAP, intégrant les modules Finance (FI), Gestion des approvisionnements (MM), Paie (PY) et Comptabilité fournisseurs (AP).

L'entité dispose d'une matrice de séparation des tâches validée par la DSI et la direction financière.

Cette matrice recense les combinaisons de rôles incompatibles au sein de SAP (ex. : saisie + validation de factures, gestion fournisseurs + paiement), et un outil a été récemment implémenté pour détecter les violations de SoD.

Travaux à réaliser

À la suite d'une demande de la gouvernance, nous avons intégré à notre programme d'audit un volet dédié à l'évaluation de la mise en œuvre effective des règles de séparation des tâches.

L'objectif est de :
- → Vérifier la couverture et la mise à jour de la matrice SoD,
- → Identifier les violations de SoD actives dans les systèmes,
- → Évaluer les contrôles compensatoires et les plans de remédiation éventuels.

Ce contrôle vise à prévenir :
- → Les risques de fraude interne (ex. : auto-validation de paiements),
- → Les erreurs comptables non détectées,
- → Une gouvernance inefficace des accès critiques.

Démarche

L'audit se déroule en deux étapes :

1. **Évaluation de la conception du contrôle** *(Design Effectiveness)* :
   Objectif : évaluer si la matrice SoD est exhaustive, validée et bien alignée avec les processus métiers.
   Question clé : Le dispositif en place permet-il de prévenir efficacement les conflits de fonctions ?

2. **Évaluation de l'efficacité opérationnelle du contrôle** *(Operating Effectiveness)* :
   Objectif : tester si les règles SoD sont bien respectées dans les systèmes en production.
   Méthodologie :
   - → Obtenir les rapports d'analyse GRC identifiant les conflits de fonctions utilisateurs,
   - → Comparer les profils attribués à chaque utilisateur avec les fonctions listées comme incompatibles,
   - → Évaluer la criticité des conflits et la présence de contrôles compensatoires actifs.

Séquences de tests détaillées

Revue de la matrice des tâches incompatibles
- → Vérifier qu'elle couvre les principaux processus métiers (achats, paie, compta…).
- → Identifier les combinaisons à haut risque (ex. : création + validation des fournisseurs).

Analyse des violations SoD détectées par l'outil GRC
- → Exporter le rapport des utilisateurs ayant des profils conflictuels.
- → Évaluer le nombre et la nature des conflits (mineur, majeur, critique).
- → Vérifier si des dérogations documentées existent.

Évaluation des contrôles compensatoires
- → Pour les utilisateurs avec droits conflictuels : vérifier l'existence d'un journal d'activité, d'une supervision managériale, ou d'un double contrôle opérationnel.
- → Examiner les preuves d'exécution de ces contrôles (ex. : signature, log, rapprochement périodique).

Observations attendues

Sur la conception du contrôle :
- → La matrice SoD est-elle formalisée, validée et alignée avec les risques métiers ?
- → Les rôles SAP sont-ils conçus sur un modèle RBAC (contrôle d'accès basé sur le rôle) cohérent ?
- → Un contrôle de monitoring des règles SoD est-il défini et mis en place ?

Sur l'application du contrôle :
- → Les dérogations des règles SoD sont-elles documentées et monitorées ?
- → Des conflits de fonctions existent-ils sans justification ?
- → Les alertes remontées sont-elles traitées efficacement ?
- → Les contrôles compensatoires sont-ils actifs et documentés ?

Conclusion

L'analyse du dispositif de séparation des tâches chez « Smart Supply » met en lumière une démarche structurée, appuyée par une matrice formalisée et l'usage d'un outil GRC.

La conception du contrôle est globalement cohérente, bien qu'une mise à jour plus régulière de la matrice et un alignement renforcé avec les processus métiers soient nécessaires.

L'exploitation des rapports GRC a révélé plusieurs violations actives, dont certaines sans justification formelle ni contrôle compensatoire documenté. Cette situation accroît les risques de fraude interne ou d'erreurs non détectées.

Il est donc recommandé de renforcer la revue périodique des conflits identifiés, de formaliser systématiquement les dérogations accordées, et de garantir l'effectivité des contrôles compensatoires pour les profils à risque.

Impact pour notre stratégie d'audit

Les résultats de cette analyse auront un impact direct sur :
- → Notre évaluation du contrôle interne général et IT, notamment sur les cycles achats, trésorerie et paie,
- → La confiance que nous pouvons accorder au paramétrage applicatif et à la fiabilité des données issues de SAP,
- → La nature des tests à réaliser sur les écritures sensibles : il pourra être nécessaire de renforcer les travaux substantifs si des conflits SoD critiques sont identifiés sans mesures de contrôle compensatoires adéquates.

En cas de faiblesses constatées, nous pourrons recommander une mise à jour de la matrice SoD, une meilleure formalisation des rôles dans SAP et/ou une automatisation renforcée des alertes de conflits via les outils GRC.

FICHE 02

CONTRÔLE DES ACCÈS

Séquence 4

Allez plus loin

Missions SACC

- donner un avis quant au processus d'attribution des droits d'accès aux applications et infrastructures sous-jacentes
- revoir la politique des mots de passe et son application ainsi que les règles d'authentification
- revoir la conception des rôles et profils mis en œuvre dans les applications pour s'assurer notamment de leur conformité en termes de séparation de fonctions
- revoir l'attribution de ces rôles et profils aux utilisateurs afin de s'assurer qu'ils ne cumulent pas des droits incompatibles
- s'assurer qu'un processus est en place de revue périodique des utilisateurs et des rôles et profils et le tester

Ressources pratiques

- NEP 240 : Prise en considération de la possibilité de fraudes lors de l'audit des comptes
- NEP 250 : Prise en compte du risque d'anomalies significatives dans les comptes résultant du non-respect des textes légaux et réglementaires
- NEP 265 : Communication des faiblesses du contrôle
- 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
- Norme ISO CEI 27001 : Gestion de la Sécurité des Systèmes d'Information
- Guide ANSSI
- COBIT : Control Objectives for IT (référentiel de gouvernance des Systèmes d'Information)

Formations recommandées

Formation dispensée par la CRCC et l'Université Paris-Dauphine

CONDUITE DE PROJETS

En bref

Avec l'accélération actuelle de la transformation digitale, les entreprises multiplient leurs projets informatiques, accroissant ainsi leur exposition au risque d'échec, estimé à près de 50 %.

Le commissaire aux comptes doit ainsi redoubler de vigilance concernant l'alignement stratégique de ces projets avec les objectifs clés de l'organisation.

Les principaux risques financiers à surveiller comprennent les dépassements budgétaires et l'impact sur la rentabilité globale.

Les risques opérationnels critiques à intégrer concernent notamment les retards fréquents, les difficultés techniques imprévues et l'insuffisance éventuelle des ressources allouées.

Une attention particulière doit être portée à la qualité de la gestion contractuelle, notamment en matière de coûts et délais garantis par les fournisseurs.

La sécurité informatique et l'efficacité du contrôle interne restent des points sensibles nécessitant un suivi constant.

Enfin, le facteur humain doit être intégré au cœur de l'évaluation, via une gestion rigoureuse du changement et une mobilisation effective des équipes.

Séquence 1

Comprendre la thématique

Contexte et enjeux

La transformation digitale accélère fortement les projets informatiques, augmentant ainsi les risques liés à leur réalisation. Le commissaire aux comptes doit appréhender de manière claire les enjeux spécifiques du projet audité pour anticiper ses impacts potentiels sur l'entité.

Parmi les enjeux majeurs figurent le respect de l'équilibre budgétaire, les risques de dérives financières et leur incidence sur les états financiers. Il convient également d'évaluer les risques opérationnels, notamment les retards d'exécution pouvant affecter la performance et la continuité de l'activité.

L'efficacité du contrôle interne lié au projet, particulièrement sur la sécurité et la fiabilité des données, doit être vérifiée.

L'impact organisationnel et humain, en termes de conduite du changement, est un facteur essentiel à intégrer pour anticiper d'éventuelles perturbations internes.

Enfin, l'analyse approfondie des contrats permettra au CAC d'identifier tout engagement susceptible de générer des risques significatifs.

Pourquoi parler de conduite de projets ? Parce qu'en moyenne, 30% du budget d'une entreprise est consacré à des projets. Cela participe à l'évolution et à la transformation de l'entreprise et de ses activités.

Toutefois, lorsqu'un projet porte sur la migration d'un système supportant une ou des activités clés d'une organisation et impacte par conséquent la production de l'information

FICHE 03

CONDUITE DE PROJETS

financière et comptable, le commissaire aux comptes doit réaliser des diligences complémentaires au regard de ses impacts sur la production des états financiers.

Le projet impacte plusieurs dimensions de l'entreprise, qu'il s'agisse de processus, d'organisation, de systèmes ou des trois à la fois, ce qui est bien souvent le cas.

De manière triviale, on peut comparer un projet à un chantier de construction de maison (à noter qu'une grande partie du vocabulaire lié au SI est hérité du monde du BTP). Il s'agit de connaître le besoin, de le spécifier fonctionnellement, puis techniquement, de construire l'édifice, de tester, puis de valider la conformité avant de l'habiter.

Comme n'importe quel chantier, un projet est découpé en phases qui comportent des risques spécifiques (cf. tableau pour exemples).

S'agissant d'audit, les projets les plus directement impactant sont ceux touchant le SI financier, que cela soit dans le cadre d'un changement de logiciel, d'une montée de version, de la mise en place d'une nouvelle solution, de l'intégration d'une nouvelle activité dans un SI existant suite à une acquisition, etc.

Ce sont là les exemples les plus évidents, mais cela ne signifie pas que les autres projets ne concernent pas le CAC, par exemple la dématérialisation des processus (facturation électronique, dématérialisation des achats) ou leur automatisation (mise en place d'agent IA) ou encore l'évolution du dispositif de contrôle interne (refonte des circuits d'approbation, des rôles et autorisations, ou des référentiels comptables, mise en place d'un système de GRC – Gouvernance Risques et conformité).

Un projet représente pour une entreprise un changement structurel majeur pouvant affecter :
- La qualité de l'information financière,
- Les dispositifs de contrôle interne,
- La continuité d'exploitation.

Dans ce contexte et face à ces enjeux, le CAC doit s'assurer que :
- En termes d'approche : les projets ont été menés selon les règles de l'art et respectent un cadre de contrôle interne suffisant.
- En termes de données : les données et états financiers impactés ou produits à l'issue des projets sont exhaustifs, fiables, et correctement comptabilisés.

Conséquences pour le commissaire aux comptes

La norme d'exercice professionnel (NEP) impose au CAC de prendre en compte les changements significatifs dans l'environnement de l'entité (NEP 315 notamment sur l'identification et l'évaluation des risques d'anomalies significatives).

Le commissaire aux comptes doit ainsi effectuer une revue de ce type de projet car il a l'obligation de certifier la régularité, la sincérité et la fidélité des comptes.

Or, un projet mal maîtrisé peut :
- Remettre en cause la continuité d'exploitation (retards, surcoûts, échec, dysfonctionnement post migration)
- Entraîner des pertes financières importantes ou des litiges.
- Impacter la fiabilité de l'information financière et comptable (erreurs de comptabilisation ou de cut-off, perte d'intégrité des données, augmentation des écritures manuelles).
- Générer une rupture dans le contrôle interne ou de la piste d'audit.
- Impacter les délais de clôture
- Impacter l'image et la réputation de l'entreprise.

Le CAC doit réaliser une revue de projet de migration chaque fois qu'un changement de système d'information ou de structure organisationnelle est susceptible d'impacter la production, le traitement ou la fiabilité de l'information financière.

Par conséquent, le CAC doit mettre en œuvre des diligences complémentaires pour pallier ces risques. Ces diligences peuvent faire l'objet d'honoraires complémentaires et consiste en :
- Une revue de la gouvernance du projet
- Une évaluation des impacts que la migration a eu sur les process métiers et le contrôle interne
- Une identification et une revue des contrôles clés embarqués dans le nouveau système
- Une approche davantage substantielle si le contrôle interne est affaibli pendant ou après la migration.
- Des contrôles spécifiques sur la reprise de données pour en garantir l'intégrité et l'exhaustivité,
- Une revue de la recette fonctionnelle, de sa couverture des fonctionnalités clés et de son exécution
- Une vigilance accrue sur traçabilité des écritures comptables et leur correcte imputation avant et après le basculement ainsi que sur l'évolution du nombre d'écritures manuelles.
- Des contrôles visant à vérifier la cohérence des profils et la légitimité des habilitations octroyées dans le nouveau système.
- Une revue des anomalies post migration

Si le CAC ne détecte pas un problème significatif lié au projet (par exemple calcul erroné, perte de données ayant un impact sur l'information financière de l'exercice), sa responsabilité peut être engagée.

Si les éléments fournis par l'entité sont incomplets ou flous, cela peut également compromettre l'opinion du CAC.
En cas de migration au cours de l'exercice, il est essentiel d'effectuer des travaux d'audit informatique sur les deux systèmes ayant coexisté sur l'exercice.

Séquence 2

Mission du CAC : objectifs, bonnes pratiques et outils

Thématique 1

Gouvernance, planification et suivi (GGM)

Objectifs

Sur les volets gouvernance, planification et suivi, pour assurer sa mission conformément aux Normes d'Exercice Professionnel (NEP) et référentiels applicables, le commissaire aux comptes doit :

- Évaluer le dispositif de gouvernance du projet, en s'assurant de l'existence d'une structure de pilotage claire, avec des responsabilités définies et une supervision effective par les organes compétents (ex. : comité de direction, comité d'audit).
- S'assurer de la formalisation des objectifs du projet, de leur alignement avec la stratégie globale de l'entité, et de leur validation par les instances de gouvernance.
- Vérifier l'existence d'un planning initial structuré, intégrant les jalons clés, les livrables, les ressources allouées, ainsi que les délais et les budgets.
- Examiner les modalités de suivi et de reporting : fréquence, qualité des indicateurs de performance (KPI) et remontée à la direction.
- Apprécier le système de contrôle interne appliqué au projet, incluant la gestion des risques (cartographie, analyse, plans d'action) et les dispositifs d'alerte en cas de dérive.
- Analyser la traçabilité des décisions majeures du projet, ainsi que leur documentation (procès-verbaux, arbitrages budgétaires, validations techniques…).
- Contrôler la maîtrise des coûts, en confrontant les dépenses engagées au budget prévisionnel, et en vérifiant les justifications des écarts significatifs.
- Valider la fiabilité des données utilisées dans le suivi de projet, notamment celles intégrées dans les comptes ou les prévisions financières.
- S'assurer de la conformité du projet aux normes réglementaires et contractuelles, notamment en cas de financement public, subventions, ou partenariats.
- Porter une attention particulière à la clôture du projet, en vérifiant que les livrables ont été validés, que les retours d'expérience ont été collectés, et que les impacts comptables ont été correctement enregistrés.

Bonnes pratiques

Renforcer la gouvernance des projets

- Mettre en place un comité de pilotage dédié pour les projets structurants, avec une implication claire des dirigeants, et des comptes rendus formalisés.
- Définir un rôle clair pour chaque acteur (sponsor, chef de projet, utilisateurs clés, directions métiers…) avec des responsabilités et des pouvoirs de décision bien identifiés.

Formaliser une charte de projet

- Promouvoir la rédaction systématique d'une charte de projet validée par la direction, précisant les objectifs, les enjeux, les parties prenantes, les ressources, le budget et les délais.
- S'assurer que cette charte soit revue en cas de changement majeur.

Mettre en place un plan projet structuré et suivi

- Recommander l'utilisation d'un planning détaillé, intégrant les jalons clés, les dépendances, les ressources critiques, et un plan de gestion des risques actualisé régulièrement.
- Favoriser l'usage d'outils de gestion de projet (type Gantt, PERT, logiciels spécialisés) pour une meilleure visibilité des avancées.

Renforcer le suivi budgétaire et la gestion des écarts

- Mettre en place un tableau de bord budgétaire, comparant les prévisions et les réalisations, avec des analyses d'écarts systématiques et documentées.
- Définir des seuils d'alerte pour déclencher des actions correctives.

FICHE 03

CONDUITE DE PROJETS

Adopter des procédures de reporting projet régulières
- → Instaurer un reporting périodique (mensuel ou selon l'importance du projet), adressé à la gouvernance, contenant des indicateurs de performance, de risques et d'avancement.
- → Inciter à la transparence des difficultés rencontrées, pour une meilleure réactivité.

Mettre en place une cartographie des risques projet
- → Aider le client à établir et actualiser une cartographie des risques spécifique au projet, identifiant les risques de délai, de budget, de qualité, réglementaires ou humains.
- → Prévoir des plans de mitigation et suivre les actions correspondantes

Documenter les décisions et arbitrages
- → Insister sur la traçabilité des décisions majeures, avec archivage des validations, arbitrages de ressources, dérogations budgétaires ou changements de périmètre.

Organiser des revues de projet intermédiaires
- → Suggérer des points d'étape formels avec bilans partiels, impliquant les instances dirigeantes et les parties prenantes, permettant d'ajuster le projet si nécessaire.

Intégrer les enseignements des projets passés
- → Mettre en œuvre un retour d'expérience systématique (REX) en fin de projet, pour capitaliser sur les bonnes pratiques et éviter la répétition des erreurs.

Outils & documentations mises à disposition

Pour documenter ses contrôles, structurer ses échanges avec l'entité auditée et étayer ses conclusions *(volets : gouvernance de projet, planification, suivi d'avancement)*

Supports et outils pratiques
- → Grille d'analyse de projet SI (à adapter selon le secteur) comprenant :
  - Matrice RACI des responsabilités projet,
  - Planning Gantt de référence vs réalisé,
  - Budget prévisionnel vs réalisé,
  - Registre des risques projet,
  - Tableaux de bord de pilotage projet (KPI, jalons, livrables, etc.).
- → Checklist de gouvernance de projet incluant :
  - Existence d'un comité de pilotage régulier,
  - Compte-rendu de comitologie,
  - Processus d'arbitrage des écarts / incidents,
  - Implication effective de la DSI, de la direction métier, et de la direction générale.
- → Modèle de note de synthèse pour formaliser les constats et les impacts potentiel sur :
  - La qualité des livrables,
  - Le respect des délais et des budgets,
  - Le maintien du contrôle interne adapté pendant la phase de transformation.

Outils d'échange et de collecte
- → Modèles d'entretien semi-directifs avec :
  - Le chef de projet,
  - Le sponsor métier,
  - Le RSSI / responsable conformité,
  - Le responsable des tests et de la recette.
- → Templates de documentation projet :
  - Cahier des charges / Expression de besoins,
  - Plan de management de projet,
  - Plan assurance qualité,
  - Plan de conduite du changement,
  - Plateformes collaboratives (Teams, SharePoint, drive sécurisé…) pour suivre et centraliser les documents, versions, et éléments de preuve collectés.

Outils de documentation des travaux du CAC
- → Dossier de travail numérique (DTN) incluant :
  - Liens vers les documents analysés,
  - Fiches de contrôle avec scoring de maturité projet,
  - Synthèse des points d'alerte remontés,
  - Recommandations et suivi des plans d'actions.
- → Revue des projets à enjeu significatif dans le cadre de la mission CAC :
  - Lien avec l'évaluation du contrôle interne,
  - Impact éventuel sur les comptes (immobilisations en cours, provisions, etc.),
  - Communication avec le comité d'audit (si présent).

Impact dans la stratégie du commissaire aux comptes

Influence sur l'évaluation du risque d'audit

L'analyse des projets structurants (ERP, refonte SI, déploiement d'un outil métier, migration cloud, etc.) permet au CAC de :
- → Identifier des zones de risque significatif : erreurs potentielles de comptabilisation (immobilisation, charges), mauvaise évaluation des provisions, atteinte au contrôle interne,
- → Relever des défaillances de gouvernance (pilotage faible, absence de suivi budgétaire, décisions mal tracées) qui peuvent accroître le risque de fraude ou d'anomalies non détectées,

→ Détecter un niveau de maturité projet insuffisant, source d'incertitude sur la fiabilité des livrables SI et leur impact sur les états financiers.

