L'audit SI, une partie intégrante de la démarche de l'audit des états financiers

Mémoire présenté en vue d'obtenir le diplôme MASTER CCA

Année universitaire 2017/2018

Directeur de mémoire : Patrice CHARLIER

Maître de stage : Christophe LETT

Soutenu le 2 juillet 2018

Alisa VARBANOVA

REMERCIEMENTS

Je tiens tout d'abord à remercier mon maître de stage Christophe LETT de sa disponibilité tout au long de mon stage, de sa réactivité et des ses précieux conseils.

Je voudrais remercier particulièrement Caroline ADAM et Aurélien ALBERT pour l'aide apportée dans mes recherches sur mon mémoire, l'orientation, les réflexions et le temps consacré sur ma mission de rédaction de ce mémoire. De plus, je remercie les deux auditeurs SI, Bruno LIVERNAIS et Florent SUM, de m'avoir fait part de leurs connaissances sur le sujet de l'informatique.

Je remercie également l'ensemble du personnel du service audit pour l'accueil, la présence et disponibilité pendant ces quatre mois de stage, pour les connaissances et conseils partagés à travers les missions qu'ils m'ont confiées.

Je tiens par ailleurs à remercier Monsieur Patrice CHARLIER, mon directeur de mémoire, pour ses conseils, son aide et son suivi tout au long du stage.

Enfin, j'adresse mes remerciements à l'ensemble des professeurs et intervenants de l'EM Strasbourg pour leurs enseignements de qualité durant ces deux années d'études qui m'ont permis de préparer au mieux ce stage, ainsi que mon projet professionnel.

PRESENTATION DU CABINET D'ACCUEIL

Dans le cadre de ma dernière année d'études en Master CCA, j'ai effectué un stage au sein du cabinet d'expertise-comptable et de commissariat aux comptes MAZARS, se situant au 1 rue des Arquebusiers à Strasbourg. Ce stage s'est déroulé du mois de janvier au mois d'avril.

Mazars est une organisation internationale, intégrée et indépendante, spécialisée dans l'audit, le conseil et les services comptables, fiscaux et juridiques[1]. Son existence date depuis 1940 quand Robert Mazars crée son premier cabinet près de Rouen. Le cabinet a connu une évolution et un développement très rapide mais il a su rester fidèle aux valeurs de son fondateur. Aujourd'hui le groupe est présent sur 102 pays et territoires, dont 86 font partie du partnership international intégré de Mazars, et 16 sont des correspondants et des bureaux de représentation. Mazars est également membre fondateur de l'alliance internationale Praxity qui est une Alliance globale d'organisations indépendantes présente dans le monde entier et qui s'engage à respecter les standards internationaux les plus exigeants. Par ce biais le groupe dispose d'un réseau supplémentaire de 21 pays.

Le chiffre d'affaires de Mazars en fin 2017 est marqué par une croissance de 12,8% et dépasse donc 1,5mds d'euros. Avec cette expansion géographique et les changements profonds qui affectent le métier de l'audit, Mazars mise son succès sur l'innovation et la transparence.

En Alsace, le cabinet dispose de deux bureaux qui comptent au global 100 collaborateurs dirigés par six associés :

- Gilles CONTESSE
- Christian EINHORN
- Laurence FOURNIER
- Olivier GRAMLING
- Jean-Louis KOESSLER
- Valentin WITTMANN

L'activité du cabinet est organisée autour de deux pôles principaux : audit financier et accompagnement comptable et financier. Ces derniers sont en collaboration constante avec les services social et juridique.

Mon stage s'est déroulé au sein des équipes d'audit financier et j'ai été amenée à effectuer des travaux de phase finale (cycles clients, immobilisations, trésorerie, fournisseurs, capitaux propres, autres

[1] Cf. Annexe 1 : Description des métiers de Mazars

créances/autres dettes) et phase de bouclage (contrôle des comptes annuels, d'annexes, des rapports de gestion, des textes de résolution, contrôle des conventions réglementées). Les entités sur lesquelles j'ai pu intervenir couvraient le secteur industriel, le transport, la santé ainsi que le secteur associatif. Cette diversité des travaux confiés et les clients avec qui j'ai pu échanger ont été très enrichissants et formateurs pour moi. L'expérience acquise me conforte dans mon choix d'évoluer au sein du cabinet Mazars.

Table des matières

INTRODUCTION

Dans le monde actuel, l'information est devenue centrale et procure un avantage concurrentiel à une grande partie des entités quelle que soit leur taille. Elle est un vecteur de communication au sein de chaque entité et son absence ou incertitude a un impact direct sur l'avis des tiers. La gestion de cette information se réalise au travers du systèmes d'information (SI). Ce dernier est devenu un facteur clé du développement des entités et son organisation passe nécessairement par des applications de gestion et/ou des modules segmentés par fonction métier (production, distribution, achats, ventes, comptabilité, trésorerie, etc.).

La dépendance à l'informatique est un nouveau paramètre à prendre en compte. Le recours aux nouvelles technologies pose de plus en plus la question de la sécurité des informations, que ces dernières soient privées ou publiques. De ce point de vue, la politique de sécurité des systèmes d'information est devenue une préoccupation majeure.

Depuis des décennies, les systèmes d'information participent pleinement dans l'organisation des entités et ils déterminent souvent leur niveau de performance et de développement. Cette évolution de l'informatisation a comme incidence pour les entités une standardisation des flux de données, une interconnexion entre eux et une volumétrie importante[2]. Les états financiers sont gérés par ces flux d'information et ils conditionnent leur fiabilité.

Cette évolution entraine une profonde mutation de la mission du commissaire aux compte. Les systèmes d'information de plus en plus complexes mis en place par les entités amènent le commissaire aux comptes à se poser la question de la maîtrise des risques inhérents liés à ceux-ci. Ces « nouveaux » risques touchent directement l'activité de l'entité avec une éventuelle indisponibilité du système d'information, la fiabilité des états financiers, qui pourrait être erronée suivant la qualité des données comptables utilisées, et enfin, ils sont impactés par les accès à des informations confidentielles. C'est justement cette révolution numérique qui a forcé les commissaires aux comptes à repenser leur mission dans l'objectif de s'assurer de la sécurité et la pérennité des systèmes d'information utilisés par leurs clients. Cette évolution présente une réelle opportunité pour la profession, car elle introduit l'audit des systèmes d'information comme incontournable. L'intérêt de ce mémoire réside notamment dans ce point, et a pour objectif de démystifier l'audit SI et de démontrer que désormais celui-ci peut et doit être, dans une certaine mesure, réalisé par l'auditeur financier dans sa mission de certification des comptes. Il s'agit d'une montée en compétences techniques pour

[2] Carole Cherrier, Vice-présidente de l'IFEC dans « Les logiciels d'analyse de données au service de l'audit légal en PME » par François Gérard

l'auditeur, mais aussi d'un renforcement de la plus-value apportée au dirigeant. Cette nouvelle relation inclut le directeur des systèmes d'information comme l'un des principaux interlocuteurs.

L'intervention davantage en matière d'audit des systèmes d'information a un double objectif. Dans un premier temps, elle améliore la pertinence et l'efficacité de l'approche d'audit. Dans un second temps, elle répond aux normes d'exercice professionnel.

Ce mémoire a un triple objectif : de **démontrer** la nécessité de réaliser un audit des systèmes d'information dans toutes les entités quelle que soit leur taille tout en **expliquant pourquoi** cet audit est indispensable dans la mission de certification des comptes, et enfin, de démontrer **quels sont les contrôles** que l'auditeur financier doit réaliser afin de s'assurer de la pérennité des systèmes d'information utilisés par l'entité. Ainsi une problématique se dégage :

Comment l'auditeur financier peut intégrer l'audit SI dans sa mission de certification des comptes ?

Avant de présenter les contrôles que l'auditeur financier réalise sur la partie informatique (II), il convient d'expliquer pourquoi l'audit SI s'intègre désormais dans l'approche d'audit (I) dont l'aboutissement pour le commissaire aux comptes est le fait d'exprimer une opinion sur les comptes. Et pour finir, un cas d'application (III) sera présenté à titre d'illustration des travaux mis en œuvre par l'auditeur financier.

I. L'AUDIT SI DANS LA MISSION DE CERTIFICATION DES COMPTES

Dans cette partie, nous allons chercher à savoir pourquoi l'audit SI est devenu incontournable dans la mission légale du commissaire aux comptes. Nous expliquerons pourquoi ce travail réalisé par l'auditeur financier est un préalable à l'orientation de son approche d'audit (A) et comment celui-ci lui permet d'adapter la taille de ses échantillons et sondages. De plus, nous mettrons en avant les risques que ce travail nous permet d'identifier (B) si le niveau des moyens de prévention mis en place n'est pas suffisant.

