

**MEMOIRE EN VUE DE L'OBTENTION DU  
DIPLOME NATIONAL D'EXPERT COMPTABLE**

**REVISION DANS UN ENVIRONNEMENT INFORMATISE :  
PROPOSITION D'UNE NORME D'AUDIT POUR LE  
COMMISSARIAT AUX COMPTES**

**Présenté par Mlle Leïla FALAKI**

**MEMBRES DU JURY**

Président : Mr. Mohamed EL MOUEFFAK – Directeur des études  
à l'ISCAE  
Directeur de recherche : Mr. Abdelaziz EL MECHATT – Expert-Comptable  
DPLE  
Suffragants : Mr. Mohamed ASFARI – Expert-Comptable DPLE  
: Mr. Larbi KZAZ - Enseignant à l'ISCAE

**SOMMAIRE**

**Introduction**

- Intérêt du sujet	2
- Evolution des systèmes d'information	3
- Complexité croissante des travaux et des programmes	5
- Le volume des informations traitées	5
- Propos méthodologiques	6

**Partie 1 : Les spécificités de la démarche d'audit dans un milieu informatisé****Chapitre 1 : Impact de l'informatique sur l'entreprise et l'organisation de la mission d'audit financier**

Section 1 : Les caractéristiques du système comptable dans un milieu informatisé	9
1.1.1 – La structure organisationnelle	9
1.1.2 – Conséquence des évolutions des techniques informatiques	11
1.1.3 - La nature des traitements	13
Section 2 : Les risques liés à la fonction informatique	17
1.2.1 – Les risques généraux	19
1.2.2 – La maîtrise des risques	21
Section 3 : Les conséquences sur la conduite de la mission	26
1.3.1 – Connaissance et compétence	26
1.3.2 – Planification	28

## **Chapitre 2 : Intégration de l'environnement informatique dans le déroulement de la mission**

Section 1 : Prise de connaissance de l'entreprise	35
2.1.1 – Objectif et étendue de la prise de connaissance	36
2.1.2 – Méthode de collecte des informations	38
Section 2 : Appréciation du contrôle interne	40
2.2.1 – Appréciation du contrôle interne de la fonction informatique	41
2.2.2 – Appréciation du contrôle interne des systèmes informatisés	42
Section 3 : Contrôle des comptes	49
2.3.1 – Les techniques d'audit utilisant l'ordinateur	51
2.3.2 – Les travaux effectués directement sur les fichiers de l'entreprise	54
Conclusion de la première partie	56 bis

## **Partie 2 : Normalisation de la démarche d'audit en environnement informatisé**

### **Chapitre 1 – Etude comparée avec les normalisations internationales**

Section 1 : Les normes françaises	57
1.1.1 – Cadre juridique et fiscal	57
1.1.2 – Synthèse des recommandations de l'OECCA et le CNCC	62

Section 2 : Les normes américaines	68
1.2.1 – Cadre juridique	68
1.2.2 – Synthèse des recommandations	71
Section 3 : Les normes IFAC	72
1.3.1 – Cadre juridique	72
1.3.2 – Synthèse des recommandations de l'IFAC	73

## **Chapitre 2 : Ebauche d'un projet de norme**

Section 1 : Analyse critique du champ juridique, comptable et fiscal au Maroc	78
2.1.1 – La réglementation juridique	80
2.1.2 – La réglementation comptable	81
2.1.3 – La réglementation fiscale	84
Section 2 : Les principes de base	86
2.2.1 – Norme de gestion et de sécurité	86
2.2.2 – Information sur les systèmes et l'environnement informatique	87
Section 3 : Etude et évaluation du système comptable et des ses contrôles internes	88
2.3.1 – Les contrôles généraux	88
2.3.2 – Les contrôles d'applications informatisées	88

Section 4 : Les techniques de contrôle assisté par ordinateur	89
2.4.1 – Description des techniques de contrôle assisté par ordinateur	89
2.4.2 – L'utilisation des techniques de contrôle assisté par ordinateur	89
2.4.3 – Les contrôles à mettre en œuvre	91
<u><b>Recommandation</b></u>	<b>92</b>
<u><b>Conclusion</b></u>	<b>98</b>
<u><b>Annexes</b></u>	
<u><b>Bibliographie</b></u>	
<u><b>Lexique</b></u>	

## **AVANT - PROPOS**

Je tiens à remercier :

- Mr Abdelaziz Al Mechatt, mon directeur de recherche, pour les conseils précieux qu'il m'a prodigué pour mon encadrement, et l'aboutissement de cette recherche ;
- Mr Gérard Morin, Associé de PricewaterhouseCoopers, pour son encouragement

Et toutes les personnes qui m'ont assisté de près ou de loin dans l'élaboration de cette recherche.

# INTRODUCTION

*« Il faut que chaque professionnel comprenne que s'il ne consacre pas un temps important à sa formation informatique, il risque simplement de ne plus trouver sa place dans l'économie de demain »*

CNCC

### Intérêt du sujet

Depuis une dizaine d'années, l'utilisation de l'informatique et des ordinateurs s'est considérablement développée dans le domaine de la gestion comptable et financière des entreprises. Ce développement et son accélération ont conduit les auditeurs financiers, que leur mission soit contractuelle ou s'inscrive dans un cadre légal, à s'interroger sur la validité de l'approche et des outils traditionnels de l'audit financier, à adapter progressivement leur démarche et surtout à développer de nouveaux moyens d'investigation.

L'auditeur financier, pour atteindre ses objectifs, ne peut plus, dans bon nombre de situations, se contenter de procédures manuelles de vérification. Ses objectifs d'ailleurs, s'ils demeurent inchangés dans un environnement même informatisé, sont plus difficiles à réaliser du fait :

- des barrières techniques que posent l'informatique, ses langages, ses outils de traitement ;
- du volume plus important des données et des transactions traitées ;
- des budgets d'intervention qui restent sensiblement au même niveau, que l'informatique occupe une place prépondérante ou non dans l'organisation générale de l'entreprise.

L'auditeur financier a de plus en plus intérêt à faire « faire » à l'ordinateur tout ou partie des tests d'audit qu'il réalisait auparavant manuellement. L'emploi de ces techniques permet en outre à l'auditeur financier de mettre en œuvre des procédures de vérification qui lui était quelquefois impossible jusqu'ici de suivre.

Ce mémoire est tout à fait d'actualité car il correspond à l'évolution observée dans la vie des entreprises : la présence toujours accrue de l'informatique dans le système d'information comptable et financière ainsi que les importantes évolutions et mutations que ce système subit au sein de l'entreprise doivent être prise en compte dans la démarche de travail de l'auditeur. En effet, leur incidence sur la qualité et la fiabilité de l'information financière peut être significative. : « pendant de nombreuses années l'informatique était un point accessoire à la mission de l'expert-comptable, mais les problèmes à traiter évoluent et elle tend à devenir de plus en plus importante, ce qui oblige l'expert comptable à « repositionner » son intervention. Le développement du métier d'expert-comptable passe par celui d'auditeur et de consultant en informatique »<sup>1</sup>.

*Cazalet, président de l'OECCA (Revue française de l'audit et du conseil informatique n° 31 – juin 1992).*

### Evolution des systèmes d'information

Pour pouvoir apprécier l'évolution des systèmes d'informations et leurs éventuels impacts en cas de défaillances, il suffit de regarder autour de soi : aujourd'hui, l'informatique joue un rôle stratégique dans les banques, les assurances, les télécommunications, en raison des répercussions pour la société dans lequel une difficulté apparaîtrait, mais aussi pour ses clients si les problèmes rencontrés sont suffisamment importants pour que des données disparaissent.

Les risques induits par les défaillances informatiques sont plus élevés dans ces secteurs que pour d'autres secteurs de l'économie parce qu'ils peuvent également entraîner des conséquences fâcheuses pour les autres sociétés qui sont en relation avec eux, et même, à la limite, avoir des répercussions pour l'économie nationale. Pour les établissements de crédit et télécommunication, l'informatique est un « outil de production » principal et « incontournable ». Si

une entreprise industrielle perd son informatique, il lui restera, en stock, sa production, qu'elle pourra toujours vendre en attendant de rebâtir un nouveau système informatique : celui-ci étant moins intégré au mode de production, une reprise plus ou moins totale de l'activité de l'entreprise pourra intervenir. En revanche la banque, les télécommunications ou les assurances, possèdent la particularité d'avoir l'argent en « input » et en « output ». Si elles perdent leur informatique, comme leur matière première est « l'argent et l'information » - ce qui est immatériel -, elles auront perdu leur outil de production.

Par ailleurs, de tous les progrès qui ont accompagné la profession comptable ces dernières années, l'Echange de Données Informatisé (EDI) est certainement le plus imminent.

L'EDI n'est pas une nouveauté en soi car il allie l'informatique et la télécommunication. Ce qui est nouveau, c'est la façon d'utiliser conjointement ces deux techniques ; aujourd'hui, les ordinateurs parlent aux ordinateurs, ne laissant aux humains que les tâches irrésolues ou qui sortent de l'ordinaire, les « tâches nobles ».

Prenons l'exemple des opérations commerciales entre entreprises. L'ordinateur d'une entreprise demande un prix pour une commande, l'ordinateur du fournisseur le lui communique automatiquement. Le premier lui passe une commande et le second l'enregistre, la confirme et déclenche dans sa propre entreprise soit une mise en production suivie d'une livraison, soit une livraison si une disponibilité existe en stock. L'ordinateur du fournisseur transmet un ordre pour le transport et le processus de livraison est enclenché pour que le client soit livré à la date prévue.

Il ne s'agit pas là d'une vision futuriste. Toutes ces opérations peuvent désormais se passer de papier et, si nous interrogeons les opérateurs commerciaux et les magasiniers des entreprises ainsi organisées, nous constaterons qu'ils répugnent maintenant à utiliser le papier.

Ce nouvel environnement qui est déjà celui de nombreuses sociétés ne peut nous laisser indifférents. Nous devons nous impliquer activement dans ce processus, voire le promouvoir, si nous voulons rester les conseillers privilégiés de nos clients.

S'impliquer, c'est participer activement à toutes les opérations de dématérialisation qui modifient sensiblement l'organisation et le paysage économique de l'auditeur financier.

### Complexité croissante des travaux et des programmes

L'évolution générale des ordinateurs permet aux utilisateurs de bénéficier de moyens informatiques de plus en plus puissants. La « course à la puissance » permet donc aux utilisateurs de demander la programmation d'applications nouvelles.

Progressivement, les solutions informatiques deviennent plus complexes et la simple compréhension des systèmes informatiques par l'auditeur financier plus longue et plus difficile à atteindre.

### Le volume des informations traitées

Des ordinateurs plus puissants peuvent traiter des volumes accrus : il est courant de rencontrer des systèmes informatiques qui traitent des millions d'informations. Les nouveaux matériels ont rendu possible le traitement d'informations élémentaires, auparavant centralisées et totalisées manuellement dans les applications informatiques.

### Propos méthodologiques

Le but de la première partie est de proposer une méthodologie claire, simple et précise permettant à l'auditeur financier d'adopter une démarche d'audit prenant en compte les spécificités liées au traitement automatisé de l'information dans le cadre de ses travaux.

Les composantes essentielles d'une méthodologie sont :

- une démarche
- des techniques
- des outils.

(a) La démarche correspond à l'application en milieu informatisé de la démarche générale. L'apport réside plus précisément dans :

- la prise en compte des évolutions technologiques, de leurs incidences sur les systèmes (matériels et logiciels) et sur les missions des professionnels (par exemple, le développement de la micro-informatique) ;

- l'approfondissement de certains aspects jugés importants et la présentation d'éléments utiles à une approche prospective de l'audit en milieu informatisé.

(b) Les objectifs de l'auditeur ainsi que les méthodes et les techniques à sa disposition sont présentés et explicités d'une façon souhaitée la plus complète et la plus claire possible. Les techniques présentées doivent pouvoir être utilisées par tout auditeur généraliste ne disposant pas de connaissances approfondies en informatique.

(c) La présentation d'une méthodologie resterait théorique sans l'existence d'outils destinés à en faciliter la mise en œuvre. Des supports opérationnels sont proposés pour l'appréciation des éléments de contrôle interne de la fonction informatique et des applications.

En toute logique, l'audit en milieu informatisé ne doit pas être considéré comme un domaine sous-traité de la mission d'audit, mais en faire partie intégrante. Il ne s'agit pas d'un support supplémentaire en sus de la mission principale mais d'une nouvelle orientation de la mission elle-même. Celle-ci doit être dirigée par le responsable d'audit, que l'intervention d'auditeurs spécialisés en informatique soit prévue ou non.

Dans une seconde partie, nous nous intéresserons à une normalisation comptable du commissariat aux comptes dans un environnement informatisé : nous présenterons un projet de normes pour la certification des comptes des sociétés marocaines dans un environnement où l'informatique tient une place prépondérante.

## **PREMIERE PARTIE**

### **LES SPECIFICITES DE LA DEMARCHE D'AUDIT DANS UN MILIEU INFORMATISE**

## **Chapitre 1 : Impact de l'informatique sur l'entreprise et l'organisation de la mission d'audit financier**

### **Section 1 : Les caractéristiques du système comptable dans un milieu informatisé**

Pour mener à bien sa mission de certifications des comptes, l'auditeur financier doit tenir compte de certains paramètres :

- structure organisationnelle ;
- les conséquences des évolutions technologiques ;
- la nature des traitements.

#### **1.1.1 - La structure organisationnelle**

L'application à un environnement informatisé de l'approche traditionnelle, essentiellement conçue et orientée pour l'audit de systèmes manuels, se traduit par nombre de difficultés du fait des changements et des modifications dans l'environnement, notamment au niveau des services où s'organise et s'opère le traitement de l'information.

Ainsi la présence de l'informatique implique :

- la connaissance d'un langage spécifique ;
- une nouvelle répartition des tâches au sein de l'entreprise ;

#### **Le langage spécifique de l'informatique**

L'auditeur financier se doit de comprendre et maîtriser les concepts et le vocabulaire de l'informatique s'il veut étudier et évaluer ensuite les systèmes informatiques chargés du traitement de l'information comptable et financière dans l'entreprise.

L'audit de son côté implique un langage spécialisé, généralement connu de la direction financière et du personnel des services comptables.

Décrire un système informatique dans son architecture, en apprécier la qualité et le degré de fiabilité exige de l'auditeur d'être familiarisé avec beaucoup de termes plus ou moins hermétiques.

De plus en plus d'entreprises ont tendance aujourd'hui à informatiser tout ou partie de leur gestion administrative, financière et comptable, certaines d'entre elles se dotant même de gestion intégré. Les systèmes informatiques qui en résultent sont de plus en plus complexes, ils nécessitent de ce fait un contrôle plus sophistiqué et plus performant.

*L'informatique ou une complète redistribution des tâches au sein de l'entreprise* L'ordinateur, lorsqu'il est opérationnel dans l'entreprise contribue grandement à décharger les différents services, notamment les services administratifs, d'une partie des travaux qu'ils devaient effectuer par le passé et à concentrer, au sein d'un service particulier, le service informatique, un certain nombre de fonctions autrefois réparties.

En outre, si la mise en place d'un outil informatique se matérialise par une nouvelle répartition des fonctions et des travaux, elle a également pour conséquence un transfert des travaux et des responsabilités.

A ce titre, l'informaticien devient responsable de la validité des traitements qu'il conçoit et exploite. Il doit s'assurer que la collecte de l'information n'a pas dénaturé celle-ci, que les résultats qu'il restitue au(x) service(s) utilisateurs(s) sont exhaustifs et justes.

Pour assumer cette responsabilité, il dispose d'outils particuliers et utilise l'ordinateur comme moyen de contrôle privilégié : contrôle de l'information en entrée par des programmes de traitement spécifiques, insertion de contrôles dans les programmes de mise à jour ou d'édition, utilisation tout au long de l'exploitation des possibilités en matière de contrôle et de sécurité offertes par le système d'exploitation de l'ordinateur, etc. Toutefois, comme tout outil technique, un système informatique se traduit pour l'entreprise par une plus

grande performance dans le traitement de son information, mais également un niveau de risque accru.

### **1.1.2 - Conséquence des évolutions des techniques informatiques**

Certaines évolutions dans les possibilités de traitement ou en matière d'organisation et de contrôle des données entraînent des transformations quelquefois profondes sur les contrôles que l'auditeur financier doit normalement effectuer et soulignent par là même les limites de l'approche traditionnelle d'audit. Deux domaines d'évolution peuvent paraître particulièrement significatifs à cet égard, il s'agit :

- du traitement distribué
- de l'organisation des fichiers en base de données.

Le traitement distribué : ce type d'organisation informatique repose sur le principe de centralisation de l'outil de traitement (unité centrale et mémoires auxiliaires) et sur le principe de décentralisation des outils de saisie et de consultation (mise à la disposition des différents utilisateurs de terminaux postes de travail). Un tel environnement informatique a des incidences sur l'organisation même de l'entreprise considérée, dont l'auditeur financier doit impérativement tenir compte :

- la séparation traditionnelle des tâches et des responsabilités s'atténue ou disparaît ; l'utilisateur d'un poste de travail saisit lui-même ses données, il contrôle et corrige ses erreurs, il consulte et/ou met à jour de l'information saisie par un tiers, il peut même déclencher à distance des enchaînements de travaux ;
- les fichiers de données et les programmes se trouvent éventuellement exposés à des accès non autorisés au travers du réseau des terminaux ;

- les documents de base qui permettent de justifier ou de retrouver l'origine des mouvements et des transactions et d'en vérifier la validité sont assez souvent conservés de façon dispersée, quand ils ne sont pas complètement supprimés.
- le contrôle de l'accès aux terminaux et donc à l'information, l'usage des transactions sont généralement surveillés par programme, correspondant à un système de protection par mots de passe .

Avant de se fier à ces contrôles et s'il veut les étudier ou les analyser, l'auditeur financier n'a d'autre choix que de les décrire, les évaluer avec l'aide éventuelle d'un spécialiste et en vérifier le fonctionnement.

#### *L'organisation des fichiers en base de données*

Dans une base ou un ensemble de bases de données, les informations « critiques » sous l'angle du contrôle interne, c'est à dire celles qui régissent l'accès des utilisateurs aux différents postes de travail du système, l'autorisation d'utiliser ou non telle ou telle transaction se trouvent enfermées dans les bibliothèques du système de gestion de la base de données (SGBD). Ainsi, la fiabilité et la validité des résultats que produisent les programmes d'application utilisant la ou les bases de données dépendent en grande partie du bon fonctionnement du SGBD d'une part, de la qualité et de la pertinence des informations de contrôle qu'il gère d'autre part. Le volume des informations à forte incidence comptable ou financière stockées dans une base de données peut être très important, posant de façon aiguë le problème :

- de la prévention des accès non autorisés ;
- du risque d'erreur en cascade ;
- de la difficulté à déterminer l'origine des erreurs ou à circonscrire le champ des anomalies.