Conséquence directe : le CAC rehausse le niveau de risque inhérent ou de risque de non-détection, ce qui influence la profondeur des contrôles à mener.

Ajustement du périmètre de contrôle

En fonction des constats, le CAC peut :

→ Étendre le périmètre des tests à certaines entités, processus ou périodes clés (ex. : période de bascule ou de déploiement d'un nouveau système).
→ Intégrer des cycles spécifiques (achats, facturation, paie, etc.) fortement impactés par le projet.
→ Vérifier les impacts comptables : activation des dépenses, test de dépréciation d'actifs SI, retraitements dans les comptes consolidés, etc.

Exemple : si la gouvernance du projet est défaillante, le CAC peut décider de tester manuellement certaines écritures au lieu de s'appuyer sur le contrôle interne.

Détermination de la nature des recommandations

Les constats issus de l'audit du projet alimentent les recommandations sur :

→ La gouvernance de projet : renforcement de la comitologie, clarification des responsabilités, formalisation des décisions.
→ La planification : mise à jour des jalons, intégration de la gestion des risques, alignement des ressources.
→ Le suivi d'avancement : amélioration des tableaux de bord, du reporting projet, de la gestion des écarts (délais, coûts, qualité).

Ces recommandations peuvent :

→ Être intégrées dans la lettre d'observations du CAC ;
→ Alimenter le rapport au comité d'audit ;
→ Servir à orienter les plans d'action en lien avec le contrôle interne.

Lien avec la continuité d'exploitation

Si les dysfonctionnements projet mettent en péril l'activité (retard critique, arrêt de production, perte de données, etc.), le CAC doit :

→ Réévaluer l'hypothèse de continuité d'exploitation ;
→ Renforcer les travaux sur les mesures de redressement ou de résilience.

Thématique 2

Conduite de projet

Objectifs

Sur le volet conduite de projet, pour assurer sa mission conformément aux Normes d'Exercice Professionnel (NEP) et référentiels applicables, le commissaire aux comptes doit s'assurer de :

1. l'adéquation du nouvel environnement aux besoins métiers et la stratégie de l'entreprise,
2. la conformité de ce nouvel environnement avec les exigences réglementaires,
3. évaluer les risques d'erreurs ou de fraudes induits par le changement induit par le projet (perte de données, séparation des tâches, paramétrage erroné, rupture de contrôle interne…),
4. Identifier les changements dans les processus métiers et les points de faiblesse temporaire ou durable dans le dispositif de contrôle,
5. la continuité de la qualité des informations produites dans le cadre du processus d'arrêté.

En cas de mise en place d'une nouvelle solution, le commissaire aux comptes doit veiller à s'assurer de

→ d'un niveau de couverture suffisant de la recette,
→ du bon niveau de documentation des tests réalisés,
→ de l'existence d'un environnement dédié, différent de l'environnement de production pour la réalisation des tests,
→ d'analyser les anomalies significatives identifiées et qualifier leur impact ainsi que les modalités de correction ou de contournement,
→ la sécurisation du démarrage de la solution en effectuant une revue du processus de bascule et d'accompagnement associé,
→ la revue des paramètres clés du système au regard de la réglementation et des bonnes pratiques sectorielles,
→ la revue des interfaces clés afin de vérifier la fiabilité des traitements de données,
→ le suivi des critères de GO/NO GO pour acter la bascule,
→ la correcte implémentation des droits utilisateurs conformément à la matrice de séparation des rôles de l'entreprise.

En cas de reprise de données, le commissaire aux comptes doit veiller à s'assurer de :

→ la cohérence du périmètre et de l'historique de reprise,

- la définition et le suivi de la méthodologie de reprise des données pour les différents types de données (règles métier, prérequis en matière de nettoyage et d'enrichissement, règles d'extraction et de formatage des données),
- l'efficacité des procédures de contrôles mises en place pour garantir l'exhaustivité et l'intégrité des données migrées conformément à la stratégie de reprise de données.

En synthèse, en tant que commissaire aux comptes, il est essentiel d'évaluer les risques liés à un projet et d'en contrôler les impacts sur la production des comptes annuels.

L'objectif étant de s'assurer de la continuité, de l'intégrité et de la fiabilité des données comptables et financières produites.

Bonnes pratiques

Mettre en place un cadre et un suivi périodique et robuste
- Définir les rôles et responsabilité de chaque partie prenante (formaliser par exemple un RACI),
- Effectuer un suivi régulier et cadrer de la conduite de chaque phase du projet avec des objectifs spécifiques,
- Identifier clairement et en amont les risques liés au projet et inclure systématiquement leur suivi dans le dispositif de pilotage du projet,
- Ne pas négliger la conduite du changement,
- Solliciter les fonctions de contrôles (contrôle interne, direction des risques, RSSI etc.) sur certains aspects comme la RGPD, la sécurité de la solution, l'impact pendant et après le projet sur le dispositif de contrôle,
- Définir des modèles permettant d'encadrer la formalisation des livrables clés (expression des besoins, spécifications fonctionnelles et techniques, cahier de recette...)

Identifier les impacts
- Dresser la liste des fonctions, processus et fonctionnalités clés impactées par le projet en particulier les impacts sur le dispositif de contrôles et sur la production de l'information financière et comptable et le processus d'arrêté des comptes,
- S'assurer que les contrôles clés ont été adaptés ou recréés dans le nouvel environnement,
- Vérifier que des contrôles ont été mis en place pendant la période de transition.

Vérifier la réalisation de tests dans le cadre du projet
- S'assurer qu'un plan de tests a été formalisé, qu'il couvre l'exhaustivité des fonctionnalités clés, qu'il a été suivi et que les résultats de ces tests ont été consignés et qu'ils s'appuient sur des éléments de preuves documentés,
- S'assurer que des tests de non régression sont prévues et clairement définies.

S'assurer de la correcte reprises de données
- Obtenir une documentation complète des phases de migration (ETL : Extraction – Transformation – Chargement),
- Vérifier la traçabilité des données : correspondance entre balances avant/après migration, compteurs de contrôle, sommes, fichiers de mapping, etc.

Identifier et gérer les anomalies identifiées
- Recenser et prioriser les anomalies identifiées dans le cadre du projet,
- Qualifier leurs impacts éventuels,
- Identifier les solutions de contournement mis en place et qualifier leur impact éventuel sur le dispositif de contrôle.

Définir et tester le processus de bascule
- Définir en amont des critères de GO/NO GO visant à décider de la bascule,
- Effectuer une ou des bascules à blanc et identifier les éventuels plans d'actions permettant de sécuriser la bascule réelle,
- Identifier les réserves éventuelles qui impacteraient potentiellement la bascule.

Outils & documentations mises à disposition

Pour documenter ses contrôles, structurer ses échanges avec l'entité auditée et étayer ses conclusions, le CAC peut utiliser les moyens ci-dessous.

Supports et outils pratiques
- Point régulier avec le chef de projet et les parties prenantes,
- Comptes rendus de comité de suivi et de pilotage du projet,
- Modèles de livrables clés (expression des besoins, spécifications fonctionnelles et techniques, cahier de recette...),
- Point régulier avec les fonctions de contrôles pour échanger sur le projet et ses impacts notamment sur le dispositif de contrôles,
- Plan de tests montrant son étendu, son avancement et les résultats des tests,
- Suivi des risques liés au projet,
- Planning projet,
- Plan de bascule,
- PV de recette,
- Critères de GO/NO GO,

→ Compte rendu des bascules à blanc,
→ Liste des anomalies identifiées incluant leur suivi,
→ Modèle de note de synthèse pour formaliser les constats et les impacts potentiels sur :
  - La qualité des livrables,
  - Le respect des délais et des budgets,
  - Le maintien du contrôle interne pendant la phase de transformation.

Outils d'échange et de collecte
→ Modèles d'entretien semi-directifs avec :
  - Le chef de projet,
  - Le sponsor métier,
  - Le RSSI / responsable conformité / Contrôle interne,
  - Le responsable des tests et de la recette,
  - Responsable de la migration des données.
→ Plateformes collaboratives (Teams, SharePoint, drive sécurisé…) pour suivre et centraliser les documents, versions, et éléments de preuve collectés.

Outils de documentation des travaux du CAC
→ Dossier de travail numérique (DTN) incluant :
  - Liens vers les documents analysés,
  - Fiches de contrôle avec scoring de maturité projet,
  - Synthèse des zones de risques et suivi,
  - Synthèse des points d'alerte remontés,
  - Synthèse des tests réalisés,
  - Recommandations et suivi des plans d'actions.
→ Revue des projets à enjeu significatif dans le cadre de la mission CAC :
  - Lien avec l'évaluation du contrôle interne,
  - Impact éventuel sur les comptes (immobilisations en cours, provisions, etc.),
  - Communication avec le comité d'audit (si présent).

Impact dans la stratégie du commissaire aux comptes

Influence sur l'évaluation du risque d'audit
La revue de projets structurants (ERP, refonte SI, déploiement d'un outil métier, migration cloud, etc.) permet au CAC d'identifier des zones de risque significatif : erreurs potentielles de calcul ou de comptabilisation, solution de contournement et rupture du contrôle interne, impacts sur la clôture etc.

Ajustement du périmètre de contrôle
En fonction des constats, le CAC peut rehausser le niveau de risque inhérent ou de risque de non-détection, ce qui peut et doit l'amener à :
→ Étendre le périmètre des tests sur de nouvelles entités, processus impactés ou de périodes clés (ex. : période de bascule ou de déploiement d'un nouveau système) ;
→ Étendre le périmètre des tests en incluant les nouveaux contrôles clés embarqués, les nouveaux key report, les nouveaux déversements de données ;
→ Intégrer des cycles spécifiques (achats, facturation, paie, etc.) fortement impactés par le projet ;
→ Étendre la profondeur des tests à mener et la taille des échantillons ;
→ Effectuer une revue analytique comparative (variations anormales entre exercices, incohérences post-migration) ;
→ Vérifier les impacts comptables : activation des dépenses, test de dépréciation d'actifs SI, retraitements dans les comptes consolidés, gestion du curtoff etc.

Si des déficiences sont identifiées sur la conduite du projet, le CAC peut aller jusqu'à décider de tester manuellement certaines écritures au lieu de s'appuyer sur le contrôle interne.
En cas de déficiences avec un impact jugés significatif, il convient d'alerter le comité d'audit ou le conseil sur les risques financiers ou de continuité.

Le CAC peut aller jusqu'à envisager une modification de l'opinion si les comptes sont affectés et que les erreurs ne sont pas corrigées.

Détermination de la nature des recommandations
Les constats issus de l'audit du projet en amont de la bascule alimentent les recommandations sur :
→ La couverture des tests, leur formalisation ;
→ La stratégie de reprise de données et la formalisation du contrôle clé visant à garantir l'intégrité et l'exhaustivité des données ;
→ Le suivi des anomalies et de leurs impacts notamment concernant les solutions de contournement.

Ces recommandations devront être prises en considération pour les futurs projets. Elle peuvent toutefois :
→ Être intégrées dans la lettre d'observations du CAC ;
→ Alimenter le rapport au comité d'audit ;
→ Servir à orienter les plans d'action en lien avec le contrôle interne.

Lien avec la continuité d'exploitation
Si les dysfonctionnements projet mettent en péril l'activité (retard critique, arrêt de production, perte de données, etc.), le CAC doit :
→ Réévaluer l'hypothèse de continuité d'exploitation,
→ Renforcer les travaux sur les mesures de redressement ou de résilience.

FICHE 03

CONDUITE DE PROJETS

Thématique 3

Post bascule & Maintenance

Objectifs

Concernant le volet « Post-bascule & Maintenance », le commissaire aux comptes (CAC) intervient principalement pour s'assurer de la continuité, de la fiabilité et de la conformité des systèmes d'information et de leur impact sur les comptes, en se référant aux Normes d'Exercice Professionnel (NEP), notamment la NEP 315, NEP 240, NEP 530, ainsi qu'aux référentiels de contrôle interne et de gouvernance IT (ex. COSO, COBIT, ISO 27001 pour la sécurité).

Bascule réelle
- Récupérer la dernière version du chronogramme de bascule ainsi que le PV associé et s'assurer qu'aucune anomalie impacte significativement les process clés et les comptes,
- Suivi des anomalies identifiés dans le cadre de la bascule.

Intégrité des traitements post-mise en production
- Vérifier que les traitements automatisés (calculs, interfaces, extractions) fonctionnent conformément aux spécifications d'origine,
- Contrôler que les écarts ou anomalies identifiés en production sont traités et tracés dans un outil de suivi.

Contrôles applicatifs opérationnels
- Valider la mise en place effective de contrôles-clés sur les traitements comptables, fiscaux, ou réglementaires issus du nouveau SI,
- Revoir les comptes de supervision, les alertes automatisées, les journalisations d'événements critiques.

Suivi des incidents et correctifs
- Examiner la gestion des tickets et incidents (outils ITSM type ServiceNow, GLPI…) : volumétrie, criticité, délais de résolution,
- Évaluer si les correctifs apportés sont formalisés, testés et documentés dans le cadre de processus validés.

Période de stabilisation et stratégie de maintenance
- S'assurer qu'une stratégie de maintenance (préventive, corrective, évolutive) est bien définie, validée et suivie,
- Vérifier l'existence de plans de reprise après incident (PRA/PCA) testés après la bascule.

Gouvernance et gestion des accès
- Contrôler la revue des habilitations post-bascule : les accès sont-ils bien conformes aux principes de séparation des tâches ?
- Examiner les processus de gestion des droits utilisateurs (création, modification, suppression).

Documentation et traçabilité
- Vérifier que la documentation post-mise en production (procédures, guides utilisateurs, plans de tests de maintenance) est complète et disponible pour les utilisateurs et les auditeurs,
- Rechercher la formalisation des décisions (comités de pilotage, comités d'anomalies, arbitrages de priorisation).

Impact sur les comptes et les risques d'anomalies significatives
- Évaluer les zones à risque de distorsion dans les comptes liés à la bascule ou à la maintenance (ex : stocks, provisions, chiffre d'affaires),
- Rechercher des preuves d'une revue spécifique ou d'un audit interne sur cette phase critique.

Bonnes pratiques

- Recenser les anomalies,
- Mettre en place un outil de suivi des anomalies avec workflow,
- Prioriser les anomalies identifiées,
- Évaluer leur impact,
- Identifier les solutions de contournements mises en place le cas échéant et leur impact sur le contrôle interne et la production de l'information financière et comptable.

Outils & documentations mises à disposition

Extraction / liste des anomalies identifiées post mise bascule avec les notions ci-dessous :
- Id anomalie,
- Description,
- Déclarant,
- Date de déclaration,
- Date de résolution le cas échéant,
- Collaborateur en charge du suivi/de la résolution,
- Criticité,
- Priorité,
- Impact,
- Solution de contournement, le cas échéant.

Impact dans la stratégie du commissaire aux comptes

Évaluation du risque d'audit (NEP 315 – compréhension de l'entité et de son environnement)
Les constats sur la phase post-projet permettent au CAC :
- D'identifier des risques significatifs d'anomalies dans les comptes liés à des dysfonctionnements post-bascule (ex. erreurs de calcul, ruptures de piste d'audit, interfaces défaillantes),
- D'analyser le processus de gestion des anomalies par criticité, priorité au regard du processus défini et revoir l'impact des solutions de contournement mises en place le cas échéant, notamment sur le contrôle interne,
- D'évaluer la maturité du dispositif de maîtrise des risques IT, notamment si la transition entre projet et exploitation a été bien contrôlée,
- D'ajuster le niveau de scepticisme professionnel : par exemple, en cas de stabilisation difficile ou documentation absente, un niveau de risque plus élevé sera retenu, entraînant des tests plus étendus.

Impact direct : augmentation du niveau de risque pour certains cycles comptables ou processus métiers (ex : chiffre d'affaires, immobilisations, stocks), justifiant un renforcement des procédures substantielles.

Définition du périmètre de contrôle et nature des tests à mener
Les éléments relevés en post-projet orientent :
- Le choix des processus à auditer plus en profondeur, notamment ceux fortement modifiés ou à fort enjeu comptable,
- Le type de tests de conformité à réaliser : par exemple, revue de paramétrage d'un ERP, test des contrôles automatisés post-mise en production, validation de la qualité des données migrées et de leur maintien,
- Le niveau d'interaction avec les fonctions SI et contrôle interne, si la documentation est lacunaire ou si des failles de supervision sont identifiées.

Impact direct : focalisation sur les zones de vulnérabilité du SI en production, extension du périmètre d'audit à des éléments techniques si les impacts comptables sont significatifs.

Recommandations à émettre et formulation des points d'attention
En fonction des constats :
- Le CAC peut être amené à formuler des recommandations relatives à la gouvernance post-projet, à la documentation ou à la supervision des processus de maintenance.
- Il pourra souligner des insuffisances de contrôle interne, voire signaler une faiblesse significative ou un risque de non-conformité réglementaire (notamment si des dispositifs comme les revues d'habilitation sont absents).
- Des points d'attention seront portés à la connaissance de l'organe chargé de la gouvernance, avec un lien explicite aux risques sur l'information financière.

Impact direct : recommandations formalisées dans le rapport au comité d'audit ou à l'organe dirigeant (NEP 260), voire mention dans le rapport général si le risque est avéré et non maîtrisé.

Séquence 3

Cas d'usage

Migration de données – Data audit

Dans le cadre de la migration d'un SI comptable, il convient de collecter :
- La balance de clôture de l'ancien système,
- La balance d'ouverture du nouveau système,
- La matrice de correspondance des comptes mettant en évidences les modifications apportées sur le plan de comptes.

Dans le cadre de la migration d'un SI de gestion, il convient de collecter les extractions relatives aux données migrées et les détails de la stratégie de migration (profondeur d'historique, granularité, règle de gestion, table de correspondances, etc.)

Un plan de test détaillé est fourni en annexe de ce guide.

FICHE 03

CONDUITE DE PROJETS

Séquence 4

Allez plus loin

Missions SACC

Une entité peut souhaiter confier à son commissaire aux comptes une intervention tendant à évaluer le dispositif de la conduite des projets informatiques.

Toutes les entités peuvent être concernées par l'évaluation de leur dispositif de conduite de projet, mais cette intervention s'inscrit en premier lieu dans un contexte de projet de migration.

Les travaux ont pour objet, à la demande de l'entité, de s'assurer de :
- la conformité du nouvel environnement avec les exigences comptables et réglementaires françaises,
- l'efficacité des procédures de contrôles mises en place pour la reprise des données,
- l'exhaustivité et l'intégrité de la migration des données,
- l'adéquation des nouveaux outils avec le processus d'arrêté des comptes,
- la validation de la persistance de la qualité des informations produites dans le cadre du processus d'arrêté.

Les avis peuvent être assortis de recommandations visant à contribuer à l'amélioration des traitements de l'information financière et qui portent sur des éléments du contrôle interne, objets de la consultation.

Dans les Entités d'Intérêt Public, les travaux du commissaire aux comptes ne peuvent pas inclure la participation :
- à la conception et la mise en œuvre de procédures de contrôle interne ou de gestion des risques en rapport avec la préparation et/ou le contrôle de l'information financière,
- à la conception et la mise en œuvre de systèmes techniques relatifs à l'information financière,
- aux services liés à la fonction d'audit interne de l'entité contrôlée.

Pour documenter ses contrôles, structurer ses échanges avec l'entité auditée et étayer ses conclusions *(volets : gouvernance de projet, planification, suivi d'avancement)*

Référentiels et guides professionnels

- Guide CNCC sur l'audit des projets informatiques : cadre de référence pour l'identification des risques, des points de contrôle et des bonnes pratiques d'audit,
- Référentiel COBIT (Control Objectives for Information and Related Technologies) : appui à l'évaluation de la gouvernance SI et de la gestion des projets IT.
- NEP 315 révisée : identification et évaluation des risques, y compris les risques liés aux projets de transformation.
- Norme ISO 21500 / ISO 10006 : lignes directrices pour le management de projet, utiles pour benchmarker les pratiques de l'entité auditée.