Afin d'expliquer cela, nous allons poser les bases, dans un premier temps, avec une définition du système d'information et avec son inscription dans l'approche d'audit par les risques.

A. DÉFINITION ET APPORT DANS L'APPROCHE PAR LES RISQUES

1. Cadre réglementaire

La profession de commissariat aux comptes est fortement réglementée par des textes dont la plupart sont d'application obligatoire, mais qui sont, de plus, hiérarchisés. Avec la globalisation de l'économie, le besoin de la mise en place des règles et références communes est de plus en plus présent. Cette nécessité a inspiré la création de la Loi de sécurité financière de 2003 (LSF) ainsi que la réforme européenne de l'audit. Dans cet objectif, la LSF a confié à la Compagnie nationale des commissaires aux comptes (CNCC) d'élaborer des normes d'audit qui sont connues aujourd'hui sous le nom des normes d'exercice professionnel (NEP) dont le caractère public les rend opposables aux tiers. Elles définissent la démarche d'audit du commissaire aux comptes et l'organisation de ses travaux.

2. Prise de connaissance de l'entité

Au cœur de cette démarche d'audit, le commissaire aux comptes est guidé par la NEP 315 relative à la connaissance de l'entité et de son environnement et l'évaluation du risque d'anomalies significatives dans les comptes. A ce stade, il prend connaissance de l'activité de l'entité, de sa stratégie et ses objectifs ainsi que des contrôles internes qu'elle met en place et, plus globalement, de sa manière d'élaborer les informations financières. Autrement dit, le commissaire aux comptes étudie les « *moyens mis en œuvre par la direction pour identifier les risques liés à son activité, leur incidence sur les comptes et les actions à mettre en œuvre pour répondre à ces risques*[3] ».

[3] CNCC – NI. XV - Le commissaire aux comptes et l'approche d'audit par les risques - Décembre 2016, page 34-35

Comme précédemment évoqué, la production des état financiers passe nécessairement par le système d'information mis en place par la entité. La NEP 315 relative à la prise de connaissance dispose dans son paragraphe 14 que :

« *(…) le commissaire aux comptes prend notamment connaissance des éléments suivants :*

- (…)

- le système d'information relatif à l'élaboration de l'information financière. À ce titre, le commissaire aux comptes s'intéresse notamment :

- *aux catégories d'opérations ayant un caractère significatif pour les comptes pris dans leur ensemble ;*
- *aux procédures, informatisées ou manuelles, qui permettent d'initier, enregistrer, traiter ces opérations et de les traduire dans les comptes ;*
- *aux enregistrements comptables correspondants, aussi bien informatisés que manuels ;*
- *à la façon dont sont traités les événements ponctuels, différents des opérations récurrentes, susceptibles d'engendrer un risque d'anomalies significatives ;*
- *au processus d'élaboration des comptes, y compris des estimations comptables significatives et des informations significatives fournies dans l'annexe des comptes ;*
- *à la façon dont l'entité communique sur les éléments significatifs de l'information financière et sur les rôles et les responsabilités individuelles au sein de l'entité en matière d'information financière. À ce titre, le commissaire aux comptes s'intéresse notamment à la communication entre la direction et les organes mentionnés à l'article L. 823-16 du code de commerce ou les autorités de contrôle, ainsi qu'aux actions de sensibilisation de la direction envers les membres du personnel afin de les informer quant à l'impact que peuvent avoir leurs activités sur l'élaboration de l'information financière. ».*

Lors de cette phase il va recenser les applications supports des processus métier afin d'analyser leur relation avec le système d'information. Ce travail lui permet d'identifier dans un premier temps les risques significatifs liés, par exemple, à des interfaces non contrôlées, le manque de maintenance de certains logiciels ou des maintenances non adaptées aux besoins de l'entité ou bien des saisies manuelles.

3. Définition du système d'information

La note d'information éditée par la CNCC citée ci-dessus décrit le système d'information comme étant « *constitué des procédures et des documents conçus et destinés à :*

- *initier, enregistrer, traiter et présenter les opérations de l'entité (de même que des événements et des situations) et à suivre les actifs et les passifs qui leur sont liés ;*
- *résoudre les traitements incorrects d'opérations, par exemple les fichiers automatisés de suspens et les procédures suivies pour apurer les écritures en suspens en temps voulu ;*
- *enregistrer les cas où le système a été contourné ou des contrôles outrepassés ;*
- *transférer l'information à partir du système de traitement des opérations au grand livre ;*
- *saisir l'information pour les besoins de l'élaboration de l'information financière concernant des faits ou des situations autres que des opérations, tels que les provisions et l'amortissement des actifs ; et*
- *s'assurer que l'information devant être fournie selon le référentiel comptable applicable est saisie, enregistrée, traitée, récapitulée et présentée de manière appropriée dans les comptes.* »

Ainsi, pour satisfaire à ses multiples rôles le système d'information est composé de[4] :

- *« l'infrastructure technique (serveurs, routeurs, salles informatiques d'hébergement, etc.)*
- *logiciels, progiciels et interfaces inter-applications*
- *personnel chargé de maintenir le service informatique*
- *procédures et données qui centralisent les informations des différents systèmes de traitement des opérations au grand livre ».*

En principe, les entités tiennent une documentation relative au système d'information sur laquelle le commissaire aux comptes s'appuie lors de cette phase de prise de connaissance. Il réalise également des entretiens avec la direction des systèmes d'information (DSI).

Précisons que le commissaire aux comptes ne s'attachera durant ses diligences qu'au système d'information comptable et financière (système d'information ayant un lien direct avec la production des états financiers).

4. Apport du système d'information dans l'approche par les risques

Les traitements informatisés ont, en général, l'avantage d'être plus efficaces par rapport aux traitements manuels. Notamment, ils permettent de réaliser des calculs complexes des volumes importants dans des délais limités. Ils assurent également un niveau d'exactitude plus élevé en limitant le risque de contournement de certains contrôles. De plus, avec les contrôles de sécurité et d'accès aux différentes applications, une

[4] CNCC – NI. XV - Le commissaire aux comptes et l'approche d'audit par les risques - Décembre 2016, page 36

séparation des tâches, principe important dans l'audit, peut être garantie. Ce mode d'accès assure un suivi disponible nécessaire au bon fonctionnement de l'activité.

Malgré ces points positifs du système d'information, il convient de garder à l'esprit que celui-ci induit certains risques spécifiques au contrôle interne. Il s'agit notamment à des accès non autorisés, des modifications voire destructions des données. Ce risque est d'autant plus élevé lorsque des utilisateurs différents accèdent à une base de données commune, ce qui est fréquemment le cas dans les entités. Un autre point important est le fait que le personnel du service informatique dispose souvent d'accès privilégiés.

Le commissaire au compte est le garant de la transparence financière. Il a une mission légale, c'est-à-dire définie par le législateur dont l'objectif principal est d'assurer aux partenaires (actionnaires, établissements de crédit, salariés, fournisseurs et clients) une information fiable qui traduit les états financiers de l'entité. En ce qui concerne le système d'information, le commissaire aux comptes prend en considération dans son programme de travail l'analyse du fonctionnement des logiciels et leur convenance avec les procédures mis en place par l'entité.

Au cours de son intervention, le commissaire aux comptes va examiner la qualité du contrôle interne et il va apprécier le niveau du risque d'audit ce qui va se traduire par les diligences qu'il va mettre en œuvre.

5. La notion de risque d'audit

Nous avons évoqué à plusieurs reprises la notion de risque d'audit. Naturellement, il convient de faire un rappel sur cette notion. Elle est définie par la NEP 200 comme : « *le risque que le commissaire aux comptes exprime une opinion différente de celle qu'il aurait émise s'il avait identifié toutes les anomalies significatives dans les comptes* ». Ce risque d'audit est composé d'une part, par le risque que les comptes comportent des anomalies significatives (risque propre à l'entité) et, d'autre part, par le risque de non-détection de ces anomalies par le commissaire aux comptes (risque propre à l'auditeur)[5]. Le commissaire aux comptes cherche une assurance raisonnable, suffisante que les comptes sont sincères et réguliers. Il est donc impossible d'isoler tous les risques. Par conséquent, le commissaire aux comptes élabore son programme de travail selon les zones de risque qu'il a pu identifier lors de la phase de prise de connaissance.