Pour s'adapter aux différents changements qui résultent de l'évolution des techniques informatiques, précédemment illustrées par l'étude du traitement distribué et des systèmes gestionnaires de bases de données, l'approche traditionnelle, doit être reconsidérée. Il convient en particulier d'effectuer au préalable une analyse des différents types de contrôles spécifiques de l'environnement informatique considéré et de leurs interrelations.

Plus les entreprises et les organisations sont informatisées, plus elles sont dépendantes du bon fonctionnement de leurs systèmes informatiques.

### **1.1.3 - La nature des traitements**

Les traitements peuvent être effectués en temps réel ou en temps différé. Ce dernier mode de traitement est souvent appelé traitement « batch » ou traitement par lot. Le plus souvent les traitements sont mixtes et font alternativement appel au temps réel et au temps différé, selon les besoins.

#### *Traitement en temps réel*

Le traitement en temps réel est un mode de traitement qui permet l'admission des données à un instant quelconque et l'obtention immédiate des résultats.

Un des avantages de ce mode de traitement est de permettre une validation immédiate des données de saisie par confrontation, pour contrôle et cohérence, avec les informations de fichiers en ligne. Néanmoins, ce traitement présente des inconvénients suivants :

- possibilité de mise à jour des fichiers ou des bases de données sans autorisation en l'absence de procédures appropriées de sécurité ;
- possibilité de dégradation de l'intégrité du système d'information et plus particulièrement des bases de données, si les procédures d'accès, de validation et contrôle a posteriori ne sont pas appropriées ;

- pas de chemin de révision en l'absence de procédures de « journalisation » spécifiques. En temps réel, la mise à jour entraîne, sauf option ou programmation appropriée, la disparition de la donnée périmée par la mise à jour ;
- complexité des procédures de sauvegarde, de restauration et de reprise.

### Traitement par lot

Le traitement par lot est défini comme le traitement suivant lequel les programmes à exécuter ou les données à traiter sont groupés par lot. La caractéristique essentielle des traitements par lots est que la mise à jour des fichiers n'est pas immédiate. Pour mettre à jour un ou des fichiers, il faut procéder successivement à la réalisation des phases de saisie, de validation, de recyclage des anomalies et finalement de mise à jour.

En raison du caractère séquentiel de ce mode de traitement, le chemin de révision est généralement facile à suivre par l'auditeur financier.

### Traitement en temps réel différé

Ce mode de traitement se caractérise par une validation de la saisie en temps réel et une mise à jour différée en traitement par lots.

Lorsque le besoin d'informations immédiates est important pour les utilisateurs, une programmation appropriée permet, lorsque l'utilisateur interroge les fichiers, de recevoir une information à jour même si les fichiers ne sont pas encore réellement mis à jour.

Dans la pratique, le traitement en temps réel différé est très répandu. Il faut également noter qu'il facilite les procédures de sauvegarde, de restauration et de reprise.

La présence d'un environnement informatisé a trois conséquences implicites pour l'auditeur financier :

- disparition du chemin de révision ou son existence pendant une période de temps excessivement courte. Dans certains secteurs d'activité, et plus particulièrement pour les sociétés de service, un seul et même document de base peut, dès sa saisie, déclencher automatiquement la quasi totalité des écritures concernant la comptabilisation de la transaction correspondante.
- disparition de la dématérialisation de certaines procédures d'autorisation et de contrôle, qui sont alors directement réalisées par les programmes. Les plus fréquentes sont les tests de validation effectués lors de la saisie des transactions dans les systèmes interactifs. En matière purement comptable, les programmes exécutent couramment :
  - des tests d'équilibrage du type débit = crédit
  - des vérifications de séquences
  - des tests de vraisemblance en fonction de seuils prédéterminés pour les montants concernant un type d'écriture particulier
  - des tests portant sur les zones obligatoires à renseigner pour qu'une écriture soit acceptée.
- le fait que certaines procédures de contrôle manuelles deviennent elles-même étroitement dépendantes de l'informatique. La revue d'un état d'exception est en effet forcément tributaire de la fiabilité et des contrôles concernant la production même de cet état.

Il est clair que l'utilisation des systèmes informatiques procure à l'entreprise des avantages indéniables notamment, une plus grande fiabilité de l'information :

- les opérations de calculs, de report et de totalisation sont plus fiables que lorsqu'elles sont exécutées manuellement ;

- il est possible d'obtenir des états d'analyse beaucoup plus complexes dans un laps de temps excessivement court ;
- les contrôles programmés inclus dans les applications sont systématiques, alors que pour des considérations de coûts ou de temps, ces mêmes contrôles ne pouvaient être effectués que sur une base de tests dans des environnements manuels.

Tous ces éléments permettent à l'auditeur financier d'alléger les travaux de vérification d'exactitude arithmétique et de procéder de façon plus rapide et exhaustive à des recoupements d'informations. Ils lui permettent donc globalement d'avoir une meilleure assurance sur la qualité de l'information comptable et financière produite par l'entreprise.

L'auditeur financier se trouve ainsi libéré de tâches fastidieuses et répétitives auxquelles il consacrait une part non négligeable de son temps d'intervention. L'économie réalisée peut alors être réaffectée à des travaux d'analyse à plus forte valeur ajoutée qui nécessitent eux, de sa part, de la réflexion et du jugement personnel. Tous ces facteurs positifs lui permettent de mieux gérer le temps global d'intervention dont il dispose.

Le recours à l'outil informatique a certes des avantages indéniables mais il présente toutefois des risques nouveaux.

## **Section 2 : Les risques liés à la fonction informatique**

Le fait de recourir à l'ordinateur dans la gestion de l'entreprise constitue un risque en soi. Nous pouvons stratifié les risques encourus du fait de l'utilisation de l'outil informatique en trois catégories de risques :

- risque économique
- risque physique
- risque logique.

### *Le risque économique*

Le risque économique est celui lié à l'utilisation de l'informatique dans la marche de l'entreprise. Pour certaines d'entre elles, le rôle de l'ordinateur est essentiel et toute anomalie dans son fonctionnement peut avoir des conséquences graves pouvant aller jusqu'à l'interruption partielle ou totale de l'exploitation. A titre d'exemple, les banques, les compagnies d'assurance, les sociétés de vente par correspondance sont très fragiles face à une défaillance de l'outil informatique et cette liste d'activité est loin d'être limitative.

Les entreprises les plus vulnérables au risque informatique sont souvent dans l'obligation de se doter de dispositifs de secours relativement évolués, malgré le coût élevé de ces systèmes.

### *Le risque physique*

Le risque physique est celui de défaillance des ordinateurs et de leurs unités périphériques, comme de l'environnement nécessaire à leur fonctionnement. Depuis les débuts de l'informatique, de gros progrès ont été réalisés en matière de protection contre le risque physique.

Toutefois, les auditeurs financiers ne peuvent « passer à côté » d'un risque majeur sans le signaler. Les risques physiques peuvent avoir un impact sur l'opinion notamment si les risques sont tels qu'ils peuvent porter atteinte à la

pérennité de l'entreprise. Si les risques physiques relevés sont sans incidence directe sur l'opinion, il appartient toutefois aux auditeurs de les signaler et d'émettre les recommandations nécessaires.

### Le risque logique

Le risque logique provient de la mise en œuvre de mauvaises procédures, c'est à dire du déroulement de séquences d'instructions mal adaptées. Il peut s'agir d'une mauvaise programmation, qui tolère l'intervention sur des informations hors du cadre prévu, ou qui permet des traitements non conformes. Il peut s'agir d'erreurs de manipulation, comme le choix d'un mauvais support lors d'opérations de sauvegarde. Enfin, il peut s'agir plus prosaïquement d'erreurs humaines, comme l'oubli d'une ou plusieurs opérations prévues.

Le risque de malveillance, toujours difficile à combattre, demeure présent. Le meilleur moyen de s'en prémunir est de doter l'entreprise d'une bonne organisation appuyée sur des procédures de qualité.

Dès qu'il s'agit d'informatique, les risques logiques sont très nombreux, puisque l'informatique est une technique qui fonctionne pour l'essentiel sur la logique. Les principaux risques logiques classiques sont les suivants :

- contrôle interne insuffisant ;
- paramétrage erroné ;
- contrôle d'accès mal adapté ;
- saisie de données non conformes ;
- erreur de manipulation de supports ;
- erreur de programmation.

La complexité et la sophistication croissante de l'informatique entraînent des risques dans les entreprises et les organisations, risques qui sont à la mesure de l'accroissement d'efficacité et de productivité que l'informatique apporte avec elle.

Ces risques, s'ils sont inhérents à l'évolution de l'informatique, sont également très souvent les conséquences d'une organisation insuffisante et d'une absence de dispositifs, parfois très simples, qui en permettent le suivi et le contrôle.

Dans cette partie, nous identifierons les principaux risques que l'informatique peut faire naître tant dans la fonction informatique elle-même que dans les applications automatisées. Nous avons également pour préoccupation de rechercher quelles sont les procédures et contre-mesures les plus utiles pour pallier et compenser les risques principaux.

### **1.2.1 – Les risques généraux**

L'existence même de l'informatique modifie sensiblement les risques généraux du fait de :

- la puissance et la fragilité qu'elle génère en facilitant la concentration des informations et leur circulation ;
- la technicité et l'évolution permanente des systèmes qui nécessitent une formation approfondie des « informaticiens » à proprement parler, mais aussi et surtout des « utilisateurs » dont elles bousculent souvent les habitudes. Ce dernier point est particulièrement important pour l'auditeur financier, qui, s'ils n'ont pas tous besoin d'être des professionnels de l'informatique, doivent avoir une connaissance suffisante de la technologie pour être à même d'en apprécier les risques, de discuter avec les informaticiens de l'entreprise, d'orienter et utiliser leurs travaux ;
- l'application systématique des opérations programmées qui apporte une sécurité plus grande qu'un système manuel si le programme est fiable,

mais implique que, dans un système mal programmé, toutes les opérations présentent la même anomalie ; le phénomène de cumul des anomalies est donc beaucoup plus important que dans un système manuel où l'intervention humaine compense souvent la faiblesse apparente d'un système ;

- la capacité de certains systèmes à générer des informations sans intervention humaine (systèmes intégrés) créant un risque de voir disparaître ce qui est appelé la « piste d'audit », c'est à dire la trace du flux d'informations de l'origine des opérations à leur traduction dans les livres ;

Outre ces risques généraux, l'informatique implique des risques spécifiques qui tiennent aux éléments suivants :

- phénomènes naturels ou accidentels : ce sont les tempêtes, inondations, incendies... qui, s'ils sont suffisamment prévus au moyen de protections appropriées, peuvent aboutir à une totale paralysie de l'entreprise privée de sa mémoire et de son outil de travail ;
- défaillances techniques : plus les systèmes sont complexes, plus ils peuvent être sujets à des pannes totales ou partielles qui peuvent aboutir aux mêmes conséquences que ci-dessus si des systèmes de maintenance préventive ou de dépannage rapide ne sont pas prévus ;
- manipulations frauduleuses : par sa puissance et sa technicité, l'ordinateur peut faciliter certaines manipulations.

La gestion du risque s'effectue soit a priori, soit a posteriori. Le premier cas est un système bloquant, fondé sur l'interdiction. Le second est un système

informatif où le contrôle s'effectue en examinant la trace des opérations passées.

Pour se forger une opinion sur la valeur des procédures, notamment sur leurs deux qualités essentielles, la pertinence et la permanence, les auditeurs doivent apprécier les conditions de recevabilité du paramétrage.

Après avoir identifié les risques généraux et les risques spécifiques liés à l'utilisation de l'informatique, nous identifierons les moyens qui devraient être mis en place par la société pour pallier ces risques.

### **1.2.2 – La maîtrise des risques**

A la fois facteur de fiabilité et de fragilité, l'informatique implique une conscience claire et précise des risques et une organisation rigoureuse assurant la fiabilité et la sécurité des données qu'elle gère et dont l'entreprise est de plus en plus dépendante. C'est pourquoi l'auditeur financier accordera beaucoup d'importance à la fiabilité de la fonction informatique dans son ensemble. Cette fiabilité passe notamment par :

- une politique informatique claire et coordonnée ;
- une séparation des fonctions ;
- des procédures strictes de développement des systèmes ;
- la protection des accès logiques ;
- le respect des procédures de protection physique ;
- la protection du système d'exploitation.

## 1 – La politique informatique

Le développement des possibilités informatiques a fait de cette fonction une fonction clé de l'entreprise dont la possibilité doit être coordonnée. Il est donc important pour chaque entreprise :

- de créer une véritable fonction informatique rattachée à la direction générale, de façon à intégrer l'informatique dans la réflexion stratégique de l'entreprise ;
- de créer une structure de concertation entre la direction générale, la direction informatique et les utilisateurs, qui soit chargée de déterminer la stratégie de l'information, la configuration du système, les priorités, qui se traduisent par un véritable « plan informatique » ;
- que la fonction informatique définisse l'ensemble des procédures qui assurent la fiabilité de l'ensemble du système.

## 2 – La séparation des fonctions

La séparation des fonctions en matière informatique est particulièrement importante dans la mesure où l'une des caractéristiques de l'informatique est de faciliter les manipulations.

La répartition des rôles en matière informatique doit donc respecter les principes suivants :

- limitation des prérogatives de la fonction informatique, et en particulier pour ce qui concerne l'initiation et la correction des données, l'autorisation des transactions, la conservation des actifs ;
- séparation des fonctions de développement, d'exploitation et de contrôle au sein même de la fonction informatique.

### 3- Les procédures de développement

La maîtrise des coûts et de la fiabilité de systèmes informatiques adaptés aux besoins de l'entreprise passe par le respect des étapes suivantes lors du développement des systèmes :

- étude de faisabilité, c'est à dire étude de l'intérêt du projet par rapport à l'existant, des délais et coûts de réalisation, ...
- étude fonctionnelle, c'est à dire estimation des volumes à traiter, des performances attendues, des compétences nécessaires, de la formation qui devra résulter de sa mise en place, ...
- analyse organique, programmation et tests parallèlement à la mise au point des procédures utilisateurs ;
- réception provisoire et jeux d'essais avec les utilisateurs ;
- réception définitive et mise en exploitation.

Chacune de ces étapes devra faire l'objet d'une documentation détaillée qui seule garantit l'entreprise contre les risques liés à l'impossibilité de faire évoluer son système ou de faire face à une défaillance après le départ du ou des concepteurs.

Les modifications de système doivent respecter les mêmes grands principes.

Il n'est pas rare que les entreprises considèrent ce formalisme comme coûteux et long, mais celles qui ont été confrontées aux coûts et pertes de temps liés au non respect de ces étapes sont généralement convaincues, a posteriori, de leur utilité.

Ces procédures sont beaucoup plus difficiles à mettre en œuvre dans le cadre de systèmes micro-informatiques et l'auditeur financier devra se montrer particulièrement vigilant quant à la fiabilité des systèmes développés sans contrôle par les utilisateurs.

#### 4- La protection des accès logiques

Les différentes ressources logiques de l'entreprise doivent être protégées contre tout accès non autorisé (volontaire ou non). Sans entrer dans les détails techniques, de plus en plus sophistiqués, des moyens de protection dont se dotent les entreprises, les principaux sont les suivants :

- définition précise des autorisations d'accès pour consultation, mise à jour, ajout, destruction, copie, ... ces autorisations devant faire l'objet de mises à jour régulières ;
- mots de passe correctement protégés et régulièrement actualisés ;
- codage éventuel des données les plus sensibles ;
- « journalisation » des accès permettant de connaître les fréquences et sources de sollicitation normales ou anormales, l'origine des tentatives de forçages, ... ;
- contrôle périodique des données contenues, notamment dans les fichiers permanents ;
- rapprochement périodique de fichiers ou utilisation de progiciels d'interrogation permettant de détecter certaines anomalies,...

#### 5- Les protections physiques

Les ressources informatiques représentent un patrimoine important de l'entreprise susceptible de remettre en cause sa pérennité s'il venait à être partiellement ou totalement détruit. Les protections à mettre en œuvre sont nombreuses, mais doivent notamment prévoir :

- la limitation de l'accès aux ressources informatiques (accès aux salles, accès à la documentation, accès aux bibliothèques de programmes et fichiers, ... ) ;
- la protection des salles informatiques contre les risques d'incendie et de dégâts des eaux ;
- une protection contre les défaillances de l'alimentation électrique ;

- une procédure régulière de sauvegarde et de restauration des fichiers et ressources logiques dont le fonctionnement est régulièrement suivi ;
- des règles de stockage (deux endroits différents minimum) rigoureuses ;
- l'existence d'un contrat « de secours » en cas de défaillance du matériel ;
- un entretien préventif régulier du matériel ;
- une assurance.

#### 6- La protection du système d'exploitation

Les procédures d'exploitation du système doivent garantir que :

- les traitements sont exécutés conformément aux instructions et dans les délais ;
- seuls des systèmes ayant fait l'objet d'une réception définitive sont mis en service ;
- les incidents, s'ils se produisent, sont identifiés puis corrigés.

Cette protection passe par :

- une bonne répartition des fonctions ;
- une planification des besoins et des ressources nécessaires ;
- un contrôle du processus de traitement.

Après avoir identifié les risques liés au recours au système informatique des sociétés, nous nous intéresserons aux conséquences sur la conduite de la mission.

### **Section 3 : Les conséquences sur la conduite de la mission**

Deux éléments principaux doivent être pris en compte :

- les compétences requises ;
- l'organisation de la mission (planification).

#### **1.3.1 – Connaissance et compétence**

Pour pouvoir maîtriser les risques cités ci-dessus, l'auditeur financier devrait disposer d'une double qualification : en effet, l'ensemble des applications d'une société constitue en général « un système complexe » ; or ce qui intéresse généralement l'auditeur financier est d'apprécier la fiabilité et la sécurité, qui dépendent de points faibles non nécessairement apparents. Il est donc indispensable que l'auditeur financier ait une formation très technique ; il serait trop facile aux informaticiens qui vivent en permanence avec la machine et dans leurs applications de « berner » celui qui a un niveau inférieur de connaissances, même s'ils n'ont rien de répréhensible à cacher : pour être débarrassé de celui qu'ils considèrent souvent comme un gêneur.