Référentiels / Certifications :
- PRINCE2
- PMBOK

Guides :
- Guide-Audit-Gouvernance-Systeme-Information-Entreprise-Numerique-Cigref-Afai-Ifaci

UTILISATION D'OUTILS D'ANALYSE DE DONNÉES

En bref

L'audit par analyse de données permet aux commissaires aux comptes de cibler plus efficacement les zones de risque en exploitant l'ensemble des données disponibles, plutôt que par un simple échantillon.

Cette démarche renforce la qualité et la précision des contrôles, tout en permettant de détecter plus rapidement les anomalies ou fraudes potentielles. Elle apporte ainsi une meilleure assurance sur la fiabilité des états financiers.

Cela permet aussi de :
- Valider les données et l'application des règles de gestion mise en place de manière exhaustive,
- De chiffrer de façon précise les anomalies rencontrées.

Séquence 1

Comprendre la thématique

Contexte et enjeux

La prise en compte de l'environnement informatique par le commissaire aux comptes est un prérequis des missions d'audit. Cela est particulièrement le cas lorsque l'activité de l'entité à auditer génère une forte volumétrie de transactions, massivement gérées au travers des outils informatiques, qui assurent également la production de ses états financiers.

Si ces outils informatiques apparaissent alors comme des éléments clés à auditer dans les approches d'audit, les commissaires aux comptes disposent aujourd'hui d'outils informatiques permettant d'analyser des volumes importants de données.

Conséquences pour le commissaire aux comptes

En raison de cette forte volumétrie, une approche standarde de tests par échantillonnage peut comporter des limites pour s'assurer de l'exactitude et l'exhaustivité de ces transactions et de leur impact en comptabilité. L'utilisation d'outils adaptés à l'analyse des données devient pertinente et même incontournable.

L'analyse des données constitue une approche qualitative qui permet au commissaire aux comptes de s'assurer de la correcte traduction dans les comptes des évènements de gestion qui se déversent de manière automatique (ou non) dans les différents systèmes de gestion de l'entreprise jusqu'en comptabilité.

Le recours à l'analyse de données en tant que technique d'audit permet :
- d'obtenir une assurance accrue du fait de son caractère exhaustif en matière de couverture,
- de prouver de manière factuelle, par la reproduction de certains traitements, des règles utilisées dans les systèmes d'information, permettant de réaliser la documentation des travaux d'audit,
- d'observer une meilleure efficacité dans la réalisation des travaux d'audit grâce au caractère reproductible de ce type d'approche,
- de promouvoir une valeur ajoutée perçue toujours plus grande des travaux d'audit, tant par les audités que par les auditeurs, notamment avec le recours à la DataViz (par exemple VizNow, développé par la CRCC de Paris) pour en restituer les résultats.

Séquence 2

Mission du CAC : objectifs, bonnes pratiques et outils

Objectifs

Le recours à l'analyse de données en tant que technique d'audit est un choix qui doit être fait lors de la définition de l'approche d'audit en prenant en considération la volumétrie des transactions.

Le commissaire aux comptes peut alors faire le choix de cette approche permettant d'atteindre un niveau d'assurance accrue en matière de couverture et de documentation ainsi qu'une efficacité évidente.

L'analyse des données peut être envisagée soit :
- → Lors de l'intérim pour cibler les zones à risques ou éliminer les risques hypothétiques non avérés,
- → Lors de la phase finale pour apporter des constats chiffrés et étayer l'opinion du commissaire aux comptes.

Bonnes pratiques

1. Définition des travaux
   - → Analyser les différents processus à auditer,
   - → Identifier les processus générant une forte volumétrie ou étant suffisamment représentatif pour nécessiter de procéder à une analyse informatisée de données,
   - → Définir les travaux d'analyse de données à réaliser.
2. Cadrage de l'intervention
   - → Exprimer suffisamment tôt auprès du client le souhait de recourir à l'analyse de données comme technique d'audit, en précisant que cela nécessitera la production d'extractions de données,
   - → Déterminer clairement le périmètre et les objectifs de contrôle,
   - → Effectuer une revue de processus pour :
     - Définir les règles de gestion mises en place par la société et de la documentation associée (attention à la mise à jour de ce type de document)
     - identifier et comprendre les outils supportant le processus audité,
   - → Valider l'entrée des données,
   - → Identifier les données nécessaires à la réalisation des analyses et les sources depuis lesquelles les extraire.
3. Collecte des extractions de données
   - → Être vigilant sur la qualité des extractions reçues (périmètre extrait vs périmètre d'audit, extraction tronquée, filtres non justifiés, etc.).Il est impératif de recueillir la requête ayant permis de réaliser l'extraction ainsi qu'une capture d'écran montrant l'exécution de la requête, avec la date et le nombre d'enregistrements produits. En cas de requête un peu complexe, il est nécessaire de se la faire expliquer, ce qui permettra, entre autres, de comprendre les filtres réalisés, les tables utilisées, les liens entre les tables...
   - → Si possible, cadrer l'extraction avec une autre source de données (la comptabilité par exemple),
   - → Vérifier systématiquement que les données référentielles (base tarifaire, ...) présentes dans les tables ont fait l'objet de test pour en vérifier l'exactitude (ex : base tarifaire vs contrat).
4. Analyse des données
   - → Identifier les éventuels problèmes de qualité de données (complétudes, cohérence, etc.) et en évaluer l'impact sur les tests prévus,
   - → Valider les résultats/anomalies (a minima par échantillonnage) dans le cadre d'une démarche contradictoire avec le client (il est possible que les règles de gestion fournies ne soient pas exhaustives ou ne soient pas celles paramétrées effectivement dans les outils),
   - → Si l'écart total identifié est supérieur aux seuils d'audit, investiguer et justifier les anomalies,
   - → Trouver des facteurs communs permettant d'identifier des « périmètres » sur lesquels se concentrent les exceptions.
5. Restitution des résultats
   - → Bien documenter ses analyses / workflows / scripts et formaliser un mémo précisant les sources, la démarche, les filtres utilisés, les analyses, le workflow, les hypothèses de travail etc. afin de justifier les résultats obtenus et de capitaliser sur le côté reproductible de ce type d'approche,
   - → Présenter les résultats sous forme de DataViz (graphiques dynamiques) présentant la démarche, les chiffres clés et les résultats.

Outils & documentations mises à disposition

Ces dernières années, les outils d'analyse de données ont évolué, permettant aujourd'hui d'être utilisés par des auditeurs n'ayant pas de formation informatique spécifique. On parle d'outil « no code » ou « low code », bien plus accessibles et favorisant ainsi la démocratisation des approches d'audit par analyse de données.

Le choix d'un outil d'analyse de données par le commissaire aux comptes doit toutefois être réfléchi pour adresser au mieux ses cas d'usage, au regard de son niveau de compétence Data et de son budget.

Les bénéfices en matière d'efficacité sont étroitement liés à la réutilisation du même outil d'analyse de données, la documentation des travaux réalisés et l'absence d'évolution du modèle de données côté client.

Les critères d'évaluation ci-dessous peuvent être utilisés pour évaluer les outils du marché.
- Capacité volumétrique
- Capacité d'import de fichiers
- Richesse des fonctionnalités
- Facilité d'utilisation
- Ressources et aide en ligne
- Fiabilité/solidité de l'éditeur
- Piste d'audit
- Coût et modèle de licensing

Deux typologies d'outils existent :
- Les outils d'analyse de données « purs », ne permettant pas une représentation graphique des résultats de façon optimum
- Des outils « mixtes » qui permettent un premier traitement des données et une représentation plus poussée des résultats.

Ces outils « mixtes » sont en général moins puissants en termes d'analyse de données et ne permettent pas de répondre à l'ensemble des fonctionnalités nécessaires mais offrent, au sein d'un même outil, de réaliser une analyse et la représentation des résultats. Ils peuvent être utilisés en complément des outils d'analyse de données.

Les outils les plus utilisés en audit sont aujourd'hui Alteryx, Knime, et les outils mixtes sont Tableau et PowerBI.

Les fonctionnalités clés des outils d'analyse de données et illustrations

FICHE 04

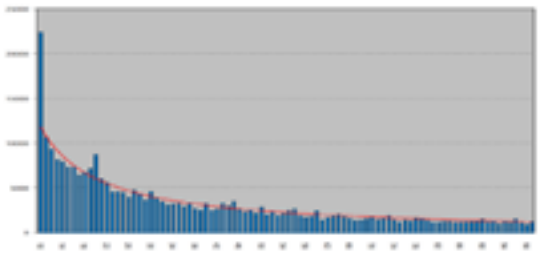
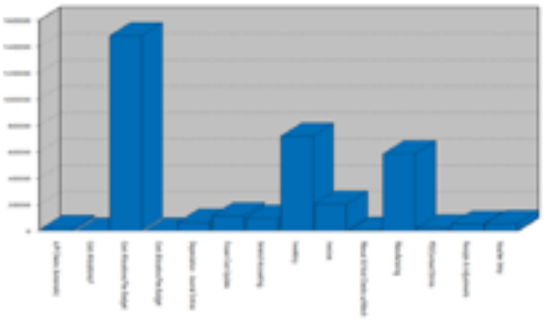
UTILISATION D'OUTILS D'ANALYSE DE DONNÉES

Afin de permettre l'analyse des données, de la rendre pertinente et permettre une restitution appropriée des travaux au client, les fonctionnalités suivantes ont été identifiées comme nécessaires :

<table>
<tr><th>Fonctionnalité</th><th>Description</th><th>Illustration</th></tr>
<tr><td>Intégration des données multi format</td><td>Les fichiers reçus peuvent être fournis sous plusieurs formes (Excel, CSV, TXT, Pdf...). L'outil doit être capable de les lire sans être obligé de les retraiter auparavant avec un autre outil et de risquer de modifier la donnée initiale reçue.</td><td></td></tr>
<tr><td>Tri</td><td>La fonction de tri permet d'organiser rapidement les informations pour repérer des valeurs atypiques, extrêmes ou incohérentes. Cela facilite l'identification de zones de risque ou d'anomalies à analyser plus en détail.</td><td>Le tri sur une date permet, par exemple, de voir si certaines écritures ont été comptabilisées en dehors de l'exercice comptable.</td></tr>
<tr><td>Classification</td><td>La fonction de classification permet de regrouper les données permettant ainsi une analyse des différentes valeurs possibles d'une même information et identifier leur impact financier.</td><td>Cette fonctionnalité permet, par exemple, de reconstituer une balance comptable à partir du FEC. Il permet aussi de lister les utilisateurs ayant réalisé une écriture comptable et identifier ceux n'ayant fait que peu d'écritures.</td></tr>
<tr><td>Filtres</td><td>L'outil doit permettre de réaliser des filtres pour réduire la population à étudier ou pour mener une analyse sur une population à auditer.</td><td>En cas d'analyse des écritures de caisse, il doit être possible de ne filtrer que sur les écritures en 531.</td></tr>
<tr><td>Jointure</td><td>Les jointures entre deux fichiers permettent de croiser différentes sources de données (sur une clé commune, comme par exemple le numéro de facture) pour reconstituer une vision complète et cohérente d'une opération. Cela permet par exemple d'identifier des informations manquantes entre systèmes.</td><td>Une jointure correspond à un « rechercheX » ou « RechercheV » dans Excel.

Attention cependant, le rechercheV va rapatrier la première valeur qu'il trouve dans le deuxième fichier. (Cas 1 ci-dessous). D'autres outils répliqueront les données du premier fichier pour chaque valeur distincte identifiée dans le second (cf. Cas 2 ci-dessous).

Fichier 1<table><tr><td>Clé</td><td>Montant</td></tr><tr><td>A</td><td>100</td></tr></table>Fichier 2<table><tr><td>Clé</td><td>Valeur</td></tr><tr><td>A</td><td>A1</td></tr><tr><td>A</td><td>A2</td></tr></table>Cas 1 - Résultat type Excel<table><tr><td>A</td><td>100</td><td>A1</td></tr></table>Cas 2 - Résultat possible<table><tr><td>A</td><td>100</td><td>A1</td></tr><tr><td>A</td><td>100</td><td>A2</td></tr></table></td></tr>
<tr><td>Doublon</td><td>L'objectif est de trouver simplement des doublons dans un fichier (doublon de factures, ...)</td><td>Recherche de doublon d'un nom ou d'un RIB dans le fichier de paie.</td></tr>
<tr><td>Rupture de séquence</td><td>La réglementation exige que les numéros de factures soient séquentiels. La rupture de séquence permet de les identifier simplement.</td><td>Les numéros d'écritures comptables, au sein d'un FEC, doivent être séquentiels au sein d'un même journal. Toute rupture de séquentialité peut être due à une suppression frauduleuse d'une écriture.</td></tr>
<tr><td>Statistique</td><td>La fonction statistique permet de résumer et d'analyser les données à travers des indicateurs clés (moyenne, écart-type, médiane, etc.), facilitant l'identification de tendances ou d'anomalies. Elle aide à appuyer les constats d'audit sur des mesures objectives et quantifiables.</td><td>Cette fonction permettra, par exemple, de voir les valeurs « hors norme », comme les montants hors écart type.</td></tr>
</table>

Fonctionnalité	Description	Illustration
Benford	M. Benford a identifié que dans toute suite de nombres, il y a une répartition des premiers digits (ex : les 2 premiers digits de 1438,13 sont 14). Toute répartition différente à cette loi peut impliquer une anomalie à analyser.	 Les paiements en liquide sont limités à 1 000 € par transaction. En cas de fractionnement régulier de la facture pour rester en dessous de ce seuil, la loi de Benford permettra d'identifier un pic anormal dans les chiffres commençant par le chiffre 9.
Totalisation	La totalisation permet de calculer des sommes ou des agrégats sur des ensembles de données, par exemple par compte, client ou période. Elle est utile pour vérifier la cohérence des montants, repérer des écarts significatifs ou confirmer des soldes comptables.	Dans le cas d'analyse des écritures de banque, la totalisation permettra d'avoir le montant total des écritures de banque.
Représentation graphique des données	Une représentation graphique permet souvent une analyse rapide d'un résultat. Il est nécessaire que, sur les grandes fonctionnalités, des représentations graphiques soient disponible au sein même de l'outil. Pour les représentations plus « complexes », l'utilisation d'outil spécifique pourra être utile.	 L'exemple ci-dessus montre la répartition des écritures par journal comptable, montrant 3 journaux majeurs.
Sélection aléatoire d'un échantillon de données	Dans le cadre des travaux de commissariat aux comptes, il est nécessaire de faire des sélections pour réaliser des tests. Les outils doivent permettre de faire automatiquement une sélection aléatoire d'un échantillon.	Dans le cadre des circularisations, une fois la taille de l'échantillon définie, l'outil doit pouvoir sélectionner aléatoirement les factures à contrôler.
Piste d'audit	La piste d'audit permet de retracer toutes les étapes et transformations appliquées aux données, garantissant ainsi la transparence du processus d'analyse. Elle facilite la vérification des résultats, la reproduction des analyses et l'identification d'éventuelles erreurs. Elle est aussi essentielle pour répondre aux exigences de conformité et d'audit réglementaire.	
Débogage	Le débogage dans les outils d'audit de la donnée sert à identifier et corriger les erreurs ou incohérences dans les traitements ou les jeux de données. Il permet de garantir la fiabilité des résultats et de s'assurer que les analyses reposent sur des bases solides	Le débogage est une étape importante permettant l'analyse des résultats trouvés avant tout analyse des écarts identifiés avec l'audité. En effet, l'anomalie est potentiellement due à une erreur dans les traitements réalisés.

FICHE 04

UTILISATION D'OUTILS D'ANALYSE DE DONNÉES

Impact sur la stratégie du commissaire aux comptes

L'utilisation de l'analyse de données a un impact direct sur la stratégie d'audit. L'approche exhaustive de la démarche permet de réduire les travaux sur le processus étudié et de s'appuyer sur les résultats pour conclure dessus.

Plusieurs cas peuvent se présenter :
- Aucun écart n'a été identifié, permettant ainsi de valider de façon fiable que les règles de gestion sont maîtrisées et que les comptes, sur le ou les processus audités n'appellent pas d'observation,
- Des écarts non significatifs ont été identifiés. Cela permet de valider le ou les processus en question avec une bonne assurance,
- Des écarts significatifs ont été identifiés. Les écarts identifiés peuvent alors avoir un impact direct sur les comptes, nécessitant un ajustement, une réserve ou, dans le cas extrême, un refus de certifier.

Il est possible que lors de la mise en œuvre des travaux d'analyse de données, le commissaire aux comptes constate l'impossibilité de les réaliser.

Ce constat implique potentiellement la remise en cause de la démarche d'audit sur le ou les processus audités.

En conséquence, le commissaire aux comptes mènera une démarche plus classique, par contrôle, avec la mise en place d'échantillon significatif.

Séquence 3

Cas d'usage

Avant toutes analyse de données, il convient :
- D'effectuer un test de cheminement sur a minima une occurrence afin de bien identifier les données à collecter et la méthode d'analyse qui permettra d'atteindre l'objectif poursuivi,
- D'évaluer la qualité des données, sur leur complétude et leur cohérence, a minima sur les données qui seront utilisés dans le cadre des travaux d'analyses,
- Valider l'exhaustivité des données reçues. Un contrôle des données par rapport aux données comptable est essentiel.

La fiche outil recense des cas d'usage type d'audit par analyse de données, notamment :
- La revue des écritures manuelles,
- La gestion et la valorisation des stocks,
- La maîtrise du processus achat, de la demande d'achat à la comptabilisation de la facture,
- La validation du chiffre d'affaire,
- La facturation des loyers et la gestion des charges en immobilier,
- Le recalcul des commissions,
- Le recalcul des intérêts de crédits,
- Le rapprochement de données,
- La vérification de l'application du principe de séparation des tâches,
- Le recalcul des primes en assurance,
- l'analyse de données RH (recalcul de la paie, des provisions pour CP/RTT/CET etc.),
- ...

Une liste de test complémentaire est disponible sur le site de la CRCC[1].

1. https://www.crcc-paris.fr/wp-content/uploads/2020/07/20200707_Audit_Donnees_V5.pdf

Séquence 4

Allez plus loin

NEP de référence

- NEP 240 : Prise en considération de la possibilité de fraudes et d'erreurs lors de l'audit des comptes
- NEP 250 : Prise en compte du risque d'anomalies significatives dans les comptes. Le CAC doit s'enquérir auprès de la direction du respect des textes et prendre connaissance des correspondances reçues des autorités administratives et de contrôles. On ne peut pas obliger le client à fournir le FEC.
- NEP 265 : Communication des faiblesses du contrôle interne
- NEP 315 : Prise de connaissance de l'entité et de son environnement. Cela implique notamment l'environnement réglementaire et numérique.
- NEP 330 : Procédures d'audit mises en œuvre par le commissaire aux comptes à l'issue de son évaluation des risques

Guides d'audit

- Recueil de tests d'audit de données – CRCC Paris 2020

CONFORMITÉ RÉGLEMENTAIRE

En bref

Risques clés :

Le non-respect du Règlement Général sur la Protection des Données (RGPD) expose l'entité à des sanctions financières pouvant être très lourdes – jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial lors d'une violation des principes de traitement des données ou du non-respect des conditions de licéité du traitement (Article 83).

Au-delà des amendes, les entreprises risquent d'importantes atteintes à leur réputation (perte de confiance des clients, déficit d'image, etc.) et engagent leur responsabilité civile, notamment via d'éventuelles actions collectives des personnes concernées.

Une violation grave peut également être la source de perturbation plus ou moins importante de l'activité (ex. indisponibilité du SI après une attaque) et mettre en danger la continuité de l'entreprise.

Points critiques à surveiller :

La **conformité RGPD** doit être démontrée par l'entreprise à tout moment (*accountability*[1]). Le commissaire aux comptes (CAC) doit donc rester attentif à :

- La **gouvernance des données** : nomination d'un DPO/DPD (Data Protection Officer/Délégué à la Protection des Données) si requis, politique interne sur la protection de la vie privée des salariés, sensibilisation du personnel aux bonnes pratiques concernant le traitement des données personnelles.
- La **cartographie des traitements** et des flux de données : existence d'un registre des activités de traitement, identification des données sensibles ou des traitements à grande échelle.
- Le **cadre légal et contractuel** : bases légales des traitements (consentement, intérêt légitime…), information des personnes et gestion de leurs droits (accès, rectification, effacement, etc.), contrats conformes avec les sous-traitants.
- La **sécurité et la gestion des incidents** : mesures de sécurité logiques et physiques pour assurer confidentialité, intégrité et disponibilité des données, dispositifs de détection des incidents et procédures de notification des violations à la CNIL sous 72h si nécessaire (Article 33 et 34).