[5] Cf. Annexe 2 : Définition du risque d'audit

6. L'impact du système d'information dans l'appréciation du risque d'audit

Une des multiples compétences requises du commissaire aux comptes est la maîtrise de l'informatique. C'est à travers cette dernière qu'il apprécie le système d'information dans son ensemble et étudie le déversement des écritures comptables de provenance diverse dans la comptabilité générale. « *Il s'assure du cheminement des flux d'un bout à l'autre de la chaîne, de la continuité de la piste d'audit, de l'origine de la pièce justificative jusqu'à son dénouement*[6] ». En annexe 3 le schéma démontre que les risques générés par l'utilisation des SI sont à plusieurs niveaux et ont des impacts considérables dans la production des comptes que le commissaire aux comptes va auditer. Ensuite, l'annexe 4 nous illustre le positionnement central du SI dans l'entité ce qui nous laisse penser que l'audit SI est désormais une partie intégrante de la démarche d'audit.

7. L'audit SI, une étape incontournable de la démarche générale de l'audit des comptes

Ainsi, nous pouvons conclure que le système d'information, son analyse et les contrôles mis en place par l'auditeur financier sont des étapes indispensables pour l'approche d'audit dans toutes les entités de toute taille et activité. Ils font donc partie de la démarche générale d'audit et constituent un moyen de collecter des preuves d'audit et aussi un moyen de détection des risques liés à l'utilisation des SI.

B. MOYEN DE PRÉVENTION ET DE DÉTECTION

Le fait pour le commissaire aux comptes de prendre connaissance du système d'information de l'entité lui permet d'apprécier la qualité du contrôle interne. Sa mission légale exclut donc toute immixtion dans la gestion. Tout de même, il lui est possible de formuler des observations concernant les points forts et les points faibles qu'il a identifié dans le cadre d'une lettre de recommandation. De cette manière, des problèmes potentiels peuvent être détectés avant qu'ils aient des conséquences plus graves, et prévenus.

La protection globale de l'entité est une préoccupation centrale pour le dirigeant. Cela englobe les brevets, l'image de la marque, sa réputation, la clientèle et parmi tous ces facteurs un soin particulier convient d'être apporté à la sécurité informatique. On parle donc de cybersécurité.

---

[6] *Benoit-René RIVIERE, « Extraction et exploitation des données du système d'information dans le cadre du commissariat aux comptes : méthodologie & outils », p. 23*

1. Cybersécurité

Dans l'ère de la digitalisation de nouveaux risques menacent les entités dont les conséquences sont souvent lourdes en termes de compétitivité, coûts et atteinte à l'image. Dans cette optique, leur prévention et la sensibilisation à cette prévention sont des enjeux importants et naturellement moins coûteux que le fait de réagir à un incident. C'est notamment la préoccupation de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui, dans une collaboration avec la Confédération générale du patronat des petites et moyennes entreprises (CPME), a publié un « Guide des bonnes pratiques informatiques » à destination des PME[7]. Son objectif est d'expliquer les risques existants liés à l'usage informatique en donnant des exemples concrets ainsi que des moyens de prévention simples afin d'améliorer la sécurisation de l'informatique en place.

Lorsque nous parlons de cybersécurité, nous nous intéressons souvent en premier lieu à la protection des données personnelles. Les entités sont souvent emmenées à collecter des données personnelles (de leurs employés, clients, fournisseurs, etc) et de renseigner leurs propres données aussi. Sur ce point la réglementation est en train de changer avec le Règlement général sur la protection des données (RGPD) voté en mai 2016 qui entre en vigueur le 25 mai 2018. Celui-ci remplace les 28 législations existantes et définit un ensemble de règles communes pour tous les acteurs traitant des données personnelles des citoyens européens[8] . Cette nouvelle réglementation oblige les entreprises collectant des données personnelles de pouvoir justifier pourquoi elles les collectent, où elles les stockent et comment elles les sécurisent. Elles doivent informer avec quelles entités ces données sont partagées et de quelle manière ces données sont exploitées. Les citoyens, quant à eux, peuvent demander l'effacement de leurs données personnelles ou leur rectification, limitation du traitement ou encore exercer un droit d'opposition. Mise à part un cadre plus strict de l'utilisation des données personnelles, ce règlement va supprimer les obligations déclaratives afin de décharger les entreprises des formalités administratives.

La mise en conformité avec cette nouvelle réglementation aura un coût important qui pèsera lourd surtout pour les PME et les TPE. D'autant plus que le non-respect des nouvelles règles expose les entreprises à une amende pouvant atteindre 20 millions d'euros ou 4 % de leur chiffre d'affaires mondial, un montant difficile

[7] Cf. annexe 5
[8] La Tribune, publication du jeudi 15 mars 2018 n°244, page 5

à supporter par une entreprise d'une telle taille. Cette menace a incité les grandes entreprises à se pencher très tôt sur le sujet en réalisant de tests de mise en conformité avec le futur cadre juridique[9].

En matière de système d'information, un des risques majeurs auxquels les entités sont exposées et auxquels les commissaires aux comptes doivent être vigilants est la cybercriminalité.

2. Cybercriminalité

La cybercriminalité désigne « *les délits perpétrés à distance par des systèmes de communication comme Internet*[10] ». Selon le guide édité par la CRCC, 2 types de cyberattaques sont à distinguer. La première qui utilise les failles techniques (attaques techniques), et la deuxième qui utilise les failles humaines (ingénierie sociale). Le document propose une série de questionnaires que l'auditeur peut mettre en place afin de valider la prise en compte des risques par la direction générale, et puis, pour évaluer les dispositifs de prévention de l'entreprise (cf. Annexe 6).

Selon Stéphane BELLANGER, expert-comptable et commissaire au comptes du cabinet CBM « *cette nouvelle donne doit être prise en compte dans la dimension conseil et veille juridique des CAC* [11]». La criminalité informatique concerne les entités quelle que soit leur taille. En matière de cyberattaques, elles ont l'obligation auprès de l'ANSSI d'établir une déclaration d'incident en cas d'attaque importante. En annexe 7 nous observons le schéma du service Cyberprotect soutenu par l'ANSSI.

Le rôle du commissaire aux comptes en la matière inclut les travaux de validation suivants définis par la NEP 315 qui sont réalisé généralement par entretien avec le DSI :

- *« politique d'habilitations définissant les accès au système d'information (mise à jour des accès en fonction des mouvements du personnel, de l'évolution de chaque personne dans la hiérarchie, revue de la politique de définition des mots de passe…),*
- *politique d'habilitations définissant les accès au système d'information (mise à jour des accès en fonction des mouvements du personnel, de l'évolution de chaque personne dans la hiérarchie, revue de la politique de définition des mots de passe…),*

[9] « Protection des données : le texte européen qui hante les nuits des patrons de PME français », LE MONDE, par Vincent FAGOT publié le 8 mai 2018
[10] « Audit informatique : tous concernés ! 10 fiches pratiques pour réussir », CRCC de Paris, juin 2017, page 67
[11] « Prévenir la cybercriminalité », Stéphane BELLANGER, Economie & Comptabilité n°243, septembre 2013, publication éditée par l'IFEC

- *politique de suivi des mises à jour des firmwares de l'infrastructure réseau (routeurs…) et des logiciels système (système d'exploitation, antivirus…) afin de maintenir un niveau élevé de sécurité et de limiter la vulnérabilité aux failles de sécurité,*
- *validation de l'origine des licences des logiciels et applications utilisés (les logiciels de provenance douteuse sont susceptibles de contenir des portes dérobées ou des codes malicieux)…*
- *prévention : tests d'intrusion,*
- *plan de continuation d'activité en cas d'incident,*
- *analyse de la police d'assurance (à noter : généralement, les polices d'assurance ne couvrent pas la reconstitution des données s'il s'avère que l'entreprise a été négligente en matière de politique de sauvegarde de données ou en matière de mise à jour de sécurité de ses systèmes informatiques)* [12]*».*

La cybercriminalité nous emmène logiquement vers la fraude car les deux possèdent les mêmes caractéristiques.

3. Fraude

Comme les NEP le précisent à plusieurs reprises, les anomalies significatives dans les comptes peuvent résulter « *d'erreur ou de fraude* ». Le risque d'anomalie significative résultant de fraude est décrit par la NEP 240. Selon celle-ci « *il existe une présomption de risque d'anomalies significatives résultant de fraudes dans la comptabilisation des produits. De ce fait, lorsque le commissaire aux comptes estime que ce risque n'existe pas, il en justifie dans son dossier* ». Cependant, il convient de préciser que « *tout risque de fraude et toute fraude ne se transforment pas en risque d'anomalies significatives résultant de fraudes*[13] ». Pour le commissaire aux comptes il ne s'agit non pas d'identifier des fraudes, mais d'identifier et d'évaluer le risque d'anomalies significatives contenues dans les comptes résultant de fraudes.