La question la plus délicate à résoudre concerne la partie informatique de la revue préliminaire. L'intervention d'une personne ayant des connaissances informatiques de base est nécessaire. Plusieurs solutions sont envisageables mais le choix fait l'objet d'une réflexion qui dépasse le cadre de la revue préliminaire et concerne l'organisation générale du cabinet du commissaire aux comptes. Les trois principales solutions sont les suivantes :

- (1) création d'un groupe d'auditeurs spécialisés constitués d'informaticiens ;
- (2) création d'un groupe d'auditeurs spécialisés en formant des auditeurs après deux ou trois ans d'expérience ;
- (3) former tous les chefs de mission du cabinet pour qu'ils soient en mesure d'intégrer l'environnement informatique.

	Avantages	Inconvénients
(1)	<ul style="list-style-type: none"> <li>-Technicité et compétence informatique</li> <li>- Apports intéressants pour les clients en dehors de la mission de révision</li> <li>- Formation interne au cabinet</li> </ul>	<ul style="list-style-type: none"> <li>- double intervention tout au long de la mission entraînant des problèmes d'organisation</li> <li>- risques de travaux trop détaillés techniquement et inutiles pour l'audit</li> <li>- absence de connaissance comptables des intervenants</li> <li>- dialogue parfois difficiles avec le chef de mission et synthèse plus longue à établir</li> </ul>
(2)	<ul style="list-style-type: none"> <li>- double connaissance comptable et informatique</li> </ul>	<ul style="list-style-type: none"> <li>- double intervention difficile à organiser</li> <li>- formation nécessaire importante, donc coûteuse et réservée à peu d'auditeur</li> <li>- difficulté pour s'adapter à la diversité des matériels et logiciels informatiques</li> </ul>
(3)	<ul style="list-style-type: none"> <li>- une seule équipe et un seul chef de mission d'où une facilité de synthèse et un gain de temps</li> <li>- travaux informatiques plus souvent limités aux seuls besoins de l'audit financier</li> <li>- formation sur le terrain des autres auditeurs aux notions de base informatique</li> </ul>	<ul style="list-style-type: none"> <li>- problèmes éventuels de dialogue avec les informaticiens de l'entreprise retranchés derrière leur technicité</li> </ul>

Il est clair que c'est la solution (3) qui présente le meilleur compromis entre l'efficacité et le coût.

L'appel à des spécialistes externes : cette solution peut être satisfaisante dans la mesure où des besoins précis ont été définis. Il sera cependant nécessaire d'assurer une supervision effective des travaux de l'informaticien.

Pour mener à bien sa mission et du fait du recours au système d'information, l'auditeur financier doit tenir compte d'autres paramètres lors de sa planification.

### **1.3.2 – Planification**

L'organisation d'un audit en milieu informatisé pose les problèmes suivants :

- approche du système : l'approche du système doit être réalisée simultanément à la prise de connaissance de l'entreprise. Cette approche aura principalement pour objectif d'évaluer, d'une part, l'importance du système et, d'autre part, sa complexité ;
- la compréhension globale de l'intégration et de la complexité du système auront permis de définir la nature et le volume des travaux : répartition entre les travaux d'audit « classiques » et les travaux sur informatique ; définition des zones de risques nécessitant un examen au niveau des procédures et/ou lors du contrôle des comptes.

En fonction de ces éléments, les budgets et les calendriers seront établis. Le planning devra prévoir les contraintes liées au contexte informatique et, en particulier :

- les besoins éventuels en formations complémentaires de l'auditeur et en documentation sur le système de l'entreprise (matériel, logiciels utilitaires, logiciels d'applications...)
- la disponibilité des ressources de l'entreprise lors de l'intervention.

Bien que l'informatique fasse courir aux entreprises certains risques importants, il faut noter qu'elle est devenue en quelques années un élément important de leur patrimoine, qu'il convient à ce titre de protéger et de contrôler à l'aide de procédures de contrôle interne adéquates sous peine de mettre en danger leur continuité d'exploitation.

Compte tenu des évolutions technologiques, l'approche d'audit « autour de l'ordinateur » c'est à dire la démarche qui consiste uniquement à considérer les données à l'entrée et les résultats à la sortie des traitements informatiques sans s'attarder sur l'organisation qui les a produites, devient chaque jour un peu plus difficile à mettre en œuvre même dans les entreprises de taille plus modeste.

L'auditeur financier ne peut pas rester insensible à ces deux constatations et par voie de conséquence, il devra donc de plus en plus se reposer sur l'appréciation qualitative du « contrôle informatique » de l'entreprise pour déterminer l'étendue des travaux nécessaires à la bonne exécution de sa mission de certification.

## **Chapitre 2 : Intégration de l'environnement informatique dans le déroulement de la mission**

L'évolution de l'informatique et sa pénétration dans tous les domaines de l'entreprise est spectaculaire.

En effet, les systèmes informatiques actuels permettent de plus en plus :

- une mise à jour et un partage des données en temps réel,
- une intégration des systèmes d'information financiers et opérationnels (ERP : Entreprise Ressource Planning),
- des échanges économiques interactifs de l'entreprise non seulement avec les clients mais aussi avec les fournisseurs (E-business).

Toutefois, cette évolution a augmenté considérablement la dépendance des entreprises envers leurs systèmes informatiques et a affecté leurs systèmes comptables et de contrôle interne. Nous en citons, essentiellement, la dématérialisation devenue totale (zéro papier) de la transaction et par suite de la preuve (absence de documents d'entrée, absence de système de références visible, absence de documents de sortie visibles).

Face à ce nouveau contexte, les auditeurs financiers ne peuvent plus ignorer le phénomène de l'informatisation des entreprises devenues de plus en plus complexes.

En effet, s'ils ont estimé, au départ, qu'il fallait traiter l'informatique à part, ils sont convaincus, aujourd'hui, que l'informatique devrait être intégrée à leur démarche professionnelle et à chacune de leurs préoccupations.

En effet, bien que n'affectant pas l'objectif global de la mission d'audit financier, le milieu informatisé peut avoir un impact sur :

- les procédures à suivre ainsi que les nouveaux domaines à examiner pour obtenir une compréhension suffisante du système de contrôle interne de l'entreprise ;

- l'analyse des nouveaux risques inhérents et des nouveaux risques de non contrôle rattachés au milieu informatique est nécessaire pour l'appréciation du risque d'audit et de planification des travaux ;
- la conception et la réalisation des tests sur les contrôles et des tests substantifs appropriés pour valider les objectifs d'audit. A ce niveau, il convient d'indiquer la nécessité de plus en plus ressentie quant au développement des techniques de contrôles assistées par ordinateur.

Ainsi la question qui se pose est de savoir comment ces nouveaux aspects informatiques sont pris en compte dans la démarche de l'audit financier.

L'objectif est de présenter la manière avec laquelle s'intègre l'audit informatique dans les différentes étapes de l'audit financier et d'anticiper le développement futur de l'audit informatique en support à l'audit financier.

Le recours à l'informatique est de plus en plus présent dans la gestion des entreprises et les techniques d'audit informatique arrivent à maturité. Avec les techniques d'audit employées jusqu'à ces derniers temps, il était délicat de porter un jugement de valeur sur les résultats issus des systèmes informatisés. L'utilisation de l'informatique augmente de façon considérable la productivité des contrôles, notamment dans les organisations où le volume des opérations traitées est important. Dans ces conditions, l'utilisation de sondages devient rapidement caduque, face à la possibilité de réaliser des traitements de contrôles exhaustifs. L'intérêt de cette méthode est tel qu'il conduit souvent l'entreprise contrôlée à intégrer dans ses traitements courants certains tests réalisés par les auditeurs financiers.

La méthodologie informatique d'audit proposée est l'approche par les risques. Cette technique consiste à rechercher les points forts d'un traitement informatique. Les auditeurs s'appuient sur ces points forts et ont recours à d'autres techniques pour étudier les risques non couverts.

Un point fort réel garantit qu'aucune anomalie ne peut mécaniquement survenir dans un domaine donné. Dès qu'un de ces points forts est pressenti, les auditeurs s'assurent de sa réalité. Si les tests de contrôle de ce point fort s'avèrent concluants, il n'est pas nécessaire de prévoir des diligences étendues. En revanche, l'absence de points forts est caractéristique de la présence de risques non couverts. Le programme de travail prévoit alors les diligences nécessaires destinées à s'assurer qu'aucune anomalie significative n'est intervenue dans les domaines présentant ces risques potentiels.

L'informatique a un triple impact sur l'approche de l'audit financier :

- lors de la phase de prise de connaissance, il doit apprécier la qualité de l'organisation de la fonction informatique et de l'environnement informatique dans son ensemble, desquels dépendent en grande partie la fiabilité des systèmes et la maîtrise des principaux risques spécifiques ;
- lors de son appréciation de la conception et du fonctionnement des systèmes significatifs, il doit prendre en considération les contrôles inclus dans chaque application au même titre que les contrôles manuels ;
- lors du contrôle des comptes, bien maîtrisée, l'informatique peut permettre à l'auditeur financier de mettre en œuvre certaines techniques de contrôle peu envisageables manuellement.

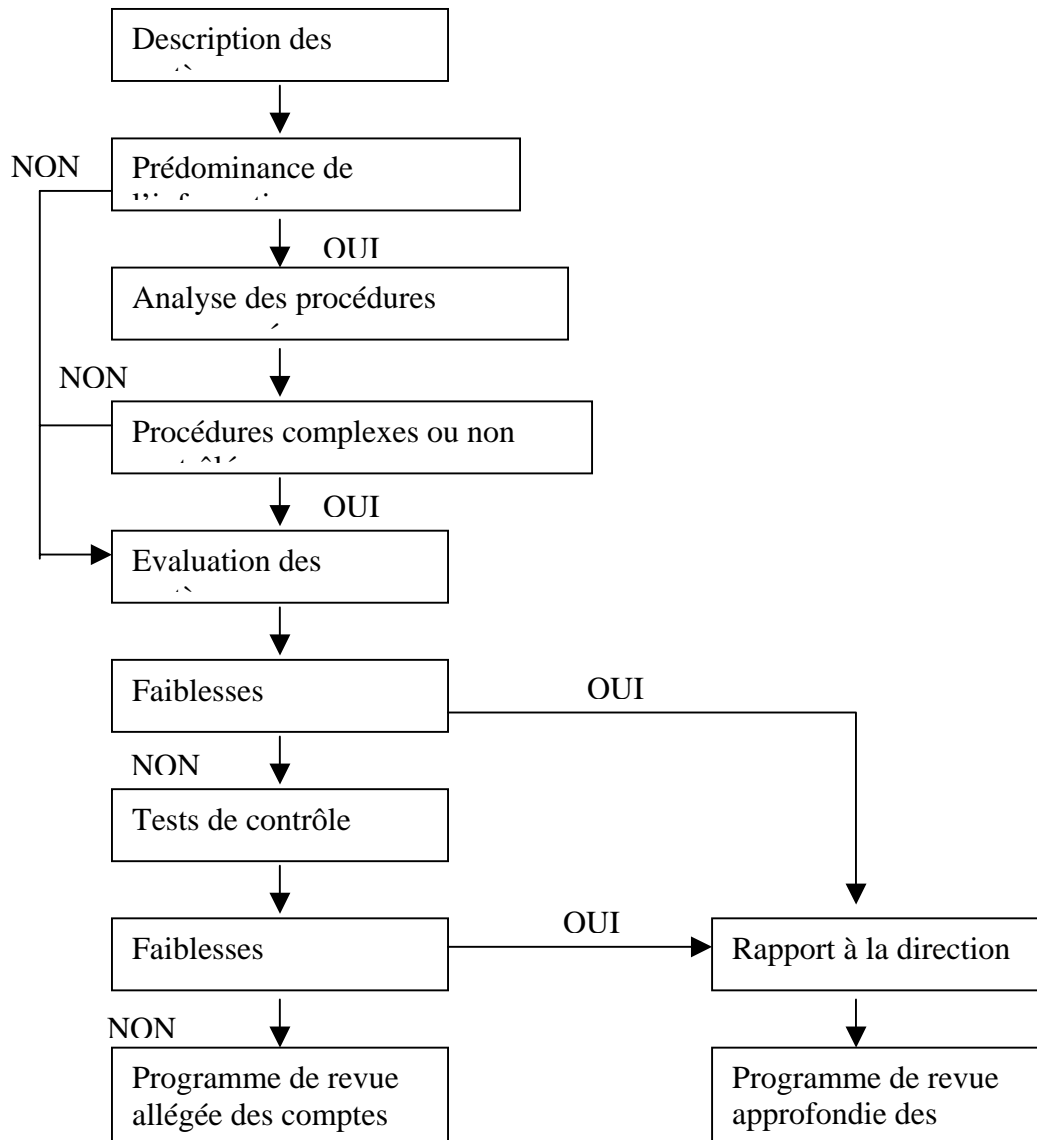
Les objectifs de l'audit financier restent les mêmes en présence d'un milieu informatisé et le cheminement d'audit (revue préliminaire, évaluation de contrôle interne et contrôle des comptes) est toujours applicable globalement. Toutefois, il est nécessaire d'y intégrer des étapes supplémentaires rendues obligatoires par les caractéristiques spécifiques des systèmes informatisés qui sont présentés brièvement ci- dessous :

- la compréhension et la description des procédures concernant les activités automatisées sont rendues plus complexes par l'absence éventuelle de circuit physique de documents ;
- les documents utilisables pour des contrôles manuels par les auditeurs financiers sont très souvent issus d'un traitement informatisé ;
- un grand nombre d'opérations ou de contrôles sont effectués par des « procédures programmées » qui remplacent une partie des contrôles utilisateurs manuels ;

Ces éléments influencent les trois grandes phases de l'approche de révision.

La revue préliminaire : l'importance relative des traitements informatisés ayant une incidence comptable doit être appréciée afin de décider la réalisation d'une première évaluation des contrôles d'intégrité et des applications automatisées. Cette évaluation sera un élément majeur pour la détermination de la stratégie à appliquer et notamment du choix entre une approche système et une vérification approfondie des comptes. Elle sera précédée d'une première prise de connaissance de l'environnement informatique de l'entreprise.

Evaluation du contrôle interne : dans le cas de figure où les conclusions de la revue préliminaire conduisent à envisager une stratégie basée sur la confiance accordée aux procédures de contrôle interne, il est nécessaire de prendre en compte les aspects spécifiques des traitements informatisés.



Ce schéma précise les réflexions supplémentaires induites par un milieu informatisé et qui concernent :

- l'intérêt de décrire et d'évaluer les contrôles d'intégrité en fonction du poids des traitements automatisés et de leur fiabilité attendue ;
- l'importance des contrôles utilisateurs et des procédures programmées ;
- le recours à des logiciels de révision informatiques pour évaluer les contrôles d'intégrité, les procédures programmées et pour tester les procédures de contrôles interne mises en évidence.

Contrôle des comptes : que la démarche adoptée soit allégée par le choix d'une approche système ou bien approfondie, peut être facilitée par l'usage de programmes informatiques qui seront susceptibles de remplacer un certain nombre de pointages manuels fastidieux et difficilement exhaustifs.

### **Section 1 : Prise de connaissance de l'entreprise**

La prise de connaissance a pour objectif de comprendre tous les facteurs pouvant avoir un impact sur les comptes annuels. L'étendue et le degré d'approfondissement de la prise de connaissance aussi bien de l'entreprise que de la fonction informatique doivent être suffisants pour permettre la définition de l'approche d'audit à appliquer aux systèmes informatisés ayant un impact sur les comptes.

La prise de connaissance doit donc porter sur les aspects suivants :

- structure du service informatique et séparation des fonctions à l'intérieur de ce service ;
- matériel utilisé ;
- procédures de conception et tests des systèmes avant leur mise en application ;
- procédures d'exploitation (logiciels, systèmes d'exploitation, contrôles sur le bon déroulement des traitements,...) ;
- procédures de traitement des données (par lot, temps réel, ...) ;
- sécurité du matériel, des programmes, des fichiers, de la documentation, des accès, ... ;
- liste des applications et des sorties informatiques ;

La qualité de l'organisation d'ensemble de la fonction informatique est pour l'entreprise, et par conséquent pour l'auditeur financier, un élément de sécurité qui affecte l'ensemble du processus d'information financière.

Les informations ainsi obtenues permettent à l'auditeur financier :

- d'apprécier si l'organisation d'ensemble de l'informatique de l'entreprise est cohérente et suffisamment fiable pour garantir la fiabilité des traitements dans leur ensemble ;
- de déterminer quelles sont les applications significatives, au regard de sa mission, qui devront être intégrées à son appréciation du contrôle interne et d'appréhender leur complexité ;
- de décider, pour chacune de ces applications, si sa complexité et les outils disponibles permettent un contrôle « autour de l'ordinateur » (c'est à dire à partir des contrôles manuels réalisés par les utilisateurs) ou un contrôle « à travers l'ordinateur ».

### **2.1.1 – Objectif et étendue de la prise de connaissance**

La première difficulté rencontrée par les auditeurs est souvent le choix des personnes avec lesquelles mener les entretiens qui leur permettront d'orienter ensuite la mission d'audit. Il est rare qu'une personne unique ait une connaissance suffisante de l'entreprise pour apporter une première réponse à l'ensemble des questions. Le responsable de l'informatique, ou parfois le responsable administratif et financier, est en général la personne la plus compétente pour que ces premiers entretiens s'avèrent productifs.

En premier lieu, les entretiens vont porter sur le risque économique lié à l'utilisation de l'informatique dans la marche de l'entreprise. Puis les entretiens vont successivement aborder :

- la politique informatique de l'entreprise ;
- la structure informatique ;
- les opérations traitées ;
- l'attitude de la direction face à l'informatique.

Pour apprécier la politique informatique de l'entreprise, il faut connaître son évolution historique, les objectifs poursuivis jusqu'ici en la matière, enfin les objectifs futurs. Les auditeurs se préoccupent de savoir s'il existe un schéma directeur informatique, voire plus simplement un plan informatique à court et moyen terme. En bons professionnels, les auditeurs confortent leur opinion par l'examen des faits qui leur sont rapportés en demandant à connaître les manifestations pratique de la politique décrite. Le lien entre la politique informatique et les risques courus est important, car certaines attitudes sont génératrices de risques substantiels :

- politique aventureuse ;
- course perpétuelle aux dernières techniques ;
- remise en question permanente en faisant table rase du passé ;
- insuffisance de formation du personnel.