En résumé, l'auditeur devra vérifier que l'entité a mis en place des processus et des contrôles adaptés pour garantir la protection des données personnelles.

1. L'*accountability* désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

FICHE 05

CONFORMITÉ RÉGLEMENTAIRE

Séquence 1

Comprendre la thématique

Contexte et enjeux

Le Règlement Général sur la Protection des Données (RGPD) s'inscrit dans un contexte européen d'harmonisation et de renforcement de la protection des données. Entré en vigueur le 25 mai 2018, il poursuit trois objectifs majeurs :

1. **Renforcer les droits des personnes** : portabilité des données, droit à l'oubli, consentement explicite, information en cas de violation, etc.
2. **Responsabiliser les acteurs traitant les données** : obligation de documentation et de preuve de conformité (accountability), privacy by design[2], obligation de notification des violations, etc.
3. **Crédibiliser la régulation** : coopération renforcée entre autorités de protection des données, sanctions dissuasives, etc.

Le RGPD s'applique à toute organisation qui collecte ou traite des données personnelles de résidents européens, indépendamment de sa localisation géographique. Une donnée à caractère personnel est définie comme toute information se rapportant à une personne physique identifiée ou identifiable, directement (nom, prénom, etc.) ou indirectement (identifiant en ligne, localisation, etc.).

Le paysage réglementaire s'est depuis 2018 enrichi de nouveaux textes qui viennent compléter le RGPD :

- Le règlement ePrivacy qui renforce la protection des communications électroniques
- Le Digital Services Act (DSA) et le Digital Markets Act (DMA) qui imposent des obligations supplémentaires aux grandes plateformes numériques
- La loi française « Informatique et Libertés » a été modifiée à plusieurs reprises pour s'aligner sur ces évolutions européennes
- Le Privacy Shield a été invalidé par la Cour de Justice de l'Union Européenne (arrêt Schrems II) et remplacé par un nouveau cadre transatlantique de protection des données en 2023

A cette réglementation RGPD s'ajoute l'« IA Act », Règlement européen sur l'Intelligence Artificielle (RIA) dont l'objectif est double : protéger les citoyens (sécurité, droits fondamentaux) sans freiner l'innovation. Le RIA veut créer un climat de confiance (une sorte de ceinture de sécurité juridique) pour encourager le développement d'une IA fiable et éthique. Le RIA est entré en vigueur le 1er août 2024, mais avec une entrée en application progressive, du 2 février 2025 au 31 décembre 2030 selon les thématiques,

Les points clés du RIA, qui s'applique à tous les secteurs économiques sont les suivants :

- **Obligations en matière de gestion des risques :** Le RIA Act impose aux entreprises d'évaluer et de gérer les risques associés à l'utilisation de l'IA, notamment ceux qui touchent à la sécurité des données et à la vie privée.
- **Transparence et traçabilité :** L'IA doit être conçue et utilisée de manière transparente. Cela inclut la nécessité de fournir des explications compréhensibles aux utilisateurs lorsqu'une décision automatisée a un impact significatif sur eux.
- **Conformité croisée avec le RGPD :** En ce qui concerne le traitement des données personnelles, le RIA Act impose aux entreprises de respecter les règles de confidentialité et de sécurité des données définies par le RGPD. Cela inclut la mise en place de mécanismes pour garantir la protection des données dans le cadre des traitements automatisés, en particulier ceux impliquant des algorithmes de machine learning.

2. Intégrer dès la conception les principes de protection des données personnelles (« **privacy by design** »)

Conséquences pour le commissaire aux comptes

Pour le commissaire aux comptes, l'évaluation de la conformité au RGPD s'inscrit principalement dans le cadre :

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

Pour le commissaire aux comptes le RGPD s'inscrit comme un texte de catégorie 3, selon la nomenclature proposée par les normes en vigueur. Cependant, il reste nécessaire d'évaluer les risques que les manquements au RGPD font peser sur l'entité contrôlée :

1. **Impact sur les comptes** : provisions pour risques et charges (contentieux RGPD), amendes administratives, investissements nécessaires à la mise en conformité
2. **Risques de continuité d'exploitation :** en cas de sanctions importantes ou d'interdiction de traitement des données critiques pour l'activité
3. **Information dans l'annexe :** vérification de la pertinence de l'information relative aux risques liés à la protection des données personnelles
4. **Opportunité de missions de prestations** : le commissaire aux comptes peut proposer des missions complémentaires d'accompagnement à la conformité RGPD

L'évaluation des risques liés à la protection des données personnelles peut s'appuyer sur la matrice suivante :

Facteur de risque	Niveau de criticité	Impacts potentiels
Volume et nature des données traitées	Élevé pour les données sensibles (santé, biométrie, opinions, etc.) et les traitements à grande échelle	Sanctions accrues, nécessité d'analyses d'impact
Exposition internationale	Élevé en cas de transferts hors UE	Complexité juridique, exigences supplémentaires
Niveau de maturité de la gouvernance	Criticité inversement proportionnelle à la maturité	Défaut de contrôle interne, inefficacité des mesures
Sensibilité des activités	Élevée pour les secteurs réglementés (santé, finance, etc.)	Contraintes réglementaires supplémentaires
Antécédents de violation	Élevé en cas d'incidents passés	Surveillance accrue des autorités
Sous-traitance et cloud	Élevé en cas de multiples intervenants ou services cloud	Dilution des responsabilités, perte de maîtrise

S'agissant du RIA, le commissaire aux comptes sera conduit à

- **Évaluer les risques associés à l'IA** : Le commissaire aux comptes devra évaluer la conformité croisée des entreprises à la fois au **RIA Act** et au **RGPD** lorsqu'elles utilisent des systèmes d'IA pour traiter des données personnelles. Cela inclut la vérification de la mise en œuvre des évaluations d'impact sur la protection des données (AIPD) lorsque les technologies d'IA impliquent un risque élevé pour les droits et libertés des personnes concernées.
- **Vérifier les critères de transparence** : Il faudra également vérifier que les systèmes d'IA sont transparents et que les utilisateurs sont informés des décisions automatisées qui peuvent les affecter, conformément aux exigences des deux législations.

FICHE 05

CONFORMITÉ RÉGLEMENTAIRE

Séquence 2

Mission du CAC : objectifs, bonnes pratiques et outils

Objectifs

Dans le cadre de sa mission de certification des comptes, le commissaire aux comptes doit :

1. **Identifier les risques significatifs** liés à la protection des données personnelles susceptibles d'impacter les états financiers,
2. **Évaluer le contrôle interne** mis en place pour assurer la conformité au RGPD, RIA et autres réglementations applicables : le commissaire aux comptes devra notamment vérifier que l'entreprise a réalisé une Analyse d'Impact relative à la Protection des Données pour les technologies d'IA utilisées et qu'elle a mis en place des mesures d'atténuation des risques,
3. **Vérifier la comptabilisation adéquate** des coûts liés à d'éventuelles provisions pour risques,
4. **S'assurer de la pertinence de l'information financière** communiquée dans l'annexe concernant les risques liés à la protection des données.

Bonnes pratiques

Évaluation du niveau de conformité RGPD

Le commissaire aux comptes peut s'appuyer sur le questionnaire d'évaluation suivant :

Thématique	Questions clés	Éléments de preuves à collecter
Gouvernance et accountability	- Un Délégué à la Protection des Données (DPO) a-t-il été désigné ? - La documentation requise par le RGPD est-elle à jour ? - Les rôles et responsabilités sont-ils clairement définis ?	- Lettre de mission du DPO - Registre des traitements - Politiques et procédures internes
Gestion des risques	- Des analyses d'impact (AIPD) sont-elles réalisées pour les traitements à risque ? - Les risques sont-ils régulièrement réévalués ? - Des audits de conformité sont-ils menés ?	- Rapports d'analyses d'impact - Cartographie des risques - Rapports d'audit
Droits des personnes	- Les mentions d'information sont-elles complètes et accessibles ? - Les processus de gestion des demandes d'exercice des droits sont-ils opérationnels ? - Les consentements sont-ils recueillis et conservés ?	- Politiques de confidentialité - Procédures de traitement des demandes - Registres des consentements
Sécurité des données	- Des mesures techniques et organisationnelles sont-elles en place ? - Les incidents de sécurité sont-ils détectés et gérés ? - Des tests d'intrusion sont-ils réalisés ?	- Politique de sécurité des SI - Procédure de gestion des incidents - Rapports de tests
Sous-traitance	- Les contrats avec les sous-traitants incluent-ils les clauses RGPD ? - Un suivi des sous-traitants est-il assuré ? - Les garanties sont-elles suffisantes ?	- Contrats de sous-traitance - Procédures d'évaluation des sous-traitants - Audits des sous-traitants
Transferts internationaux	- Les transferts hors UE sont-ils identifiés ? - Des garanties appropriées sont-elles mises en place ? - Les évolutions réglementaires sont-elles suivies ?	- Cartographie des flux - Clauses contractuelles types - Règles d'entreprise contraignantes

Intégration dans l'approche d'audit
Le commissaire aux comptes intègre l'évaluation de la conformité RGPD dans son approche d'audit par :

1. **Phase de planification :**
   - → Identification des traitements de données personnelles significatifs,
   - → Évaluation préliminaire des risques associés,
   - → Détermination du niveau d'expertise nécessaire (recours éventuel à un spécialiste).
2. **Phase intérimaire :**
   - → Évaluation du contrôle interne lié à la protection des données,
   - → Tests de procédures sur la gouvernance des données,
   - → Vérification des processus de gestion des incidents.
3. **Phase finale** :
   - → Examen des éventuelles provisions pour risques liés au RGPD,
   - → Vérification des informations fournies dans l'annexe,
   - → Évaluation des événements postérieurs à la clôture (incidents, contrôles CNIL, etc.).

Outils & documentations mises à disposition

Pour évaluer les points ci-dessus, le commissaire aux comptes devra mettre en œuvre un **programme de travail ciblé**, s'appuyant à la fois sur des entretiens, des revues documentaires et éventuellement des tests. Parmi les **outils d'audit** et diligences à réaliser, on peut citer :

→ **Entretiens avec les responsables clés** : En premier lieu, rencontrer le DPO (s'il y en a un) ou à défaut un référent RGPD, ainsi que les responsables IT et métiers concernés, afin de comprendre l'organisation mise en place. Ces entretiens permettent de cerner la culture de l'entreprise vis-à-vis des données personnelles, d'identifier les traitements majeurs et de repérer d'éventuels incidents passés.
Par exemple, interroger le DPO sur les principaux risques qu'il a identifiés, sur la fréquence des demandes de droits reçues, sur d'éventuelles plaintes CNIL ou failles de sécurité rencontrées, etc.

→ **Collecte et analyse de la documentation** : Demander et examiner les documents *clés de conformité* :

- Le **registre des traitements** : vérifier qu'il est tenu à jour, complet (finalités, bases légales, catégories de données/personnes, destinataires, durées de conservation, mesures de sécurité, transferts hors UE…) et qu'il couvre bien tous les processus métiers impliquant des données personnelles. Son absence totale serait un signal d'alerte sérieux.

- Les **analyses d'impact (AIPD)** : pour les traitements sensibles identifiés, s'assurer qu'une AIPD a été réalisée conformément à l'article 35 RGPD. Le CAC en fera une revue critique – par exemple, il regardera si les risques résiduels jugés "élevés" ont fait l'objet d'une notification préalable à la CNIL, ou si les mesures d'atténuation recommandées ont été effectivement mises en œuvre.

- Les **politiques et procédures internes** : politique de protection des données ou charte informatique, procédures sur les droits des personnes (modèles de réponse aux demandes d'accès, processus interne pour canaliser ces demandes), procédure de gestion des incidents de sécurité (escalade en 72 h, notification type à la CNIL), plan de continuité d'activité IT en cas de sinistre, etc.
  L'idée est de voir si le cadre formel existe et est cohérent avec la réglementation.
  Une attention particulière sera portée aux procédures assurant l'exercice des droits des personnes (droits d'information, d'opposition, d'accès, de rectification, d'effacement, de portabilité…) : le CAC peut par exemple tester sur un échantillon comment une demande d'accès serait traitée, ou si des demandes reçues ont bien obtenu réponse dans les délais.

- Les **mentions d'information et contrats** : examiner les modèles de mentions RGPD communiquées aux clients ou utilisateurs (sur le site web, formulaires, CGV/CGU) afin de vérifier qu'elles couvrent les points obligatoires (finalités, droits, contact DPO, base légale…) et ne sont pas trompeuses vis-à-vis des pratiques réelles.
  De même, passer en revue les clauses des contrats de sous-traitance les plus critiques pour voir si elles intègrent les engagements requis (confidentialité, aide au responsable de traitement, notification des violations, mesures techniques…).

- **Cartographie des flux et des systèmes** : Lorsque c'est pertinent, réaliser ou exploiter une cartographie du système d'information et des flux de données personnelles, notamment si l'entité n'en dispose pas formellement.
  Cela permet d'identifier des traitements *cachés* ou non documentés (par ex. des exports de données vers un prestataire non mentionné) et de repérer les transferts internationaux.
  Le CAC peut demander un schéma des applications utilisées avec les données personnelles qu'elles traitent, et vérifier, pour chaque flux sortant de l'UE, qu'un mécanisme juridique est en place (décision d'adéquation, clauses types signées, BCR, etc.). Cette approche rejoint la vérification de l'inventaire des données, mais sous un angle technique.

- **Tests de fonctionnement des contrôles** : Selon le risque évalué, l'auditeur peut décider de tester concrètement certains contrôles.
  Par exemple, tester l'autorisation des accès : vérifier sur un échantillon d'utilisateurs que leurs droits d'accès aux applications métiers manipulant des données personnelles respectent bien la règle du *moindre privilège* (besoin d'en connaître).
  Ou simuler une demande d'exercice de droit (droit d'accès) pour voir si l'entreprise répond dans les délais et de manière conforme.
  Ou encore examiner le journal des incidents de sécurité pour voir s'ils ont été correctement catégorisés et s'il n'y a pas eu d'omission de notification alors qu'un incident le requérait.
  Si l'entité utilise un outil de gestion des consentements cookies/traceurs, le CAC peut vérifier son paramétrage (ex. est-ce que le dépôt de cookies non essentiels est bien bloqué avant consentement ?).
  Ces tests fournissent des preuves tangibles du niveau d'application des procédures affichées.

- **Revue des mesures techniques de sécurité** : Impliquer éventuellement l'auditeur IT ou s'aider de questionnaires techniques pour évaluer le niveau de sécurité lié aux données personnelles.
  Par exemple, contrôler que les postes de travail avec accès à des données sensibles sont chiffrés, que des sauvegardes chiffrées sont réalisées régulièrement, que les mises à jour logicielles sont déployées (pour éviter des vulnérabilités exploitées par des attaquants), ou encore que des tests d'intrusion ou analyses de vulnérabilités sont effectués périodiquement sur les systèmes critiques. On se référera aux guides de l'ANSSI et de la CNIL en la matière (*guide de sécurité des données personnelles* de la CNIL, etc.).

L'ensemble de ces démarches vise à recueillir suffisamment d'éléments probants pour étayer l'opinion de l'auditeur sur le niveau de risque résiduel.

Tous les constats (forces et faiblesses) seront consignés dans le dossier de travail, avec leurs impacts potentiels.

Si nécessaire, le CAC pourra alerter les organes de gouvernance sur un risque de non-conformité sérieux (par exemple, absence de toute procédure alors même que des données sensibles sont exploitées), ce qui pourrait relever d'une faiblesse significative du contrôle interne.

Impact dans la stratégie du commissaire aux comptes

L'évaluation des risques liés à la protection des données personnelles influence la stratégie d'audit :

1. **Ajustement du seuil de signification** : en fonction de l'exposition aux risques RGPD et des enjeux associés,
2. **Orientation des travaux** : concentration sur les zones de risque identifiées (secteurs sensibles, traitements massifs, transferts internationaux, secteurs médico-social et associatif),
3. **Communication avec les organes de gouvernance** : alerte sur les risques significatifs identifiés lors des travaux,
4. **Approche pluriannuelle** : suivi de l'évolution de la maturité RGPD de l'entité,
5. **Proposition de SACC** : en fonction des besoins identifiés et dans le respect des règles d'indépendance (Diagnostique de maturité ou audit de compliance ?).

Séquence 3

Cas d'usage

Évaluation de la conformité RGPD d'une PME du secteur e-commerce

Contexte

La société WebShop SA est une PME de 45 salariés spécialisée dans la vente en ligne de produits cosmétiques. Elle réalise un chiffre d'affaires de 8,5 millions d'euros, dont 30% à l'international.
La société dispose d'une base de données clients de plus de 150 000 contacts et utilise des outils marketing avancés (CRM, emailing, ciblage publicitaire).

Identification des risques par le commissaire aux comptes

1. **Lors de la prise de connaissance :**
   - → Traitement de données clients à grande échelle,
   - → Collecte de données de paiement,
   - → Transferts de données vers des prestataires aux États-Unis (hébergement cloud, outils marketing),
   - → Absence de DPO désignée,
   - → Utilisation intensive de cookies et traceurs sur le site web.
2. **Évaluation du contrôle interne :**
   - → Registre des traitements incomplet,
   - → Absence d'analyses d'impact pour les traitements à risque,
   - → Mentions d'information non conformes sur le site web,
   - → Contrats de sous-traitance non mis à jour post-RGPD,
   - → Absence de procédure formalisée de gestion des violations de données.
3. **Évaluation des impacts financiers potentiels :**
   - → Risque d'amendes administratives (jusqu'à 4% du CA mondial),
   - → Coûts de mise en conformité non provisionnés,
   - → Absence d'information dans l'annexe sur les risques RGPD.

Approche d'audit adaptée

1. **Travaux complémentaires :**
   - → Examen approfondi des contrats avec les sous-traitants hors UE,
   - → Vérification des mécanismes de recueil du consentement,
   - → Évaluation de la sécurité des données de paiement,
   - → Examen des processus de gestion des droits des personnes.
2. **Communication avec la gouvernance :**
   - → Point spécifique sur les risques RGPD lors de la réunion de synthèse,
   - → Recommandation de désigner un DPO ou référent RGPD,
   - → Alerte sur les transferts hors UE non sécurisés (post-Schrems II).
3. **Impact sur l'opinion :**
   - → Incorporation des risques RGPD dans l'évaluation globale des risques,
   - → Vérification de l'absence d'impact significatif sur les comptes,
   - → Recommandation d'information dans l'annexe sur les risques liés à la protection des données.

Proposition de prestations

Le commissaire aux comptes propose une mission d'accompagnement à la mise en conformité RGPD, incluant :

- → L'établissement d'une cartographie complète des traitements,
- → L'évaluation détaillée des risques pour les droits et libertés des personnes,
- → La validation de la mise à jour des mentions d'information et politiques,
- → L'évaluation des risques liés aux contrats de sous-traitance conclus par l'entreprise.

Checklist pratique pour l'audit des enjeux RGPD dans une PME e-commerce

- → Vérifier l'existence et la complétude du registre des traitements,
- → Examiner les mentions d'information sur le site web (politique de confidentialité),
- → Contrôler les mécanismes de recueil du consentement (cookies, prospection),
- → Évaluer la sécurité des données sensibles (paiement, coordonnées),
- → Vérifier les contrats avec les prestataires hébergeant des données,
- → Examiner la localisation des données et les transferts internationaux,
- → Contrôler les procédures de réponse aux demandes d'exercice des droits,
- → Évaluer les mesures de sécurité techniques et organisationnelles,
- → Vérifier l'existence d'une procédure de gestion des violations de données,
- → Examiner la formation et la sensibilisation des collaborateurs.