Lors de la prise de connaissance de l'entité, l'auditeur apprécie les arbitrages opérés par la direction sur le niveau des contrôles mis en place ainsi que les risques qu'elle assume. Il doit rester particulièrement vigilant sur des écritures proches de la clôture, toutes les hypothèses et évaluations réalisées, des opérations inhabituelles ou très complexes. Il est tenu de prendre du recul par rapport aux documents justificatifs qui lui sont transmis ainsi qu'aux explications obtenues. Lorsqu'il l'estime nécessaire, le commissaire aux comptes prévoit des procédures d'audit différentes de celles appliquées lors de l'audit de l'exercice précédent ou bien

[12] « Le commissaire aux comptes et la prévention de la cybercriminalité », Benoît-René RIVIERE, publié le 19 mars 2014 sur son blog

[13] CNCC – NI. XV - Le commissaire aux comptes et l'approche d'audit par les risques - Décembre 2016, page 48

il peut également changer le calendrier de l'intervention. Une autre option qui se propose au commissaire aux comptes est l'utilisation d'un logiciel d'analyse de données. Celui-ci analyse les informations des fichiers informatiques qui lui sont intégrés, préalablement ciblés par l'auditeur, et ressort des exceptions (la connexion d'un utilisateur à une date ou heure inhabituelle, une opération forcée ou une suppression ou modification d'un paramètre sensible (exemple : RIB d'un fournisseur) ou bien une incohérence entre le login de l'utilisateur et l'emplacement de l'ordinateur)[14]. À sa disposition l'auditeur a des outils comme les tableaux de bord EXCEL et ACCESS ou bien la loi de Benford qui l'accompagnent dans ses investigations de risque de fraude.

En ce qui concerne les petites entités, la NEP 910 permet « *dès lors que le commissaire aux comptes est en mesure d'apprécier le comportement et l'éthique professionnels du dirigeant, l'implication de ce dernier dans le processus d'autorisation et de contrôle des opérations peut constituer un élément de contrôle interne pertinent pour l'audit que le commissaire aux comptes peut utiliser pour alléger les procédures mises en œuvre à l'issue de l'évaluation des risques* ». Ce qui permet assez fréquemment à l'auditeur de conclure que le niveau de risque d'anomalie résultant de fraude n'est pas élevé, est la traçabilité des informations dans le système d'information. Elle consiste en un moyen de « *protection de l'intégrité des données du système d'information*[15] ». Elle permet notamment l'identification de l'utilisateur ainsi que le traitement de l'information exercé par celui-ci et l'heure de son enregistrement. Cela permet une remontée et une traçabilité des éventuelles erreurs ou tentatives de fraude.

Après avoir défini le système d'information, son rôle majeur dans le fonctionnement des entités et donc son inscription dans la démarche d'audit devenue non subsidiaire, nous allons faire un focus sur les travaux que réalise l'auditeur financier sur cet aspect.

[14] « Les logiciels d'analyse de données au service de l'audit légal en PME », François Gérard, page 20
[15] « Maîtriser le risque de fraude à l'aide de la traçabilité de l'information », Benoît RIVIERE, publié le 2 mai 2010 sur son blog

II. LES CONTRÔLES MIS EN PLACE PAR LE COMMISSAIRE AUX COMPTES DANS LE CADRE DE L'EXAMEN DU SYSTÈME D'INFORMATION

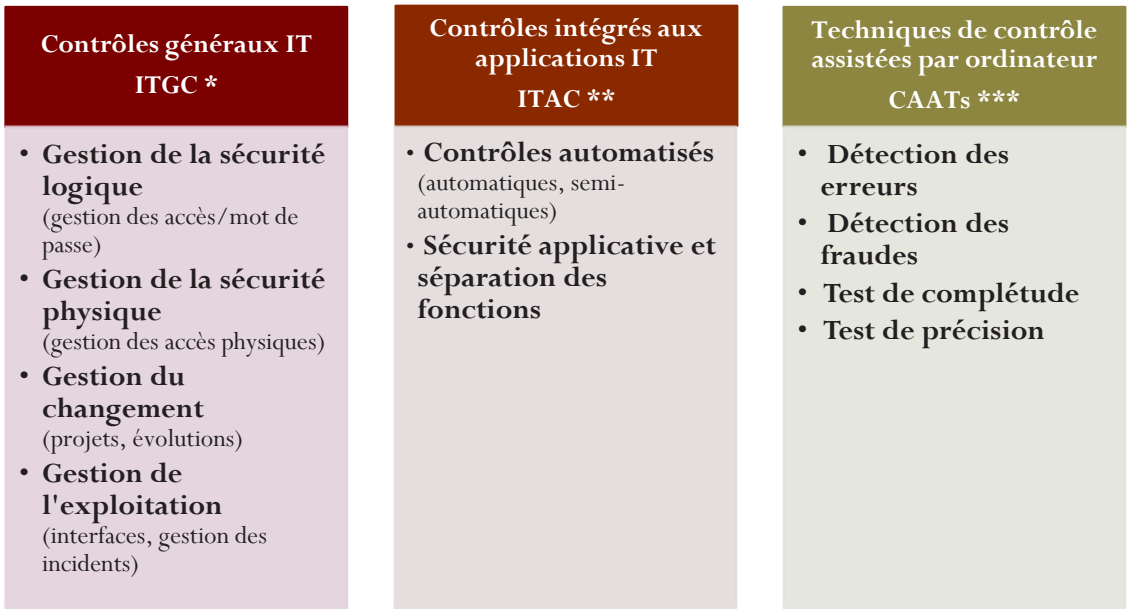
Dans cette partie, nous allons développer dans un premier temps les contrôles qui sont incontournables (A) lorsque l'on réalise des tests sur le SI dont la mise en place ne diffère pas en fonction de la taille et l'activité de l'entité. Dans un second temps, nous mettrons en évidence les travaux que le commissaire aux comptes adapte selon l'approche d'audit (B).

Dans certains secteurs ou entités le volume important des transactions impose l'intervention d'un auditeur IT spécialisé, car l'approche d'audit va être telle qu'elle va s'appuyer sur des contrôles informatisés afin de collecter des preuves d'audit (exemple : le secteur de banques et assurances). De plus, lorsque l'auditeur financier estime que les systèmes informatiques sont déterminants pour la fonction comptable, il fait participer à son approche un auditeur IT spécialisé. C'est un spécialiste qui fait partie de l'équipe d'audit et qui participe à la réunion d'approche.

En fonction de la taille de l'entité les travaux sur le SI peuvent être réalisés par l'auditeur financier-même. L'objectif de ce mémoire étant d'illustrer notamment ce cas de figure, nous allons nous concentrer sur les travaux réalisés dans des entités de taille moyenne, et par la suite, nous allons illustrer ces travaux par un cas d'application sur une association X.

En parlant des contrôles, il convient de noter que la criticité d'un contrôle est intrinsèquement liée à la criticité du risque qu'il couvre. Nous pouvons envisager le cas où un contrôle couvre plusieurs risques, mais également le cas où la maîtrise d'un risque nécessite plusieurs contrôles. Pour le commissaire aux comptes il est important de mettre en place des contrôles qui sont en lien avec les assertions envisagées.

L'audit SI réalisé par un auditeur financier est, en principe, composé par 3 étapes illustrées ci-dessous :



* *Information Technology General Controls = Contrôles généraux informatiques*
** *Information Technology Automated Controls= Contrôles intégrés aux Applications IT*
*** *Computer Assisted Audit Tools = Techniques de contrôle assistées par ordinateur*

Dans l'annexe 8, que nous avons déjà utilisé afin d'étudier la propagation des risques d'anomalies significatives générées par le SI, nous pouvons observer ces étapes ainsi que les contrôles sur lesquels elles s'appliquent. Dans la pratique, des contraintes budgétaires et au niveau du temps ne permettent pas la réalisation de la totalité de ces contrôles. Selon la complexité et l'intégration du SI mis en place par l'entité, ces contrôles ne sont pas toujours d'application obligatoire. La partie développée ci-après présentera les contrôles dont la mise en place est d'ordre général lorsque l'on réalise de l'audit SI.

A. CONTRÔLES INCONTOURNABLES

Dans un premier temps il s'agit pour l'auditeur de faire une évaluation de l'impact de l'IT sur l'entité auditée. Cette première étape concerne la phase de prise de connaissance.