Les auditeurs prennent connaissance de la structure informatique de l'entreprise, notamment du rôle des hommes qui la gèrent. Ils dressent l'inventaire des différents systèmes utilisés en se faisant préciser les matériels et les techniques informatiques retenus et les principales mesures prévues en matière de sécurité physique et logique.

Les auditeurs recueillent enfin le degré de satisfaction des utilisateurs souvent révélateur des risques réels.

Toujours au cours des entretiens, les auditeurs prennent connaissance des opérations traitées. Ils se renseignent sur les domaines couverts, le volume des opérations, leur fréquences et leur impact sur la marche de l'entreprise. Ces éléments seront fondamentaux pour établir le programme de travail détaillé.

Enfin, les auditeurs se font préciser l'attitude de la direction générale de l'entreprise et de la direction informatique, afin de mieux apprécier leurs influences respectives dans les différentes décisions.

### **2.1.2 – Méthode de collecte des informations**

Les auditeurs vont demander le schéma général du système d'information de l'entreprise et celui des applications informatiques en service. Néanmoins, en cas d'absence de ce document, il conviendra de l'établir car il est quasiment indispensable pour comprendre le fonctionnement de systèmes informatiques.

Au cours de la revue analytique, les auditeurs recherchent les documents essentiels qui vont les guider dans leur approche. C'est ainsi qu'ils vont demander, ou faire établir les listes suivantes :

- documents et informations qui sont saisis dans le système ;
- transactions proposées aux utilisateurs ;
- principaux fichiers utilisés ;

et toute autre liste dont l'opportunité leur sera apparue au cours des différents entretiens d'approche de la mission. Il est conseillé d'essayer d'obtenir ces différents documents au cours des entretiens. L'intérêt de cette démarche est de pouvoir se faire expliquer immédiatement certains points relevés lors de leur examen.

#### *Revue des systèmes informatiques*

Chaque grand domaine informatisé de l'entreprise fait à son tour l'objet d'une revue rapide. L'objet de cet examen est de connaître le mode de développement des applications principales et leur fonctionnement actuel.

Les auditeurs se font décrire l'application examinée de façon macroscopique, sans entrer dans un trop grand niveau de détail. Ils passent rapidement en revue les points suivants :

- quelles sont les données en entrée ?
- comment ces données sont-elles acheminées ?
- quels sont les traitements essentiels ?
- quels sont les principaux fichiers utilisés en amont ?
- en aval, quelle est l'incidence des traitements sur les fichiers ?
- quels sont les principaux contrôles prévus ?

- comment la correction des anomalies est-elle suivie ?
- dans quelles conditions s'effectuent les déversements en comptabilité ?

Naturellement, ce dernier point est essentiel dans le cadre de la certification de comptes en milieu informatisé et fait l'objet d'un examen un peu plus précis.

Ensuite, les auditeurs se font communiquer ou établissent eux-mêmes un schéma de synthèse de chaque application, afin d'appréhender les grandes lignes de leur fonctionnement. Pour chaque application, ils examinent ensuite plusieurs points bien ciblés :

- les normes et techniques de développement de l'application ;
- les tests de mise en œuvre, notamment de la part des utilisateurs ;
- les conditions de réalisation de la maintenance ;
- les difficultés rencontrées au plan informatique.

Une mauvaise réalisation de ces points ou une insatisfaction des utilisateurs sont une source de risques potentiels. A cette occasion, les auditeurs s'informent des conditions dans lesquelles ils pourront mettre en place les tests destinés à vérifier que les risques non couverts n'ont pas produit d'effet. Pour cela, ils relèvent :

- les matériels successifs éventuellement utilisés,
- la nature des bases de données ou la structure des fichiers,
- l'existence d'outils d'interrogation propres aux systèmes vérifiés,

Par ailleurs, les auditeurs s'inquiètent du délai de conservation des données sur lesquelles porteront les travaux de vérification, notamment le contrôle final sur les comptes de l'exercice. Dans la mesure du possible, ils demanderont à l'entreprise de conserver telle ou telle information dans des conditions de durée adaptées et sur des supports exploitables (balance âgée client, état des stocks, arrêtés à la date de clôture comptable).

## **Section 2 : Appréciation du contrôle interne**

Lors de l'appréciation du contrôle interne des systèmes significatifs, l'auditeur financier doit prendre en considération :

- les fichiers utilisés (qui lui permettront éventuellement de prévoir le recours à des comparaisons de données, des tris informatiques, ...)
- les programmes utilisés ;
- les contrôles des utilisateurs en amont et en aval de l'informatique ;
- les contrôles pré-programmés inclus dans les applications elles-mêmes.

La présence de l'informatique ne modifie pas les principes quant à l'appréciation de la conception et du fonctionnement des contrôles internes utilisés par l'auditeur financier, à l'exception des deux points suivants :

- la complexité de certaines applications peut nécessiter le recours à des techniques de contrôle spécifiques ;
- la fiabilité des fichiers de données permanentes (création, mise à jour, maintenance,...) prend une importance particulière car ces données affectent l'intégralité des transactions.

Exemples : liste des clients, tarifs de vente, fournisseurs référencés

Par contre, lorsqu'il est possible de démontrer la finalité d'un contrôle pré-programmé, et que l'environnement général informatique est satisfaisant, l'auditeur financier peut conclure que toutes les transactions sont vérifiées et s'appuyer sur les listings d'anomalies produites par l'informatique pour s'assurer qu'elles ont été correctement recyclés en fin de période.

### **2.2.1 – Appréciation du contrôle interne de la fonction informatique**

Le plus gros reproche que l'on puisse lui faire, est de ne pas exister à proprement parler. L'informatique est la dernière branche de l'activité industrielle ou commerciale que l'on pense à auditer, et dans laquelle on ose entrer.

D'abord parce que les décideurs ont trop rarement conscience des vulnérabilités introduites dans l'entreprise avec l'ordinateur, sauf dans des systèmes de commande ou de contrôle de type industriel. Il est fréquent que les informaticiens n'aient jamais vu d'auditeur.

Mais il est rare que le propriétaire des informations et le responsable des contrôles soient bien identifiés ; que l'informatique soit vue comme le support des activités (un système nerveux) plutôt qu'un support technique ; que les systèmes soient conçus pour être « auditables ». Alors que l'intégration y est de plus en plus poussée (bases de données, réseaux), et donc que les contrôles sont moins visibles.

Il y a aussi des obstacles psychologiques tenant surtout aux dirigeants : le sentiment que l'informatique est trop technique pour être auditée, ou que l'audit est un coût et non un moyen efficace de réduire les risques. En fait, une fois que l'auditeur a expliqué son rôle et montré sa compétence, vis-à-vis des informaticiens, cet obstacle est généralement surmonté.

Ensuite parce que le niveau technique de l'auditeur est souvent insuffisant devant une tâche très complexe, mal définie, et le temps imparti parfois trop court.

Enfin, parce qu'il y a un manque de normes, de références, de principes et des règles bien acceptés, voire de terminologie. Aussi la qualité de l'audit de la fonction informatique dépend-elle beaucoup des capacités et connaissances personnelles de l'auditeur. Encore maintenant, on peut voir une confusion entre l'audit informatique (où l'objet d'étude est le système d'informations) et

l'audit par l'informatique (où l'ordinateur est un simple outil pour l'étude d'un objet hors système d'information).

Le fossé se creuse entre les techniques matérielles, logicielles et d'exploitation de plus en plus sophistiquées (bases de données, télétraitement et réseaux, temps réel, multi-processeurs) et les techniques de l'auditeur, qui part généralement des documents observables.

Pourtant l'ordinateur est cohérent et beaucoup plus fiable, s'il est bien contrôlé, qu'un système manuel où une défaillance est toujours possible.

### **2.2.2 – Appréciation du contrôle interne des systèmes informatisés**

L'appréciation du contrôle interne des systèmes informatisés pourra se faire selon un questionnaire que nous avons préconisé et qui se présente en deux parties.

#### **1 – Guide de prise de connaissance de la fonction informatique**

Selon la taille de l'installation, les éléments collectés seront plus ou moins détaillés

##### **Service informatique**

- Effectifs
- Organigramme
- Budgets de fonctionnement et d'investissement (2 ans au moins)
- Rapports internes ou externes

##### **Personnel informatique**

- Profil, ancienneté, formation
- Plan de formation
- Evolution récente

## Matériels informatiques (y compris terminaux éloignés)

### Modèle

- Configuration initiale et actuelle
- Date d'installation
- Matériel précédent
- Projets d'extension, modification ou remplacement
- Evolution récente et projets

### Logiciels de base

- Aide à la programmation
- Aide à l'exploitation
- Evolution récente et projets

### Logiciels d'application

Pour chaque application

- nombre de programmes
- date de mise en service
- langage utilisé
- logiciels spécifiques ou standard ?
- évolution et projets d'extension ou de modification

### Procédures écrites

- Liste des documents qui les fixent
- Evolution récente et projets

## 2- Appréciation du contrôle interne d'un système informatisé

### Organisation et structure

Les structures permettent-elles un contrôle efficace sur la fonction informatique ?

Le service informatique est-il séparé des services exerçant des fonctions non compatibles ?

- négociation ou autorisation des opérations
- enregistrement initial des opérations

La division des tâches est-elle assurée dans le service informatique ?

- conception, programmation et exploitation de l'ordinateur
- contrôle des données entrées et sorties
- accès aux fichiers

Les dispositions ont-elles été prises pour fixer par écrit les procédures et responsabilités des personnes remplissant une fonction informatique ? (utilisateurs et informaticiens)

#### Organigramme et définitions des fonctions

- Manuel des procédures administratives
- Règles d'élaboration et mise à jour, de diffusion et de conservation de la documentation informatique
- La direction générale exerce-t-elle un contrôle sur le service informatique ?
- Le service informatique est-il rattaché à la direction générale ?
- La direction, les services émetteurs et utilisateurs, les auditeurs internes participent-ils à la conception, à l'élaboration et à l'évolution des applications ?

#### Etudes et décisions importantes

L'étude préalable et les travaux préparatoires pour l'acquisition et la mise en œuvre d'un ordinateur prévoient-ils les sécurités et les moyens de contrôle indispensables ?

### Programmation

- Les dispositions sont-elles prises pour assurer le développement d'applications et de programmes limités ?
- Les représentants des services utilisateurs, y compris le service comptable, participent-ils à la mise au point des applications et des programmes ?
- La séparation des fonctions incompatibles est-elle respectée ? (fonction de programmation séparée des fonctions d'exploitation)
- Les techniques et procédés de programmation et de conception des applications sont-ils normalisés ?
- Chaque phase principale du développement de tout projet d'application est-elle autorisée et approuvée au préalable ?
  - projet d'application étudié et approuvé par la direction générale et les utilisateurs
  - état d'avancement des travaux revu périodiquement avec le plan et le calendrier
  - approbation avant mise en service de toute nouvelle application
- Les applications et programmes sont-ils testés suffisamment pour s'assurer qu'ils ont la fiabilité requise ?
  - tests conduits par les informaticiens et les utilisateurs
  - tests finals portant sur l'ensemble de l'application, tâches manuelles et informatisées
- Exerce-t-on un contrôle efficace sur la conversion des fichiers et les traitements initiaux ?
- les contrôles effectués sur les traitements initiaux assurent-ils l'obtention de résultats complets et précis, et empêchent-ils des changements non autorisés des fichiers.

Les applications et programmes sont-ils mis à jour dans de bonnes conditions ?

Les modifications de programmes et d'applications sont-elles soumises aux mêmes contrôles que les nouveaux programmes ?

- autorisation préalable par un responsable désigné
- interdiction faite aux opérateurs de modifier les programmes
- contrôle des tests effectués et de l'approbation finale des modifications

Documentation

Existe-t-il une bonne documentation des applications ?

- énoncé clair et précis des problèmes à résoudre
- présentation de chaque application conçue pour résoudre un problème donné
- définition des responsabilités et des fonctions et procédés de contrôle
- Existe-t-il une bonne documentation de tous les programmes ?

Evaluer la qualité de la documentation préparée pour le personnel d'exploitation, de saisie et de contrôle

Exploitation

Evaluer les dispositions prises pour prévenir ou déceler les erreurs accidentelles durant les traitements informatiques

A-t-on mis en place des contrôles pour que les données reçues pour traitement soient complètes, exactes et autorisées ?

A-t-on mis en place des contrôles sur les fichiers d'entrée et de sorties et sur les paramètres de traitement ?

A-t-on mis en place des contrôles pour détecter rapidement les erreurs et pannes des appareils ?

Evaluer les dispositions prises pour prévenir ou déceler les manipulations non autorisées ou frauduleuses

Le service informatique est-il séparé des services émetteurs et des services utilisateurs ?

Evaluer le contrôle sur les différentes fonctions à l'intérieur du service informatique

- séparation entre les fonctions de programmation et d'exploitation
- connaissance limitée des programmes par les opérateurs
- supervision de l'exploitation de l'ordinateur
- accès aux salles d'ordinateur limité au personnel d'exploitation
- bibliothécaire chargé de contrôler la sortie et le stockage des fichiers

Evaluer les dispositions prises pour protéger les enregistrements contre la destruction accidentelle et assurer une exploitation continue

Des méthodes générales visant à prévenir ou déceler les erreurs accidentelles causées par la faute de l'opérateur, par un dérangement des appareils ou par une lacune du programme sont-elles mises en place ?

Des méthodes permettant de reconstituer les fichiers à la suite d'erreurs mineures de traitement sont-elles mises en place ?

Les moyens de protection physique des fichiers sont-ils appropriés ?

La continuité d'exploitation est-elle certaine en cas de destruction majeure des fichiers ou de panne des appareils ?

- fichiers de secours dans un autre bâtiment
- ordinateur de secours compatible et disponible
- documentation des méthodes à suivre en cas d'urgence
- assurances suffisantes

Le traitement comprend –il toutes les informations ?

Toutes les données sont-elles identifiées et enregistrées ?

Le contrôle commence-t-il dès le point d'origine de l'information ?

Toutes les erreurs détectées sont-elles corrigées et tous les rejets recyclés ?

Les données traitées sont-elles exactes et vraisemblables ?

### **Section 3 : Contrôle des comptes**

Le développement actuel des équipements informatiques à tous les stades de l'entreprise entraîne un renouvellement des méthodes traditionnelles d'analyse de la profession comptable. En effet, de plus en plus, le système informatique comptable est alimenté en amont par d'autres sources d'informations automatisées (stock, paie...). Comme pour tout outil technique, ceci se traduit pour l'entreprise par une plus grande performance, mais également par un niveau de risque accru. Il apparaît donc difficile pour un auditeur financier de certifier les comptes sans porter une appréciation sur les systèmes informatiques d'où ils sont issus. En fait, il ne peut plus se contenter de procédures manuelles de vérification, mais doit rechercher une automatisation plus grande de ses outils de contrôle.

Les interrogations de fichiers sont donc un des outils privilégiés de contrôle et d'automatisation des travaux de l'auditeur financier. En effet, les fichiers de données sont au cœur du traitement de l'information. Ils constituent la mémoire de l'entreprise car ils contiennent des informations aussi diverses que l'historique des mouvements de stock, les salaires du personnel ou les budgets prévisionnels.

Les interrogations de fichiers peuvent être utilisées dans les cas suivants :

- lorsque le volume d'information est tellement important qu'il rend superflu et illusoire tout contrôle manuel ; c'est le cas par exemple, des applications bancaires ou financières qui peuvent traiter plusieurs milliers d'informations par jours ;
- lorsque des travaux répétitifs sont réalisés manuellement à chaque intervention sur des données conservées dans des fichiers de l'entreprise. Par exemple, des feuilles maîtresses peuvent être informatisées ;

- lorsque la trace entre les données en entrée et en sortie d'une chaîne ou de plusieurs ne sont pas « rapprochables » aisément. Il en est ainsi d'une absence de rapprochement entre les sorties de stock, les ventes facturées et les ventes comptabilisées sur un mois ;
- lorsque les conclusions que l'on doit porter sur certaines informations nécessitent l'utilisation de techniques de sondages ou lorsqu'il est nécessaire de procéder à une sélection sur la base de critères statistiques d'un certain nombre d'information pour une analyse complémentaire manuelle.

Dans la pratique, l'utilisation des interrogations de fichiers donne à l'auditeur un champ d'investigation très large. Néanmoins, on retrouve des constantes à la fois dans le choix des applications interrogées et dans le type de test réalisé.

On peut donc énumérer les domaines suivants qui sont très souvent interrogés :

#### Les achats

- écarts entre les quantités commandées, livrées et facturées ;
- extraction des factures d'achats les plus importantes pour justification des autorisations d'achat ;
- circularisation automatique des fournisseurs.

#### Les ventes

- contrôle sur les tarifs pratiqués : tarifs « anormalement » haut ou bas ;
- reconstitution des chiffres d'affaires par client sur une période donnée (mois, année) et recoupement avec les données comptabilisées ;
- circularisation automatique des clients ;
- constitution d'une balance âgée.

Les immobilisations

- re-calculation de la dotation aux amortissements, des valeurs nettes d'amortissement, des plus ou moins values, des régularisations de TVA ;
- extraction d'immobilisation ayant des caractéristiques anormales : valeur nette d'amortissement négative.
- contrôle du passage des immobilisations en cours aux immobilisations définitives.

La paie

- contrôle des variations importantes de salaires, de prime ;
- re-calculation de la provision pour congés à payés.

Gestion de la production

- correcte valorisation des stocks ;
- re-calculation de la provision pour dépréciation des stocks.

**2.3.1 – Les techniques d'audit utilisant l'ordinateur**

Outre la prise en compte des risques qui lui sont spécifiques, l'existence d'un système informatique peut mettre en œuvre des techniques spécifiques. La mise en œuvre de telles techniques suppose toutefois :

- un minimum de formation technique, surtout lorsqu'il choisi de travailler sur les programmes et fichiers de l'entreprise ;
- la possibilité d'utiliser des logiciels ou progiciels adaptés aux besoins de l'audit.

### Le jeu d'essai

Cette technique consiste à injecter, dans une chaîne de traitement, des données préparées par l'auditeur financier, destinées à tester l'existence et le fonctionnement des contrôles programmés.

Cette technique est normalement utilisée par l'entreprise elle-même avant la mise en application d'une chaîne.

Pour l'auditeur financier, cette technique doit tenir compte des éléments suivants :

- pour prouver que les contrôles prévus fonctionnent régulièrement, le jeu d'essai devrait tourner périodiquement sur les programmes effectivement utilisés par l'entreprise ;
- si elle est utilisée sur des copies de programmes, l'auditeur financier doit trouver un moyen de s'assurer que ces copies correspondent bien aux programmes qui sont en exploitation.