FICHE 05

CONFORMITÉ RÉGLEMENTAIRE

Séquence 4

Allez plus loin

Ressources pratiques

- Guide CNIL sur la tenue du registre des traitements : https://www.cnil.fr/fr/rgpd-et-tpepme-comment-tenir-votre-registre-de-traitement
- Modèles de clauses contractuelles types pour les transferts internationaux : https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_fr
- Lignes directrices du Comité Européen de la Protection des Données (CEPD) : https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_fr
- Outil PIA de la CNIL pour les analyses d'impact : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil
- Référentiel CNIL sur les durées de conservation : https://www.cnil.fr/fr/les-durees-de-conservation-des-donnees

Formations recommandées

- CNCC - Protection des données personnelles : enjeux pour le commissaire aux comptes
- CRCC - Audit informatique et conformité réglementaire
- CNIL - Délégué à la protection des données : formation de base
- AFAI/ISACA - Audit de la gouvernance des données

Évolutions réglementaires à surveiller

- Application du Data Governance Act qui établit un cadre pour faciliter le partage des données
- Mise en œuvre du Data Act qui vise à réguler l'économie des données en Europe
- Évolution de la jurisprudence post-Schrems II concernant les transferts internationaux
- Nouvelles lignes directrices du CEPD sur l'intelligence artificielle et les données personnelles
- NIS / NIS 2
- RIA

EXPLOITATION DES SI

En bref

L'exploitation des systèmes d'information regroupe l'ensemble des activités opérationnelles assurant la disponibilité, la performance, la sécurité et la cohérence des systèmes informatiques. Elle couvre notamment la supervision des serveurs, la gestion des sauvegardes, le suivi des obsolescences, le suivi des incidents et la bonne exécution des flux applicatifs.

Pour le commissaire aux comptes, une exploitation mal maîtrisée peut générer des pertes ou corruptions de données, des interruptions de services ou des désynchronisations entre systèmes, altérant la fiabilité de l'information financière. Il s'agit donc d'un point structurant de la cartographie des risques (NEP 315).

Séquence 1

Comprendre la thématique

Contexte et enjeux

L'exploitation informatique est le socle technique sur lequel repose le traitement quotidien des opérations comptables, financières et opérationnelles de l'entité. Elle permet notamment de :

- Maintenir la disponibilité des systèmes et des environnements applicatifs,
- Garantir l'intégrité des données et la disponibilité des données traitées,
- Assurer la détection, l'analyse et le traitement des anomalies.

Une exploitation défaillante peut avoir des conséquences immédiates sur la fiabilité de l'information financière. À titre d'exemples :

- Un flux non traité (ex. : intégration paie-comptabilité) peut passer inaperçu et altérer les comptes,
- Une rupture de synchronisation entre modules peut désynchroniser les référentiels (stocks, ventes, achats…) et générer des interruptions d'activités ou des doublons,
- Une saturation du système peut bloquer l'exécution et l'enregistrement d'opérations critiques en clôture,
- Un échec de sauvegarde ou une mauvaise restauration peut entraîner des pertes de données comptables et/ou opérationnel.

Dans un environnement SI de plus en plus intégré et externalisé (ERP, SaaS, infogérance…), la robustesse de l'exploitation devient un enjeu clé de maîtrise des risques. La transformation numérique accélère la complexité des chaînes de traitement, rendant la supervision et le suivi des flux plus critiques que jamais.

FICHE 06

EXPLOITATION DES SI

Le CAC doit s'assurer que l'organisation a mis en place des mécanismes de supervision, de gestion des incidents, et de reprise en cas de défaillance, à la fois sur les infrastructures internes et les services externalisés.

Dans cette optique, la cartographie des flux applicatifs et des prestataires devient un outil essentiel. Elle permet d'identifier les traitements critiques, les dépendances entre systèmes, et les éventuels prestataires tiers intervenant sur des domaines sensibles (ex. : application de paie en SaaS, module de facturation externalisé).

Conséquences pour le commissaire aux comptes

Une mauvaise gestion de l'exploitation des systèmes peut avoir un impact sur les données comptables. Par exemple :

- Les flux entre applications ou entre modules d'une même application sont souvent automatiques, faisant que les utilisateurs font confiance dans les données présentes dans leur système, sans remettre en cause l'information présente. Or, même au sein d'une application, une information peut ne pas être transférée (comme dans SAP qui prévoit par exemple la possibilité d'identifier les factures clients qui n'ont pas été transférées en comptabilité (fonction VFX3) et ainsi fausser les comptes.
- Le mauvais ordonnancement ou une erreur dans l'ordonnancement des flux peut engendrer une désynchronisation des données entre systèmes.
- Une saturation du système peut bloquer l'exécution et l'enregistrement d'opérations critiques en clôture. Il peut engendrer une perte d'exploitation le temps de faire évoluer les systèmes ou faire perdre de la donnée.
- Un échec de sauvegarde ou une mauvaise restauration peut entraîner des pertes de données comptables et/ou opérationnelles. Il existe malheureusement trop de sociétés qui, n'ayant pas de sauvegardes ou n'ayant jamais contrôlé que le système de sauvegarde remplissait ses fonctions perdent des données, avec un impact plus ou moins important, allant jusqu'à l'impossibilité de reconstituer les données comptables.

Une exploitation mal gérée peut donc avoir un impact fort sur les comptes, comme la perte de continuité d'exploitation ou la perte de données partielle ou totale.

Le commissaire aux comptes devra alors adapter ses travaux et renforcer ses contrôles en augmentant les tests de détail pour valider les processus touchés n'ont pas subi de dommage faussant les comptes.

Séquence 2

Mission du CAC : objectifs, bonnes pratiques et outils

A noter : Lorsqu'une application critique est externalisée, le commissaire aux comptes doit rechercher l'existence d'un rapport de type ISAE 3402 ou SOC 1, qui pourrait apporter des garanties sur l'environnement de contrôle du prestataire (notamment sur les points ci-après).

Thématique 1

Sauvegardes

Objectifs

Le commissaire aux comptes doit s'assurer que l'entreprise a mis en place un dispositif de sauvegarde fiable, couvrant l'ensemble des données critiques et répondant aux exigences de disponibilité, d'intégrité et de sécurité.

L'objectif est de garantir la restauration rapide et complète des données essentielles en cas de sinistre, sans perte significative susceptible d'impacter les comptes. Il doit vérifier :

- L'existence de sauvegardes automatiques et régulières,
- Leur externalisation ou sécurisation,
- Et la réalisation de tests de restauration pour valider leur efficacité.

Bonnes pratiques

Vérifier l'existence d'une politique de sauvegarde claire

Le CAC doit s'assurer que les règles de sauvegarde sont définies et connues : fréquence, périmètre, modalités de stockage, durée de rétention.

Astuce : demander un document de type « politique de sauvegarde » ou « procédure d'exploitation », même sommaire.

S'assurer que les sauvegardes sont fréquentes, externalisées et monitorées
Les données critiques doivent faire l'objet de sauvegardes quotidiennes, avec une copie externalisée ou dans un environnement sécurisé distinct.
Astuce : demander les rapports journaliers de sauvegarde et identifier les éventuels échecs ou alertes non résolus.

Obtenir la preuve de tests de restauration
Il ne suffit pas de sauvegarder, encore faut-il pouvoir restaurer efficacement les données.
Astuce : demander la dernière preuve de test de restauration (PV, capture d'écran, logs) et vérifier si elle correspond aux engagements (RTO/RPO) annoncés.

Outils & documentations mises à disposition

Le CAC peut s'appuyer sur :
- La politique de sauvegarde ou la documentation d'exploitation associée
- Les rapports automatiques de sauvegarde (quotidiens, hebdomadaires, avec statut d'exécution)
- Les preuves de tests de restauration réalisés
- La cartographie des données critiques (comptabilité, paie, GED, etc.)
- Les guides de bonnes pratiques (ISO 27002 – Sécurité des opérations)

Impact dans la stratégie du commissaire aux comptes

Une stratégie de sauvegarde insuffisante ou non testée constitue un risque majeur pour la fiabilité de l'information comptable. En cas de perte ou de corruption des données, l'entité pourrait être dans l'incapacité :
- de reconstituer les écritures comptables,
- de justifier certains soldes,
- ou de produire les états financiers dans les délais requis.

Le commissaire aux comptes devra alors :
- Adapter ses travaux de vérification pour s'assurer que les données utilisées sont complètes et fiables,
- Demander des preuves de restauration récentes,
- Revoir son évaluation du contrôle interne, notamment en ce qui concerne les cycles sensibles,
- Et, si la situation est jugée critique, alerter la gouvernance ou envisager une limitation de ses travaux (voire une réserve dans les cas extrêmes).

Ce point est à documenter dès la cartographie des risques (NEP 315), avec un focus particulier sur les processus comptables appuyés par des systèmes critiques.

Thématique 2

Surveillance

Objectifs

Le commissaire aux comptes doit s'assurer que les environnements, les systèmes et les applications sont suivis afin d'éviter une perte de donnée et une désynchronisation des données entre les systèmes. Cela implique de regarder :
- l'état des systèmes,
- la disponibilité des applications,
- l'ordonnancement des flux entre les différentes applications.

Bonnes pratiques

Suivre l'état des systèmes :
Les systèmes doivent être suivis afin de s'assurer qu'il n'y aura pas un arrêt ou une rupture des systèmes (plus de place sur les disques durs, mémoire insuffisante, disponibilité des réseaux…) bloquant les systèmes ou empêchant l'enregistrement des données.
Astuce : demander l'état de suivi des systèmes ou analyser s'il y a eu des incidents liés à un manque de ressource (place sur les disques durs…).

La disponibilité des applications
L'indisponibilité d'une application, quelle qu'en soit la cause, doit être identifiée au plus tôt pour éviter une perte d'exploitation.
Astuce : demander le mode de suivi des applications. En cas de sous-traitance, s'assurer que le prestataire met en place les contrôles nécessaires pour éviter l'indisponibilité des applications.

L'ordonnancement des flux
Certaines applications / modules d'une application communiquent eux. La rupture de ces flux peut générer par exemple une désynchronisation entre les systèmes – situation des stocks fausses, commandes d'achat non prises en compte, facturation non réalisée…
Astuce : interroger sur l'existence d'alertes automatiques ou de journaux d'ordonnancement, notamment pour les flux quotidiens (stocks, ventes, paie…).

FICHE 06

EXPLOITATION DES SI

Outils & documentations mises à disposition

Le CAC peut s'appuyer sur :
- la restitution des outils de suivi de l'état des systèmes (ex : Grafana),
- l'état des incidents montrant les interruptions d'activité *(Cf. partie « gestion des incidents »)*
- la cartographie applicative présentant les applications et les différents flux,

Impact dans la stratégie du commissaire aux comptes

Un problème d'exploitation non contrôlé et traité au sein d'une société pourra avoir comme impact :
- Un arrêt ou indisponibilité des systèmes et des applications non identifiés,
- Une perte de données dans une ou plusieurs applications,
- Des données incomplètes en comptabilité.

En cas de contrôle insatisfaisant, le CAC devra renforcer ses contrôles pour s'assurer que les données intégrées en comptabilité sont correctes :
- Soit par des tests substantifs,
- Soit par des tests d'analyse de données (comme un test pour valider que les données de l'application amont se sont correctement déversées en comptabilité, *cf. Fiche 04 - Utilisation d'outils d'analyses de données*).

Les recommandations à mettre place dépendent des faiblesses identifiées :
- Réaliser une cartographie applicative comprenant les différents flux entre applications,
- Mettre en place un système de suivi des flux et des systèmes,
- Mettre en place un système de remonter des anomalies,
- Définir les procédures d'exploitation permettant de résoudre les problèmes.

Thématique 3

Gestion des incidents

Objectifs

Le commissaire aux comptes doit s'assurer que l'entreprise dispose d'un dispositif structuré de gestion des incidents informatiques, permettant d'identifier, tracer et traiter les événements susceptibles de perturber le fonctionnement des systèmes. L'objectif est triple :
- Limiter l'impact des incidents sur les processus critiques (notamment comptables et financiers),
- Assurer un rétablissement rapide des services,
- Prévenir la récurrence des anomalies par une analyse des causes et la mise en œuvre d'actions correctives.,
- Assurer le cas échéant la conformité au dispositif de protection des données RGPD.

Le CAC doit apprécier :
- L'existence d'un registre formalisé ou d'un outil de ticketing dédié,
- La capacité de réaction de l'organisation face aux anomalies,
- Et l'existence de procédures post-incident permettant de capitaliser sur les retours d'expérience, permettant, *in fine*, de traiter l'incident quand celui-ci intervient de nouveau.

Bonnes pratiques

S'assurer de l'existence d'un registre des incidents
Chaque incident (panne, bug applicatif, perte de données) doit être tracé dans un outil dédié ou un registre manuel, avec description, cause, date, et action corrective.
Astuce : demander la liste des incidents sur la période auditée, même sous format Excel ou ticketing.

Vérifier l'existence de procédures d'escalade et de suivi
Les incidents doivent être classés par niveau de criticité et faire l'objet d'un suivi adapté, avec des seuils d'alerte, des délais de traitement cibles et des responsabilités formellement définies.
Astuce : interroger sur les incidents critiques passés et la manière dont ils ont été gérés (temps de réaction, communication interne, correctifs).

Évaluer la capacité à mettre en œuvre des actions correctives
Un incident récurrent ou mal résolu constitue un facteur aggravant. L'organisation doit être en mesure d'appliquer des correctifs techniques, de sécuriser les flux à l'avenir, et de documenter les mesures mises en œuvre.
Astuce : demander s'il existe des fiches permettant, par type d'incident, de résoudre rapidement un incident.

Contrôler la mise en place de retours d'expérience post-incident
Les entreprises les plus matures mènent une analyse « post-mortem » pour identifier les causes racines et ajuster les dispositifs (procédures, paramétrages, ressources). Ces retours permettent également de renforcer les dispositifs de prévention.
Astuce : demander s'il existe des analyses post-incident ou un retour d'expérience formalisé (surtout après une interruption ou un sinistre IT).

Outils & documentations mises à disposition

Le CAC peut s'appuyer sur :
- Le registre des incidents ou l'outil de ticketing (GLPI, Jira, ServiceNow, etc.),
- Les procédures internes de gestion des incidents et de communication de crise,
- Les rapports de clôture d'incidents ou bilans d'exploitation,
- Les documents de retour d'expérience (fiches d'analyse post-mortem),
- Les référentiels ITIL (gestion des incidents / problèmes) et ISO 27001.

Impact dans la stratégie du commissaire aux comptes

Une gestion défaillante ou incomplète des incidents peut entraîner des interruptions non maîtrisées, la corruption de données, ou pire, des flux applicatifs non traités sans alerte. Cela nuit directement à la fiabilité de l'information financière et à la complétude des écritures comptables.

Le CAC adaptera son approche en :
- S'assurant de la traçabilité des corrections apportées, notamment pour les incidents impactant les comptes,
- Adapter ses tests de substance ou renforcer les vérifications manuelles dans les zones concernées,
- Et, si nécessaire, intégrant ses constats dans la lettre de recommandations ou en informant la gouvernance, notamment en cas de défaut structurel de détection ou de traitement.

Divers

Politique de sécurité des systèmes d'information (PSSI)
La PSSI encadre les règles d'exploitation du SI (gestion des comptes, sauvegardes, mises à jour, etc.) et participe à la cohérence globale des pratiques.
Cf. Fiche 08 - Cybersécurité pour une évaluation détaillée des enjeux de cybersécurité

Cartographie fonctionnelle et technique (applications, réseaux, sous-traitance)
Une bonne exploitation repose sur une cartographie à jour des environnements critiques :
- Applications supportées,
- Flux inter-applicatifs,
- Réseaux, serveurs, points de défaillance,
- Prestataires impliqués,
- Parc matériel en place : postes, serveurs, OS, périphériques.

Gestion du parc informatique et maintenance
Le bon fonctionnement du SI repose sur un parc matériel et logiciel maîtrisé. Le CAC doit s'assurer de l'existence :
- D'un inventaire actualisé (postes, serveurs, OS, applications),
- D'un suivi du cycle de vie (fin de support, vétusté, remplacement),
- D'un plan de renouvellement priorisant les environnements critiques,
- Et d'une maintenance organisée (planning, contrats de support actifs, historiques d'intervention).

Un matériel vieillissant ou non maintenu peut provoquer des pannes récurrentes, des pertes de données ou des incompatibilités avec les applications clés, altérant ainsi la fiabilité des traitements comptables.

FICHE 06

EXPLOITATION DES SI

Séquence 3

Cas d'usage

Contexte de l'entité

La société LOGEX INDUSTRIE est une entreprise industrielle multisites disposant d'un ERP centralisé, d'un outil de paie en SaaS et d'une GED interne. Les traitements critiques (comptabilité, production, stocks) s'appuient sur une infrastructure hybride (serveurs locaux + cloud), avec une infogérance partiellement externalisée.

L'environnement est structuré autour de flux automatisés inter-applicatifs (production ↔ ERP ↔ comptabilité), dont la robustesse est essentielle à la fiabilité des données.

Problématiques rencontrées

Le CAC souhaite évaluer la fiabilité des traitements comptables, de gestion de production et de paie dans un environnement technique complexe et partiellement externalisé.

Les précédents travaux ont mis en évidence :
- → L'absence de supervision active des flux entre applications,
- → L'insuffisance des tests de restauration de sauvegarde,
- → Une documentation peu détaillée sur les incidents critiques et leur résolution

Travaux à réaliser

1. Cartographie et architecture des systèmes
   - → Identifier les applications critiques et leur niveau d'externalisation (ERP, paie, GED...),
   - → Localiser les flux inter-applicatifs (automatisés ou manuels) et leurs points de défaillance potentiels,
   - → Vérifier l'existence et l'actualisation d'une cartographie formelle du SI incluant les flux.
2. Dispositif de sauvegarde et de restauration
   - → Obtenir la politique de sauvegarde en vigueur (fréquence, type, localisation, conservation),
   - → Vérifier si les sauvegardes sont externalisées et si elles couvrent l'ensemble des environnements critiques,
   - → Obtenir le fichier recensant l'historique des sauvegardes réalisées,
   - → Rechercher des preuves de tests de restauration sur l'exercice en cours,
   - → Identifier les responsabilités internes et externes liées à la restauration.
3. Ordonnancement et supervision des flux
   - → Analyser l'outil ou les procédures assurant le bon déroulement des flux entre applications (notamment production ↔ ERP ↔ comptabilité),
   - → Identifier les alertes ou contrôles déclenchés en cas d'échec de traitement,
   - → Recenser les actions mises en place afin de résoudre les incidents,
   - → Obtenir la liste de l'ensemble des éléments rejetés et/ou annulés.
4. Gestion des incidents
   - → Rechercher l'existence d'un registre ou outil de ticketing retraçant les incidents techniques, leur résolution et leur criticité,
   - → Vérifier les procédures d'escalade et les délais de résolution formalisés,
   - → Demander les supports de communications liés aux incidents (supports de copil, ...),
   - → Identifier l'impact des incidents sur les traitements comptables ou opérationnels.
5. Relations avec les prestataires et contrats critiques
   (Cf. Fiche 09 « Sous-traitance & Cloud »)
   - → Demander les contrats encadrant l'infogérance et l'hébergement du SaaS (paie),
   - → Rechercher la présence de clauses relatives aux SLA, aux sauvegardes, à la sécurité et à la réversibilité,
   - → Vérifier si des audits tiers (ISAE 3402/SOC) sont disponibles et couvrent le périmètre audité.

Impact pour l'approche d'audit

- → Renforcement des tests de détail sur les cycles critiques (stock, production, comptabilité).
- → Revue spécifique des flux inter-applicatifs, avec analyses de données pour valider l'intégrité et la cohérence des intégrations automatiques et semi-automatiques.
- → Réévaluation du contrôle interne sur la base des faiblesses identifiées : ordonnancement, sauvegardes, gestion des incidents.
- → Communication à la gouvernance sur les risques d'intégrité des données et les insuffisances du dispositif d'exploitation.
- → Intégration d'une recommandation formelle sur la nécessité :
  - D'une supervision active des flux critiques,
  - D'une politique de sauvegarde testée,
  - Et d'un registre d'incidents structuré.

