

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.

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...).

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.

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)