Exemple : en vérifiant dans le système informatisé « Personnel » l'application « Salaires », l'auditeur financier va reconstituer divers cas normaux ou anormaux pour tester les réactions des programmes : heures affectées à un salarié après son départ de l'entreprise, vingt heures de travail sur la même journée, augmentation brusque du salaire etc...

### Les progiciels d'audit

Il s'agit de progiciels spécialement conçus pour explorer les fichiers qui peuvent tourner, soit sur l'ordinateur de l'entreprise, soit sur un ordinateur indépendant choisi par l'auditeur financier.

Ils nécessitent des adaptations, soit liées aux spécificités de l'ordinateur de l'entreprise, soit pour que les copies de fichiers utilisées soient lisibles.

Ces progiciels peuvent permettre, par exemple :

- de vérifier la fiabilité des utilitaires de calcul, addition, ... de l'entreprise ;
- d'extraire des échantillons, après avoir introduit les paramètres de sélection ;
- de comparer des fichiers pour en extraire des anomalies apparentes.

Ces progiciels peuvent être propres à l'auditeur financier, mais on peut également envisager, si son évaluation de la fonction informatique est suffisante, d'utiliser des logiciels équivalents appartenant à l'entreprise.

Certains de ces progiciels, sont aujourd'hui développés sur micro-ordinateur et permettent, soit de se brancher sur le système central limitant les problèmes de compatibilité, soit, après récupération des données tourner en circuit indépendant.

#### Les outils d'aide à la mission

Comme pour l'ensemble de la mission, le développement de la micro-informatique permet à l'auditeur financier d'utiliser des progiciels qui améliorent la qualité de son dossier. Parmi ces progiciels, figurent notamment :

- les traitements de texte qui permettent la préparation et l'actualisation des programmes de travail ou la réalisation de certaines feuilles de travail adaptées ;
- les tableurs qui permettent également la réalisation de certaines feuilles de travail ;
- les progiciels de tracé de diagrammes ;

### **2.3.2 – Les travaux effectués directement sur les fichiers de l'entreprise**

Si l'essence même des travaux de l'auditeur repose sur une obligation de moyens, il n'en est pas de même au niveau des tests informatisés qui impliquent une obligation de résultat : un programme, même prêt à 99%, n'est pas opérationnel et risque alors de bouleverser toute l'organisation d'une mission basée sur les travaux informatiques.

De nombreuses entreprises fonctionnent avec des bases de données dédiées, la journée, aux travaux transactionnels. Le soir, après une phase de sauvegarde, ces bases de données sont consultées et mises à jour par des travaux par lot. Durant toutes ces périodes, les bases de données ne sont en général pas partageables avec d'autres travaux. Aussi l'auditeur se retrouve-t-il avec des possibilités de travail fractionnées et très réduites.

Cette situation est un frein très important dans le développement de tests informatisés et demande une organisation particulière :

- préparation des travaux d'analyse sur des bases de données de test, qu'il faudra quelquefois constituer de toutes pièces (ces bases n'existant pas en permanence dans l'environnement de tests) ;
- soumission différée des travaux d'audit.

La mise à « plat » de la base est une possibilité souvent évoquée pour pallier ces problèmes, l'auditeur travaillant alors sur un fichier indépendant de l'exploitation. Il faut remarquer que la mise à plat d'une structure à plusieurs dimensions va très souvent « briser » des liens, donnant une image déformée ou incomplète de la base à l'auditeur. Suivant le type d'interrogation requis, il sera alors nécessaire de procéder à plusieurs mises à plat, apportant des contraintes de temps machine et de volume de stockage.

Une autre solution consiste à dupliquer la base de données, la figeant ainsi pour les travaux de l'auditeur. Cette hypothèse, dans la pratique, n'est que rarement réaliste, face aux problèmes organisationnels et aux besoins de capacité (disque complémentaire). En plus de ces problèmes matériels le fait que la base de données est, par sa nature même, un ensemble vivant ; sa photographie instantanée implique alors des contraintes de planning draconiennes.

## Conclusion de la première partie

Tout au long de cette première partie, nous avons relevé que la prédominance de l'outil informatique avait certes des avantages indéniables mais qu'elle présentait, par ailleurs, des risques nouveaux pour la société.

Ce changement de l'environnement organisationnel de la société devrait être pris en compte par le commissaire aux comptes lors du déroulement de sa démarche d'audit.

Cette présence a un impact tout au long de sa mission :

- dès la prise de connaissance de l'environnement de la société (mise en place des équipes adéquates, planification en tenant compte des contraintes informatiques du client) ;
- lors de la phase d'intérim (contrôle interne du système informatique d'une part et des applications d'autre part) ;
- lors de l'audit des comptes .

Il est clair que la démarche d'audit doit être adaptée en conséquence.

Pour répondre à cet objectif, nous préconisons dans une seconde partie, une recommandation d'audit.

Cette recommandation se fera en tenant compte :

- d'une part de ce qui se passe dans les autres pays (France, Etats-Unis) et ce qui est préconisé par les normes internationales d'audit ;
- d'autre part par une étude de l'existant au Maroc, sur le plan juridique, fiscal et comptable.

## **DEUXIEME PARTIE**

# **NORMALISATION DE LA DEMARCHE D'AUDIT EN ENVIRONNEMENT INFORMATISE**

## **Chapitre 1 – Etude comparée avec les normalisations internationales**

L'auditeur financier doit tenir compte, dans son approche d'audit des états financiers, des risques particuliers qu'entraîne l'informatisation des traitements. Les organismes internationaux de tutelle de la profession comptable ont émis des normes en ce sens.

Nous examinerons successivement :

- les normes françaises
- les normes américaines
- les normes préconisées par l'IFAC (International Federation of Accountants)

### **Section 1 : Les normes françaises**

Les normes de révision en milieu informatisé proviennent, en France, de la Compagnie Nationale des Commissaires aux Comptes (CNCC) pour les missions de Commissariat aux Comptes et de l'Ordre des Experts-Comptables et Comptables Agréés (OECCA) pour les missions d'Expertise comptable.

Après avoir rappelé les textes applicables, nous étudierons les recommandations préconisées par ces organismes.

#### **1.1.1 – Cadre juridique et fiscal**

Les textes réglementaires ont été mis à jour par le législateur pour tenir compte des difficultés qu'engendrent la présence des systèmes informatique dans les entreprises.

### Cadre juridique

Les modalités de traitement, de circulation et de stockage de l'information font courir aux sociétés des risques juridiques divers.

La seule parade consiste à connaître les lois, et à les faire respecter dans l'entreprise ; l'esprit et les grandes lignes des principales d'entre elles sont rappelés ci-dessous :

Plan comptable général (arrêté du 27/04/82 modifié par l'arrêté du 9/12/86) prévoit le cas des comptabilités informatisées dans ses « Dispositions générales relatives à l'utilisation des traitements informatisés ». Pour qu'une comptabilité tenue à l'aide de l'informatique soit valable, il est nécessaire que toute opération puisse être suivie, du document d'origine, au total final ou inversement. Pour cela :

- l'organisation du système de traitement doit garantir toutes les possibilités d'un contrôle éventuel ;
- le système de traitement doit établir sur papier, ou éventuellement sur tout support offrant les conditions de garantie et de conservation définies en matière de preuve, des états périodiques numérotés et datés récapitulant dans un ordre chronologique toutes les données qui y sont entrées, sous une forme interdisant toute insertion intercalaire ainsi que toute suppression ou addition ultérieure.

Code de commerce : le décret du 29 novembre 1983 (dispositions prises en application des articles 8 et 17 du code de commerce) contient des dispositions visant les systèmes informatisés. Selon l'article 2, tout commerçant tient obligatoirement :

- un livre-journal ;
- un grand livre ;
- un livre d'inventaire.

La conservation des livres obligatoires fait l'objet de l'article 1, qui précise les conditions de délai et de forme. Les documents comptables doivent être conservés pendant dix ans, sous la forme suivante :

- les livres obligatoires doivent être conservés sous la forme originale, ce qui exclut la possibilité de les archiver sur microfilms ou sur bandes magnétiques.
- les autres documents comptables, comme les journaux auxiliaires centralisés une fois par mois sur le livre journal, peuvent être conservés autrement que sous leur forme originale, comme les pièces justificatives, c'est à dire sous forme de photocopies, microfilms, supports magnétiques.

Informatique et libertés (loi du 6 janvier 1978) : son objectif est d'éviter que l'informatique « ...ne puisse porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». Pour ce faire, elle crée les obligations suivantes :

- informer les personnes (physiques) fichées lors de la collecte des informations leur donner un droit d'accès et de rectification ;
- déclarer, préalablement à la mise en place des applications, les traitements à la Commission Nationale Informatique et Libertés (CNIL) ;
- assurer la confidentialité des informations nominatives.

Auxquelles s'ajoutent quelques interdits :

- collecter des informations sur la race, la religion, l'appartenance politique ;
- divulguer les informations sur les personnes ;
- détourner les traitements de leur finalité déclarée.

Protections des logiciels (loi du 3 juillet 1985) : son objectif est d'étendre aux logiciels le régime de protection du droit d'auteur (loi du 11 mars 1957), basé sur les principes suivants :

- sauf s'il est salarié d'une entreprise qui l'emploie à cette fin, l'auteur d'un logiciel en conserve la propriété intellectuelle ;
- l'utilisateur « n'achète » pas le logiciel, mais seulement un droit d'utilisation. Ce droit doit être défini dans un cadre contractuel ;
- la loi interdit toute modification ou duplication du logiciel, sans accord préalable de son propriétaire.

Fraude informatique (loi du 5 janvier 1988) : elle interdit :

- l'accès ou le maintien non autorisé dans tout ou partie d'un Système d'Information ;
- d'entraver ou de fausser le fonctionnement d'un Système d'Information ;
- d'introduire ou de modifier des données ou leur code de traitement ou de transmission ;
- de falsifier des documents informatisés ;
- de faire usage de documents informatisés falsifiés.

Protection des télécommunications (loi du 10 juillet 1991) : son objectif est de préserver le « secret des correspondances émises par la voie des télécommunications » ; elle ne comprend pas que les écoutes téléphoniques, mais aussi les transmissions de données.

Elle interdit :

- d'installer des appareils d'interception
- d'intercepter, de détourner, d'utiliser, de divulguer des informations transmises par télécommunication.

### Cadre fiscal

L'article 54 du Code Général des Impôts précise :

« Si la comptabilité est établie au moyen de systèmes informatisés, le contrôle s'étend à la documentation relative aux analyses, à la programmation et à l'exécution des traitements. Afin de s'assurer de la fiabilité des procédures de traitement automatisé de la comptabilité, les agents des impôts peuvent procéder à des tests de contrôle sur le matériel utilisé par l'entreprise dont les conditions seront définies par décret ».

En outre, la loi de finances pour 1990 a apporté des précisions complémentaires (article 103). Les principales sont résumées ci-dessous :

- les informations, données, traitements, documents informatiques doivent être conservés pendant 3 ans (délai de reprise)
- trois modalités techniques peuvent être retenues pour le contrôle :
  - l'entreprise met son propre matériel à la disposition des agents de l'administration ;
  - l'entreprise préfère effectuer elle-même les traitements. Dans ce cas, l'administration précise par écrit les travaux à réaliser ;
  - l'entreprise ne s'estime pas en mesure d'effectuer les travaux. Elle peut alors remettre une copie de ses fichiers. Dans ce cas, ces copies lui seront restituées après contrôle.

En cas d'opposition à la mise en œuvre du contrôle, le contribuable encourt la sanction « d'évaluation d'office pour opposition à contrôle ».

Ces dispositions entraînent une double obligation pour l'entreprise :

- obligation de documentation des systèmes comptables ;
- obligation de mettre l'administration en mesure d'effectuer des tests sur le fonctionnement des systèmes.

Le risque fiscal est double :

- risque de rejet de la comptabilité pour irrégularité.
- risque d'évaluation d'office pour opposition à contrôle.

### **1.1.2 – Synthèse des recommandations**

#### **Recommandations de l'OECCA**

Le développement des techniques informatiques de gestion des entreprises a obligé l'ordre des experts comptables à édicter un certain nombre de recommandation concernant la révision en milieu informatisé. Selon l'OECCA : « la révision a pour objet ...l'image fidèle du patrimoine, de la situation financière et des résultats ».

On comprend dès lors que la mission de l'expert comptable ne peut être parfaite si son travail de contrôle et de validation des comptes ne prend pas en compte le phénomène informatique sur deux plans :

- appréciation de la qualité et de la sécurité des techniques informatiques mises en œuvre par les entreprises ;
- utilisation du matériel informatique en vue de réaliser des contrôles plus approfondis, voire exhaustifs, que ceux réalisés manuellement.

Afin d'orienter les travaux des experts comptables, l'OECCA a donc émis les trois recommandations suivantes sur la révision en milieu informatisé :

22.07.1 : principes généraux de révision en milieu informatisé ;

22.07.2 : incidence du milieu informatique sur l'étude et l'évaluation du système de contrôle interne ;

22.07.3 : techniques de contrôle assisté par ordinateur.

La norme 22.07.1 a pour but de montrer comment prendre en compte l'informatique dans une mission de révision comptable, elle rappelle que l'objectif de la révision, à savoir l'expression d'une opinion motivée sur les comptes annuels d'une entreprise, reste inchangée quels que soient les moyens utilisés pour la production de l'information comptable et financière.

Elle fait obligation au réviseur d'adapter son plan d'intervention pour tenir compte des particularités propres à un environnement informatisé. Elle précise à ce titre qu'il doit vérifier que les applications informatiques répondent bien aux exigences de contrôle interne en ce qui concerne la sécurité et la fiabilité des traitements, ainsi qu'en matière de conservation de la totalité des données entrées.

Cette recommandation autorise par ailleurs l'expert comptable à utiliser directement l'ordinateur comme outil pour procéder à ses travaux de révision. Enfin, elle souligne que la révision en milieu informatisé nécessite de la part du réviseur des connaissances en informatique suffisantes et que, même dans le cas où il ferait appel à des experts extérieurs, il conserve en tout état de cause l'entière responsabilité de la bonne exécution de sa mission.

La norme 22.07.2 décrit de manière plus détaillée la démarche de révision du contrôle interne en milieu informatisé : contrôle sur les entrées, les sorties, les traitements, les fichiers, les sauvegardes, l'organisation et la documentation. La recommandation insiste sur le fait que l'expert comptable doit faire porter ses contrôles sur les applications qui ont une incidence sur les états financiers et que, dans ce but, il peut avoir recours à l'ordinateur.

Les contrôles généraux sont regroupés autour de quatre pôles :

- contrôle ayant trait à l'organisation du département informatique pour laquelle le réviseur doit vérifier avant tout que le principe de séparation des fonctions est correctement assuré ;
- les contrôles se rapportant à la sécurité, à la sauvegarde et à la reprise des travaux, pour lesquels il est fait référence en particulier aux

procédures de protection physique et logique et à l'existence d'un plan de secours ;

- les contrôles concernant les traitements, pour lesquels il est fait mention des restrictions d'accès aux programmes en exploitation, à la qualité des contrôles programmés des applications et au respect des principes d'autorisation, d'exactitude et d'intégralité du traitement des données ;
- enfin, les contrôles relatifs aux méthodes de développement et de maintenance des applications et à la qualité des procédures de documentation et de mise en exploitation.

Pour les contrôles d'application, il est opéré une distinction entre les contrôles portant :

- sur les données d'entrée ;
- sur les traitements ;
- sur les sorties et les résultats.

Selon la norme 22.07.3 : « l'utilisation de techniques de contrôle assisté par ordinateur devient indispensable lorsque l'expert comptable se trouve en situation de perte du chemin de révision et n'a pas la preuve de la réalité des contrôles effectués au cours de traitements. Il doit, en outre, s'assurer que ces contrôles ont effectivement fonctionné pendant toute la période révisée ».

Pour réaliser ces contrôles par ordinateur, la norme propose les moyens suivants :

- programme utilitaires (Query) : ceux-ci ne permettent pas la réalisation de programmes complexes, mais simplement des tris, extraction, ou interrogations simples ;
- les logiciels spécifiques : programmes d'interrogations développés spécifiquement pour le client ;
- les progiciels d'aide à la révision : programmes d'interrogations souples et adaptables à des clients différents et comportant de

nombreuses fonctionnalités d'audit (tris, tests de doublons ou de trous de séquence, ...);

- les jeux d'essai : introduction de données dans le système informatique de l'entreprise en vue de comparer les résultats obtenus et les résultats attendus ;
- l'utilisation de la micro-informatique : le micro-ordinateur peut être utilisé soit pour gérer la mission, soit « pour traiter des données provenant des fichiers de l'entreprise contrôlée ». Les traitements peuvent consister en l'utilisation de programmes utilitaires (tableurs, gestionnaires de fichiers), logiciels spécifiques (programmation directe) progiciels d'aide à la révision.

### Recommandations de la CNCC

Vers la fin de l'année 1987, la CNCC a publié un ouvrage reprenant l'ensemble des règles et obligations professionnelles appelées « normes » qui s'imposent au commissaire aux comptes dans le cadre des missions qui lui sont fixées par la loi. Ces normes sont accompagnées de commentaires qui, bien que n'ayant pas de caractère obligatoire, apportent certaines précisions et explications complémentaires pour leur mise en œuvre pratique.

Nous nous proposons d'étudier les normes et commentaires qui se rapportent à la mission générale de certification des comptes annuels pour y relever les principales références aux travaux à effectuer sur les systèmes informatisés d'une entreprise.

#### *Orientation et planification de la mission :*

Cette première étape a comme objectif, à partir d'une prise de connaissance globale de l'entreprise et d'une identification des risques généraux, la rédaction d'un programme général de travail.

Comme il en est fait mention dans les commentaires, il est évident que le commissaire aux comptes devra collecter toutes les informations qu'il estime

nécessaires à sa bonne compréhension du système de traitement de l'information financière et comptable.

Implicitement nous pouvons considérer qu'il devra dans le cas où ce système est informatisé, apprécier dans quelle mesure la société est dépendante de son informatique pour l'établissement de ses comptes, et quel est le degré de confiance préalable qu'il accepte de placer dans les traitements informatisés.

Un paragraphe spécifique des commentaires de cette première norme est consacré aux risques généraux résultant de l'insuffisance ou de l'absence de sensibilisation de la direction de l'entreprise pour les questions financières, comptables et administratives.