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 de certification des comptes (SACC) à forte valeur ajoutée :

Évaluation du dispositif d'exploitation informatique

- Diagnostic de la supervision, de l'ordonnancement, des sauvegardes et de la gestion des incidents.
- Recommandations sur l'amélioration des procédures (monitoring, alertes, PRA).

Ressources pratiques

Outils

- Cyber'AUDIT - CNCC
- MonaideCyber - ANSSI

Documentation technique

- COBIT (ISACA) – Référentiel de gouvernance IT (notamment le domaine DSS et EDM)
- ISO 27001 - norme internationale de sécurité des systèmes d'information
- ISO 27002 – norme sur les bonnes pratiques de sécurité opérationnelle

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
- Formations ITIL

Organismes spécialisés

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

PLAN DE CONTINUITÉ D'ACTIVITÉ ET PLAN DE REPRISE INFORMATIQUE

En bref

Le Plan de Continuité d'Activité (PCA) regroupe l'ensemble des mesures anticipées permettant à une organisation de maintenir ou restaurer ses activités critiques à un niveau acceptable en cas de crise majeure (cyberattaque, sinistre, défaillance IT…). Il inclut une composante spécifique aux systèmes d'information : le **Plan de Reprise Informatique (PRI)**, qui définit les modalités techniques de redémarrage du SI.

Pour le commissaire aux comptes, l'enjeu est double : évaluer l'impact potentiel sur la continuité d'exploitation et la fiabilité des états financiers.

Les principaux risques clés à surveiller portent sur :
- L'absence d'identification des processus critiques et d'objectifs de reprise (RTO/RPO),
- L'obsolescence du PCA/PRI face aux évolutions de l'environnement et du SI,
- Le défaut de tests réguliers rendant le PCA potentiellement inefficace en situation réelle,
- La méconnaissance du plan par les acteurs censés le mettre en œuvre,
- La non-intégration des prestataires essentiels dans la stratégie de continuité.

Le commissaire aux comptes devra ainsi s'assurer de :
- Évaluer l'existence et la pertinence des PCA et PRI,
- Vérifier l'implication de la gouvernance dans le pilotage du PCA
- Évaluer l'adéquation entre les objectifs métier et les capacités de reprise informatique
- S'assurer de la réalisation et de la documentation des tests réguliers
- Apprécier l'impact potentiel des lacunes du PCA sur la continuité d'exploitation

Séquence 1

Comprendre la thématique

Contexte et enjeux

Le plan de continuité d'activité (PCA) vise à établir un ensemble de mesures pour assurer la continuité des activités essentielles de l'entreprise en cas de sinistre ou d'événement perturbateur majeur. Il intègre notamment :
- Une analyse d'impact métier (BIA) identifiant les processus critiques,
- Des objectifs de reprise (RTO : temps maximal d'interruption, RPO : perte de données admissible),
- Un volet informatique appelé Plan de Reprise Informatique (PRI) qui constitue sa déclinaison technique pour le redémarrage du système d'information et la restauration des données essentielles.

L'enjeu principal est de permettre à l'entité de maintenir ou de reprendre rapidement ses activités critiques à la suite d'un incident informatique. Il contribue à la résilience organisationnelle en assurant que l'entité puisse continuer à remplir ses obligations légales, contractuelles et opérationnelles, même dans des conditions dégradées.

La dépendance croissante des organisations envers leurs systèmes d'information et l'augmentation des menaces (cyberattaques, catastrophes naturelles, pandémies) rendent le PRI plus crucial que jamais.

Un PCA/PRI pertinent doit permettre à l'organisation de répondre aux questions suivantes :
- Quelles sont les activités essentielles à maintenir ?
- Quels sont les délais de reprise acceptables (RTO) et les pertes de données tolérables (RPO) ?
- Quelles ressources (humaines, techniques, informationnelles) sont nécessaires à la reprise ?
- Comment s'organiser la gestion de crise et qui en a la responsabilité ?

FICHE 07 PLAN DE CONTINUITÉ D'ACTIVITÉ ET PLAN DE REPRISE INFORMATIQUE

- Quelles sont les procédures dégradées permettant de fonctionner pendant la crise ?
- Les prestataires critiques sont-ils intégrés dans le dispositif ?

Les caractéristiques d'un PCA robuste incluent sa formalisation, son appropriation par les acteurs concernés, sa mise à jour régulière, son test périodique et son alignement avec la stratégie de résilience de l'entreprise.

Conséquences pour le commissaire aux comptes

Pour le commissaire aux comptes (CAC), l'absence ou la faiblesse d'un Plan de Continuité d'Activité (PCA) ou d'un Plan de Reprise Informatique (PRI) constitue un facteur de risque, à intégrer dès la phase d'évaluation du contrôle interne et de la cartographie des risques.

Continuité d'exploitation
D'un point de vue normatif, ce risque renvoie à la NEP 570 relative à la continuité d'exploitation. Lorsqu'un incident grave (cyberattaque, sinistre, défaillance technique majeure) est susceptible de compromettre la survie de l'entité, l'absence de PCA/PRI peut faire naître une incertitude significative sur la continuité d'exploitation.

Dans un tel cas, le CAC doit en évaluer l'impact comptable (dépréciations d'actifs, pertes d'exploitation, provisions éventuelles) et se poser la question d'un signalement dans son rapport, voire d'une observation ou d'une réserve si l'incertitude n'est pas suffisamment documentée ou traitée par la direction.

Fiabilité des systèmes d'information et des données comptables
Une défaillance du SI sans solution de secours claire peut également remettre en cause la fiabilité des comptes, notamment si les sauvegardes sont absentes, incomplètes ou mal testées.

Le CAC doit intégrer ces éléments dans son analyse des risques (NEP 315), en particulier lorsque des processus critiques (paie, facturation, stock, clôture) sont concernés. Par exemple, l'indisponibilité prolongée d'un outil de paie ou de facturation peut générer des erreurs ou des omissions dans les enregistrements comptables.

Adaptation de la stratégie d'audit
Lorsque l'organisation ne peut fonctionner qu'avec ses outils numériques (ce qui est souvent le cas aujourd'hui), l'absence de solution de repli pour des applications critiques impose au CAC de revoir sa stratégie d'audit. Cela peut se traduire par :

- un renforcement des tests de sauvegarde/restauration,
- des entretiens plus poussés avec les responsables IT,
- ou encore la mise en œuvre de procédures spécifiques pour s'assurer que les données exploitées sont complètes et fiables en cas de reprise informatique.

Contrôle interne et procédures dégradées
En l'absence de plan formalisé ou de solution de repli informatique, l'entité recourt souvent à des procédures manuelles ou improvisées. Ces modes dégradés sont rarement encadrés et peuvent être sources d'anomalies ou de fraudes.

Le commissaire aux comptes doit alors évaluer dans quelle mesure ces modes dégradés et/ou la reprise des données peuvent altérer la production d'une information financière fiable, et s'ils doivent faire l'objet de recommandations ou d'une communication aux organes de gouvernance.

Conformité réglementaire
Dans certains secteurs, la mise en place d'un PCA/PRA n'est pas seulement une bonne pratique, mais une exigence réglementaire. Le commissaire aux comptes, sans se substituer à l'organe de contrôle sectoriel, doit rester attentif à la conformité de l'entreprise avec ses obligations réglementaires en matière de continuité d'activité.

Le défaut de conformité peut non seulement constituer un risque juridique ou opérationnel pour l'entité, mais également un signal d'alerte pour le CAC quant au degré de maîtrise globale du dispositif de contrôle interne.

Dans les cas les plus sensibles, cela peut justifier une communication spécifique aux organes de gouvernance, voire à l'ACPR ou l'AMF selon les cas.

Séquence 2

Mission du CAC : objectifs, bonnes pratiques et outils

Thématique 1

Identification des activités critiques (BIA, RTO/RPO), des sauvegardes, des ressources employés

Objectifs

Dans le cadre de l'évaluation du dispositif de continuité d'activité, le CAC doit s'assurer que l'entité a identifié ses activités critiques, ses ressources essentielles (humaines, techniques, logicielles) et qu'elle a défini des objectifs de reprise réalistes et cohérents en cas de sinistre.

Les principaux éléments à rechercher sont :
- L'existence d'une Business Impact Analysis (BIA) ou d'une analyse équivalente permettant d'identifier les processus vitaux et leur criticité.
- La définition claire, par le métier et partagées avec la DSI, des RTO (Recovery Time Objective) et RPO (Recovery Point Objective) pour les applications clés.
- L'évaluation des ressources nécessaires à la reprise (personnes, outils, sites de repli...).
- Le lien entre ces éléments et les choix technico-opérationnels (sauvegardes, redondance, plans de secours).
- Le RTO correspond au délai maximal admissible d'interruption d'un service, au-delà duquel les conséquences sur l'activité de l'entité deviennent significatives. Il détermine le temps de redémarrage requis pour chaque application critique.

Le RPO, quant à lui, représente la durée maximale de perte de données tolérée. Il traduit le niveau de sauvegarde nécessaire : un RPO de 4 heures implique que les sauvegardes doivent être programmées pour garantir qu'en cas de restauration, seules les 4 dernières heures de données puissent être perdues, et non davantage.

L'objectif du CAC n'est pas de valider techniquement la stratégie de continuité, mais de vérifier qu'elle est alignée avec les enjeux financiers de l'entité, et qu'un sinistre sur les ressources critiques n'entraînerait pas de perte significative non anticipée dans les comptes.

Bonnes pratiques

Assurer l'alignement stratégique avec la direction générale
Avant tout, le CAC doit vérifier que les enjeux de continuité d'activité sont connus, compris et portés au niveau de la gouvernance de la société. Un PCA/PRI ne peut être efficace s'il reste cantonné à la DSI.
Astuce : lors des entretiens, poser des questions simples mais révélatrices à la direction comme :
« En cas d'indisponibilité totale du SI, quelles sont les fonctions que vous considérez comme vitales ? »
« Avez-vous validé formellement les délais de reprise (RTO) proposés par vos équipes ? »
« Existe-t-il une instance ou un plan de crise identifiée pour prendre les décisions si un sinistre survient ? Quelle sont ces membres ? »

Encourager la formalisation d'une BIA (Business Impact Analysis)
Même sous forme simple, une BIA permet de structurer la réflexion de l'entreprise sur :
- les activités critiques,
- les impacts financiers d'une interruption,
- et les objectifs de reprise (RTO/RPO) associés.

Astuce : s'appuyer sur des guides existants (CRCC, ISO 22301) ou proposer un canevas simplifié pour initier la démarche dans les PME.

Maintenir un dialogue structuré avec la DSI
La DSI est souvent dépositaire de la mise en œuvre technique du PRI, mais elle ne porte pas, à elle seule, la responsabilité du PCA dans son ensemble, qui relève d'une démarche transversale pilotée par la direction générale.
Le CAC doit s'assurer que la DSI :
- Connaît les ressources critiques à protéger,
- Dispose d'une vision claire des priorités de reprise,
- Et peut démontrer que les sauvegardes et les tests sont en phase avec les objectifs métiers.

Astuce : utiliser une trame d'entretien commune DSI/Directions métiers, pour évaluer le niveau de coordination et éviter les silos.

FICHE 07 PLAN DE CONTINUITÉ D'ACTIVITÉ ET PLAN DE REPRISE INFORMATIQUE

Vérifier la robustesse des stratégies de sauvegarde et de reprise

Le CAC doit s'assurer que les sauvegardes :

- sont fréquentes et externalisées,
- sont testées régulièrement pour garantir leur efficacité,
- couvrent bien l'ensemble des données critiques (compta, paie, facturation, GED, etc.).

Astuce : demander à voir un journal de sauvegarde ou un rapport de test de restauration récent, et croiser les résultats avec les RTO/RPO affichés.

(Cf. Fiche 06 « Exploitation Informatique »)

Analyser la couverture des ressources humaines critiques

Le CAC peut également alerter sur la dépendance à des personnes clés dans la gestion de crise (ex. : une seule personne connaît les procédures de redémarrage).

Astuce : interroger la DSI ou la direction sur les mesures prises en cas d'indisponibilité des référents : « Les procédures sont-elles formalisées ? Qui prend le relais ? Avez-vous formalisé les rôles de crise ? »

Outils & documentations mises à disposition

Le CAC peut s'appuyer sur :

- Les documents internes : BIA, schéma directeur IT, tableau des RTO/RPO par application, fiches de processus critiques, fiches de poste de crise.
- Des grilles d'entretien types avec la DSI ou les métiers pour identifier les ressources essentielles et les dépendances SI.
- Les rapports de test de PCA et/ou PRI (si existants), logs de sauvegarde/restauration, tableaux de criticité par système.
- Les référentiels externes : ISO 22301 (management de la continuité), guides CRCC/CNIL sur le PCA, trames proposées dans le cadre de cette fiche.

Impact dans la stratégie du commissaire aux comptes

Une absence d'identification claire des activités critiques ou d'objectifs de reprise peut révéler une méconnaissance du risque de continuité par l'entité. Cela accroît le risque d'interruption non maîtrisée ayant un impact sur les comptes.

Le CAC adaptera alors sa stratégie d'audit en :

- Réalisant des tests spécifiques sur la qualité des sauvegardes,
- Demandant des justificatifs sur les délais de restauration déclarés,
- Ajustant ses procédures sur les cycles sensibles (paie, ventes, stocks) en fonction des scénarios à risque,
- Et, si nécessaire, intégrant ce point dans sa communication à la gouvernance, voire dans son rapport.

Thématique 2

Formalisation/exactitude/complétude du PCA/PRI et sa mise en œuvre

Objectifs

Le commissaire aux comptes doit apprécier dans quelle mesure le PCA/PRI de l'entité est formalisé, complet, mis à jour et réellement opérationnel.

Il s'agit d'évaluer la gouvernance du dispositif, la cohérence des documents, et le niveau de mise en œuvre réelle (tests, maintenance, communication…).

Les objectifs sont :

- Vérifier que le PCA/PRI est documenté et validé par la direction,
- S'assurer qu'il couvre l'ensemble des processus et ressources critiques,
- Évaluer s'il est testé régulièrement, mis à jour, et intégré aux pratiques courantes de l'entreprise,
- Identifier les écarts entre théorie et réalité, notamment dans la préparation des équipes.

Bonnes pratiques

S'assurer de la formalisation d'un PCA/PRI structuré et validé
Un PCA non formalisé ou limité à un fichier technique ne permet pas une réponse efficace en cas de crise.
Astuce : demander le dernier plan validé, vérifier la date de mise à jour et la signature de la direction.

Contrôler l'exhaustivité du périmètre couvert
Le PCA doit couvrir les processus critiques métiers, les applications associées, les sites, les personnels clés et les prestataires essentiels.
Astuce : croiser la liste des processus avec la cartographie des risques et les exigences clients/tiers.

Vérifier que des tests sont réalisés et donnent lieu à des actions correctives
Un plan non testé est un plan théorique. L'efficacité opérationnelle repose sur l'expérience des équipes et les retours d'expériences.
Astuce : exiger la dernière synthèse de test et vérifier si les recommandations ont été suivies.

S'assurer que le plan est maintenu à jour
Un PCA figé est vite obsolète (nouveaux logiciels, départs de personnel, prestataires modifiés…).
Astuce : interroger la direction sur la fréquence de revue et les déclencheurs de mise à jour.

Évaluer le niveau de préparation des acteurs en cas de crise
Même avec un bon plan, l'absence de formation ou de communication limite l'efficacité.
Astuce : demander si les différents acteurs ont été formés ou briefés récemment.

Outils & documentations mises à disposition

Le CAC peut s'appuyer sur :
- Le document PCA/PRI officiel (version validée, avec date et diffusion),
- Les rapports de tests, comptes rendus et plans d'action associés,
- La liste des processus, ressources, applications et prestataires critiques,
- Les procédures de restauration, de communication de crise, d'escalade,
- Les preuves de formation ou sensibilisation du personnel impliqué,
- Les référentiels externes : ISO 22301, guide ANSSI, proposées dans le cadre de cette fiche.

Impact dans la stratégie du commissaire aux comptes

Un PCA non formalisé ou non testé crée une incertitude majeure sur la capacité de l'entreprise à assurer la continuité de ses processus comptables et financiers. Cela peut affecter directement :
- L'hypothèse de continuité d'exploitation (NEP 570),
- La fiabilité des données financières (perte d'historique, rupture d'exploitation, erreurs de clôture),
- Et la capacité à répondre à des obligations contractuelles ou réglementaires.

Le CAC adaptera sa stratégie d'audit en :
- Renforçant les tests sur les cycles critiques (notamment si dépendance à l'outil) en cas de crise,
- Et documentant ses constats pour communication à la gouvernance ou justification de son opinion.

Séquence 3

Cas d'usage

Contexte de l'entité

La société MÉTALPLUS est une PME industrielle spécialisée dans la fabrication de pièces métalliques pour l'aéronautique. Elle emploie 80 collaborateurs et génère un chiffre d'affaires de 15 M€. Son activité repose sur une GPAO et un ERP intégré, déployé récemment pour la gestion des commandes, des stocks et de la production.

Le commissaire aux comptes intervient dans le cadre de la certification des comptes au 31/12/2024. Dès la phase de prise de connaissance, il identifie une dépendance forte à l'outil de production, et prend connaissance d'un incident informatique significatif l'année précédente (48 h d'interruption, pénalités clients).

FICHE 07

PLAN DE CONTINUITÉ D'ACTIVITÉ ET PLAN DE REPRISE INFORMATIQUE

Problématiques rencontrées

- L'entreprise ne dispose pas de PCA/PRI formalisé,
- Les sauvegardes sont internes et non testées,
- Aucune exigence contractuelle en matière de continuité vis-à-vis des prestataires critiques n'est formulée,
- La compétence technique est concentrée sur une seule personne, sans documentation claire des procédures de redémarrage.

Travaux à réaliser

Organisation et analyse métier
Le CAC doit évaluer la cohérence entre les besoins métiers et les capacités de reprise prévues :
- L'entité a-t-elle mené une analyse d'impact métier (BIA) ?
- Les activités critiques sont-elles clairement identifiées et hiérarchisées ?
- Les objectifs de reprise (RTO = temps ; RPO = données) sont-ils définis et réalistes ?
- Existe-t-il des procédures dégradées documentées pour les fonctions vitales (facturation, paie, stock) ?
- Une dépendance excessive à une personne clé a-t-elle été identifiée ? Des mesures de relais sont-elles prévues ?

Dispositif technique et infrastructure
Le CAC s'assure de la robustesse du socle technique censé garantir la résilience :
- Les sauvegardes sont-elles régulières, externalisées, testées ? Existe-t-il un journal ou rapport associé ?
- Le PRI (Plan de Reprise Informatique) a-t-il été testé ?
- Les procédures de restauration sont-elles formalisées, accessibles et maintenues à jour ?
- Des ressources de secours (site de repli, matériel, cloud) sont-elles identifiées ? Sont-elles suffisantes ?
- Des tests de montée en charge ou de cyber-résilience ont-ils été réalisés récemment ?

Prestataires et environnement externe
(Cf. Fiche 09 : « Sous-traitance & Cloud »)
Le CAC évalue l'intégration des tiers dans la stratégie de continuité :
- Les prestataires critiques (ERP, hébergeur, infogérant) sont-ils formellement inclus dans le PCA ?
- Des engagements de service (SLA) sont-ils définis contractuellement (disponibilité, délais de reprise) ?
- Existe-t-il une clause de réversibilité ou de portabilité des données en cas de rupture ?
- Le prestataire a-t-il fourni des rapports (ISAE 3402, SOC, tests PRI) exploitables pour l'audit ?
- En cas de défaillance du tiers, quelles solutions alternatives ou délais de redémarrage sont prévus ?

