

**CENTRE AFRICAIN D'ETUDES SUPERIEURES EN
GESTION (CESAG)**

MEMOIRE DE FIN DE CYCLE

L'AUDITEUR FACE A L'INFORMATIQUE

DIPLOME D'AUDIT INTERNATIONAL ET CONTROLE



Présenté et soutenu par :

ASSOUMANA Hassoumi

Sous la direction de :

**M. YAZI Moussa
Chef du département
Comptabilité, Audit et contrôle**

M0108AUDIT00

2



Janvier, 2000

REMERCIEMENTS

La réalisation de ce mémoire est le fruit des conseils et de l'appui de nombreuses personnes envers lesquelles je manifeste ma sincère gratitude.

Néanmoins, qu'il me soit permis de remercier plus particulièrement :

- La Société Nationale des Eaux du Niger et la GTZ NIGER pour leur soutien financier ;
- La Direction Générale et tout le corps professoral du CESAG ;
- Messieurs Moussa YAZI, Chef du Département Comptabilité, Audit et Contrôle de gestion , BOSSA Gilbert et SARR Ababacar Professeurs au CESAG qui, malgré leurs multiples occupations ont accepté de m'encadrer pour la réalisation de ce travail ;
- Monsieur Hassane KANEYE, Associé Fondateur du Cabinet KMC Niger et Madame Mariame BA, Directrice du Cabinet MARIAME BA Sénégal pour m'avoir accueilli et fortement responsabilisé au sein de leurs équipes;
- Monsieur Hama TINI, Chef de mission au Cabinet KMC pour son encadrement ;
- A tous mes amis de la dixième promotion d'audit.

L'AUDITEUR FACE A L'INFORMATIQUE

	Pages
INTRODUCTION GENERALE	1
PROBLEMATIQUE	1
OBJECTIF DE L'ETUDE	1
INTERET DE L'ETUDE	2
PREMIERE PARTIE : GENERALITES SUR L'AUDIT	3
PREMIER CHAPITRE : L'EVOLUTION HISTORIQUE DE L'AUDIT	4
DEUXIEME CHAPITRE : L'AUDIT A L'AVENEMENT L'INFORMATIQUE	17
DEUXIEME PARTIE : L'AUDIT INFORMATIQUE	21
PREMIER CHAPITRE : CARACTERISTIQUES D'UN MILIEU INFORMATISE	24
I. INCIDENCES SUR LA STRUCTURE ORGANISATIONNELLE	28
II. INCIDENCES SUR LES TRAITEMENTS	30
III. INCIDENCES SUR LA CONCEPTION DES PROCEDURES	31
DEUXIEME CHAPITRE : NORMES D'AUDIT ET DEMARCHE DE L'AUDITEUR FACE A L'INFORMATIQUE	32
I. NORMES D'AUDIT EN MILIEU INFORMATISE	32
II. DEMARCHE DE L'AUDITEUR FACE A L'INFORMATIQUE	34
TROISIEME CHAPITRE : L'ORDINATEUR : UN OUTIL POUR L'AUDIT	50
TROISIEME PARTIE : CAS D'APPLICATION : L'AUDIT DU LOGICEL 'COMPTAB' D'UNE SOCIETE X	53
CONCLUSION GENERALE	97
BIBLIOGRAPHIE	100

LISTE DES TABLEAUX ET FIGURES

Tableaux

N°	Intitulés	Pages
01	Evolution historique de l'audit	5
02	Insuffisances de contrôle au service informatique et risques potentiels	39
03	Insuffisances de contrôle d'accès et risques potentiels	40

Figures

N°	Intitulés	Pages
01	Cycle général d'opérations de gestion	10
02	Cycle comptable encastré dans le cycle général de gestion	11
03	Démarche pour l'appréciation du contrôle interne	12
04	Organigramme type d'un grand centre informatique	29
05	Organigramme type d'un centre moyen	29
06	Organigramme d'un petit centre	30
07	Démarche de l'audit informatique	35
08	Appréciation du contrôle interne de la fonction informatique	38
09	Démarche de l'audit des applications	44



INTRODUCTION GENERALE

PROBLEMATIQUE

Jadis, calculateur épargnant le scientifique des calculs fastidieux, l'ordinateur a envahi tous les domaines de la vie pour multiplier nos capacités, faciliter ou supprimer des tâches, accroître les possibilités de l'effort mental ou remplacer l'effort physique.

Dans cette invasion de l'ordinateur – de l'informatique pour être plus complet- , les entreprises n'ont pas été épargnées. Cependant, si tous les aspects de l'entreprise sont aujourd'hui guettés par l'informatique, c'est surtout au niveau du traitement des informations financières que l'ordinateur a connu un développement rapide. De nos jours, les informations financières qu'examinent les auditeurs sont dans leur quasi totalité produites par un système informatisé contrairement à ce qui se passait avant l'avènement de l'informatique, il y a une cinquantaine d'années. Mais dans la pratique, on constate que les professionnels d'audit ne tiennent pas compte de cette nouvelle donne. On peut alors se poser la question de savoir si l'ordinateur peut être neutre dans l'opinion que ceux-ci sont amenés à émettre sur les états financiers qu'ils auditent.

OBJECTIF DE L'ETUDE

L'objectif de ce mémoire « L'AUDITEUR FACE A L'INFORMATIQUE » est de répondre à la question suivante :

« Faut-il adopter la même démarche d'audit dans une organisation informatisée que dans une organisation où la production des informations financières est manuelle ? ».

Plus spécifiquement, quelle a dû être la position de l'auditeur ? Peut-il s'en débarrasser et faire l'audit « around the computer » ? Les documents informatiques sont-ils plus fiables que les documents manuels ? Peut-on auditer la fonction informatique comme on auditerait n'importe quelle autre fonction de l'entreprise ? Quels sont les problèmes inhérents à

l'informatique pour l'auditeur ? Faut-il avoir des connaissances solides en informatique pour mener une mission d'audit dans un système fortement informatisé ?