Enfin, en ce qui concerne l'identification des systèmes comptables significatifs, il est clairement indiqué dans les commentaires que le commissaire aux comptes devra déterminer s'il lui paraît souhaitable de faire appel à un spécialiste, dans le cas où les traitements sont informatisés, pour procéder à la revue spécifique de certaines applications.

#### Appréciation du contrôle interne

Dans cette seconde étape, le commissaire aux comptes procède à une revue et à une évaluation qualitative des procédures de traitement et de contrôle interne de l'entreprise pour établir un programme de révision des comptes annuels approprié.

Les commentaires de cette norme accordent une large place à la revue des systèmes de traitement informatisés de l'information puisqu'un paragraphe spécifique lui est entièrement consacré.

L'interprétation de ce paragraphe permet d'aboutir aux constatations suivantes :

- il est possible de considérer que, comme dans les recommandations de l'OECCA, il existe deux niveaux de revue distincts bien que ce terme ne soit pas employé dans le commentaire :

- un niveau général qui est celui de la « fonction informatique » définie comme l'ensemble composé par le service informatique mais étendu aux utilisateurs dans leurs relations avec ce service ;
  - un niveau plus détaillé qui est celui d'un système ou d'une application particulière.
- l'objectif de sécurité et de continuité des travaux est clairement rappelé dans le commentaire en même temps que ceux de la fiabilité des informations produites et de protection du patrimoine.

Les procédures de contrôles à étudier au niveau des applications font, elles explicitement référence :

- à la préparation et à la saisie des données, aussi bien au niveau des utilisateurs qu'à celui du service informatique ;
- à l'exploitation, avec mention à la fois des termes d'erreurs et de fraudes ;
- à la qualité de la documentation ;
- aux modifications de programmes ;
- au maintien du chemin de révision.

## **Section 2 : Les normes américaines**

### **1.2.1 – Cadre juridique**

Trois organismes contribuent à la réglementation financière aux Etats-Unis et à fixer les modalités d'établissement et de publication des documents financiers :

- la SEC (Securities and Exchange Commission)
- l'AICPA (American Institute of Chartered Public Accountants)
- le FASB (Financial Accounting Standard Board)

#### **La SEC**

Les sociétés qui veulent être cotées sur les grandes bourses américaines doivent être inscrites auprès de la SEC qui est l'équivalent du CDVM (Conseil Déontologique des Valeurs Mobilières) au Maroc. Le rôle de la SEC est de réglementer la mise sur le marché et la négociation des titres. Elle est dirigée par un conseil de cinq membres nommés par le Président des Etats-Unis pour une période de cinq années et exerce ses pouvoirs sur les méthodes de présentation des documents financiers et les règles d'audit des sociétés inscrites auprès d'elle. Bien qu'elle ait le pouvoir légal d'établir des normes comptables, la SEC a délégué ses pouvoirs au secteur privé dès 1939 à l'AICPA dans la promulgation et la mise en application des normes comptables.

#### **AICPA**

L'AICPA est l'équivalent américain de l'ordre des Experts Comptables.

De 1939 à 1959, un Comité des Procédures Comptables (Committee Accounting Procedures-CAP) créé par l'AICPA a publié 51 Accounting

Research Bulletins (ARB) qui portent davantage sur des problèmes techniques spécifiques que sur des principes généraux ou théoriques.

En 1959, le CAP été remplacé par l'Accounting Principles Board (APB) qui est aussi une émanation de l'AICPA mais avec une représentation plus large : les membres de l'APB provenaient non seulement de la profession comptable mais aussi de l'industrie, de la communauté financière, des universités et du gouvernement. L'APB publia 31 opinions et quatre statements. Les premières constituent de véritables normes ayant force obligatoire, alors que les secondes ne sont que des recommandations.

### Le FASB

Créé en 1973, le FASB est un organisme privé chargé de l'élaboration des principes comptables généralement admis connus sous l'appellation de l'US GAAP (Generally Accepted Accounting Principles). Le FASB succède à l'Accounting Principles Board (1959-1973).

Le pouvoir de réglementation appartient légalement à la SEC. Elle élabore parfois une norme sous la forme d'un Accounting Series Release (bulletin dans la série comptabilité). Toutefois, ses interventions sont rares, la SEC déléguant généralement au FASB le pouvoir de définir les principes comptables généralement admis. Le FASB est aujourd'hui l'organisme de normalisation comptable aux Etats-Unis ; il a émis plus de 100 normes et a créé un cadre conceptuel.

Le FASB comprend sept personnes salariées à plein temps nommées pour cinq ans renouvelables. Ce sont en général d'anciens associés de cabinet ou de directeurs comptables de grandes sociétés. Ils disposent d'une équipe technique d'une centaine de personnes qui travaillent sur les normes. Le FASB est financé par de multiples organisations dont aucune ne contribue au budget dans des proportions élevées de manière à préserver une indépendance financière et garantir son autonomie. Le FASB dispose aussi de comités de contact qui facilitent le dialogue avec le monde économique sur les questions de politique et de stratégie.

Les activités du FASB sont surveillées par la Financial Accounting Fondation(FAF) dont les administrateurs mandataires proviennent de plusieurs organisations.

Le FASB émet deux catégories de textes :

- les Statements of Financial Accounting Concepts(SFAC) qui énoncent les concepts fondamentaux sur lesquels reposent les normes d'établissement et de présentation des comptes. L'élaboration des SFAC a été réalisée dans le cadre de la conception du cadre conceptuel(conceptual framework) qui constitue le cadre théorique de la comptabilité.
  
- les Statements of Financial Accounting Standards(SFAS) qui définissent les principes et règles comptables applicables à la préparation et à la présentation des comptes, et qui sont considérés comme des GAAP.

Il est à souligner que les ARB, Opinions du CAP et de l'APB restent toujours en vigueur et constituent des GAAP jusqu'à ce qu'ils soient amendés ou remplacés par le FASB.

A ce jour plus de cent vingt SFAS ont été publiés dont un tiers sont des amendements ou des compléments à des normes antérieures.

### **1.2.2 – Synthèse des recommandations**

Il est intéressant de constater qu'il n'y a pas de différence sensible au niveau des textes sur l'approche et la nature des travaux qui doivent être réalisés dans le cadre d'une mission de révision ou de certification par les professionnels comptables.

Dès 1977, l'American Institute of Certified Public Accountants AICPA avait publié un Statement on Auditing Standards SAS 3 consacré aux effets de l'informatique sur l'étude et l'évaluation par l'auditeur du contrôle interne. Ce SAS a été remplacé en 1984 par le SAS 48 qui traite des effets des traitements informatisés sur l'examen des états financiers. Ce « statements » reprend pour les intégrer dans les autres « statements », les mêmes obligations que celles qui s'imposent à un auditeur financier français :

- il est indiqué que lors de la phase de planification de son intervention, l'auditeur doit prêter attention à :
  - l'étendue de l'utilisation de l'informatique pour chaque application comptable significative ;
  - à la complexité des travaux informatisés, y compris ceux pouvant être effectués par un centre de traitement extérieur ;
  - à l'organisation générale des activités informatiques ;
  - à la disponibilité des données ;
  - à l'utilisation possibles de techniques de contrôles assistées par ordinateur.
  
- il est également précisé qu'il peut utiliser les compétences d'un spécialiste extérieur, mais que la responsabilité qu'il a vis-à-vis des travaux de ce dernier est la même que pour ceux effectués par ses propres collaborateurs.

En ce qui concerne l'étude et l'évaluation du contrôle interne, le « statement » rappelle tout d'abord quelles sont les caractéristiques propres à l'informatique qui sont susceptibles d'avoir un effet sur le système de contrôle interne comptable de l'entreprise, puis précise que l'objectif d'un système de contrôle interne comptable reste inchangé en cas de traitement informatisé : donner une assurance raisonnable, que les actifs sont correctement protégés contre un usage non autorisé, et que les enregistrements comptables sont suffisamment fiables pour permettre la préparation d'états financiers.

Le « statement » rappelle également l'importance de la séparation des tâches dans un environnement informatisé et indique qu'il semble plus efficace de procéder à une revue des contrôles informatiques généraux avant une revue des contrôles d'applications. Il décrit ensuite la nature des tests qu'il est envisageable d'effectuer dans un environnement informatisé par recoupements et utilisation de techniques d'audit assistées par ordinateur.

En ce qui concerne la séparation des tâches incompatibles, le « statement » précise que celle-ci doit s'apprécier non seulement au niveau du département informatique, mais aussi entre ce département et les services utilisateurs chargés des autres travaux de contrôle, et qu'il doit exister par ailleurs, des procédures de restrictions d'accès aux programmes et aux données.

### **Section 3 : Les normes IFAC (International Federation of Accountants)**

#### **1.3.1 – Cadre juridique**

**L'IFAC est une organisation privée à but non lucratif et non politique. Elle a pour objet le développement et le renforcement de la profession comptable pour l'aider à fournir des prestations de haute qualité pour le bienfait du public.**

L'IFAC, créée en 1977, complète le rôle de l'IASC (International Accounting Standards Committee) en prenant en charge l'audit, la formation, la

déontologie, la comptabilité de gestion, le secteur public et les techniques de l'information.

L'IAPC (International Auditing Practice Committee) a pour objet d'uniformiser les pratiques d'audit financier et les missions s'y rattachant. L'IAPC publie « des normes internationales d'audit » (ISA pour International Standards on Auditing).

Depuis 1984, les membres de l'IFAC sont également membres de l'IASC et réciproquement.

Les membres de l'IFAC sont des instituts professionnels, non des Etats, et certains Etats comptent plusieurs instituts professionnels. La France, par exemple, comprend deux instituts professionnels membres de l'IFAC (la CNCC et l'Ordre des Experts Comptable et des Comptables Agréés).

### **1.3.2 – Synthèse des recommandations de l'IFAC**

L'IAPC a élaboré la norme 401 et les directives suivantes :

- 401 relative à l'audit dans le contexte d'un système d'informatisé ;
- 1001 relative à un système d'information fondé sur un micro-ordinateur autonome ;
- 1002 relative à un système d'information interconnecté ;
- 1003 relative à un système à base de données ;
- 1009 relative à l'utilisation des techniques d'audit fondées sur l'informatique.

#### **Norme 401**

Cette norme relative à l'audit dans le contexte d'un système d'information informatisé pose comme principe de base que :

- la manière dont une entité utilise les technologies d'information aura normalement un impact sur l'approche d'audit ;
- l'auditeur doit posséder la compétence et le savoir-faire nécessaire pour comprendre l'impact de l'informatique sur l'audit ;
- l'auditeur doit apprécier si l'équipe d'audit possède les compétences en informatique nécessaires pour effectuer l'audit ou si l'assistance d'un spécialiste informaticien est requise ;
- l'auditeur doit apprécier le risque inhérent et le risque lié au contrôle relatif à l'informatique ;
- l'auditeur doit concevoir et mettre en œuvre des procédures d'audit destinées à diminuer le risque d'audit résultant de l'utilisation de l'informatique à un niveau faible acceptable.

#### Directive 1001

Cette directive relative à un système d'information fondé sur un micro-ordinateur autonome énumère les facteurs qui conduisent à ce qu'en général le risque lié au contrôle est plus élevé ; dans cette situation l'auditeur peut estimer plus approprié d'accroître les contrôles substantifs, la taille des échantillons et les contrôles physiques, et d'utiliser de façon plus large les techniques d'audit assistées par ordinateur.

#### Directive 1002

Cette directive relative à un système d'information fonctionnant en réseau et/ou en temps réel comporte :

- une description des caractéristiques de ces systèmes ;
- une énumération des contrôles que peuvent comporter ces systèmes ;
- une analyse de l'impact de ce type de système sur les fonctions comptables et sur les contrôles internes comptables ;
- une appréciation de l'impact de ce type de système sur les procédures d'audit.

Dans le cas d'un système bien conçu comportant les contrôles nécessaires, il est probable que l'auditeur effectue des tests de contrôles et, si ces tests se révèlent satisfaisants, qu'il s'appuie de façon plus importante sur le contrôle interne pour déterminer la nature et l'étendue des procédures d'audit.

### Directive 1003

Cette directive relative à un système de base de données comporte :

- une description des caractéristiques de ces systèmes : principalement l'existence de deux composants – la base de données et le système de gestion de la base de données, l'indépendance des données par rapport aux programmes applicatifs, le dictionnaire de base de données et l'administration de la base de données ;
- une description des contrôles dans un environnement à base de données ; l'importance des contrôles généraux relatifs à :
  - la démarche générale concernant le développement et la maintenance des programmes applicatifs ;
  - les responsabilités pour l'intégrité et l'exactitude des données ;
  - l'accès à la base de données ;
  - la séparation des fonctions.
- une analyse de l'impact des bases de données sur le système comptable et sur le contrôle interne ;
- une appréciation de l'impact des bases de données sur les procédures d'audit : les caractéristiques du système de gestion de base de données seront déterminantes. Il peut être plus efficace pour l'auditeur de réaliser une revue avant la mise en place du système de base de données qu'après. Il lui sera alors possible de demander des modifications et/ou de développer des procédures d'audit appropriées.

### Directive 1009

Cette directive relative à l'utilisation des techniques d'audit fondées sur l'utilisation d'informatique pose comme hypothèse que ces techniques permettent d'améliorer l'efficacité et l'efficience des procédures d'audit. De plus, dans les cas où il n'y a pas de documents de saisies ou de chemin d'audit visible, elles permettent d'inventer des tests de conformité et des contrôles substantifs appropriés.

Cette directive comporte une description des techniques et les utilisations possibles :

- des tests des opérations et des soldes, et la sélection des éléments importants ;
- l'identification des incohérences ou des variations importantes ;
- la conception des systèmes pour l'évaluation de risques, la planification et l'élaboration des programmes d'audit ;
- les tests sur les contrôles généraux et sur les contrôles programmés ;
- la création des feuilles de travail « électroniques ».

Les programmes utilitaires et les programmes de gestion de systèmes peuvent parfois être utilisés pour mettre en œuvre des procédures d'audit. Il existe aussi des programmes développés spécialement à l'intention des auditeurs.

La directive pose aussi comme principe l'obligation pour l'auditeur de posséder les connaissances nécessaires pour planifier et pour réaliser des tests fondés sur ces techniques, et pour utiliser les résultats à bon escient. Les connaissances nécessaires dépendront de la nature et de la complexité du système informatique de l'entité et des techniques d'audit dont l'utilisation est envisagée. Il faudrait aussi décider si la mise en œuvre des techniques se fera chez l'entité-client ou ailleurs. Il peut être nécessaire d'obtenir la coopération du personnel informatique de l'entité.

**SYNTHESE DES NORMES FRANCAISES, AMERICAINES ET IFAC**

L'analyse comparée des textes des différentes structures fait apparaître des lignes directrices générales et des points essentiels dans la conduite de la révision. Quatre points nous semblent devoir être soulignés :

- le milieu informatisé ne modifie pas fondamentalement l'approche du réviseur comptable ;
- l'informatisation des traitements entraîne une modification de l'organisation du contrôle interne dont l'auditeur financier doit tenir compte ;
- l'examen du contrôle interne comprend d'une part l'examen de la fonction informatique et d'autre part l'examen des applications ;
- la mission d'audit en milieu informatique inclut nécessairement la réalisation de tests complétant l'examen de la fonction informatique et les applications.

## **Chapitre 2 : Ebauche d'un projet de norme**

### **Section 1 : Analyse critique du champ juridique, comptable et fiscal au Maroc**

Depuis quelques années, sous l'effet de la mondialisation (ouverture internationale du Maroc), des mesures d'accompagnement ont été entreprises par les pouvoirs publics et portent sur la modernisation du cadre réglementaire et institutionnel.

Concernant le cadre réglementaire, des efforts ont été consentis en matière d'actualisation des principaux textes et lois ayant une incidence directe sur la vie des entreprises. Il s'agit particulièrement de :

- la refonte du droit de sociétés : Loi n°17-95 relative aux sociétés anonymes et Loi 5-96 relative aux autres formes sociétaires ;
- la refonte du code commerce : Loi n°15-95 formant code de commerce ;
- l'instauration des tribunaux de commerce : Loi n°53-95 instituant les juridictions de commerce ;
- la normalisation comptable marocaine s'est caractérisée par une fidélité aux principes et normes comptables admis sur le plan international.

Les organismes établissant des recommandations sont :

- le Conseil National de la Comptabilité (CNC)
- l'Ordre des Experts-Comptable (OEC)
- le conseil déontologique des valeurs mobilières

### Le Conseil National de la Comptabilité

Le Conseil National de la Comptabilité a été institué par le Décret n°2-88 du 16 novembre 1989 qui fait du CNC le principal organisme de normalisation comptable au Maroc. En effet, l'article 2 de ce décret stipule que ce conseil est chargé des missions suivantes :

- la coordination et la mise en synthèse des recherches théoriques et méthodologiques en matière comptable et de ses applications pratiques ;
- la conception, l'élaboration et la proposition de normes comptables générales ou sectorielles ;
- la collecte et la diffusion de toutes les informations relatives à la normalisation, de l'enseignement et la formation comptable ;
- la recommandation de mesures susceptibles d'améliorer l'information comptable au niveau national et au niveau des entreprises ;
- la coordination et l'encouragement de recherches, d'études et le perfectionnement de la discipline comptable ;
- de représenter l'Etat auprès des organismes internationaux de normalisation comptable.

### L'Ordre des Experts Comptables ( O.E.C)

L'Ordre des Experts Comptables a été institué par la loi n°15-89 qui régit la profession d'expert comptable. Celle-ci attribue à l'OEC les prérogatives de :

- édicter tout règlement nécessaire à l'accomplissement de la mission d'expert comptable et l'établissement de code de devoirs professionnels ;
- défendre les intérêts matériels et moraux de la profession d'expert comptable

- et de représenter la profession auprès de l'administration

### Le Conseil Déontologique des Valeurs Mobilières ( CDVM)

Le CDVM a été institué par le Dahir portant loi n° 1-93-212 du 21 septembre 1993 relatif au conseil déontologique des valeurs mobilières et aux informations exigées des personnes morales faisant appel public à l'épargne.

Le CDVM est un organisme à caractère public dont la mission générale est de veiller à la protection de l'épargne investie en valeurs mobilières ou tous autres placements donnant lieu à un appel public à l'épargne, à l'information des investisseurs et au bon fonctionnement des marchés de valeurs mobilières ou de produits financiers cotés.

Toute personne morale qui fait appel public à l'épargne, soit à l'occasion de l'émission d'actions en numéraire ou d'obligations, soit au moment de l'introduction de ses titres à la bourse des valeurs, est tenue d'établir une note d'information qui doit être visée par le CDVM préalablement à sa publication et à sa diffusion.