1. Prise de connaissance / Cartographie

Le commissaire aux comptes étudie l'importance de l'informatique au sein de l'entité, la complexité des SI mis en place et l'étendue de leur utilisation. Pour ce faire, il va recenser les applications ayant un impact sur les états financiers sous forme d'une cartographie. Il va identifier les cycles sur lesquels l'approche d'audit

sera concentrée et sur lesquels l'utilisation des SI aura potentiellement un impact. Il cherche à identifier de manière générale les risques générés par l'IT (cf. annexe 9). Cette étape, réalisée par entretien avec la DSI, vise à apprécier la flexibilité des SI, la capacité à évoluer, les objectifs de l'informatique, la perception de l'utilisation de l'informatique par la direction, les principaux prestataires et les mesures prises pour réduire les risques informatiques. L'auditeur va également demander si des projets d'évolution du SI sont prévus.

Afin de mieux connaitre son interlocuteur, l'auditeur prend connaissance de l'organigramme du service informatique. Lors de cet entretien l'auditeur s'intéresse aux évolutions et incidents majeurs survenus sur de l'exercice. Il identifie les applications et outils utilisés pour supporter les principaux processus fonctionnels ainsi que les interfaces automatiques et semi-automatiques contribuant de manière significative à la production des états financiers. Ceux-ci sont présentés sur une cartographie applicative.

La cartographie applicative identifie les applications utilisées pour traiter l'information ayant un impact sur les états financiers. Elle permet de comprendre l'organisation des flux d'information financiers entre les applications en mettant en évidence leur origine, destination, contenu, traitement ou contrôles. Le fait de disposer d'une cartographie, permet au commissaire aux comptes d'orienter son approche d'audit, car de cette manière il acquiert une connaissance des flux non contrôlés ou des flux manuels par exemple.

Ces deux étapes sont indissociables et complémentaires car la prise de connaissance permet d'identification des flux, alors que la cartographie permet la qualification de ces flux. Fréquemment une cartographie est fournie directement par le client. L'auditeur peut s'appuyer sur celle-ci en restant vigilent sur certains points. Il doit notamment la faire valider par le responsable informatique de l'entité ou même par des spécialistes du cabinet d'audit. Il doit également la mettre à jour d'un exercice à un autre même si des modifications majeures n'ont pas été relevées. Il porte une attention particulière aux changements des flux potentiels. Cette cartographie doit être complète et explicite, mais au même temps elle doit se limiter aux besoins de l'audit pour ne pas rendre sa lecture difficile à comprendre.

Dans le cadre de ses travaux, l'auditeur financer examine ensuite les contrôles généraux informatiques mis en place par l'entité. En langage technique, nous avons adopté le terme anglais ITGC : *Information Technology General Controls*.

2. ITGC : Contrôle interne sur les processus IT

Cette étape couvre l'examen des contrôles prévus au sein de l'entité sur 4 aspects différents :

- La sécurité logique (gestion des accès, gestion des mots de passe)

- La sécurité physique (gestion des accès, protection face aux risques environnementaux)
- La gestion du changement (projets, évolution, paramétrages)
- La gestion de l'exploitation (interfaces, incidents, continuité)

Ces 4 contrôles s'appliquent sur 3 périmètres de l'informatique de l'entité : les applications, les bases de données et les systèmes d'exploitation. Afin de tester ces 4 contrôles, 3 types de tests sont à réaliser par l'auditer :

◊ Test sur son « design » : cela signifie de vérifier si le contrôle, tel qu'il est conçu, est pertinent et couvre le risque envisagé, autrement dit de savoir quelle est la procédure rédigée

◊ Test sur son implémentation : comment le contrôle est mis en place. A ce moment l'auditeur documente son test de design et on parle alors de D&I (*Design & Implementation*).

◊ Test d'efficacité opérationnelle (*OE : Operating Effectiveness*) : consiste à vérifier si le contrôle est systématiquement appliqué en sélectionnant un échantillon et en vérifiant si la procédure est correctement suivie.

Pour chacun des 4 contrôles l'auditeur réalise ces 3 types de tests avant de conclure s'ils sont effectifs, s'il y a des points à améliorer, etc. Maintenant, il va s'agir de faire un focus sur chaque contrôle cité ci-dessus et d'expliquer les risques qu'il permet de couvrir afin de mieux comprendre le cas d'application développé dans la partie suivante.

a. Sécurité logique

La sécurité logique est associée à la sécurisation des accès aux données. Les risques potentiels liés à la sécurisation des accès sont, en général, l'usurpation d'identité, la perte des informations confidentielles, l'accès non autorisé à des informations confidentielles, la réalisation d'actions malveillantes ou frauduleuses ainsi que des opérations non autorisées. Les précautions possibles que l'auditeur va rechercher sont, par exemple, la définition de paramètres de sécurité adéquats, l'application de règles strictes des droits d'accès aux systèmes, une validation de la mise en place de ces droits par un supérieur prédéterminé, une revue régulière et documentée des habilitations des utilisateurs, le respect de la séparation des fonctions dans l'attribution des droits des utilisateurs.

A titre d'exemple, concernant les mots de passe, ce que l'auditeur peut vérifier c'est d'obtenir dans un premier temps la politique de sécurité de l'organisation. Ensuite il peut demander une extraction de la stratégie de mot de passe implémentée au niveau de l'application. Et enfin, il mettre en concordance les deux

documents afin d'en tirer les écarts, c'est-à-dire afin de vérifier si la stratégie appliquée correspond à la politique adoptée. A la fin de chaque test l'auditeur matérialise s'il a relevé des points perfectibles ainsi que les points forts afin d'assurer un suivi du dossier.

b. Sécurité physique

La sécurité physique fait référence à la partie matérielle de l'informatique. Cela peut être des destructions des éléments informatiques, des vols de composants, des actes de malveillance ou mal attentionnés ou, de manière générale, tout risque environnemental. L'auditeur s'intéressera aux accès de la salle d'hébergement des serveurs (accès avec clé ou badge, personnes ayant accès, etc.), la localisation de cette salle, les dispositifs de sécurité (alarmes et détecteurs), les dispositifs de prévention (climatisation, alimentation électrique).

c. Gestion des changements

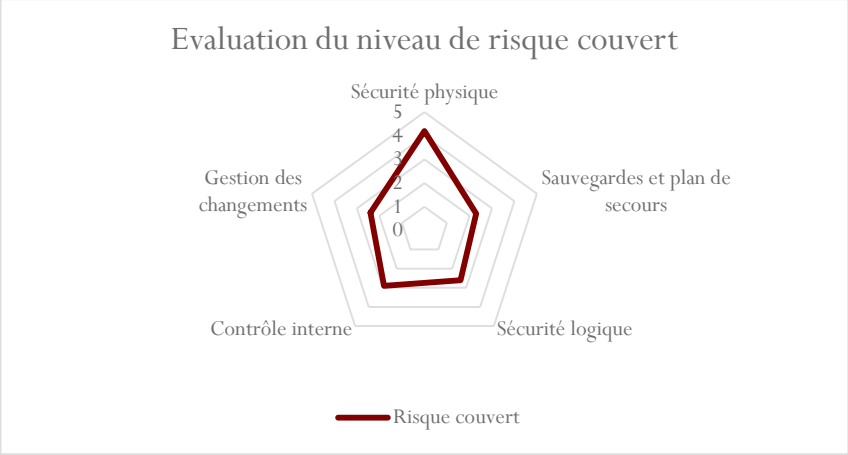
Lorsque nous parlons de gestion de changements, nous parlons d'évolution des serveurs. Pour l'auditeur la gestion des changements comprend les procédures et les contrôles qui s'assurent que les systèmes mis en place sont maintenus correctement et correspondent aux besoins de l'entité. Ce que l'organisation vise à éviter, c'est des traitements informatiques non fiables, des erreurs des états financiers résultant des systèmes, régression de la qualité des fonctionnalités ou le déploiement d'applications qui ne correspondent pas aux besoins des utilisateurs. Dans l'objectif de ne pas devoir faire face à ces problèmes, l'entité peut mettre en place un dispositif de formalisation des besoins des utilisateurs qui sera par la suite validé ou non par un validateur, réaliser des tests avant la mise en œuvre du changement envisagé, contrôler la période de transition en assurant une reprise correcte des données de l'ancien système vers le nouveau. L'auditeur vérifiera notamment ces mesures afin de valider que la gestion des changements ne présente pas d'anomalie significative. Il va collecter une liste des changements survenus sur l'exercice et, en identifiant leur impact au niveau comptable, il établira un échantillon de cas à tester. Pour ceux-ci, il demandera la demande du changement formalisée, sa validation par une personne habilitée et il analysera la pertinence de la demande par rapport aux besoins (plus la demande est explicite, plus cela facilite la tâche de l'auditeur dans son estimation).

d. Exploitation informatique

La gestion de l'exploitation informatique concerne le bon fonctionnement de l'informatique au quotidien. Les risques potentiels du fonctionnement peuvent être des exécutions incomplètes des traitements informatiques, des anomalie récurrentes non résolues, une double intégration de donnée ou l'échec de

l'intégration de la donnée, des retards ou des délais anormaux des traitements informatiques, la non restauration des données en cas d'incident. Les précautions de ces problèmes passent par un suivi des incidents et des actions correctives menées, une supervision régulière et efficace des traitements sensibles, un système de sauvegarde et restauration des données assurant la continuité de l'activité.