Pour répondre à ces questions, nous avons jugé utile de traiter de l'évolution de l'audit jusqu'à l'avènement de l'informatique, puis analyser la démarche traditionnelle d'audit relativement aux caractéristiques d'un milieu informatisé et ensuite relever les aménagements nécessaires pour mieux réussir une mission d'audit dans ce milieu.

INTERET DE L'ETUDE

Cette étude présente l'intérêt d'attirer l'attention des professionnels d'audit sur les risques supplémentaires qu'engendre un milieu informatisé et de les amener à adopter une démarche de façon à réduire à un niveau acceptable les risques d'audit.

S'agissant de la démarche générale, nous avons jugé nécessaire de diviser le travail en trois(3) grandes parties :

- ♦ La première partie « Généralités sur l'audit et l'informatique » portera sur une analyse succincte de l'évolution historique de l'audit ; les conséquences de l'avènement de l'informatique sur les systèmes d'informations et le métier de l'auditeur.
- ♦ La deuxième partie « Audit informatique » consistera en une présentation de l'audit informatique après avoir passé en revue les caractéristiques d'un milieu informatisé.
- ♦ La dernière partie concernera un cas sur l'audit d'un logiciel de comptabilité dans une entreprise X

PREMIERE PARTIE : GENERALITES SUR L'AUDIT ET L'INFORMATIQUE

L'auditeur n'a commencé à s'intéresser à l'informatique que dans les années 1970 quand éclatèrent les premiers scandales financiers favorisés par des utilisations frauduleuses des ordinateurs. Dans un article paru en 1990, Lionel COLLINS cite le cas de EQUITY FUNDING ASSURANCE qui en 1973 « avait bourré ses fichiers informatisés avec des renseignements faux. L'objectif du dirigeant fut de maintenir la valeur de l'action en Bourse pour en tirer un profit personnel. Pour ce faire , il déclara des bénéfices fictifs tirés d'une clientèle inexistante ». La supercherie a été détectée grâce à un employé mécontent alors que la société disposait d'un auditeur externe. Comment ce dernier n'a pas pu relever cette irrégularité ? L'analyse de l'histoire de l'audit peut peut-être nous donner un début de réponse.

CHAPITRE I

L'EVOLUTION HISTORIQUE DE L'AUDIT

L'audit est né d'abord dans le secteur public avant de s'intéresser au secteur privé. Il a été historiquement une vérification des comptes dans un but de contrôle de régularité : le mot contrôle lui-même vient de « contre-rôle » du vieux droit administratif français. Il consistait à comparer des listes des soldats ou des dettes fiscales notamment, figurant sur des « rôles » (à l'époque des rouleaux de parchemins ou de papier) avec ce que le contrôleur constatait dans la réalité des effectifs ou des versements (GISCARD D'ESTAING, 1990). On voit que le contrôle repose sur l'idée de comparaison avec des références. Il en est de même de l'audit à son début surtout, mot issu des glissements de sens du verbe latin « audire » qui signifia d'abord entendre, écouter puis connaître et comprendre et enfin estimer, apprécier et évaluer. Pour évaluer après avoir écouté et compris, il faut aussi disposer d'une référence. Il ressort aisément que l'audit au début a comme objectif la régularité, la conformité par rapport à des références, des normes. Ceci permettait essentiellement de détecter les fraudes et les actes anormaux ; repérer les vols des clercs et mettre à nue les excès libertins des conseillers des rois. L'audit pendant cette période était commandité par les rois, empereurs, églises et les Etats.

Mais l'audit a évolué pour aller d'une recherche spécifique des fraudes dans les écritures comptables à une appréciation globale des procédures, des écritures comptables d'une organisation et des états financiers que celle-ci élabore. Le point de départ de l'audit peut se situer en France par exemple à partir du code commercial de Colbert en 1673, bien que l'obligation faite aux entreprises commerciales de se faire auditer annuellement date de 1867 quand fut créé le titre de commissaire aux comptes. A ce niveau encore, l'audit

financier présentait beaucoup de lacunes parce qu'il manquait de doctrine professionnelle précise : il a fallu en 1936 pour que les Commissaires aux Comptes se soient organisés en groupement national et que des règles , méthodes et pratiques en matière d'audit soient quelque peu clarifiées. Le tableau ci-dessous donne une synthèse de l'évolution de l'audit.

Tableau n°1 : Evolution de l'audit

Périodes	Prescripteur de l'audit	Auditeurs	Objectifs de l'audit
Avant 1700	Rois, empereurs, églises et états	Clercs ou écrivains	Punir les voleurs pour les détournements de fonds ; Protéger le patrimoine
De 1700 à 1850	Etats, tribunaux commerciaux et actionnaires	Comptables	Réprimer les fraudes et punir les fraudeurs. Protéger le patrimoine.
De 1850 à 1900	Etats et actionnaires	Professionnels de la comptabilité ou juristes	Eviter les fraudes et attester la fiabilité du bilan.
De 1900 à 1940	Etats et actionnaires	Professionnels d'audit et de comptabilité	Eviter les fraudes et les erreurs et attester la fiabilité des états financiers historiques.
De 1940 à 1970	Etats, banques et actionnaires	Professionnels d'audit et de comptabilité	Attester la sincérité et la régularité des états financiers historiques.
De 1970 à 1990	Etats, tiers et actionnaires	Professionnels d'audit et de comptabilité et du conseil	Attester la qualité du contrôle interne et le respect des normes comptables et normes d'audit.
A partir de 1990	Etats, tiers et actionnaires	Professionnels d'audit et du conseil	Attester l'image fidèle des comptes et la qualité du contrôle interne dans le respect des normes. Protection contre la fraude internationale.