Gouvernance, pilotage et communication de crise
Le CAC doit vérifier l'ancrage du PCA dans la gouvernance :
- Le PCA est-il validé et porté par la direction générale ?
- Le plan a-t-il été mis à jour au cours de l'exercice en fonction des évolutions (SI, structure, sites) ?
- Une instance de pilotage est-elle identifiée ? Les rôles sont-ils définis ?
- Existe-t-il un plan de communication (interne, clients, partenaires) ?
- Le personnel clé a-t-il été formé ou sensibilisé ?

Impact pour l'approche d'audit

- Le CAC évalue l'incidence de l'absence de PCA et évalue l'impact potentiel des risques de continuité sur les états financiers au regard de la NEP 570,
- Il renforce ses travaux sur les en-cours de production et les transactions issues de l'ERP,
- Il documente et communique de manière formelle aux organes de gouvernance avec une recommandation de formalisation du PCA, test inclus.

Séquence 4

Allez plus loin

Évolutions réglementaires récentes

Directive NIS 2 (Network and Information Security)
Adoptée en 2022 et applicable à partir de 2024, cette directive européenne renforce les exigences en matière de cybersécurité et de résilience opérationnelle pour les entités essentielles et importantes. Elle impose notamment la mise en place de mesures de gestion des risques incluant des plans de continuité d'activité.

Règlement DORA (Digital Operational Resilience Act)
Applicable au secteur financier européen à partir de 2025, ce règlement impose des exigences strictes en matière de résilience opérationnelle numérique, incluant des plans de continuité d'activité robustes et des tests réguliers.

ISO 22301 :2019
Cette norme internationale sur les systèmes de management de la continuité d'activité a été mise à jour en 2019, avec un accent sur l'approche par les risques et l'intégration avec les autres systèmes de management.

Ressources pratiques

Outils CRCC
- Guide d'audit informatique complet (disponible sur le site de la CRCC)
- Questionnaire d'évaluation du PCA (format Excel, disponible en téléchargement)

Documentation technique
- Guide ANSSI : « Élaborer un plan de continuité d'activité système d'information » (version 2023)
- Guide CLUSIF : « Plan de Continuité d'Activité - Stratégie et solutions de secours du SI »
- AFNOR : Guide de mise en œuvre de l'ISO 22301

NEP et référentiels
- NEP 315 (Connaissance de l'entité et évaluation des risques)
- NEP 330 (Procédures d'audit mises en œuvre à l'issue de l'évaluation des risques)
- NEP 570 (Continuité d'exploitation)
- ISAE3402 (Rapports d'assurance sur les contrôles au sein d'une société de services)

Formations recommandées

Formation CNCC/CRCC

Organismes spécialisés
- BCI (Business Continuity Institute) : "Introduction to Business Continuity Management"
- ISACA : "IT Disaster Recovery Planning and Management"

E-learning
- MOOC ANSSI : « Sécurité numérique »

CYBERSÉCURITÉ

En bref

La cybersécurité regroupe l'ensemble des mesures techniques, organisationnelles et humaines visant à protéger les systèmes d'information contre les menaces numériques : attaques externes, erreurs internes, compromission de comptes, etc.

Ces menaces peuvent altérer la disponibilité, l'intégrité ou la confidentialité des données critiques, avec un impact direct sur la fiabilité des états financiers et la continuité d'exploitation de l'entité.

Pour le commissaire aux comptes, la cybersécurité constitue désormais un facteur de risque transversal, à intégrer dans la cartographie (NEP 315) et à articuler avec les autres volets SI (accès, exploitation, sous-traitance, PCA/PRI…).

Les points de vigilance majeurs portent notamment sur :
- La présence d'un Responsable Sécurité des Systèmes d'Information (RSSI) identifié et d'une Politique de Sécurité du Système d'Information (PSSI) formalisée et actualisée ;
- L'existence de procédures de gestion d'incident (détection, traitement, notification, documentation) ;
- La sécurisation des accès critiques (authentification renforcée – MFA, journalisation, accès distants) ;
- La résilience opérationnelle, via des sauvegardes effectives, testées, et un plan de reprise informatique (PRI) adapté ;
- La sensibilisation du personnel aux risques cyber (phishing, fraude au président, erreurs humaines) ;
- La prise en compte des tiers critiques (éditeurs, infogérants, hébergeurs) dans la politique de sécurité.

Une faiblesse sur ces points peut affecter directement l'information financière et justifier un renforcement des contrôles ou prise en considération dans la stratégie d'audit.

Séquence 1

Comprendre la thématique

Contexte et enjeux

La cybersécurité permet de lutter contre la cybercriminalité qui désigne les délits perpétrés à distance par des systèmes de communication comme Internet.

La cybercriminalité concerne non seulement les formes traditionnelles de criminalité, opérées via Internet, mais aussi l'atteinte à la confidentialité, l'intégrité et la disponibilité des systèmes d'information.

Une cyberattaque est donc un acte malveillant destiné à perturber le bon fonctionnement d'un système d'information.

Elles peuvent être distinguées :
- **L'attaque technique par le canal internet :** ces attaques exploitent une faille technique du site web ou du réseau de l'entreprise pour ensuite s'introduire dans son système d'information ou installer des logiciels malveillants. Ce type d'attaque nécessite des outils informatiques capables de contourner les dispositifs de sécurité du système d'information.
- **L'ingénierie sociale :** ces attaques exploitent les failles humaines, le maillon faible de la sécurité informatique. Grâce à des techniques manipulatoires, les cybercriminels amènent les collaborateurs de l'entreprise à compromettre la sécurité du système d'information.

NEP, textes et références :
- **NEP 240 :** Conformément à cette norme, le commissaire aux comptes doit évaluer les risques d'anomalies significatives dans les comptes résultant de ce type de fraude. La cybercriminalité a toutes les caractéristiques de la fraude telles que définies par cette norme.

FICHE 08

CYBERSÉCURITÉ

- **Doctrine de la CNCC** relative aux prestations entrant dans le cadre des Services Autres que la Certification des Comptes (SACC)
- **NIS2** : Directive européenne visant à renforcer la sécurité des réseaux et des systèmes d'information au sein de l'UE, en imposant des mesures de sécurité plus strictes et des sanctions harmonisées.
  Pour les PME non directement concernées, cette directive peut servir de référentiel de bonnes pratiques.
  Elle contient :
  - Des mesures de sécurité informatique adaptées,
  - La notification des incidents graves,
  - Et prévoit des sanctions harmonisées.
- **DORA** : Réglementation européenne visant à garantir la résilience opérationnelle des entités financières face aux risques numériques, en imposant des exigences en matière de gestion des risques informatiques et de notification des incidents.
  Bien que DORA ne s'applique pas aux PME en dehors du secteur financier, elle constitue un cadre de référence pertinent pour renforcer les dispositifs de cybersécurité dans toute organisation, en s'inspirant de ses principes : gestion des risques, continuité d'activité, et protection des systèmes critiques.
  Les exigences clés de la réglementation incluent :
  - Une gestion structurée des risques TIC (identification, protection, détection, réponse et rétablissement)
  - Des tests réguliers de résilience numérique, adaptés à la taille et à la complexité de l'entité
  - Une surveillance renforcée des prestataires de services numériques (cloud, hébergeurs, etc.)
  - L'obligation de notifier rapidement les incidents majeurs aux autorités compétentes
- **CobiT** dont les défaillances peuvent rendre l'entité vulnérable aux cyberattaques.

Conséquences pour le commissaire aux comptes

La cybersécurité est un enjeu crucial pour les commissaires aux comptes, car les cyberattaques peuvent gravement compromettre la fiabilité des états financiers et la continuité des activités de l'entité auditée.

Il est important pour les commissaires aux comptes d'intégrer les risques liés à la cybersécurité dans leur évaluation globale des risques, en identifiant les vulnérabilités potentielles et les menaces spécifiques à l'entité.

Ils doivent également évaluer les dispositifs de gestion de la cybersécurité mis en œuvre par l'entreprise (stratégie, gouvernance, comitologie, procédure, cartographies des risques cyber, plans de formation, veille, etc.).

Ils doivent également vérifier l'efficacité des contrôles internes mis en place pour prévenir, détecter et suivre les cyberattaques, en portant une attention particulière aux failles humaines exploitées par l'ingénierie sociale.

Les cyberattaques peuvent entraîner des pertes financières directes, telles que des rançons payées, et indirectes, comme des interruptions d'activité. Il est essentiel d'évaluer l'impact de ces pertes sur les états financiers et de vérifier si l'entité a correctement comptabilisé et divulgué les incidents de cybersécurité.

De plus, il est nécessaire de s'assurer que des plans de continuité des activités et de reprise après sinistre sont en place et efficaces, afin de garantir la pérennité des opérations de l'entité.

Il faut également être conscient des obligations légales et réglementaires en matière de cybersécurité auxquelles l'entité est soumise, telles que les exigences de notification des incidents dans le cadre de la réglementation DORA et les normes de protection des données personnelles RGPD.

Le non-respect de ces obligations peut entraîner des sanctions et des amendes, impactant la situation financière de l'entité.

Séquence 2

Mission du CAC : objectifs, bonnes pratiques et outils

Thématique

Analyse des risques et facteurs de criticité

Objectifs

Dans le cadre de sa mission et conformément à la NEP 240 (évaluation des risques d'anomalies significatives dans les comptes résultant de fraudes), le commissaire aux comptes doit intégrer les risques liés à la cybersécurité dans son évaluation globale des risques.

Il s'attache à identifier les vulnérabilités potentielles et les menaces spécifiques à l'entité auditée.

Il doit évaluer la conception et l'efficacité des dispositifs de gestion de la cybersécurité mis en œuvre par l'entreprise (stratégie, gouvernance, comitologie, procédures, cartographies des risques cyber, plans de formation, veille, etc.).

Il doit vérifier l'efficacité des contrôles internes mis en place pour prévenir, détecter et suivre les cyberattaques, en portant une attention particulière aux failles humaines exploitées par l'ingénierie sociale.

Le commissaire aux comptes doit également s'assurer que l'entité a correctement comptabilisé et divulgué les incidents de cybersécurité dans ses états financiers. De plus, il est nécessaire de valider l'existence et l'efficacité des plans de continuité des activités et de reprise après sinistre, afin de garantir la pérennité des opérations de l'entité.

Ces travaux visent à garantir la fiabilité des états financiers, la sécurité des systèmes d'information et la continuité des activités de l'entité auditée.

Les failles usuellement exploitées par les attaques techniques concernent principalement la sécurité des applications Web. Trois raisons peuvent en être à l'origine :
- La gestion incorrecte de l'authentification, des habilitations et du contrôle d'accès,
- L'injection de données qui est une technique consistant à insérer des données en entrée d'un programme informatique afin de les détourner de leur fonction d'origine,
- Les fuites d'information si les fonctionnalités ou composants internes à une application ne sont pas suffisamment « cloisonnés ».

Certes l'ingénierie sociale tire profit de la naïveté et de la crédulité de ses victimes, mais plusieurs autres facteurs de criticité sont de nature à favoriser ce type de cyberattaques :
- La facilité d'accès aux informations décrivant l'organisation de l'entreprise,
- L'accès aux informations personnelles des collaborateurs via les réseaux sociaux ou des portails RH,
- L'utilisation par les collaborateurs de technologies non sécurisées,
- L'utilisation par les collaborateurs d'équipements personnels dans un contexte professionnel (BYOD : Bring Your Own Device ou AVEPC en français : Apportez Votre Équipement Personnel de Communication),
- La complexité et la décentralisation des organisations,
- La généralisation du travail à distance,
- Le nomadisme professionnel et le télétravail,
- Le manque d'exemplarité des dirigeants,
- Et bien évidemment, le manque de contrôle interne et de formations associées.

Quelques exemples de cyberattaque

- Hameçonnage (phishing) ou harponnage (spear phishing),
- Logiciel malveillant (malware),
- Cassage de mot de passe,
- Attaques par déni de service (DoS) et par déni de service distribué (DDoS),

Quelques exemples récents

- **Virus Cryptolocker** : Un mail intitulé « relance facture impayée » est envoyé au comptable d'une entreprise. Le document joint contient un virus qui va chiffrer toutes les données accessibles par l'ordinateur contaminé et les rendre inutilisables. La clé de déchiffrement est fournie contre le paiement d'une rançon.

FICHE 08

CYBERSÉCURITÉ

- **Fraude aux virements :** Un important groupe industriel français a reçu un avis de changement de RIB, expédié soi-disant par un fournisseur, juste avant le règlement d'échéances importantes. Cette escroquerie a permis de dérober 1,6 M€ à la victime.
- **Espionnage économique :** Un Ministère français a fait l'objet d'une intrusion informatique et d'un vol de données. Le point de départ a été l'ouverture de fichiers contaminés par des utilisateurs manipulés et crédules.
- **Ransomware sur l'infrastructure cloud :** Une grande entreprise de services numériques a été touchée par une attaque de ransomware. L'attaque a entraîné le chiffrement de données hébergées dans le cloud, causant une paralysie partielle des opérations pendant plusieurs jours. Les attaquants ont exigé une rançon en cryptomonnaie pour fournir la clé de déchiffrement.
- **Fuite de données via un fournisseur tiers :** Une entreprise de distribution a subi une fuite massive de données, impliquant une faille chez un prestataire externe. Des données personnelles de millions de clients ont été rendues publiques. La fuite incluait des adresses, numéros de téléphone, et historiques d'achat, provoquant un tollé auprès des clients et des autorités de régulation.
- **Compromission par phishing ciblé :** Une société financière a été victime d'une attaque de type spear-phishing. Des employés ont été piégés, ce qui a permis aux attaquants de s'introduire dans les systèmes internes et d'accéder à des informations sensibles. L'attaque a été facilitée par l'utilisation de faux mails imitant parfaitement ceux de la direction, rendant la détection très difficile.
- **Attaque DDoS à grande échelle :** Une plateforme en ligne a été visée par une attaque par déni de service distribuée, qui a rendu ses services indisponibles durant près de 24 heures à un moment crucial de l'année. Des millions de requêtes malveillantes ont saturé les serveurs, empêchant les utilisateurs d'accéder à la plateforme pendant le pic des ventes saisonnières.
- **Fraude au président :** Une entreprise française de BTP a été victime d'une fraude au président. Un escroc s'est fait passer par téléphone pour le PDG, prétextant une opération confidentielle et urgente. Grâce à une mise en scène soignée et à des techniques de manipulation psychologique, il a convaincu la directrice financière de réaliser plusieurs virements internationaux. Le préjudice s'est élevé à plus de 20 millions d'euros. Cette attaque a été rendue possible grâce à une phase de renseignement préalable sur l'organigramme et les procédures internes de l'entreprise.

Top menaces

Menace	Principales contre-mesures
Phishing / Spear-phishing	→ Formation et sensibilisation régulières des collaborateurs → Simulations d'attaques → Filtrage des e-mails (anti-spam, antivirus) → Authentification multifactorielle (MFA)
Ransomware (ex : Cryptolocker)	→ Sauvegardes régulières et hors ligne → Plan de continuité et reprise d'activité (PCA / PRA) → Mise à jour régulière des systèmes → Détection comportementale (EDR)
Fuite de données via tiers (prestataires)	→ Audit des prestataires (sécurité, conformité RGPD) → Clauses de sécurité dans les contrats → Contrôles d'accès stricts → Cartographie des flux de données sensibles
Attaques DoS / DDoS	→ Pare-feu applicatifs (WAF) → Services de mitigation DDoS (ex. CDN) → Surveillance du trafic réseau (SOC) → Test de résilience des systèmes critiques

Bonnes pratiques

Mesures préventives :

- Nommer un responsable de la sécurité du système d'information (RSSI) qui serait garant de la correcte applications des règles de sécurité,
- Définir et formaliser une politique globale de sécurité des systèmes d'information (PSSI) reflétant la vision stratégique de la direction de l'organisme en matière de sécurité des systèmes d'information (SSI) et incluant les règles et les principes en matière de cybersécurité permettant ainsi de renforcer considérablement la sécurité de l'organisation en définissant des mesures de sécurité proactives pour les systèmes et les données, la PSSI et en prévenant les accès non autorisés, les pertes de données et les cyberattaques.

La PSSI doit se composer à minima des sections suivantes :
- L'introduction permettant de situer la place de la PSSI dans le référentiel normatif de la SSI au sein de l'organisme et de préciser les bases de légitimité sur lesquelles elle s'appuie,
- La méthodologie présente, de façon détaillée, la conduite de projet d'élaboration d'une PSSI, ainsi que des recommandations pour la construction des règles de sécurité,
- Le référentiel de principes de sécurité détaillant les différents domaines de la sécurité généralement couverts par une PSSI,
- Une liste de documents de références de la SSI (critères d'évaluation, textes législatifs, normes, codes d'éthique, notes complémentaires...).

→ Définir une stratégie et une gouvernance dédiées à la gestion de cybersécurité (organisation, rôles et responsabilités, procédures et politiques, comitologie, reporting, monitoring, veille etc.),
→ Définir une procédure de gestion et de suivi des incidents de cybersécurité,
→ Formaliser et mettre à jour régulièrement une cartographie des risques de cybersécurité, en considérant les risques cybersécurité liés aux nouvelles technologies, les événements redoutés apparus, les dispositifs de maîtrise de risques mis en place, les évaluations brutes et nettes des risques de cybersécurité, etc.,
→ Définir et mettre en place un cadre de contrôle internes permettant de prévenir, détecter et suivre les cyberattaques,
→ Définir un processus permettant d'inclure des exigences de cybersécurité par défaut dans les nouveaux projets,
→ Définir des procédures de sélection et d'autorisation de nouveaux matériels ou logiciels,
→ Définir des procédures de gestion d'accès aux informations par des tiers,
→ Définir une politique de déclassement de matériel informatique,
→ Définir une politique de cryptage des données,
→ Renforcer les mécanismes d'authentification au travers la mise en place de l'authentification multi-facteurs (MFA) et l'utilisation de mot de passe fort et conformes aux bonnes pratiques en place (CNIL, ANSSI, etc.),
→ Mettre à jour de manière régulière les logiciels, les anti-virus et configurer le pare-feu,
→ Limiter les accès aux informations sensibles au travers la correcte définition des profils et des droits et la mise en place des règles de séparation des tâches,
→ Différencier les usages personnels des usages professionnels du matériel informatique,
→ Sensibiliser et former le personnel à la question de la cybersécurité et aux risques liés aux emails,
→ Sécuriser les accès réseaux de l'entreprise.

Mesures détectives :
→ Mettre en place des diagnostics pré ou post implémentation permettent d'identifier les insuffisances en termes de cybersécurité dans la conception et dans l'implémentation d'un projet et de vérifier le respect des bonnes pratiques de sécurité,
→ Réaliser régulièrement des audits de cybersécurité afin de fournir au management une vue globale de la maturité de la cybersécurité, de se comparer par rapport aux pairs et d'identifier les actions correctives à mettre en œuvre,
→ Réaliser périodiquement des tests d'intrusion permettant de mettre en évidence les vulnérabilités du SI, les risques de cybersécurité encourus et les actions correctives nécessaires,
→ Réaliser régulièrement des tests de continuité d'activité et de secours informatique,
→ Réaliser des diagnostic cyber-résilience conformément à la réglementation NIS2 afin d'évaluer le potentiel de résilience par rapport à des attaques de type ransomware et d'identifier les actions pragmatiques pour renforcer la résilience de l'entreprise,
→ Vérifier la conformité RGPD afin d'obtenir une vision globale du niveau de conformité, puis identifier les non-conformités et le reste à faire afin de répondre aux exigences du régulateur.