L'évaluations de ces contrôles par l'auditeur donne lieu à une estimation du niveau du risque couvert qui peut être représenté de la manière suivante :



Après avoir évoqué les contrôles de base que l'auditeur réalise dans le cadre de d'audit des SI, nous allons, à présent, nous concentrer sur les contrôles qu'il adapte en fonction de l'approche d'audit choisie. Il s'agit des contrôles qui ne sont pas à réaliser sur toutes les entités, mais de tests bien ciblés.

B. CONTRÔLES ADAPTABLES SELON L'APPROCHE D'AUDIT

Une fois les contrôles généraux validés, l'auditeur porte son attention aux contrôles embarqués dans les applications (1). Ce sont des contrôles automatiques et semi-automatiques pour lesquels il convient de s'assurer de leur efficacité. Après cette vérification le commissaire aux comptes met en place des contrôles de substance ciblés en fonction des assertions et des risques identifiés (2).

1. ITAC : Contrôles intégrés aux applications IT

Les contrôles intégrés aux applications informatiques sont des contrôles automatiques ou bien semi-automatiques. C'est notamment sur ces contrôles que porte cette partie de l'audit SI. Dans le cadre des contrôles automatiques, nous pouvons distinguer 4 types de contrôles :

- Les contrôles d'accès à l'application

- Les contrôles à la saisie des données (saisie, reprise, déversement des données)
- Les contrôles des traitements
- Les contrôles des sorties.

Lorsqu'il s'agit de plusieurs applications qui communiquent des données entre elles, nous parlons alors des interfaces. Ces dernières doivent être vérifiées par l'auditeur dans la mesure où cette communication de données représente un risque au niveau de leur exhaustivité. Après chaque importation des données, l'interface génère automatiquement un fichier d'anomalies qu'il convient d'analyser et traiter manuellement. C'est notamment ce contrôle que l'auditeur va examiner.

La méthode adoptée par l'auditeur est la même comme celle des contrôles généraux. A savoir, il cherche à s'assurer de la correcte conception et implémentation des contrôles mis en place par l'entité. Après avoir validé le design et l'implémentation des contrôles, l'auditeur va s'attaquer à l'efficacité opérationnelle des contrôles en réalisant un test sur un échantillon déterminé. Si cette première étape n'est pas validée (D&I), le commissaire aux comptes peut être emmené à repenser son approche et mettre en place une approche entièrement substantive.

Selon les contraintes du temps, budget ou capacités, ainsi que le besoin identifié par le commissaire aux comptes, une analyse des données peut être effectuée dans l'objectif d'obtenir une assurance raisonnable concernant le niveau du risque et d'avoir des éléments probants le justifiant. C'est la dernière étape à laquelle l'auditeur financier peut avoir recours dans le cadre de sa mission de certification des comptes.

2. Data analytics : analyse de données

L'analyse de données, encore connue comme techniques d'audit assistées par ordinateur (CAATs), permet à l'auditeur de réaliser des tests de détail et de mettre en place des procédures de substance. Il consiste à tester une multitude de transactions afin de déterminer si le contrôle sur celles-ci a pu être défaillant à un moment. En pratique cela peut être une vérification de calculs, une comparaison de fichiers, un tri des fichiers selon des critères différents. Pour ce faire l'utilisation d'un logiciel d'analyse de données est souvent nécessaire.

L'utilisation d'un logiciel d'analyse de données permet à l'auditeur un gain de temps et d'efficacité. Cela réduit également le risque d'audit et permet une meilleure formalisation des travaux. Le fait d'avoir recours à un tel logiciel n'est pas conditionné par la taille du cabinet d'audit mais par la spécificité de la mission. Cependant, la mise en place d'un logiciel d'analyse de données dans un cabinet est une décision de la direction importante. Elle dépend du nombre de mandats concernés ainsi que la durée prévue d'utilisation. Cela génère

un coût important, un investissement important en termes de temps et formation du personnel, un changement et donc un bouleversement des méthodes de travail déjà établies. De nouveaux rôles sont créés et une incertitude est engendrée. Le dirigeant du cabinet a comme principal défi de combattre la réticence et l'attitude réfractaire des collaborateurs en leur appropriant l'idée du changement. L'objectif d'un tel projet est de permettre la réalisation des travaux d'audit qui jusqu'alors n'étaient pas possibles ainsi que d'automatiser certains traitements pour gagner du temps. Dans la démarche générale d'audit cette étape s'inscrit au niveau des contraintes techniques de collecter et traiter des éléments comme suit :

Source : « *Les logiciels d'analyse de données au service de l'audit légal en PME* », François Gérard, page 39

Parmi les logiciels d'analyse de données les plus répandus nous pouvons citer ACL, IDEA, Odd-it, Onward et Active Data. Le choix du logiciel à mettre en place dépend essentiellement des difficultés rencontrées lors des missions. Le fait de qualifier ces difficultés permet d'orienter au mieux ses recherches vers un logiciel d'analyse de données en particulier.

Nous allons faire un rapide focus sur le fonctionnement du logiciel ACL sans pour autant développer en détail ce système, car il s'agit juste d'un zoom à titre d'explication. Il possède « *toutes les fonctionnalités d'un logiciel d'analyse de données (totalisation, stratification, jointure, fusion, rupture de séquence, doublons, échantillonnage) […] et permet de fusionner des centaines de fichiers*[16] ». Au niveau de son mode de fonctionnement, il manipule des cellules comme des blocs de données et il sauvegarde toujours un historique des travaux permettant la restauration de chaque traitement. Son avantage principal, mise à part une large gamme de fichier qu'il permet d'intégrer, est son interface sobre et son système de script qui le rend très flexible. Cependant, c'est un des logiciels d'analyse de données qui demande plus de temps et donc de formations afin de le maîtriser

[16] « Les logiciels d'analyse de données au service de l'audit légal en PME », François Gérard, IFEC, septembre 2015

et l'exploiter correctement. Un manque de formation suffisante peut même ralentir l'auditeur dans ses travaux et générer de la perte de temps dans l'exécution de la mission.

En conclusion, nous pouvons dire que la mise en place d'un logiciel d'analyse de données permet au commissaire aux comptes de réaliser des synergies et d'augmenter son efficacité globale. Ce logiciel est une composante de l'audit.

A présent, nous allons développer un cas d'application afin de mettre en pratique les travaux précédemment expliqués.

III. CAS D'APPLICATION : AUDIT SI DE L'ASSOCIATION X

L'association X sur laquelle un audit SI a été réalisé par l'équipe d'audit est une association réalisant 6 986 K€ de chiffre d'affaires et dont le total bilan s'élève à 5 134 K€. Elle a dégagé un résultat positif de 93 K€ pour l'exercice audité. Pour sa mission, l'équipe d'audit n'a eu recours à aucune consultation d'expert.

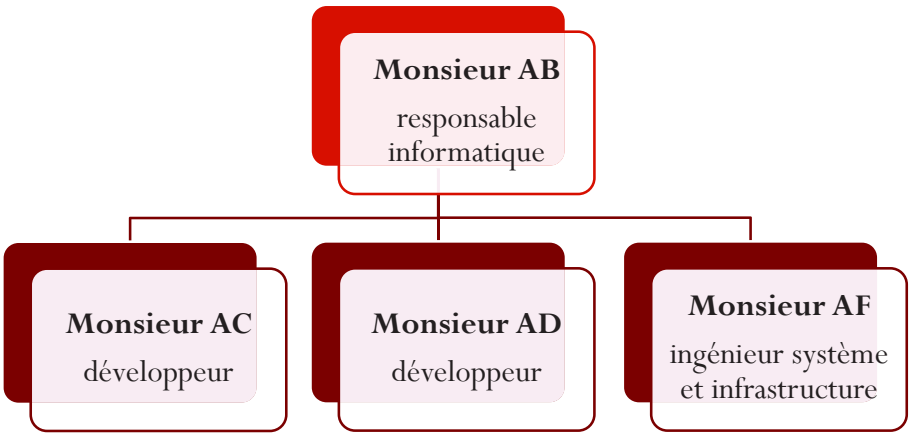
Comme la partie précédente l'indique, dans un premier temps une prise de connaissance de l'environnement informatique est à réaliser par entretien avec Monsieur AB, responsable informatique et le responsable financier.