Source : COLLINS et VALIN , 1992

A partir des objectifs assignés à l'audit durant ces six périodes, il est clair que la démarche des professionnels d'audit a dû subir des adaptations pour suivre cette évolution.

Au tout début, l'auditeur effectuait **un full audit** c'est à dire que toutes les écritures dans les comptes étaient comparées avec les pièces justificatives, elles mêmes vérifiées dans leur intégralité. Il effectuait un pointage en matérialisant ses contrôles par un signe devant chaque chiffre pour indiquer qu'il l'avait contrôlé. Les conditions pendant cette période le permettaient car en général le volume des transactions n'était pas très contraignant.

Il faut remarquer que la technique de pointage ne prouvait que le bon équilibre, elle ne permettait pas de s'assurer de la réalité de l'écriture (par exemple qu'une facture d'achat avait été précédée par une livraison des biens concernés). Cette méthode avait comme seul objectif de vérifier l'exactitude des comptes.

Très vite avec le temps, l'auditeur s'est confronté à des problèmes pour effectuer un full audit : volume des transactions dépassant nettement ses capacités pour honorer ses engagements en termes de délais, insuffisance des honoraires. C'est ainsi que **le contrôle analytique** fut imaginé . Il s'agit à partir de cet examen analytique d'aider à orienter l'auditeur vers les aspects sur lesquels il doit opérer un contrôle approfondi. Ce contrôle analytique consiste en une analyse comparative des comptes sociaux de l'entreprise avec ceux de l'année précédente pour en ressortir les aberrations et les écarts anomaux ; identifier les comptes à risques potentiels. Par exemple :

- Un accroissement notable des consommations intermédiaires sans rapport avec l'évolution du Chiffre d'affaires peut cacher un détournement des matières premières (comparaison des marges).
- Un compte débiteur qui aurait un solde ancien et qui n'aurait pas été mouvementé peut cacher un détournement de l'encaissement ou une créance fictive.
- Un accroissement de délais clients peut indiquer un problème de recouvrement des créances d'où un éventuel problème de provisions pour créances douteuses.

Le contrôle analytique a consisté, après, à élargir le champ de comparaison sur 3 ou 5 années. Il permettait ainsi d'attirer l'attention de l'auditeur sur les évolutions en dents de scie très prononcées et d'en tenir compte dans ces travaux. Par exemple, une évolution du résultat net qui va, d'année en année, d'un bénéfice à une perte de façon très aberrante peut indiquer un lissage du résultat pour des raisons inavouées ; c'est le cas de la modulation des provisions pour risques et charges qui consiste à surestimer ces charges pendant les périodes fastes et à les minimiser les années difficiles ceci d'autant que l'évaluation de ces pertes probables est à la discrétion des dirigeants de l'entreprise. Un changement de méthodes comptables peut aussi avoir le même effet. Aussi l'auditeur doit en être conscient et en tenir compte dans ses investigations.

L'examen analytique a ensuite évolué pour opérer des comparaisons dans l'espace avec des données de l'environnement dans lequel évolue l'entreprise à auditer : entreprises du même secteur, de même taille pour dégager les écarts anormaux sur le CA, productivité, frais de personnel, etc. Une autre forme de contrôle analytique consiste à comparer les postes du bilan par rapport au total et de décider de n'étudier que les postes ayant une certaine importance relative parmi les actifs de l'entreprise (par application de la loi de PARETO ou la méthode ABC par exemple).

Il faut remarquer que la technique de l'examen analytique ne permet que d'expliquer les soldes des comptes. C'est pourquoi aujourd'hui, les méthodes de travail intègrent **la circularisation** et l'assistance à **la prise d'inventaire** afin de justifier à la fois l'existence des actifs et les soldes des comptes.

D'autre part, la logique du contrôle analytique est de permettre à l'auditeur de justifier son choix d'échantillons des comptes à examiner. Or la méthode d'échantillonnage présente des lacunes intrinsèques comme toute méthode de sondage.

Pour pallier ces lacunes et surtout pour une meilleure orientation de l'audit, **l'approche par les systèmes** a vu le jour. C'est une approche qui se veut globalisante et consiste en l'évaluation du Contrôle Interne (Recommandation de l'OECCA) de l'entreprise à auditer. L'idée en filigrane dans cette approche est que si l'entreprise dispose d'un système de Contrôle interne très performant, si l'entreprise maîtrise parfaitement le solde d'un compte, l'auditeur pourra alléger très sensiblement ses travaux sur ce compte.

Mais il avait fallu pour ce faire définir le contenu du Contrôle interne. Ainsi l'OECCA (Organisation des Experts Comptables et Comptables Agréés) donne la définition suivante : « Le Contrôle Interne est l'ensemble des sécurités contribuant à la maîtrise de l'entreprise. Il a pour but, d'un côté d'assurer la protection, la sauvegarde du patrimoine et la qualité de l'information , de l'autre l'application des instructions de la Direction et de favoriser l'amélioration des performances . » (OECCA, 1977).

L'IFACI (Institut Français des Auditeurs et Consultants Internes) définit le Contrôle interne au travers de ses objectifs et souligne que « les objectifs du système du Contrôle interne sont d'assurer :

- la fiabilité et l'intégrité de l'information ;
 - le respect des politiques, plans, procédures, lois et règlements ;
 - la sauvegarde des biens ;
 - l'utilisation économique et efficace des ressources ;
 - la réalisation des objectifs et des buts attribués à une activité ou programme ».
- (IFACI, 1978).

Pour la CNCC (Compagnie Nationale des Commissaires aux Comptes), « le Contrôle interne est constitué par l'ensemble des mesures de contrôle comptable et autres que la Direction définit, applique et surveille sous sa responsabilité afin d'assurer :

- la protection du patrimoine;
- la régularité et la sincérité des enregistrements comptables et des comptes qui en

résultent ;

- la conduite ordonnée et efficace des opérations de l'entreprise ;
- la conformité des décisions avec la politique de la Direction ». (CNCC, 1984).