En dehors de ces missions ponctuelles, le CDVM surveille le marché et entreprend des enquêtes et vérifications : il peut à cet effet demander aux commissaires aux comptes des sociétés faisant appel public à l'épargne la communication des documents sur la base desquels ils ont procédé aux certifications des comptes. Il peut également leur demander de procéder auprès de ces mêmes sociétés à toute analyse complémentaire ou vérification qui lui paraîtrait nécessaire ( article 22 du Dahir).

#### **2.1.1 – La réglementation juridique**

En dépit du « jeune âge » de nos textes législatifs (code de commerce, loi sur les sociétés anonymes, et la loi sur les obligations comptables des commerçants), il apparaît à la lecture de ces derniers que le législateur n'a pas

accordé d'importance particulière à la prolifération des systèmes informatiques ainsi que les risques que ces derniers présentent.

Ainsi, aux termes des articles 19 et 26 du Code de commerce :

« le commerçant tient une comptabilité conformément aux dispositions de la loi n° 9-88 relative aux obligations comptables des commerçants promulguée par le dahir n° 1-92-138 du 30 Joumada II 1413 (25 décembre 1992). Si elle est régulièrement tenue, cette comptabilité est admise par le juge pour faire preuve entre commerçants à raison des faits de commerce.

Les originaux des correspondances reçues et les copies des correspondances envoyées doivent être classés et conservés pendant dix ans à compter de leur date. »

Un correct respect de ces articles du Code de Commerce cités implique-t-il que la société doive conserver pendant dix ans :

- la documentation relative aux analyses, à la programmation et à l'exécution des traitements ;
- les logiciels (systèmes d'exploitation, logiciels d'application) et les fichiers de données sur support magnétique, ce qui impliquerait des travaux de restauration au moins annuels des supports ;
- voire, lorsqu'elle utilise du matériel obsolète ou peu répandu pour réaliser ses traitements, les matériels eux-mêmes ?

### **2.1.2 – La réglementation comptable**

L'obligation de tenir des livres comptables et la manière dont ceux-ci doivent être tenus sont définies par les articles 2, 3, 8 et 22 du Dahir 1-92-138 du 30 joumada II 1413 (25 décembre 1992) portant promulgation de la loi 9-88 relative aux obligations comptables des commerçants.

Les prescriptions de la loi s'en tiennent à l'obligation d'un livre journal et d'un livre d'inventaire cotés et paraphés « tenus sans blanc ni altérations d'aucune sorte ».

La loi a ouvert une porte à la simplification en prévoyant que les reports dans le livre journal pouvaient n'être que mensuels (article 3). La pratique a usé et abusé de cette possibilité au point qu'aujourd'hui, même dans le cas de comptabilité non informatisée, le livre journal – lorsqu'il est encore tenu, car ce n'est pas toujours le cas – n'est jamais qu'une suite de reports mensuels.

Le report sur un document ayant un caractère officiel a pour objet de fixer les opérations comptables à un moment donné. Toutefois, la globalité de ces reports permet de passer les écritures plusieurs mois après les opérations réelles et, le plus souvent, les écritures sont passées une fois par an seulement, au moment de la clôture des comptes.

Souvent les reports au livre journal ne sont faits que lorsque l'on est certain que la comptabilité se trouve dans l'état que l'on souhaite définitif. Par ailleurs, même lorsque les reports ont été effectués, la globalité même de ces reports ne permet pas de s'assurer de l'irréversibilité des opérations incluses, des compensations ultérieures pouvant modifier les montants élémentaires sans pour autant entraîner une modification des montants globaux.

L'introduction de l'informatique dans le traitement comptable impose des choix à deux niveaux : d'une part, il y a lieu de s'interroger sur les éléments de comptabilité sur lesquels doivent être imposées des contraintes ; d'autre part, il faut déterminer la nature des contraintes que l'on veut imposer et les moyens susceptibles d'être utilisés.

Les contraintes peuvent être imposées à titre d'exemple pour la validité des pièces justificatives : toute comptabilité doit s'appuyer sur des pièces justificatives, or la mise en place de systèmes informatiques tend à supprimer l'établissement d'une telle pièce. Pour un système qui ne génère aucune « trace », la création d'une pièce paraît indispensable pour répondre à ce

principe fondamental de la comptabilité. Un point essentiel peut être précisé concernant la valeur de preuve de cette pièce justificative. S'il s'agit de pièces élaborées par l'entreprise elle-même, rien n'empêche cette dernière de modifier, d'altérer, de créer une nouvelle pièce en substitution de l'ancienne. Tant qu'il n'existe pas, à un certain niveau d'élaboration de la pièce justificative, une intervention externe à l'entreprise, le commerçant a toute liberté pour créer ses propres pièces justificatives.

Il serait judicieux d'harmoniser les textes et pratiques en abandonnant les obligations non respectées par les commerçants car a priori inutiles dans un environnement informatique :

- cote et paraphe ;
- livre d'inventaire.

Le manuel des normes marocaines de commissariat aux comptes s'est intéressé aux comptabilité en environnement informatisé. Ainsi les normes :

- 2101 : lors de sa définition de la stratégie de révision et l'établissement de son plan de mission, le commissaire aux comptes doit considérer s'il doit ou non faire appel à des spécialistes pour étudier les applications informatiques ;
- 2102.09 : traite de l'évaluation du contrôle interne, cette dernière précise que la même démarche est adoptée et comprend deux parties :
  - l'évaluation du contrôle interne de « la fonction informatique »
  - l'évaluation du contrôle interne d'un système ou d'une application ;
- 2108.05 : cette norme s'intéresse aux problèmes engendrés par l'informatisation des petites entreprises et aux difficultés rencontrées (« risques dus à l'absence fréquente de formalisation de l'accès aux données et des traitements informatiques »).

- 213 : cette norme met l'accent sur les difficultés rencontrées quant à la collecte d'éléments probants :
  - « impossibilité d'extraire des informations des fichiers informatiques du fait du manque de documentation ou d'une documentation périmée du contenu des enregistrements ou des programmes ;
  - un grand nombre de modifications des programmes ne sont pas documentées, approuvées ou testées ;
  - l'incohérence dans le rapprochement entre les transactions informatiques et les bases de données d'une part, et la comptabilité générale d'autre part. »

Tout comme les normes de la CNCC, les normes marocaines ont attiré aux risques engendrés quant à l'informatisation des systèmes comptables, toutefois, ces dernières sont générales alors que le présent mémoire a pour objectif de préciser les spécificités du commissariat aux comptes en milieu informatisé.

### **2.1.3 – La réglementation fiscale**

Sur un plan fiscal, le législateur s'est intéressé à l'obligation des redevables pour restituer les archives « informatisés » de manière à pouvoir les contrôler.

Article 42 de la TVA: « si la comptabilité est tenue par des moyens informatiques ou si les documents conservés sous forme de microfiches, le redevable doit consentir aux agents toutes facilités pour l'exercice du contrôle et l'analyse sur place des données enregistrées ».

Article 33 de l'IS: « les sociétés sont tenues de conserver pendant 10 ans au lieu où elles sont imposées, ..., notamment les livres sur lesquels les opérations ont été enregistrées, le livre d'inventaire, les inventaires détaillés s'ils ne sont pas recopiés intégralement sur ce livre ainsi que le livre journal et les fiches des clients et des fournisseurs... »

Si les documents sont conservés sous forme de micro-fiches, la société doit consentir aux agents toutes facilités pour l'exercice du contrôle et l'analyse des données enregistrées. »

Dahir n° 1-89-235 du 30 décembre 1989 portant promulgation de la loi de finance 1990 dans sont article 203 bis :

« le dépôt des déclarations,..., peut sur autorisation de l'administration, s'effectuer par des procédés électroniques ou informatiques ».

## **Section 2 : Les principes de base**

Nous énumérerons les principes essentiels qui devront être pris en compte par l'auditeur financier lors de sa mission. Ces derniers nous permettront d'établir une ébauche de normes d'audit.

### **2.2.1 – Norme de gestion et de sécurité**

Des tâches autrefois dévolues aux différents utilisateurs sont aujourd'hui exécutées par le seul département informatique. Cette concentration peut conduire au non respect du traditionnel principe de séparation des fonctions.

Aussi, l'auditeur financier recherchera-t-il si les fonctions, donc les responsabilités, sont bien séparées, notamment entre :

- les services d'étude, c'est à dire les organisateurs responsables de l'implantation des systèmes dans leur ensemble, les analystes chargés de la conception des applications et les programmeurs chargés de traduire ces analyses en langage informatique, qui ne doivent avoir accès qu'aux programmes en développement ;
- les services d'exploitation, c'est à dire les opérateurs qui ne doivent avoir accès qu'aux programmes et aux supports de fichiers en exploitation ;
- les utilisateurs, qui peuvent procéder à des interrogations de fichiers, à des saisies de données et à des éditions d'informations.

Le traitement informatique des données conduit à une concentration d'éléments du patrimoine dans un même lieu (matériels, logiciels, supports et informations stockées). L'auditeur financier devra vérifier que la protection de ces éléments est suffisante et que la confidentialité est assurée.

La protection physique vise en particulier le contrôle efficace de l'accès physique aux locaux d'exploitation ainsi que les protections contre les dommages physiques, quelle que soit leur origine.

La protection logique est principalement obtenue par l'utilisation de moyens de contrôle d'accès tels que badges ou mots de passe régulièrement modifiés et par l'enregistrement des tentatives d'accès non autorisé.

L'auditeur financier doit aussi évaluer les mesures prises pour pallier d'éventuelles pertes de capacité de traitement, ponctuelles ou prolongées.

Il doit contrôler l'existence d'un équipement de secours et/ou des procédures de reprises (existence d'un plan de sauvegarde, de procédure d'arrêt...).

### **2.2.2 – Information sur les systèmes et l'environnement informatique**

Il s'agit des caractéristiques générales du milieu informatique de traitement des systèmes comptables informatisés.

Les principales informations à obtenir concernent :

- l'organigramme détaillé du service informatique et sa position au sein de la société, notamment par rapport à la direction générale,
- la localisation de l'installation et du stockage d'éléments sensibles (copies de fichiers, programmes, documentation...), ainsi que les accès extérieurs (terminaux, moyens de communication...)
- le manuel des procédures mises en place, notamment pour les mesures générales de sécurité,
- le matériel, aussi bien l'unité centrale que les périphériques (lecteur de bandes, de disques, imprimante...)
- les applications utilisées, qu'elles aient été développées par la société, acquises à l'extérieur ou qu'elles soient traitées à façon. On s'intéressera plus particulièrement à celles qui traitent des informations comptables et financières.

### **Section 3 : Etude et évaluation du système comptable et de ses contrôles internes**

#### **2.3.1 – Les contrôles généraux**

Les spécificités d'un milieu informatique entraînent une démarche particulière pour l'évaluation du contrôle interne dans les organisations où l'on utilise un ordinateur pour traiter les informations comptables.

En effet, un milieu informatique pose des problèmes nouveaux tels que :

- la concentration des fonctions et des connaissances, qui provoque un risque de mauvaise séparation des fonctions ;
- l'absence éventuelle de matérialisation sur un support-papier des entrées, du traitement et des sorties ;

#### **2.3.2 – Les contrôles d'applications informatisées**

Les contrôles de traitement sont étudiés plus en détail par l'auditeur financier lors de son contrôle d'applications informatiques traitant d'informations à conséquences comptables et financières.

Il s'agit principalement d'apprécier :

- la qualité des procédures d'exploitation, notamment des procédures de restriction d'accès aux bibliothèques de programmes en exploitation ;
- le degré de confiance que l'on peut avoir dans les contrôles et les procédures programmées des applications comptables informatisées, ainsi que dans les opérations « générées » par le système,
- le respect des principes d'autorisation, d'exactitude et d'intégralité du traitement des données.

## **Section 4 : Les techniques de contrôle assisté par ordinateur**

### **2.4.1 – Description des techniques de contrôle assisté par ordinateur**

L'ordinateur est un moyen matériel susceptible d'être utilisé par l'auditeur financier.

Le recours à l'ordinateur peut réduire la durée de mobilisation des interlocuteurs de l'entreprise et permettre une meilleure adaptation aux délais imposés à l'auditeur financier pour l'accomplissement de sa mission.

En outre, des contrôles plus approfondis, voire exhaustifs, sont possibles.

### **2.4.2 – L'utilisation des techniques de contrôle assisté par ordinateur**

La décision d'avoir, ou non recours aux techniques de contrôle assisté par ordinateur implique la prise en compte d'un certain nombre d'éléments :

- disponibilité d'installations informatiques satisfaisantes : l'auditeur financier devra examiner la disponibilité de l'ordinateur de l'entreprise et l'accessibilité aux fichiers. En fonction de ces installations, il devra décider du moyen compatible le plus efficace et le plus économique à utiliser ; en général pour les interrogations de fichiers, ce choix s'exercera dans l'ordre suivant : progiciel de révision, programme utilitaire, programme spécifique.
- faisabilité des tests manuels : certains contrôles sont impossibles à exécuter manuellement dans la mesure où il n'existe pas de trace écrite suffisante des traitements effectués.

Exemple : saisie en direct d'ordres de vente sans documents préalables (documents d'entrée inexistants)

Contrôles programmés non édités, tels que mise en correspondance automatique des bons de livraison et des factures

Etats de sortie comportant des totaux récapitulatifs et non le détail des mouvements

- Efficacité : il est possible de tester par ordinateur certaines opérations de façon plus efficace ou plus complète pour un coût équivalent, comme par exemple l'interrogation exhaustive d'un fichier de transactions.

Dans une procédure d'examen analytique, la possibilité de passer en revue le détail des opérations et les soldes et d'éditer les éléments inhabituels peut se faire rapidement et de façon exhaustive.

- Calendrier : dans certains cas, les fichiers informatiques ne sont conservés que sur une courte période. L'auditeur financier devra prendre des dispositions afin de conserver ces données dans les meilleures conditions et dans les délais impartis.

- Coût : l'auditeur financier devra intégrer dans l'analyse des coûts les éléments suivants :

- temps nécessaire pour organiser, concevoir et mettre en œuvre les techniques de contrôle assisté par ordinateur ,
- temps d'assistance technique ,
- conception et édition des états
- codification et vérification des données d'entrée
- temps de travail de l'ordinateur.

Le coût de mise en œuvre d'une première application peut être élevé mais la réutilisation de celle-ci sur plusieurs années peut permettre d'amortir le coût global.

- Disponibilité des informations dans les fichiers : l'absence de certaines informations dans les fichiers pourra limiter les possibilités d'effectuer certains contrôles (par exemple, la date de dernier mouvement de stock est nécessaire pour contrôler la rotation).

### **2.4.3 – Les contrôles à mettre en œuvre**

Lorsqu'une technique de contrôle assisté par ordinateur est mise en place, il est nécessaire, d'une part d'en contrôler l'utilisation afin de s'assurer que cette technique n'est pas utilisée irrégulièrement par le personnel de l'entreprise, d'autre part, de s'assurer que les objectifs d'audit sont atteints.

Le rôle de l'auditeur financier est donc d'apprécier les conditions de sécurité d'utilisation de la technique

Il est en outre nécessaire que l'auditeur financier, assisté éventuellement d'un spécialiste intervienne :

- pour participer à la conception du programme de travail de contrôle assisté par ordinateur
- pour vérifier la programmation ou le paramétrage afin de s'assurer de leur conformité aux objectifs visés
- pour s'assurer de l'utilisation de ces techniques dans les conditions prévues (vérification des fichiers utilisés), à l'aide, par exemple, de totaux de contrôle
- pour s'assurer que des mesures de sécurités suffisantes ont été prises pour sauvegarder les données du client.

## **RECOMMANDATION**

### **Proposition d'un texte de norme relatif au commissariat aux comptes en milieu informatisé**

Un milieu est dit informatisé, lorsqu'un ordinateur, quels que soient sa taille ou son type, intervient dans le traitement de l'information financière qui présente une importance pour l'audit, que cet ordinateur soit exploité par l'entité ou par un tiers.

**Les objectifs généraux et l'étendue de l'audit ne sont pas modifiés en milieu informatisé.** Toutefois, l'utilisation d'un ordinateur modifie le traitement et la conservation de l'information financière et peut affecter l'organisation et les procédures utilisées par l'entité pour satisfaire à la mise en place d'un contrôle interne fiable. En conséquence, les procédures mises en œuvre par l'auditeur dans son évaluation du système comptable et de ses contrôles internes ainsi que la nature, le calendrier et l'étendue de ses autres procédures d'audit peuvent être influencés par l'existence d'un milieu informatisé.

Le commissaire aux comptes se doit d'une part d'apprécier la qualité et la sécurité des techniques informatiques mises en œuvre par les entreprises ; d'autre part s'appuyer sur le matériel informatique en vue de réaliser des contrôles plus approfondis, voire exhaustifs, que ceux réalisés manuellement.

### **DISPOSITION GENERALE**

Le système de traitement doit établir, sur papier ou éventuellement sur tout support offrant les conditions de garantie et de conservation définies en matière de preuve, des états périodiques numérotés et datés récapitulants, dans un ordre chronologique, toutes les données qui y sont entrées, sous une forme

interdisant toutes insertions intercalaires, ainsi que toutes suppressions ou additions ultérieures.

L'exercice de tout contrôle doit comporter un droit d'accès à la documentation relative aux analyses, à la programmation et à l'exécution des traitements en vue de procéder aux tests nécessaires.

Les procédures de traitement automatisé des comptabilités doivent être organisées de manière à permettre de contrôler si les exigences de sécurité et de fiabilité requises en la matière ont bien été respectées.

### **APTITUDES ET COMPETENCE**

#### **Le commissaire aux comptes ne peut plus ignorer l'informatique.**

Dans le cadre d'un audit effectué en milieu informatisé, le commissaire aux comptes doit avoir une connaissance suffisante du matériel informatique, du logiciel et des systèmes de traitement, afin de planifier sa mission et de maîtriser l'influence de l'informatique sur l'étude et l'évaluation du contrôle interne et sur la mise en œuvre des procédures d'audit, et notamment sur ses techniques de contrôle assisté par ordinateur.

Il doit également posséder des connaissances suffisantes en informatique lui permettant de mettre en œuvre les procédures d'audit adaptées.