A. PRISE DE CONNAISSANCE DE L'ENVIRONNEMENT INFORMATIQUE

Cette phase se décompose en plusieurs parties. Tout d'abord, un regard général est porté sur le fonction informatique.

1. Fonction informatique

Pour la prise de connaissance, l'auditeur cherche, dans un premier temps, à connaitre l'organisation de la fonction informatique : quelles sont les personnes qui la composent et quelles sont leurs fonctions, quel est le type d'organisation (centralisée ou plutôt décentralisée). Ensuite, l'auditeur établit un organigramme comme suit :



La fonction informatique est donc centralisée au siège de l'association X se trouvant à Strasbourg.

Puis, l'auditeur s'intéresse aux principaux prestataires auxquels a recours la fonction informatique et leurs activités. Ceux-ci sont matérialisés dans le tableau suivant :

Prestataire	Objet du contrat	Période	Remarques
AXIANS	Infrastructure réseau + logiciels	Annuelle	Maintenance et licences
QUONEX	Infrastructure	Annuelle	Maintenance, réseaux et serveurs
OCI	Sage	Annuelle	Maintenance Compta
PRODAXIS	Sage	Annuelle	Maintenance Paye
CANON	Impression	Annuelle	Copieurs & imprimantes
OVH	Sites Web	Annuelle	Hébergements sites
INGETEL	WinACA	Annuelle	Gestion commerciale
BODET	Badgeages	Annuelle	Maintenance logicielle
ORANGE	Téléphonie, réseaux	Annuelle	Maintenance

Ensuite, l'auditeur note les évolutions survenues au cours de l'exercice qui ont eu un impact sur la fonction informatique ou le SI, celles qui sont en cours et celles qui sont à venir. Dans notre cas, l'auditeur identifie une migration vers Office 365 concernant la messagerie et la suite bureautique. Une migration de la gestion commerciale est en cours afin d'être déployée pour 2018 de WinACA à Sage Gestion commerciale. Après la stabilisation de cette nouvelle gestion commerciale, des interactions auprès de la clientèle sont prévues.

Par la suite, il convient d'identifier les éventuels incidents ou événements majeurs ayant un impact sur la fonction informatique, qui ont pu avoir lieu durant la période auditée. Pour notre cas il n'y a pas d'incident significatif recensé. Cependant, si tel n'est pas le cas, l'auditeur devrait analyser l'impact et les conséquences de l'événement au niveau du SI.

Et enfin, l'auditeur recueille des informations d'ordre général sur le SI comme le nombre de salles serveurs et leur localisation – une seule salle située au siège de l'association à Strasbourg – et les dispositifs de secours et de continuité mis en œuvre sur le SI. Sur cette dernière question l'auditeur note les informations suivantes :

- Les serveurs de l'association sont virtualisés sur une infrastructure « *Vmware* » composée de deux nœuds[17] dont l'objectif et d'assurer la continuité de service si un nœud est défaillant. La sauvegarde est effectuée par un serveur de sauvegarde qui est délocalisé en dehors de la salle serveurs. Les équipements sont organisés de telle sorte qu'ils arrivent à assurer un fonctionnement correct en cas de coupure d'électricité pendant 15 minutes. Les données et machines virtuelles sensibles sont externalisées par un cloud vers le service « *Adista* ».

[17] A savoir que chaque nœud a la même capacité d'émettre, de recevoir et de calculer que les autres nœuds.

Une fois ces informations générales documentées, l'auditeur va recenser les applications sur un tableau récapitulatif.

2. Applications

Le tableau reprenant les applications de l'association X, présenté en annexe 10, recense : les processus concernés, les utilisateurs, l'hébergeur, la base de données, le système d'exploitation, la dernière mise à jour effectuée, les évolutions significatives survenues au cours de l'exercice ainsi que les contrôles clés réalisés à travers l'application. Si un niveau de détails plus élevé est nécessaire, ceux-ci sont présentés à la suite du tableau.

Comme nous l'avons évoqué précédemment, les applications communiquent souvent entre elles ce qui nous emmène vers le point suivant, à savoir les interfaces.

3. Interfaces

Encore une fois il s'agit d'un tableau récapitulatif réalisé par l'auditeur qui regroupe donc les applications en communication. Lorsque nous parlons de communications, nous parlons nécessairement de flux ou d'interface. Une description des flux est à développer ainsi que les contrôles informatiques réalisés. Le tableau des interfaces de l'association X est présenté en annexe 11.

De ces deux tableaux nous pouvons constater que même si des contrôles informatiques sophistiqués ne sont pas mis en place, un niveau de contrôle satisfaisant est assuré par le personnel en respectant le principe de séparation des tâches. Notamment ce dernier point, l'auditeur porte son attention dans le cadre des accès informatiques.

4. Accès informatiques

Dans cette partie, l'auditeur recense les différents processus métiers en indiquant quelles sont les personnes y ayant accès. Nous parlons alors d'habilitations. Sur l'association X l'auditeur relève les processus métiers suivants :

- **SAGE Immobilisations** : Accès informatiques réservés au service comptable (Mme Z) + RAF
- **SAGE Comptabilité** : Accès informatiques réservés au service comptable + RAF + CG
- **SAGE Trésorerie** : il s'agit de préparation et émission des ordres de virement : Accès informatiques réservés au service comptable (Mme Z et Mme Y) + RAF

- **Site de banque** : Accès informatiques réservés au service comptable (Mme Z et Mme Y) + RAF. Point très important à préciser est la question de l'émission des virements : L'émission du virement est validée uniquement par confirmation (fax ou clé sécurisée selon la banque) d'un des 3 signataires autorisés (à valider avec la réponse de circularisation[18] des banques).
- **SAGE Paie** : Accès informatiques réservés au service paie (Mme N et Mme M) + CG + RAF

Cette étape est importante pour l'auditeur au point de vue du principe de séparation des tâches. Il cherche à s'assurer que le risque d'opérations malveillantes est limité.

Suite à ces étapes, l'auditeur financier établit ou cherche à valider la cartographie applicative.

B. CARTOGRAPHIE

La cartographie, présentée en annexe 12, est établie par le service informatique du client et fournie à l'auditeur. Ce dernier la valide auprès du responsable informatique en s'assurant qu'elle est bien mise à jour.

Une fois tous ces travaux réalisés, l'auditeur financier s'attaque aux contrôles généraux informatiques mis en place par l'entité.

C. ITGC : CONTRÔLES GÉNÉRAUX INFORMATIQUES

Nous suivrons les 4 contrôles que nous avons développés dans la partie précédente afin de valider le contrôle mis en place en interne.

Au niveau de la sécurité physique (cf. annexe 13), nous constatons que l'accès à la salle serveur est limité à deux personnes qui possèdent une clé chacun. La protection des risques environnementaux est satisfaisante avec un détecteur de fumée et une climatisation adéquate. Cependant, il est constaté que la salle serveurs ne dispose pas de plancher surélevé ni de caméra ou alarme. Ce constat fait l'objet d'une recommandation émise par le commissaire aux comptes. La conclusion reste positive et le contrôle est validé par l'auditeur.

En ce qui concerne la sécurité logique (cf. annexe 14), plusieurs contrôles sont à valider. La procédure d'attribution des droits est correctement établie et suivie. De même, celle de désactivation des droits en cas de départ est également satisfaisante. L'auditeur vérifie également les comptes aux droits étendus, les

[18] Défini pas la **NEP 505 Demandes de confirmation des tiers** consiste à « obtenir de la part d'un tiers une déclaration directement adressée au commissaire aux comptes concernant une ou plusieurs informations »

comptes des administrateurs ainsi que les comptes génériques. En l'espèce, de tels comptes ne sont pas relevés. Au niveau des paramétrages de la sécurité, l'auditeur compare les bonnes pratiques aux méthodes appliquées par l'entité. Nous constatons qu'il n'existe pas de système obligeant les utilisateurs à changer leur mot de passe sur une certaine périodicité. Au global la sécurité logique de l'entité est satisfaisante.

Pour ce qui est la gestion des changements (cf. annexe 15), l'auditeur valide essentiellement la procédure de demande, validation et mise en place et suivi des changements. Nous avons un changement en cours qui concerne la gestion commerciale. L'auditeur vérifie si un accord par la direction a été donné, si des tests préalables ont été réalisés, si une autorisation formelle a été donnée, si un suivi nécessaire est assuré (schéma du changement envisagé avec les besoins que celui-ci couvrirait et le plan d'action prévu). Etant donné la taille limitée de l'entité, la séparation des tâches n'est pas validée car il n'y a pas de distinction entre celui qui développe une application et celui qui la met en production. Ce point fait également l'objet d'une recommandation émise par le commissaire aux comptes. Malgré ce point le contrôle est validé compte tenu de contexte organisationnel de l'association.