L'on peut aisément identifier deux aspects dans ces définitions :

D'abord les objectifs du contrôle interne que sont:

- *la maîtrise de l'entreprise*
- *sauvegarder les actifs*
- *assurer la qualité de l'information*
- *assurer l'application des instructions de la Direction*
- *favoriser l'amélioration des performances.*

Ensuite, c'est la Direction qui « *définit, applique et surveille sous sa responsabilité* » la mise en œuvre du contrôle interne.

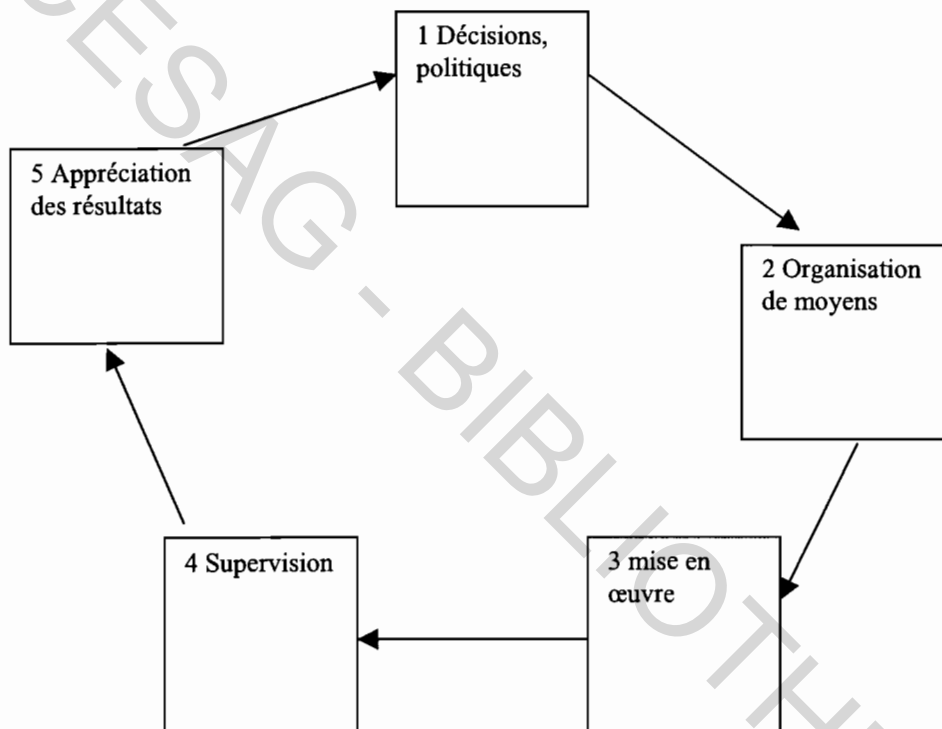
Enfin, il faut ajouter les moyens de mise en œuvre d'un Contrôle interne efficace que sont :

- *l'organisation des moyens et la supervision,*
- *les procédures,*
- *un personnel compétent et intègre.*

L'on peut donc dire que l'existence dans une entreprise d'un Contrôle Interne efficacement conçu et correctement appliqué est une sérieuse présomption de fiabilité de la comptabilité et que par conséquent l'auditeur pourra alléger ses autres travaux (notamment les travaux sur les comptes) dans cette entreprise. A contrario, si le Contrôle interne n'existe pas ou est mal conçu ou mal appliqué, cela laisse présumer que les comptes ne sont pas fiables ou, plus grave encore, que des éléments d'actif ont été détournés, bref que les comptes d'une telle entreprise ne sont pas dignes de confiance et que par voie de conséquence l'auditeur doit être très vigilant et approfondir éventuellement ses travaux avant de donner son opinion.

L'on voit ainsi tout l'intérêt de l'évaluation du contrôle interne et la démarche consiste à considérer l'entreprise comme un ensemble de systèmes (cycles) - d'où **l'approche par les systèmes**- et à les analyser en fonction des objectifs et des moyens du contrôle interne d'une part et d'autre part, de son application comme vus ci-dessus. Le cycle général d'une entreprise peut être schématisé comme suit :

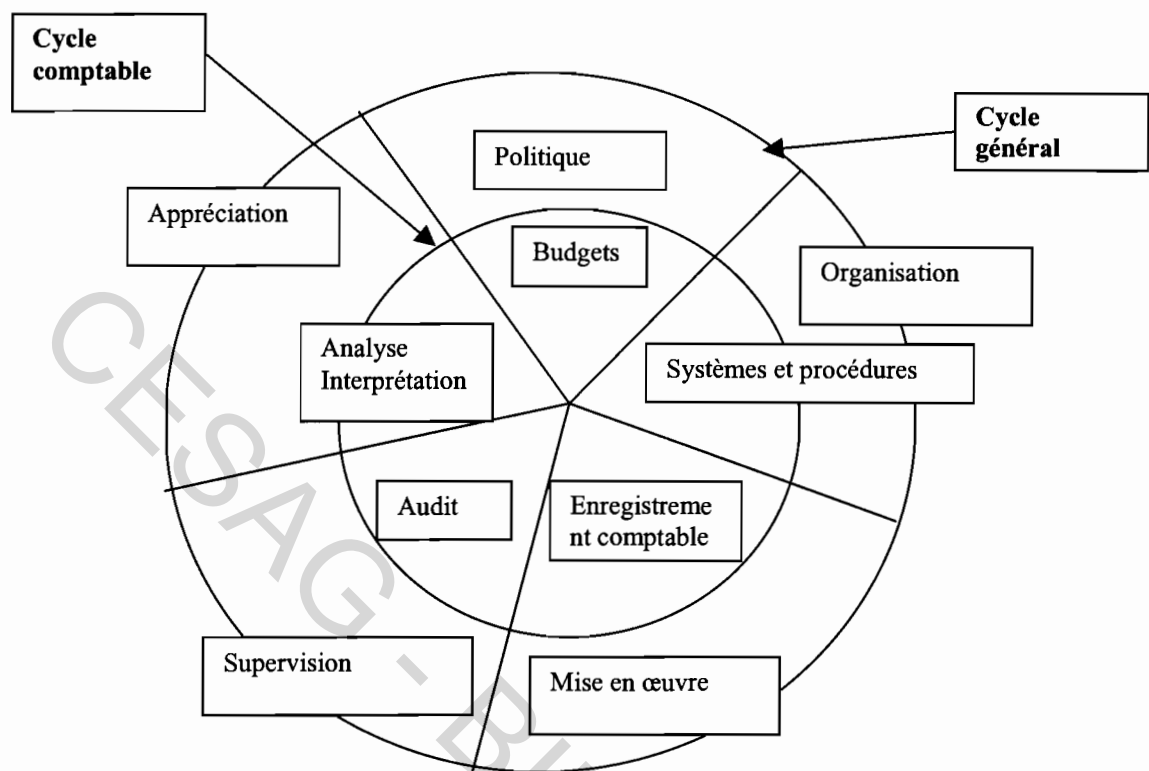
Figure n°1 : Cycle d'opérations de gestion