### **TRAVAUX EFFECTUES PAR D'AUTRES PERSONNES**

#### **Le commissaires aux comptes doit faire appel à un spécialiste chaque fois qu'il rencontre un problème pour lequel il ne s'estime pas compétent.**

Le commissaire aux comptes ne peut, en aucun cas, déléguer la responsabilité de tirer les conclusions finales de l'audit ou celle de former ou d'exprimer son opinion sur l'information financière. En conséquence, lorsqu'il délègue

certaines travaux à des tiers, l'auditeur doit posséder des connaissances suffisantes en informatique soit pour diriger, superviser et examiner les travaux des assistants qualifiés en informatique, soit pour obtenir un degré raisonnable de certitude que les travaux effectués par d'autres experts qualifiés en informatique répondent bien à ses besoins.

### **PLANIFICATION**

Dans le cadre de son programme général de travail, le commissaire aux comptes doit réunir une information pertinente sur le milieu informatisé, concernant notamment :

- l'organisation de la fonction informatique, le degré de centralisation ou de distribution des traitements informatiques au sein de l'entité ;
- le matériel et le logiciel informatiques utilisés par l'entité ;
- chaque application informatique importante, la nature des traitements (par exemple, par lots ou interactif) et les méthodes de conservation des données.

Dans le cadre de l'approche générale de sa mission, le commissaire aux comptes doit notamment :

- déterminer si, et dans quelle mesure, il entend s'appuyer sur les contrôles informatiques dans son évaluation globale du contrôle interne ;
- planifier où, quand et comment la fonction informatique sera examinée, et le cas échéant, l'intervention des experts en informatique ;
- planifier les procédures d'audit qui comprennent des techniques de contrôle assisté par ordinateur.

Certains fichiers informatiques, tels que les fichiers contenant le détail des opérations, ne sont souvent conservés en mémoire que pendant une courte

période et ainsi ils ne sont pas toujours accessibles par ordinateur lorsque le commissaire aux comptes le souhaite. Ainsi, il doit prendre des dispositions en vue d'assurer la conservation des données qui lui sont nécessaires, ou bien modifier le calendrier de ses travaux qui s'appuient sur ces données.

### **INCIDENCE DU MILIEU INFORMATIQUE SUR L'EVALUATION DU CONTROLE INTERNE**

**Le commissaire aux comptes vérifie le respect des principes généraux du contrôle interne en approfondissant l'examen de l'environnement informatique :**

**Pour cela, il s'intéresse plus particulièrement :**

- **aux contrôles portant sur l'organisation ,**
- **aux contrôles relatifs à la sécurité,**
- **à la sauvegarde et à la reprise des travaux ;**
- **aux contrôles portant sur les traitements ;aux procédures de développement, de mise en exploitation et de maintenance des applications ainsi qu'à l'existence d'une documentation.**

Le commissaire aux comptes vérifie l'application effective des procédures de contrôle. Il peut, pour ce faire, avoir recours à des techniques de contrôle assisté par ordinateur.

### **LES TECHNIQUES DE CONTROLE ASSISTE PAR ORDINATEUR**

L'ordinateur peut être utilisé par le commissaire aux comptes pour réaliser des contrôles plus rapides et plus approfondis.

La décision d'avoir ou non recours aux techniques de contrôle assisté par ordinateur implique la prise en compte de nombreux éléments tels que :

- la disponibilité d'installations informatiques satisfaisantes ;

- la faisabilité ou non des tests manuels ;
- la disponibilité sur fichier informatique des informations à contrôler ;

Les moyens susceptibles d'être utilisés par le commissaire aux comptes sont nombreux :

- les jeux d'essais ;
- les logiciels spécifiques ;
- les progiciels d'aide à la révision.

L'utilisation de ces moyens offre des possibilités variées de traitement et de contrôle.

Le recours aux techniques de contrôle assisté par ordinateur implique pour le commissaire aux comptes :

- une compétence ;
- un contrôle de la mise en œuvre pour vérifier la bonne utilisation de la technique ;
- un double contrôle de sécurité au niveau du résultat (fiabilité) et des fichiers du client (non altération) ;
- une documentation suffisante des travaux réalisés.

**CONCLUSION**

La certification des comptes ne doit pas être simplement une contrainte légale, elle doit être un apport réel pour l'entreprise. Dans cet esprit, une mission de certification des comptes réalisée selon l'approche par les risques apporte à l'entreprise :

- la confirmation de l'existence et de la validité des points forts de ses procédures ;
- le rappel ou la découverte des risques non couverts avec les recommandations destinées à y remédier.

En toute logique, les tests informatiques réalisés sur les fichiers de l'entreprises auront permis de vérifier que les risques non couverts n'avaient pas eu d'effets. Si tel n'était pas le cas, ces tests auront permis de mesurer l'impact de ces effets sur le résultat. Tant que la procédure n'a pas été modifiée pour couvrir définitivement les risques en question, il importe que la diligence citée soit systématiquement reconduite. L'expérience a montré que certaines entreprises reprenaient à leur compte, dans leurs traitements courants, les diligences initiés par le commissaire aux comptes afin de s'affranchir des risques potentiels. Pour demeurer opérationnelle dans les meilleures conditions, l'approche par les risques doit tenir compte de nombreux facteurs dans un contexte en évolution permanente.

La structure des entreprises s'adapte au contexte économique, et l'on observe des mouvements de centralisation et de regroupement, comme de décentralisation et de délocalisation.

Pour des raisons de productivité, les systèmes deviennent de plus en plus intégrés, et le recours aux techniques d'échange de données informatisées s'amplifie. La dématérialisation progressive des documents commerciaux va augmenter encore la complexité des systèmes d'information.

Enfin, beaucoup d'entreprises se recentrent sur leur métier principal et confient à des entreprises extérieures la gestion de différentes fonctions autrefois assurée en interne. Le remplacement très fréquent des logiciels développés en interne au profit de progiciels « du commerce » illustre bien cette évolution. L'essor du « facilities management », qui consiste à confier à une entreprise extérieure les ressources informatiques et leur exploitation, est une autre manifestation du phénomène actuel « d'externalisation ».

Plus les systèmes d'informations seront manuels et plus les opérations traitées seront nombreuses, moins le contrôle des résultats sera satisfaisant pour appréhender le système d'information et se forger une opinion.

Ce sont les méthodes employées par les commissaires aux comptes qui vont nécessairement évoluer avec les techniques employées. La vérification de la pertinence des procédures de l'entreprise s'appuiera toujours sur des contrôles vrais, faisant de plus en plus appel à des référentiels externes.

Dans les systèmes d'information complexes, l'approche par les systèmes prend progressivement le pas sur l'approche par les résultats. La date des clôtures des comptes sociaux est sans grande incidence sur l'examen des procédures, quelque soit le degré d'informatisation. Par ailleurs, le temps dévolu à la certification des comptes est de plus en plus réduit, car les résultats définitifs doivent être arrêtés à une date de plus en plus proche de la clôture de l'exercice.

Ces raisons poussent à développer l'approche par les systèmes au cours des phases d'intérim, en amont de la phase de contrôle final des comptes. Les diligences de contrôle des risques non couverts, déjà mises en place lors des phases d'intérim, pourront valablement être relancées lors de la phase finale, sans pour autant nécessiter des ressources de temps importantes.

Beaucoup d'entreprises souhaitent aujourd'hui que les commissaires aux comptes ne limitent plus leur intervention à l'émission d'un certificat sous la forme strictement prévue par la réglementation. Ils sont dorénavant dans l'obligation de signaler les risques majeurs dans les domaines économique,

comptable, juridique, fiscal et dans la mesure du possible, d'émettre les recommandations susceptibles de couvrir ces risques potentiels. Dans la plupart des cas, le service attendu par l'entreprise dépasse très largement la pure mission de certification des comptes.

Pour mener à bien leurs missions, les commissaires aux comptes doivent maîtriser les systèmes d'information. Ces derniers sont de plus en plus complexes et dépassent le plus souvent les capacités d'un homme seul. Pour faire face à cette nouvelle donne, il appartient aux commissaires aux comptes de se structurer en équipes pluridisciplinaires. Enfin, cette évolution de l'environnement et de la nature des missions d'audit valorise l'image des commissaires aux comptes. Forts de leur expérience et de leurs compétences obtenues dans ce type de missions, les commissaires aux comptes deviennent naturellement des conseillers écoutés de l'entreprise. Ils se trouvent ainsi dans une situation privilégiée pour étendre leur mission.

La complexité et la sophistication croissante de l'informatique entraînent des risques dans les entreprises et les organisations, risques qui sont à la mesure de l'accroissement d'efficacité et de productivité que l'informatique apporte avec elle.

Ces risques, s'ils sont inhérents à l'évolution de l'informatique, sont également très souvent les conséquences d'une insuffisante organisation et d'une absence de dispositifs, qui en permettent le suivi et le contrôle.

Tout au long de ce mémoire, nous avons recherché les principaux risques que l'informatique peut faire naître tant dans la fonction informatique elle-même que dans les applications informatisées ; nous avons également eu pour préoccupation de rechercher quelles sont les procédures et contre-mesures les plus utiles pour pallier et compenser les risques principaux. Ce sont les expériences acquises sur le terrain auprès d'entreprises de toutes tailles, de niveau et de degré d'informatisation différents qui ont conduit à ces propositions qui devraient s'avérer directement utilisables par les dirigeants

d'entreprises, les responsables de services informatiques, les utilisateurs dans les entreprises et les commissaires aux comptes eux-mêmes.

Il apparaît bien que informatique et audit sont indissolublement liés : la complexité croissante de l'informatique appelle l'extrême rigueur que propose toute démarche d'audit.

**ANNEXES**

### Typologie des missions d'audit informatique

Pour gérer efficacement ses interventions et garantir la qualité des travaux effectués, l'auditeur doit pouvoir se référer à une classification des différentes missions en milieu informatisé.

Cette classification lui sera utile en particulier dans les domaines suivants :

- organisation de la mission : évaluation de la durée prévisible, choix des intervenants en cas de travail en équipe. Il s'agit autant de l'action a priori (planification) que du suivi a posteriori (suivi des réalisations) ;
- définition des compétences nécessaires.

Dans le tableau qui suit, nous présentons une classification basée sur la distinction courante de 3 domaines en audit informatique :

- fonction informatique
- applications informatiques
- tests directs sur les données

Domaine d'intervention	Missions	Objectifs de l'auditeur et justification de la mission
Fonction informatique	<ul style="list-style-type: none"> <li>- Audit de sécurité (AO et AF)</li> <li>- Audit de la fonction informatique (AF)</li> <li>- Audit opérationnel de la fonction informatique (AO)</li> <li>- Audit des performances (AO)</li> <li>- Audit du plan de sauvegarde (AO et AF)</li> </ul>	<ul style="list-style-type: none"> <li>Efficacité des mesures de sécurité</li> <li>Connaissance et appréciation de la fonction informatique</li> <li>Optimiser l'efficacité de la fonction informatique</li> <li>Optimiser les performances de la configuration informatique</li> <li>Garantir la pérennité des données et la continuité de l'exploitation</li> </ul>
Applications informatiques	<ul style="list-style-type: none"> <li>- Audit d'une application (AF)</li> <li>- Certification de progiciel (spécifique)</li> <li>- Audit d'un projet (AO)</li> </ul>	<ul style="list-style-type: none"> <li>Fiabilité et sécurité des informations</li> <li>Respect des obligations légales et réglementaires</li> <li>Délivrance d'une attestation de conformité à certaines normes</li> <li>Respect des normes de développement, optimisation, du coût et des performances du projet informatique</li> </ul>

	- Audit du système d'exploitation (AO et AF)	Vérifier que la génération et le paramétrage du système garantissent la fiabilité et la sécurité des données et traitements (AF). Optimiser les performances (AO)
Tests directs sur les données	- Révision assistée par ordinateur (AO et AF)	Tester la fiabilité, l'exactitude, l'exhaustivité des informations

AF : Audit Financier

AO : Audit Opérationnel

**Questionnaire lors de la prise de connaissance de l'entreprise et de l'appréciation du contrôle interne**

Nom du client

Date de clôture

Dans le cas où la société auditée utilise un progiciel et n'a pas de personnel informatique dédié, répondre aux questions suivantes :

Depuis l'année précédente y a-t-il eu des mises en service de nouvelles applications ou des modifications importantes sur des applications existantes ?

Le client a-t-il la possibilité de modifier lui-même les progiciels ?

La consultation d'un auditeur informatique est nécessaire dans les cas suivants :

la réponse aux deux questions précédentes est « oui »

- le client dispose de personnels informatiques dédiés

- le client n'utilise pas que des progiciels standards au sein de son système d'information financier

**Identification des principales applications**

<b>PRINCIPALES APPLICATIONS A INCIDENCE FINANCIERE</b>			
Cycle	Application	Progiciel standard Progiciel modifié Développement spécifique	Installée sur (ordinateur/système)

Dans le cadre des applications ci-dessus mentionnées, la société a-t-elle recours à de la sous-traitance ? Si oui, indiquer si la direction s'est assurée de la qualité de l'organisation et du contrôle interne du sous-traitant au travers, par exemple, de rapports d'audit émis par des auditeurs indépendants.

De même, la société a-t-elle recours à des sociétés externes dans le cadre de ses développements informatiques (achat de progiciel) ? Si oui, indiquer s'il existe des garanties suffisantes en matière de propriété des programmes source.

### **Connaissance du contexte applicatif**

Une fiche de présentation doit être complétée pour chaque application ayant une incidence financière importante.

Description de l'application (incluant la nature des principales transactions et leurs volumes approximatifs)

Interlocuteurs habituels

Origine du développement (interne/externe/progiciel)

S'il s'agit d'une sous-traitance (développement externe, progiciel), indiquer le nom, le concepteur et la version

Date de mise en service

Langage de programmation

Date de dernière modification

Problèmes identifiés et limités de l'application

**Environnement techniques de l'informatique**

Ordinateur	Système d'exploitation	Logiciels de communication	Logiciel de sécurité

**Description de l'architecture réseau**

Identifier les principaux sites de traitement et départements utilisateurs, et indiquer les liaisons informatique existantes (faire un schéma simplifié ou joindre un document élaboré par le client).

**BIBLIOGRAPHIE**

OUVRAGES

- Marc Thorin - L'audit informatique - Editions hermes sciences publication – 2000
- Miko - Les audits financiers - comprendre les mécanismes du contrôle légal - Editions d'organisation – 1999
- L'archivage électronique - Experts Comptables Media – 1998
- Jean Paul Lamy - Audit et certification des comptes en milieu informatisé - les éditions d'organisation - 1996
- Hugues Angot - Christian Fischer- Baudouin Theunissen - Audit comptable - audit informatique - Edition de Boeck-Wesmael – 1994
- P.Sarret et S.Faurie - Audit informatique - KPMG - Audit fiduciaire de France - Nouvelles éditions fiduciaires – 1991
- Progiciels de comptabilité - Critère de conception et de choix - CNCC éditions - 1990
- Jean Raffegau et Alain Ritz - Audit et informatique - Que sais-je? - Presse universitaire de France – 1986
- Association technique d'harmonisation des cabinets d'audit et conseil - Audit et informatique - Guide pour l'audit financier des entreprises informatisées - Edition clet – 1985

- Guides des commissaires aux comptes : les contrôle dans les entreprises informatisées - Tome 2 et tome 3 - Edition Serieys Lapeyrere - Plante - Informatique de gestion – 1980
- Les techniques modernes de l'audit – El Gadi Abdelhamid – Première édition 2001
- Les contrôles comptables et la vérification en milieu informatique – Yvon Houle – Les presses de l'université Laval – 1986
- L'informatique mémoire de l'entreprise – Synthèses informatiques CNAM – Edition Hermès – 1996
- Audit & gestion stratégique de l'information – Pierre morgat – Les éditions d'organisation – 1995
- Audit et contrôle interne – Aspects financiers opérationnels et stratégiques – Lionel Collins – Gérard Valin – Edition Dalloz – 1992
- Informatique appliquée à la comptabilité et à la gestion – Tome 1 – R Reix – Edition foucher – 1979
- Une société informatisée pour qui ? pour quoi ? comment ? – Travaux de l'institut d'informatique n°7 bis – Presses universitaires de Namur - 1982

### MEMOIRES

- Laurent Carlier - L'auditeur confronté aux risques juridiques, comptables et fiscaux attachés à l'exploitation des banques de données : proposition d'une méthodologie de révision – Novembre 1995
- Luc Théron - Proposition d'une méthodologie d'audit dans le cadre de l'évaluation du contrôle interne des entreprises informatisées – Mai 1994
- Gilles Pernet - La comptabilité sans papier, peut-elle être probante? – Novembre 1993

- Emerich Jérôme - L'échange des données informatisées et la dématérialisation des documents : conséquences sur les méthodes de travail employées par l'expert comptable au cours de ses missions de révision des comptes – Novembre 1992
- Lardy Philippe - Interrogations informatiques de fichiers : quel intérêt pour la profession comptable et quelle méthode retenir ?- Novembre 1990
- Meune Pierre - Responsabilité du commissaire aux comptes et de l'expert comptable en matière de diagnostic des systèmes informatisés et ses limites – Novembre 1989
- Michel Finance - La révision en milieu informatisé : nécessité d'une approche intégrée – Novembre 1987
- Philippe Sarret - Le réviseur comptable face aux systèmes informatisés : évaluation des risques et approche d'audit – Novembre 1986
- Dominique Thouvenin - L'organisation de la révision des comptabilités traitées par des moyens informatiques – Novembre 1977

### Revue

- Agéfi - Vérifications de comptabilité : un contrôle peut-il en cacher un autre ? – Juillet 1997
- Bulletin CNC n° 52 - Etude que les procédures susceptibles de garantir les documents comptables issus d'ordinateur – 3<sup>ème</sup> trimestre 1982
- Bulletin comptable et financier n°10 - Contrôle des comptabilités informatisées : incidence sur la mission du commissaire aux comptes du non respect des dispositions fiscales – Octobre 1998

- CNCC n° 2 - Une démarche pour se mettre en conformité et le rôle du commissaire aux comptes – Avril 1998
- Collection notes d'informations n°3 - Appréciation du contrôle interne - Editions CNCC – Février 1992
- Option finance n°419 - Le contrôle des comptabilités informatisées – Juillet 1996
- Option finance n°449 - Le contrôle fiscal des comptabilités informatisées : bilan de 5 années d'expérience – Avril 1997
- Option finance n°560 - Le contrôle fiscal des comptabilités informatisées dans les entreprises – Août 1999
- Revue Française de Comptabilité n° 144 - Le contrôle des comptabilités informatisées – janvier 1995
- Revue Française de Comptabilité n° 226 - Le contrôle des comptabilités informatisées – Février 1997

**LEXIQUE**