Le dernier contrôle à valider est celui de la gestion de l'exploitation (cf. annexe 16). Un suivi des incidents est assuré en interne ainsi qu'un système de sauvegarde en cas d'incident. Une trace est conservée de tous les problèmes qui sont survenus et qui ont été résolus par la suite. Il convient de noter que le système de restauration n'a pas pu être testé lors de l'audit SI.

Les contrôles informatiques généraux mis en place par l'association X sont validés. Compte tenu de la taille de l'entité auditée, et donc de l'approche d'audit, il ne sera pas procédé à des contrôles intégrés aux applications, ni à une analyse des données. Ce cas, ayant pour objectif d'illustrer les travaux incontournables réalisés par l'auditeur financier dans sa mission de certification des comptes, reste limité et non exhaustif.

CONCLUSION

Au fil des années le métier de commissariat aux comptes a évolué et les auditeurs ont dû développer un savoir faire en matière de système d'information. L'intégration de l'informatique dans la démarche du commissariat aux comptes permet de s'assurer de l'intégrité des états financiers générés par le SI. Cela permet aux auditeurs notamment de « *connaître les risques théoriques et d'identifier des risques potentiels, mais aussi de détecter les éventuelles erreurs ou fraudes dans les processus de gestion*[19] ».

Nous avons développé dans le cadre de ce mémoire les contrôles à travers lesquels l'auditeur s'assure de la pérennité du système d'information mis en place par l'entité auditée. Cela demande une constante formation des auditeurs sur une multitude de domaines parmi lesquels le domaine informatique. Cette mutation du métier pose logiquement la question de son futur.

Avec la digitalisation, une grande partie des tâches sont aujourd'hui automatisées ce qui induit d'autres risques qui sont à suivre par les commissaires aux comptes. Le futur de la profession est un sujet souvent évoqué ainsi que la remise en cause des travaux de l'auditeur financier. Ceci est d'autant plus fort ces dernières années avec la mise en place du concept de la blockchain. Cette dernière peut être représentée comme des transactions ajoutées sous forme de « bloc » à la « chaîne » ce qui permet leur traçabilité. « *Les données des transactions sont réputées inviolables et non modifiables*[20] ». Du fait de sa conception, elle assure l'intangibilité, l'inaltérabilité et la transparence des données s'y retrouvant. Selon la définition donnée de la Banque d'Angleterre, la blockchain permet aux personnes qui ne se connaissent pas entre elles et qui sont en interaction, de se faire confiance. Ceci présente une vraie menace pour les tiers de confiance traditionnels qui ont un rôle important aujourd'hui tels que les banquiers, les assureurs ou les notaires. En ce qui concerne les commissaires aux comptes, qui n'échappent pas à la règle, si la blockchain apporte ce niveau d'assurance, cela pourrait rendre superflue son intervention.

A ce jour, le commissariat aux comptes est une profession réglementée. Ceci apporte une certaine assurance pour les tiers et les commissaires aux comptes mais ce qui reste certain est qu'une évolution du métier est en cours. Nous l'avons illustré par l'approche SI qui s'inscrit désormais dans la démarche d'audit. La question qui demeure est de savoir si la blockchain et les tiers de confiance traditionnels sont des véritables concurrents ou, au contraire, ils peuvent être complémentaires.

[19] « L'audit des systèmes d'information, une aide pour le commissaire aux comptes », Roch CAUMON, édition dans Echos.fr du 18 avril 2011

[20] « La Blockchain préoccupe les tiers de confiance traditionnels », Christine Lejoux, Le Tribune le 28/04/2016

Dans le contexte de concurrence féroce entre les cabinets, il va s'agir pour eux de revoir leur stratégie et leur positionnement afin de réagir à cette mutation. Il ne serait pas judicieux d'essayer de lutter contre ce changement car il est inévitable. Cependant, afin de s'adapter au nouveau contexte, le commissaire aux comptes doit repenser les services qu'il propose afin de maintenir la qualité de sa certification. Une stratégie de spécialisation serait une solution. Celle-ci demande un degré d'expertise plus élevé et donc une formation constante sur le domaine de spécialisation. Cependant, il doit rester vigilant au respect de la réglementation et aux services interdits aux commissaires aux comptes.

Comme ce mémoire l'a démontré, des connaissances de plus en plus techniques dans l'informatique sont requises des auditeurs. Le recours aux systèmes d'information augmente le risque d'altération, destruction, usurpation ou vol de l'information engendrant les états financiers qui reste un point important à maîtriser par le management. Le commissaire aux comptes vérifie également si des opérations frauduleuses du SI ont pu être opérées. Par les contrôles du SI mis en place par l'auditeur financier développés dans ce mémoire, nous pouvons affirmer que l'audit SI fait désormais partie de la démarche d'audit des comptes et permet de détecter des erreurs ou de fraudes ainsi que de mieux cibler les risques pour définir un programme de travail répondant à l'approche par les risques.

GLOSSAIRE

ANSSI = l'Agence nationale de la sécurité des systèmes d'information

CAATs = en anglais « *Computer Assisted Audit Tools* » - Techniques de contrôle assistées par ordinateur

CG = contrôleur de gestion

CNCC = Compagnie nationale des commissaires aux comptes

CPME = Confédération générale du patronat des petites et moyennes entreprises

CRCC = Compagnie régionale des commissaires aux comptes

DG = Direction générale/ Directeur général

D&I = en anglais « design & implementation » - conception et implémentation

DSI = Direction des systèmes d'information /Directeur des systèmes d'information

EMS = Editions Management & Société

IFEC = Institut français des experts-comptables et des commissaires aux comptes

IT = en anglais « *information technology* » - système d'infotmation

ITAC = en anglais « *Information Technology Automated Controls* » - Contrôles intégrés aux Applications IT

ITGC = en anglais « *Information Technology General Controls* » - Contrôles généraux informatiques

ISACA = en anglais *Information Systems Audit and Control Association*

LSF = Loi de sécurité financière

NEP = Norme d'exercice professionnelle

NI = Note d'information

OE = en anglais « *Operating Effectiveness* » - efficacité opérationnelle

PME = Petites et moyennes entreprises

RAF = responsable administratif et financier

RGPD = Règlement général sur la protection des données

RIB = Relevé d'identité bancaire

SI = Système d'information

TPE = Très petites entreprises

BIBLIOGRAPHIE

- « **Analyse de données** », Mathieu LAUBIGNAT, ISACA 2007

- « **Audit et contrôle interne** », Benoît Pigé, 3ème édition, édition EMS Management & Société, p. 101

- « **Audit informatique : tous concernés : 10 fiches pratiques pour réussir** », CRCC de Paris, juin 2017, p. 67 – 69

- « **Cryptomonnaie L'utopie à l'épreuve du marché** », Option Finance n°1450, 19 février 2018

- « **Extraction et exploitation des données du système d'information dans le cadre du commissariat aux comptes : méthodologie & outils** », Benoit RIVIERE, 2008

- « **Guide des bonnes pratiques de l'informatique** », Confédération des PME en collaboration avec ANSSI, septembre 2017, p. 1, 3, 7

- « **La Blockchain préoccupe les tiers de confiance traditionnels** », Christine LEJOUX, La Tribune le 28 avril 2016

- « **L'audit des systèmes d'information, une aide pour le commissaire aux comptes** », Extrait Échos du 18 avril 2011, Roch CAUMON

- « **Le commissaire aux comptes et l'approche par les risques** », Note d'information CNCC NI XV - partie sur la NEP 315, point 3.24

- « **Les logiciels d'analyse de données au service de l'audit légal en PME** », François GÉRARD, Institut Français des Experts-comptables et des Commissaires aux comptes, septembre 2015, p. 4, 10, 15, 20, 21 – 41

- « **Prévenir la cybercriminalité** », Stéphane BELLANGER, Economie & Comptabilité n°243, septembre 2013, publication éditée par l'IFEC

- « **Prise en compte de l'environnement informatique et incidence sur la démarche d'audit** », Collection Guide d'application de la CNCC, édition d'avril 2003, p. 14, 42, 79, 100

- « **Protection des données : le texte européen qui hante les nuits des patrons de PME français** », LE MONDE, par Vincent FAGOT, publié le 08 mai 2018

- Blog personnel de Benoit RIVIERE dédié à l'audit et aux systèmes d'information **https://www.auditsi.eu** consulté au mois d'avril – mai 2018 avec une multitude d'articles cités dans les notes de bas de pages du présent mémoire

- La Tribune, publication du 15 mars 2018 n°244, page 5 partie sur le RGPD