Source : COLLINS et VALIN, 1992.

Ainsi donc, l'on perçoit que toutes les opérations de l'entreprise dépendent de la mise en oeuvre de la politique de la direction , de l'organisation qu'elle a mise en place pour atteindre ses objectifs en passant par la supervision. Tous les cycles de l'entreprise (cycle ventes, cycle achats, cycle des immobilisations, cycle de trésorerie,...) peuvent être schématisés sous cette forme et ils s'intègrent parfaitement dans le cycle général. Nous prenons l'exemple du cycle comptable que l'auditeur aura à analyser.

Figure n° 2 : Cycle comptable encadré dans le cycle général



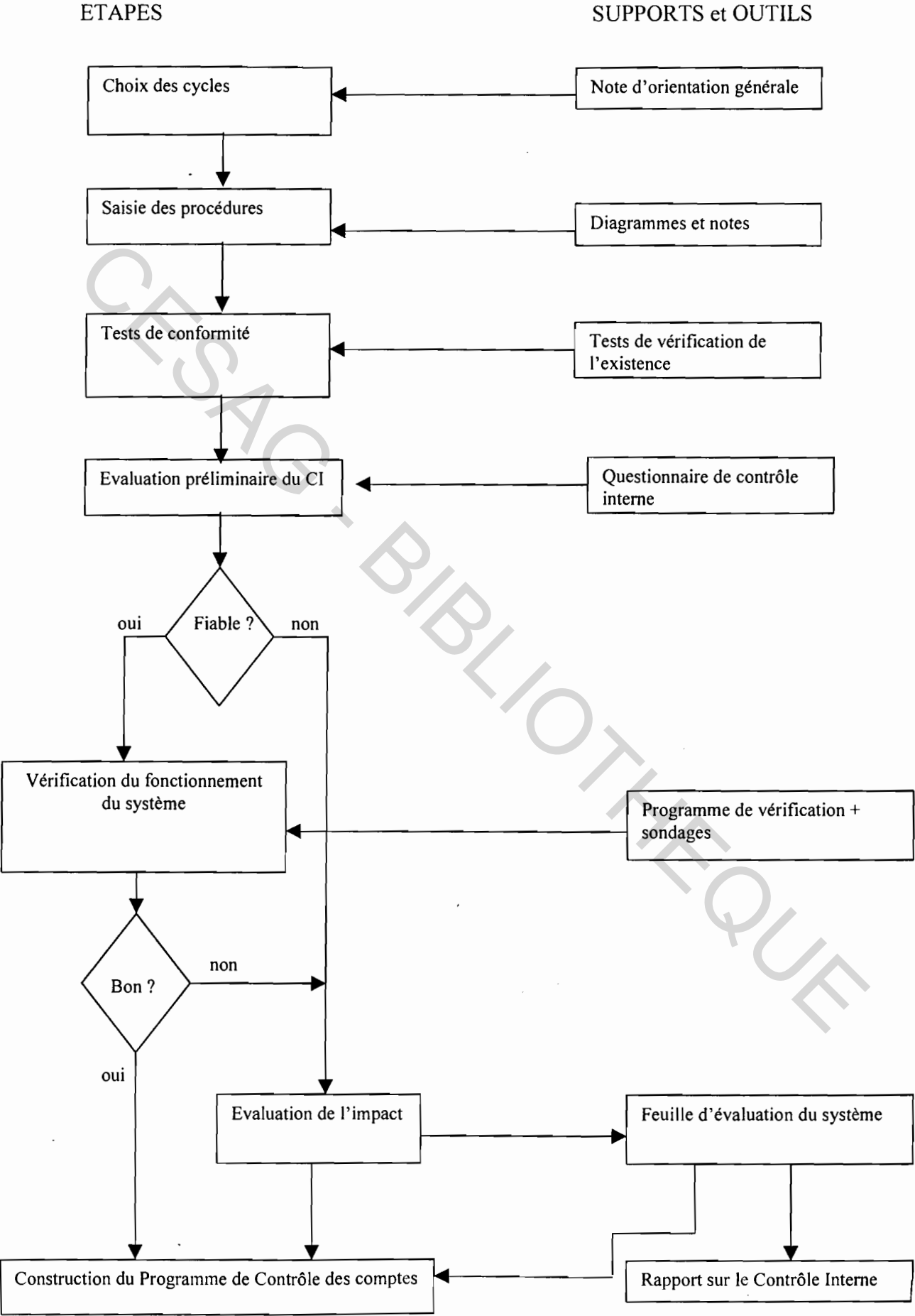
Source : COLLINS et VALIN, 1992, (adaptation)

Ainsi donc, la validité des informations comptables ne peut être valablement appréciée sans tenir compte des objectifs généraux et de la politique de l’entreprise et de son organisation et manuels de procédures.

