Département Finances et fiscalité locales 10 décembre 2020

# Note sur le guide méthodologique relatif au contrôle interne des systèmes d'information des collectivités locales dans le cadre de la démarche de fiabilisation et de certification des comptes locaux

**L'article 110 de la loi du 7 août 2015 portant nouvelle organisation de la République prévoit une expérimentation de la certification des comptes**[1] des collectivités territoriales et de leurs groupements, incitant ainsi les 25 collectivités expérimentatrices retenues à mettre en place une trajectoire de fiabilisation et d'amélioration de la qualité de leurs comptes.

Élaboré par la Mission Responsabilité Doctrine et Contrôle Interne Comptables, avec le concours du Service des Collectivités Locales, ce guide s'adresse à l'ensemble des collectivités, et en particulier à celles engagées dans la démarche de fiabilisation et de certification des comptes locaux.

Ce guide est composé de deux parties :
- Partie 1 : présentation de la démarche contrôle interne des systèmes d'information ;
- Partie 2 : renforcement du contrôle interne des systèmes d'information

## La démarche de contrôle interne des systèmes d'information dans le cadre de la fiabilisation et de la certification des comptes locaux

Un système d'information (SI) n'est pas seulement un système d'équipements informatiques et de télécommunications, mais avant tout, une organisation des ressources destinée à traiter l'information, soit pour produire, soit pour piloter. C'est un ensemble organisé de ressources (matériel, logiciel, personnel, données, procédures…) permettant d'acquérir, de stocker, de communiquer des informations sous forme de données, textes, images, sons… dans des organisations pour répondre aux besoins en information de ses utilisateurs.

Le SI traduit en outre des évènements de gestion en comptabilité. De fait, le risque numérique a également une incidence sur la production des informations financières et comptables et doit donc être considéré comme une composante de la fonction comptable.

Le risque numérique est susceptible d'avoir des impacts variés :
- impact en matière de sécurité des biens et des personnes (ex : incendie, mise en danger des personnels) ;
- impact budgétaire (ex : coût lié à la détérioration du matériel, fraude) ;
- impact organisationnel (ex : lenteur, surcharge ou indisponibilité totale ou partielle du réseau) ;
- impact juridique (ex : engagement de la responsabilité de la collectivité en raison du non-respect de la protection des données personnelles).

De part la qualité de l'information qu'il restitue, le système d'information doit donc contribuer à assurer la régularité et la sincérité des comptes. Il doit également garantir l'image fidèle du résultat de la gestion, du patrimoine et de la situation financière des collectivités locales et de leurs établissements publics.

Par ailleurs, le développement du numérique impacte de plus en plus les processus de gestion dans les collectivités. La compréhension de ces processus automatisés et de leur niveau de maîtrise et de contrôle par les collectivités, devient aujourd'hui incontournable dans le contexte de fiabilisation des comptes publics locaux.

Les collectivités locales et les établissements publics locaux doivent ainsi se préparer à répondre aux exigences de contrôle interne des systèmes d'information dans le cadre de la fiabilisation et de la certification des comptes locaux.

[1] La certification est une opinion écrite et motivée sur la fiabilité des comptes d'une entité qu'un tiers indépendant formule sous sa propre responsabilité. Elle a pour objet de donner une assurance raisonnable sur la conformité des états financiers de l'entité aux règles et principes comptables applicables et sur l'absence d'anomalies significatives susceptibles d'en altérer la lecture et la compréhension.

Afin de certifier les états financiers d'une entité, le certificateur s'appuie notamment sur la qualité du contrôle interne des systèmes d'information concourant à l'élaboration de l'information comptable et financière des collectivités territoriales.

Dans ce cadre, il peut être amené à examiner :

- les éléments d'organisation et de contrôle sur lesquels s'appuie le système d'information de l'entité ;
- la fiabilité des applications informatiques utilisées.

Ainsi, le certificateur ne s'intéresse pas seulement aux comptes, mais procède également à une revue et à une évaluation du système d'information de la collectivité, support de la comptabilité.

Le champ d'action du certificateur couvre tout ou partie des applications intervenant dans la saisie et le traitement des informations, depuis la survenance du fait générateur jusqu'à la production des états financiers.
Le périmètre inclut :

- les applications supportant les cinq principaux processus comptables : recettes, personnel, immobilisations, achats, endettement long terme et trésorerie court terme.
- les progiciels, les applications spécifiques développées en interne par les collectivités ainsi que les outils bureautiques de type tableur ou bases de données ;
- le système comptable Hélios ainsi que les interfaces mises en place avec le système d'information de la collectivité.

Ainsi, l'évaluation du dispositif de contrôle interne des SI permet de mettre en exergue les points forts et faiblesses dans le déroulé des procédures de la collectivité. Les états financiers de la collectivité étant le résultat de la traduction des informations transmises par les applications financières et « métiers » de la collectivité, et par Hélios utilisé par le comptable public, l'élaboration et la mise à jour a minima annuelle d'une cartographie[2] est une condition préalable de la fiabilité de l'information financière.

En conséquence, il est préconisé que les collectivités se dotent à minima d'une cartographie applicative représentant sous forme graphique les principales applications du système d'information (fonctionnalités, système d'exploitation, base de données…) ainsi que les flux de données (type de données, format, fréquence du flux…).

En outre, afin de disposer d'une connaissance fine du SI, il est essentiel de tenir à jour une synthèse des effectifs internes et externes agissant pour le compte de la direction des systèmes d'information (DSI) ainsi qu'une liste :

- des principales applications financières et métiers ;
- des principales interfaces internes et externes ;
- des contrats internes et externes passés par la DSI de l'établissement ou ayant un impact sur la disponibilité du SI (contrat de maintenance, de service, etc.) ;
- des données issues de chaque SI.

Enfin, il est fondamental de mettre en place un **niveau de sécurité minimal** sur l'ensemble du parc informatique de l'entité (postes utilisateurs, serveurs, imprimantes, téléphones, périphériques USB, etc.) :

- limitation des applications installées et modules optionnels des navigateurs web aux seuls nécessaires ;
- pare-feu local et anti-virus (ceux-ci sont parfois inclus dans le système d'exploitation) ;
- chiffrement des partitions où sont stockées les données des utilisateurs ;
- désactivation des exécutions automatiques.

**Pour de plus amples informations vous pouvez consulter le guide à l'adresse suivante :**
https://www.collectivites-locales.gouv.fr/guide-methodologique-pour-soutenir-demarche-fiabilisation-des-comptes-locaux

[2] Recense l'ensemble des risques majeurs de la collectivité et notamment ceux liés au système d'information financière.
La cartographie du SI est en outre un outil :

- **décisionnel :** elle permet de réaliser l'inventaire des composants du SI et leur description détaillée, d'identifier les redondances dans le SI pour optimiser les coûts. Elle facilite l'identification des applications obsolètes qui ne sont plus adaptées aux besoins de la collectivité.
- **de pilotage** afin de comprendre les interactions entre les différents acteurs, utilisateurs et fonctions et de définir les règles de gouvernance.
- **de maîtrise des risques :** elle facilite l'identification des applications les plus exposées aux menaces afin de mettre en œuvre les mesures adéquates de protection. Elle permet en outre de qualifier les impacts « métiers » et de prévoir les conséquences d'incident ou d'une attaque numérique.
- **de gestion de crise :** elle est primordiale dans le cadre de la définition des activités prioritaires de la collectivité et de la définition d'un plan de continuité d'activité.