FICHE 08

CYBERSÉCURITÉ

Outils & documentations mises à disposition

Après avoir analysé la prise en compte des risques par la direction générale, l'auditeur pourra se consacrer à l'évaluation des dispositifs de prévention de l'entreprise avec des questions telles que :

Thème / Question	Enjeu / Risque	Interlocuteur	Niveau de maturité : Non implémenté Démarche en cours de mise en œuvre Démarche en place
Existe-t-il une stratégie de cybersécurité définie ? Une gouvernance dédiée à la gestion cybersécurité est-elle définie et mise en place ?	Opérationnel	DSI	
Existe-t-il une gouvernance dédiée à la gestion de la sécurité de l'information : un comité sécurité, un responsable de la sécurité du système d'information (RSSI) et des correspondants sécurité dans les unités ?	Opérationnel	DSI	
Une politique de sécurité des systèmes d'information est-elle formalisée et mise à jour ?	Opérationnel	DSI	
Existe-t-il une attribution claire des responsabilités pour la mise en œuvre et le suivi des évolutions à apporter en matière de sécurité du SI ?	Opérationnel	DSI	
La direction a-t-elle mis en place une organisation et des contrôles Diagnostic pré ou post implémentation permettant d'identifier les insuffisances en termes de cybersécurité dans la conception et dans l'implémentation d'un projet et de vérifier le respect des bonnes pratiques de sécurité ?	Opérationnel	DSI	
Existe-t-il des procédures d'autorisation de nouveaux matériels ou logiciels ?	Opérationnel	DSI	
Existe-t-il des procédures applicables à l'accès aux informations par des tiers ?	Opérationnel	DSI	
Existe-t-il des modalités de réaction aux incidents de sécurité et aux défauts de fonctionnement conformément aux exigences réglementaires en vigueur (ex. NIS2) : → Signalement rapide des incidents de sécurité → Signalement dysfonctionnements de logiciels → Capitalisation sur la résolution d'incidents → Processus disciplinaire	Opérationnel	DSI	
Les connexions à distance sont-elles réalisées de manière sécurisée ? (VPN par exemple) Les dispositifs de cybersécurité ont-ils été adaptés par rapport à la généralisation du télétravail par suite de la crise sanitaire ?	Opérationnel	DSI	
Les échanges d'informations sont-ils réalisés de manière chiffrée ?	Opérationnel	DSI	
Les ordinateurs de bureau et les serveurs de l'organisation sont-ils tous protégés par un anti-virus ? Les vulnérabilités de de sécurité font-elles l'objet d'une analyse et d'un suivi réguliers ?	Opérationnel	DSI	
L'organisation s'assure-t-elle que tous les anti-virus sont à jour et fonctionnent correctement ? Si possible de façon centralisée, sinon selon une procédure documentée.	Opérationnel	DSI	
Les règles de contrôle d'accès sont-elles formalisées dans un format « tout est interdit sauf » plutôt que « tout est permis sauf » ? Ces règles sont-elles transmises aux salariés ?	Opérationnel	DSI	

Thème / Question	Enjeu / Risque	Interlocuteur	Niveau de maturité : Non implémenté Démarche en cours de mise en œuvre Démarche en place
La gestion des mots de passe et les systèmes de déconnexion automatique vérifient-ils les règles suivantes : Tout compte utilisateur doit être protégé par un mot de passe ; → Engagement des utilisateurs à ne pas divulguer leur mot de passe ; ne pas écrire leur mot de passe de façon trop évidente ; ne pas stocker leur mot de passe dans une procédure automatique ; changer leur mot de passe dès qu'ils le soupçonnent d'être compromis ; → Contrôle qu'un mot de passe temporaire est envoyé pour la première utilisation et qu'il est bien changé par l'utilisateur dès la première utilisation ; → Contrôle que les mots de passe temporaires sont transmis aux utilisateurs de manière sûre ; → Contrôle que le système impose un changement régulier du mot de passe ; → Contrôle que le système impose le choix de mots de passe robustes ;	Opérationnel	DSI	
La direction a-t-elle mis en place des contrôles suffisants et efficaces permettant d'évaluer le niveau de sécurité de l'annuaire Active Directory, système névralgique de l'entreprise, dont dépend la sécurité de la majeure partie du SI ?	Opérationnel	DSI	
La direction générale a-t-elle mobilisé les compétences requises pour comprendre les risques de cybercriminalité et déterminer si le management prend les actions appropriées ?	Opérationnel Juridique	DG	
La direction générale bénéficie-t-elle d'un retour direct du responsable de la sécurité pour lui expliquer en des « termes opérationnels et stratégiques » les cyber risques et leur prévention ?	Opérationnel Juridique Image	DG	
Une attention suffisante est-elle aussi bien consacrée à la défense a priori contre les attaques qu'aux opérations de remise en état des systèmes a posteriori ? La DG a-t-elle mis en place un reporting pour centraliser et suivre les différentes tentatives de fraude au sein de l'organisation ?	Opérationnel Juridique Image	DG	
Les fonctions essentielles de l'entreprise ont-elles été sécurisées pour préserver la résilience de l'entreprise en cas d'attaque ?	Opérationnel	DG	
La DG a-t-elle mis en place une cartographie des risques cybersécurité ? La DG a-t-elle identifié les scénarios possibles en fonction des types d'attaques ? Les données sensibles sont-elles identifiées et protégées ? Les plans d'actions en cas de crise sont-ils effectivement mis à jour en fonction des évolutions technologiques ou opérationnelles ?	Opérationnel Juridique Image	DG	
La cartographie des risques cybersécurité est-elle mise à jour régulièrement ? Les exigences cybersécurité liés aux nouvelles réglementations et les nouvelles menaces sont-elles prises en compte dans la mise à jour de la cartographie des risques cybersécurité (ex. DORA, NIS2)	Opérationnel	DG	
Existe-il un plan de formation et des campagnes de sensibilisation pour les collaborateurs aux règles de cybersécurité mises en place et aux nouvelles menaces de cybersécurité ?	Opérationnel	DSI	
La cartographie des risques cybersécurité est-elle mise à jour régulièrement par rapport aux nouvelles technologies et prend-elle en compte les nouveaux risques liés à l'intelligence artificielle ?	Opérationnel	DSI	

FICHE 08

CYBERSÉCURITÉ

Thème / Question	Enjeu / Risque	Interlocuteur	Niveau de maturité : Non implémenté Démarche en cours de mise en œuvre Démarche en place
La direction a-t-elle réalisé un diagnostic de maturité cybersécurité afin de fournir au management une vue globale de la maturité de la cybersécurité, de se comparer par rapport aux pairs et d'identifier les actions correctives à mettre en œuvre ?	Opérationnel	DSI	
La direction a-t-elle réalisé un diagnostic de la résilience conformément à la réglementation DORA afin d'évaluer le potentiel de résilience par rapport à des attaques de type ransomware et d'identifier les actions pragmatiques pour renforcer la résilience de l'entreprise ?	Opérationnel	DSI	

Dans le contexte d'une TPE / PME ou autre entité ne disposant pas de service informatique interne avec des personnes dédiées, le questionnaire simplifié suivant peut s'appliquer :

1. L'entité a-t-elle un annuaire ou une cartographie des applications critiques pour son activité ?
2. Des processus de gestion des comptes utilisateurs sont en place pour gérer les arrivées et les départs de collaborateurs (trices) ? *Cf. Fiche 02 – Contrôle des accès*
3. L'entité réalise-t-elle régulièrement des revues de comptes utilisateurs ? *Cf. Fiche 02 – Contrôle des accès*
4. Les paramétrages de mot des applications sensibles respectent-ils les bonnes pratiques en matière de longueur, de complexité, de durée de vie, etc. Se référer aux règles de l'ANSSI applicables à la date de l'intervention chez le client. *Cf. Fiche 02 – Contrôle des accès*
5. Les matériels nomades (PC portables, tablettes, smartphone) sont-ils dotés de moyens de protection non désactivable (chiffrement, mot de passe, etc.) *Cf. Fiche 02 – Contrôle des accès*
6. Les matériels de type PC portables, PC fixes ou serveur sont-ils dotés d'un antivirus avec des mises à jour automatiques ?
7. Un pare-feu est-il déployé et non désactivable ? Un VPN est-il déployé ?
8. Les collaborateurs sont-ils sensibilisés régulièrement aux risques liés à la cybercriminalité ?
9. L'entité a initié une démarche de continuité informatique que ce soit avec ses fournisseurs de logiciels que pour les matériels hébergés en interne ? *Cf. Fiche 07 – Plan de continuité d'activité et plan de reprise informatique*
10. L'entité a défini des modalités d'utilisation des outils d'IA (ex : ChatGPT) selon les bonnes pratiques ?

Impact dans la stratégie du commissaire aux comptes

L'intégration des risques liés à la cybersécurité dans la stratégie d'audit est essentielle pour garantir la fiabilité des états financiers et la sécurité des systèmes d'information de l'entité auditée.

Il est crucial d'être particulièrement vigilant quant aux vulnérabilités potentielles et aux menaces spécifiques à l'entité, en évaluant les contrôles internes et les plans de continuité des activités.

En promouvant les bonnes pratiques de cybersécurité, on contribue à l'amélioration des contrôles internes, ce qui permet de prévenir et de détecter les cyberattaques plus efficacement.

De plus, la vérification de la comptabilisation et de la divulgation des incidents de cybersécurité dans les états financiers assure une transparence et une fiabilité accrues des informations financières.

Un rôle clé est également joué dans la sensibilisation et la formation du personnel de l'entité auditée aux risques de cybersécurité.

En intégrant ces risques dans l'évaluation globale, on contribue à la réduction des risques d'anomalies significatives dans les comptes résultant de fraudes.

Cette approche permet de mieux protéger l'entité auditée contre les cybermenaces, d'assurer la continuité des opérations et de garantir la fiabilité des états financiers.

L'évaluation des risques cybersécurité en CAC, permet ainsi de garantir que les comptes reflètent fidèlement la réalité économique, tout en répondant aux exigences normatives et en contribuant à la sécurité financière de l'entreprise.

L'évaluation des risques liés à la cybersécurité conjointement à l'évaluation des dispositifs de contrôle interne IT dans le cadre d'un commissariat aux comptes (CAC) est devenue indispensable, car la cybersécurité peut directement impacter la fiabilité de l'information financière, permet d'avoir une vision globale et une compréhension détaillée de l'environnement informatique d'une organisation.

En effet, les cyberattaques peuvent provoquer des pertes financières directes (ex. : fraude, ransomware), affecter la disponibilité, l'intégrité ou la confidentialité des données comptables et entraîner des provisions, des dépréciations ou des pertes à constater. Par conséquent, le commissaire aux comptes doit donc évaluer si les risques liés à la cybersécurité sont susceptibles d'affecter significativement les comptes.

En outre, le CAC doit évaluer si des cybermenaces, des fraudes ou des anomalies identifiées peuvent compromettre la fiabilité des documents audités car ces attaques peuvent être l'origine de fraudes comptables (manipulation de données), d'usurpation d'identité (faux ordres de virement, faux fournisseurs) ou de disparition ou altération de preuves d'audit.

Par ailleurs, le CAC a pour mission d'évaluer la qualité du système de contrôle interne, dont la cybersécurité est aujourd'hui un maillon essentiel.

En effet, des faiblesses en cybersécurité peuvent révéler une maîtrise insuffisante des risques globaux de l'entreprise.

Une attaque cyber peut compromettre la capacité de l'entreprise à poursuivre son activité ce qui est indispensable pour assurer la fiabilité et l'intégrité des états financiers.

L'évaluation des autres dispositifs de contrôle interne IT peut s'appuyer sur les fiches CRCC dédiées à chacune des thématiques, à savoir :
→ Gouvernance des systèmes d'information,
→ Exploitation des systèmes d'information,
→ Contrôle des accès,
→ Conformité Réglementaire,
→ Plan de continuité d'activité,
→ Etc.

Séquence 3

Cas d'usage

Contexte

Dans le cadre de notre mission légale auprès de l'entité « Data & Flow », nous avons identifié, dès la phase de prise de connaissance, que le contexte de télétravail généralisé et l'utilisation massive des outils collaboratifs présentaient un risque accru d'usurpation d'identité et d'ingénierie sociale.

Au cours de l'exercice, l'entreprise a été victime d'une fraude au président : un fraudeur, en se faisant passer par e-mail pour le PDG, a convaincu un cadre du service comptabilité d'effectuer plusieurs virements urgents vers un compte à l'étranger. Le préjudice s'élève à 350 000 euros.

L'enquête interne a révélé l'absence de procédure de vérification des demandes exceptionnelles, une sécurité insuffisante des boîtes mail, et un faible niveau de sensibilisation des équipes.

Travaux à réaliser

→ **Investigation à la suite de la fraude cyber :** Vérification que les causes et conséquences de la fraude cyber ont bien été identifiées en analysant la chronologie de la fraude encourue, que les leçons ont été tirées et sont traduites en recommandations réalistes en ligne avec les attentes du top management.
→ **Revue de la messagerie électronique professionnelle :** Vérification de la configuration des protections contre l'usurpation d'identité (SPF, DKIM, DMARC) et recherche de domaines similaires à celui de l'entreprise. Analyse des journaux d'accès à la messagerie et des règles de transfert.
→ **Entretiens avec les équipes comptables et financières :** Compréhension du processus habituel de validation des virements, analyse de la réaction face à une demande inhabituelle et évaluation du niveau de vigilance des collaborateurs. Vérification avec les équipes que des actions de formation et de sensibilisation au cas de fraude identifiés sont bien menés suite à l'incident.

FICHE 08

CYBERSÉCURITÉ

- **Examen du contrôle interne :** Revue de l'existence de procédures formelles de validation en cas de paiement exceptionnel ou confidentiel, et évaluation de l'efficacité du principe de séparation des tâches.
- **Analyse de la sensibilisation au risque cyber :** État des lieux des formations internes, tests de phishing éventuels et communication interne autour des risques de fraude.

Impact pour notre stratégie d'audit

Ces éléments sont susceptibles d'influencer :
- Notre appréciation du contrôle interne sur les flux financiers et la fiabilité des systèmes d'information,
- Notre stratégie d'audit sur les opérations bancaires sensibles, notamment les paiements exceptionnels ou non récurrents,
- L'évaluation de l'environnement de contrôle et de la culture de sécurité dans l'entité,
- Le contenu de nos recommandations à destination de la gouvernance en matière de cybersécurité,
- L'analyse de la nécessité d'un ajustement de l'approche substantielle, notamment en cas de doutes sur la fiabilité des processus automatisés.

Démarche

Investigation à la suite de la fraude cyber :
Compréhension des causes et des conséquences de la fraude cyber, analyse de la chronologie de la fraude encourue, que les leçons ont été tirées et sont traduites en recommandations réalistes en ligne avec les attentes du top management.

Évaluation de la conception du contrôle (Design Effectiveness)
Objectif : Vérifier que les processus de validation de paiements et les mesures de cybersécurité préviennent efficacement ce type de fraude.
Question clé : Les processus de validation et la sécurité des communications sont-ils suffisamment robustes pour détecter une usurpation d'identité ?

Évaluation de l'efficacité opérationnelle du contrôle (Operating Effectiveness)
Objectif : tester si les dispositifs sont réellement appliqués et si les collaborateurs sont capables d'identifier une tentative d'escroquerie.

Méthodologie

- Analyse de la chronologie de la fraude encourue,
- Prise de connaissance des recommandations identifiées, des actions correctives définies à court, moyen et long terme et vérification du correct suivi des plans d'action associés par le top management,
- Analyse de la messagerie électronique de l'entreprise (SPF, DKIM, DMARC, MFA, journalisation),
- Revue des processus de validation des paiements exceptionnels : double signature, seuils d'alerte, confirmation téléphonique,
- Entretiens avec les collaborateurs exposés (comptabilité, direction financière) pour évaluer leur niveau de vigilance et de formation,
- Analyse de l'incident de fraude : déclencheur, détection, traitement, actions correctives,
- Vérification des actions de sensibilisation menées et du suivi post-incident.

Séquences de tests détaillées

Revue de la sécurité des échanges électroniques
- Les mesures anti-usurpation (SPF, DKIM, DMARC) sont-elles configurées ?
- L'authentification multifacteurs est-elle activée sur les boîtes sensibles ?
- Y a-t-il un système d'alerte pour les connexions inhabituelles ?

Analyse de l'incident de fraude au président
- Comment l'usurpation a-t-elle été rendue possible ?
- L'utilisateur ciblé avait-il reçu une formation sur les risques de fraude ?
- Des procédures existaient-elles pour vérifier les ordres de paiement exceptionnels ?

Contrôle des bonnes pratiques internes
- Des seuils de validation sont-ils définis pour les virements ?
- Existe-t-il une séparation des tâches dans le processus de paiement ?
- Les formations cybersécurité sont-elles à jour et diffusées à l'ensemble des équipes ?
- Des campagnes de simulation de fraude ou de phishing sont-elles organisées ?

Observations attendues

Sur la conception du contrôle :
- La gouvernance cyber intègre-t-elle les risques liés à l'ingénierie sociale ?
- Les procédures de validation financière incluent-elles des étapes de vérification systématique ?
- Une stratégie anti-fraude est-elle formalisée et diffusée en interne ?

Sur l'application du contrôle :
- Des mesures concrètes ont-elles été prises après la fraude ? (MFA, procédures, sensibilisation)
- Le personnel a-t-il été sensibilisé spécifiquement à la fraude au président ?
- Les incidents sont-ils documentés et utilisés comme base d'amélioration ?

Conclusion

L'audit réalisé chez « Data & Flow » a mis en lumière un environnement exposé aux risques de fraude par ingénierie sociale, notamment en raison d'un télétravail étendu, d'un usage massif des outils collaboratifs et de procédures internes insuffisamment robustes.

L'incident de fraude au président a révélé l'absence de mécanismes de vérification adaptés aux demandes inhabituelles, une sécurité technique des messageries perfectible, ainsi qu'un déficit de sensibilisation des équipes aux risques cyber.

Bien que certaines mesures aient été prises après l'incident (comme l'instauration de l'authentification multi-facteurs ou la mise à jour des procédures), ces actions doivent s'inscrire dans une démarche globale et pérenne de sécurisation des flux sensibles.

Il est ainsi recommandé de formaliser une politique anti-fraude complète, d'intégrer les contrôles de cybersécurité aux processus financiers critiques, et d'intensifier les formations ainsi que les tests de simulation auprès des équipes à risque.

Mini-checklist CAC – Cybersécurité

- L'entreprise a-t-elle été victime d'une fraude par ingénierie sociale ?
- Existe-t-il une procédure spécifique pour les paiements exceptionnels ?
- Un système de double validation est-il en place pour les virements sensibles ?
- Les collaborateurs sont-ils formés à détecter les fraudes par usurpation d'identité ?
- Un MFA est-il activé pour les comptes à privilèges et les boîtes de direction ?
- La messagerie est-elle sécurisée via SPF, DKIM, DMARC ?
- Les incidents sont-ils documentés et analysés ?
- Une culture de cybersécurité est-elle portée par la gouvernance ?
- Des tests de sensibilisation (phishing, fraude simulée) sont-ils organisés ?
- Les sous-traitants (comptabilité externalisée, DAF externalisé) sont-ils sensibilisés ?
- Les contrôles liés à la chaîne de paiement sont-ils à jour et testés ?

Séquence 4

Allez plus loin

Ressources pratiques

Outils CRCC, NEP spécifiques, guides techniques rapides
- Checklist cybersécurité – CNCC
- Grille d'audit cybersécurité (inspirée EBIOS/NIST)
- Liste des 42 mesures essentielles de l'ANSSI
- NEP 315, 330, 240, 265
- CRCC, « La cybersécurité dans la mission du CAC en PME » et « Questions types à poser au DSI / RSSI »

Formations recommandées

- CNCC – Formation « Cybersécurité et missions du CAC »
- CNAM – « Cybersécurité pour les non-informaticiens »
- ANSSI – MOOC SecNumAcadémie

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

FICHE 09

SOUS-TRAITANCE ET CLOUD

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

FICHE 09 SOUS-TRAITANCE ET CLOUD

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 limité 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.

FICHE 09

SOUS-TRAITANCE ET CLOUD

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)

CONTRIBUTION

Ce dossier de travail a été rédigé par le pôle « Informatique au service de l'audit » de la commission Innovation de la CRCC de Paris, dont les membres sont :

- Maud Bodin Veraldi
- Benjamin Deville
- Serge Yablonsky
- Frédéric Burband
- Gina Gulla Menez
- Alexandre Madrelle
- Georges de Montgolfier
- Jean-Laurent Heim-Lienhardt
- Renaud Ronchieri
- Frédérik Dupont
- Angélique Regnard
- Akram Elleuch

CRCC
COMPAGNIE RÉGIONALE DES COMMISSAIRES AUX COMPTES
PARIS