Mais comment l’auditeur procédera-t-il à cette analyse du contrôle interne ?

Le schéma ci-dessous (inspiré de DIALLO, 1999) indique les différentes étapes de l’appréciation du contrôle interne, appréciation qui a été rendue obligatoire par l’OECCA dans sa recommandation N°1 en matière de « normes de révision comptable ».

Figure n° 3 : Appréciation du contrôle interne



Le diagramme ci-dessus indique que les phases nécessaires à l'évaluation du contrôle interne peuvent se résumer comme suit :

- Saisie des procédures
- Tests de conformité
- Evaluation préliminaire du Contrôle interne
- Tests de permanence
- Evaluation définitive du Contrôle interne
- Rapport sur le Contrôle interne

1. Saisie des procédures

Elle consiste à découper l'entreprise en ses différents systèmes étant entendu que chaque système reprend des opérations homogènes et susceptibles d'un même type de contrôle (par exemple, le cycle achats ne prend en charge que les opérations d'achats et uniquement elles). Il s'agit donc d'une prise de connaissance des procédures. Si les procédures ne sont pas formalisées, l'auditeur doit les décrire. Pour ce faire, il utilise soit le diagramme de circulation (flow chart) soit la méthode narrative. Le premier présente l'avantage de mieux visualiser les bris (ruptures) des séquences dans le déroulement des opérations mais surtout les vides dans la compréhension des procédures par l'auditeur.

2. Tests de conformité

Aussi appelés tests d'existence ou de compréhension, ils consistent à confirmer la compréhension des procédures décrites. Cela permettra, le cas échéant, de rectifier la description des procédures que l'auditeur a consignées. Pour ce faire, il sélectionne une ou deux transactions pour chaque type de cycles dont il suivra le cheminement à travers les procédures décrites tout en s'assurant du respect des traitements et contrôles prévus. La transaction est ainsi testée du « berceau à la tombe ».

3. Evaluation préliminaire du contrôle interne

Une fois qu'il a acquis la certitude de l'existence effective des procédures, l'auditeur a besoin de se fixer sur la fiabilité des systèmes. En d'autres termes, il est amené à vérifier le fonctionnement des procédures.

Pour ce faire, il établit un Questionnaire de Contrôle Interne (QCI) qui lui permettra d'identifier les points faibles et les points forts des systèmes de l'entreprise.

En cas de faiblesses, il y a lieu de les discuter avec le client pour s'assurer s'il n'existe pas de contrôles alternatifs ou compensatoires. A défaut de ces contrôles, il convient d'évaluer les incidences des faiblesses décelées sur la nature et l'étendue des contrôles à effectuer. Par ailleurs, ces faiblesses doivent être signalées au client dans le rapport sur le Contrôle Interne. En ce qui concerne les points forts, leur existence théorique doit être confirmée pour qu'ils puissent être considérés comme tels. L'auditeur procède alors à des tests permanence.

4. Tests de permanence

Appelés aussi tests de bon fonctionnement, les tests de permanence consistent à s'assurer que les points forts mis en évidence précédemment font l'objet d'une application permanente et non isolée ou sporadique. Ainsi, l'auditeur fait des sondages :

- sur les opérations pour voir si tous les contrôles prévus sont effectués de façon correcte ;
- sur l'exécution pour s'assurer que les opérations de contrôles ont été effectuées par des personnes autorisées à cet effet.

Au cours de ces tests, des faiblesses peuvent apparaître et l'auditeur doit en déterminer l'incidence possible sur les états financiers et sur l'étendue des travaux à effectuer lors des contrôles des comptes et en discuter avec le client avant de procéder à l'évaluation définitive du contrôle interne.

5. Evaluation définitive du contrôle interne

Le réviseur est à même maintenant d'avoir une connaissance précise de l'ensemble des procédures théoriques et pratiques afin de faire une synthèse sur :

- les points forts réels
- les points faibles dus à un défaut dans la conception du système et
- les points faibles inhérents à une mauvaise application des procédures.

L'auditeur doit en discuter avec le client avant de rédiger son rapport définitif sur le contrôle interne.

6. Rapport sur le Contrôle interne.

Ce rapport doit être le reflet de la synthèse des discussions eues avec le client. Il constitue les termes des derniers entretiens et son contenu doit traduire les divers aspects de la révision : faiblesses constatées, conséquences, recommandations et éventuellement les commentaires du client.

Le contrôle interne est, pour l'auditeur, la base d'élaboration du Programme du Contrôle des Comptes et des suggestions d'axes d'amélioration.

Le dernier raffinement de la démarche par les systèmes est **l'approche par les risques**.

L'idée est de considérer que l'entreprise est un ensemble de risques. En effet, on peut lister une multitude de risques que les états financiers soient inexacts dans une entreprise

(COLLINS et VALIN, 1992) :

- risques liés à la qualité d'informations saisies,
- risques liés à l'exhaustivité des informations saisies,
- risques d'insécurité du patrimoine,
- risques commerciaux et du marché,
- risques sociaux et fiscaux,
- etc.

Ainsi donc, l'auditeur, après son analyse initiale, peut centrer son travail là où il prévoit les plus grands risques en valeur absolue.

Il n'est pas aisé de dater ces différentes étapes d'évolution de la démarche d'audit surtout que, aujourd'hui encore, l'auditeur les combine au besoin pour mieux effectuer ses missions.

Mais peut-il se contenter de cette combinaison face à l'avènement de l'informatique dans le traitement des informations financières ? Ne se trouve-t-il pas face à d'autres contraintes ?

C'est l'objet du chapitre qui suit.

CESAG - BIBLIOTHEQUE

CHAPITRE II

L'AUDIT A L'AVENEMENT DE L'INFORMATIQUE

A l'avènement de l'informatique dans les années cinquante, l'auditeur avait cru que l'ordinateur n'était qu'un outil comme une simple calculette. Pourtant, il occupe une place de grande importance dans tous les sous systèmes de l'entreprise.

1. Place de l'ordinateur dans les systèmes

L'ordinateur a envahi tous les aspects de l'entreprise. On le trouve à :

- La production : où il commande la fabrication des produits, lance ou arrête les machines, détecte les anomalies au cours de la fabrication.
- La vente : il établit les factures à partir des bons d'expédition, gère les fiches des clients, vérifie le niveau des crédits ou solvabilité des clients, analyse l'ancienneté des créances, relance les mauvais payeurs et génère des écritures comptables.
- La gestion de stocks et achats : pour déclencher les achats après vérification du niveau du stock, analyser les statistiques des stocks, optimiser les commandes, assainir le fichier des stocks, calculer les dépréciations et générer des écritures comptables y afférentes.
- La paie : gère les dossiers individuels du personnel, calcule la paie, déclenche certaines opérations (droits aux congés, indemnité de retraite, ...), édite les bulletins de paie et les journaux de salaire, génère les écritures comptables y afférentes,
- La comptabilité : il centralise les écritures générées et autres, contrôle l'équilibre

des écritures, élabore des journaux, balances et dresse les états financiers.

- Les budgets : effectue les comparaisons budgets/réalisations, propose une analyse des écarts et des solutions, fait des projections avec des simulations en un temps record.
- etc.

D'autre part, l'ordinateur impose, dans la plupart des cas, une nouvelle fonction dans l'organisation structurelle. C'est la fonction informatique qui sera chargée du suivi de tous les traitements informatiques, de la maintenance des ordinateurs et des programmes, du développement des applications et des actions de protection des données, cet élément essentiel à la survie de l'entreprise.

La fonction informatique est donc une fonction intégratrice, un carrefour de toutes les autres fonctions où tous les traitements peuvent être centralisés dans une certaine mesure.

De plus, l'ordinateur impose un personnel spécialisé dont le langage n'est pas forcément compris par la majorité des membres du personnel. Plus délicat encore, leurs tâches et responsabilités ne sont pas aisées à identifier par le management.

Malgré tout au début, pour l'auditeur, cette situation ne devait en rien engendrer une modification de l'approche de l'audit.

Considérant l'ordinateur comme une simple calculatrice, il s'est contenté d'effectuer ses missions d'audit « autour de l'ordinateur ». Il perdait ainsi de vue les risques inhérents à l'informatique.

2. Risques inhérents à l'informatique

Ces risques peuvent être résumés comme suit :

- risques liés à la séparation des tâches : au niveau d'un service informatique, le principe de la séparation des tâches, cher à l'auditeur, n'est pas toujours appliqué surtout dans les petites structures. Un même individu peut avoir la possibilité (ou même le droit) de faire la saisie, le traitement, le transfert et l'archivage des données traitées. Un même informaticien peut avoir la responsabilité de développer, exploiter et de maintenir les applications. Dans ces conditions, on imagine la tentation que doit subir un employé s'il maîtrise tout le cycle du traitement de son propre salaire !
- risques techniques : les programmes informatiques sont des œuvres humaines qui peuvent par conséquent être sujettes à des défauts de fabrication ou des erreurs de nature à altérer complètement les informations qui en seront générées. Ainsi, il arrive que l'auditeur constate à sa grande surprise, l'absence de contrôles élémentaires dans les états générés par les applications informatiques. On peut donner des exemples à ce niveau : totalisations erronées, écritures comptables déséquilibrées, centralisations fausses, etc..

De plus, une erreur dans une application revêt un caractère systématique : en effet, une erreur d'un taux d'amortissement donné va fausser tous les amortissements de toutes les immobilisations de même nature. Ainsi donc, les documents informatiques ne sont pas systématiquement plus fiables que les documents manuels. Les risques techniques ne se limitent pas aux programmes : le hardware (y compris les supports) requiert une sécurité et une protection accrues du fait qu'il gère l'élément vital de l'entreprise à savoir son information. En effet, sans mesures de sécurité et de protection physique des locaux, des accès, de duplication et de sauvegarde, la disponibilité et la pérennité de l'information ainsi que son intégrité et sa confidentialité ne seront pas garanties.

Il apparaît clairement que donner son opinion sur des états financiers sur la base d'un audit 'autour de l'ordinateur' présente des risques énormes pour l'auditeur. Mais ce sont surtout les

fraudes informatiques constatées par-ci, par-là, qui vont faire évoluer la vision des professionnels par rapport aux risques que recouvre l'ordinateur pour le réviseur .

PETIT (1997) rapporte que « l'enquête conduite par l'Audit Commission en Angleterre en 1993 sur les infractions en milieu informatisé fait état d'une progression de 38% du nombre de cas de fraude recensés par rapport à la précédente enquête en 1990. L'enquête annuelle 1996 menée conjointement par Informationweek et Ernest & Young LLP aux USA, également en milieu informatisé, fait apparaître que 32% des entreprises ayant répondu ont été victimes d'un acte de malveillance interne, 18% d'un acte de malveillance externe. »

Les fraudes informatiques concernent surtout les bourrages des fichiers (voir supra), la suppression des écritures comptables sans laisser de traces, l'accès à des informations par des personnes non autorisées, la copie de fichiers au profit d'un concurrent, la programmation d'avantages salariaux non autorisés, etc.

A partir des constats des fraudes informatiques, une modification des normes professionnelles s'imposa pour rendre exceptionnel « l'audit autour de l'ordinateur » et proposer de faire « l'audit à travers l'informatique ». Ainsi est né l'AUDIT INFORMATIQUE qui consiste à vérifier le bon fonctionnement des systèmes informatiques et l'efficacité des contrôles intégrés dans les applications afin de donner une opinion en toute connaissance de cause sur les états financiers ainsi produits.

Il constituera, à travers les pages qui suivent, l'objet de la deuxième partie de ce travail.

DEUXIEME PARTIE : L'AUDIT INFORMATIQUE

INTRODUCTION

La notion de l'audit informatique est très vaste. Chacun y met ce qu'il veut comme dans toute notion nouvelle. Il n'y a pas encore une unanimité de vue sur ce concept. LEGER (1989) souligne que les domaines de l'Audit Informatique « peuvent concerner divers aspects du système d'informations de l'entreprise » dont :

- **Audit du schéma directeur** : un schéma directeur détermine le plan d'ensemble pour les implantations à venir et vise à fixer une politique cohérente en matière de machines, logiciels, personnel. Ainsi, l'audit du schéma directeur vise à s'assurer que la démarche suivie est cohérente et ne laisse de côté aucun aspect fondamental. Notamment, il permet d'éviter une informatisation sauvage dans l'entreprise.
- **Audit de projet** : un projet peut être, par exemple, l'informatisation de l'exploitation informatique, la mise en place d'une nouvelle application, l'installation de messageries, le raccordement à des réseaux... L'audit d'un projet vise à s'assurer que la démarche suivie est cohérente et conforme aux règles de l'art.
- **Audit de l'application** : l'audit, cherchant à restituer une image fidèle de la réalité, va donner une vision synthétique du fonctionnement de l'application et relèvera des dysfonctionnements. L'audit permet ainsi d'évaluer le décalage entre les objectifs fixés et le fonctionnement actuel (voir infra).
- **Audit de SGBD (Système de Gestion de Base de Données)**: l'audit indique l'efficacité du SGBD, le nombre de données aberrantes ou d'anomalies dans la base et l'image de la structure actuelle de la base des données.

- **Audit du réseau:** l'audit d'efficacité du réseau est l'examen d'un accès à une donnée, d'une mise à jour ou d'un transfert de données à partir d'un écran ; il indique aussi le pourcentage d'erreurs, les protocoles de communications utilisées, les sécurités existantes.
- **Audit du centre de traitement :** l'audit peut porter non seulement sur l'adéquation de l'implantation physique aux besoins, mais aussi sur la planification et la préparation des travaux et plus particulièrement sur l'ensemble des procédures de lancement et d'arrêt de la machine, de sauvegarde, de bascule d'une bibliothèque d'études sur la bibliothèque d'exploitation et le chargement des supports mémoires. L'audit décrit alors ces procédures, vérifie si elles sont appliquées et note les insuffisances en émettant les recommandations correspondantes s'il y a lieu (voir infra).

Quant à Gérard POMPER (1990 : 34) , il considère l'audit de l'informatique comme « l'audit – comptable et financier – dans un système d'informations largement automatisé ». STOLOWY (1990) de son côté, met en garde contre la confusion souvent faite entre « l'audit de l'informatique (audit des procédures informatisées et des systèmes informatiques) et «l'audit réalisé à l'aide de l'informatique ».

Ainsi donc, les missions d'audit informatique peuvent revêtir un caractère d'audit opérationnel (optimiser les performances, les coûts,...) et un caractère d'audit financier (garantir la fiabilité , l'exactitude et l'exhaustivité des informations).

Compte tenu de ce large éventail de définitions souvent données à la notion d'Audit informatique, il nous a paru indispensable d'opérer un choix et de centrer notre travail sur **l'audit des systèmes comptables tenus par l'informatique**. L'IFAC (International Federation of Accountants) parle à ce niveau de l'audit dans un milieu informatisé et souligne que : « un milieu est dit informatisé lorsqu'un ordinateur, quels que soient son type ou sa

taille, 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 ».

Un tel système a une importante incidence sur les contrôles internes de l'entreprise; par conséquent, l'auditeur doit en tenir compte avant de donner son opinion sur les états financiers.

Le chapitre qui suit a pour objet justement de développer les caractéristiques essentielles et les incidences sur le système comptable et les contrôles internes d'un milieu informatisé.

CHAPITRE I

CARACTERISTIQUES D'UN MILIEU INFORMATISE

Un milieu informatisé est un système d'informations pris en charge dans une grande mesure par un ordinateur. Si l'on considère un système d'informations comme « un tout » composé d'une organisation, d'un personnel, des procédures, méthodes et pratiques dans une entreprise donnée, l'on perçoit aisément que l'implication de l'ordinateur est de nature à bouleverser de façon notable les composantes de ce système d'informations. En effet, l'ordinateur vient inévitablement modifier la structure organisationnelle, remplacer l'homme dans certaines tâches notamment pour accélérer le traitement de l'information, effectuer des opérations répétitives, des contrôles mécaniques et imposer une nouvelle conception des procédures et de séparation des tâches.

Ainsi, un système informatisé peut être décomposé en 6 sous-systèmes successifs, chaque sous-système incluant les précédents:

Sous système 1 : Matériel

Ce système est composé des matériels informatiques (hardware) : unité centrale, périphériques d'entrée, périphériques de sortie.

Le bon fonctionnement de ce système dépend surtout de la qualité des services après vente qu'offre le fournisseur ou le constructeur mais aussi du contrat de maintenance et de l'utilisateur qui doit faire fonctionner le matériel dans les conditions prévues.

Pour la maintenance, il est préférable de n'avoir qu'un interlocuteur quand cela est possible afin d'éviter le « rejet de faute » et la dilution des responsabilités.

Sous système 2 : Logiciel de base

Ce système inclut le système précédent auquel viennent s'ajouter le logiciel de base (Operating System) et les utilitaires utilisés ou utilisables par les applications.

Le bon fonctionnement de ce système dépend :

- du bon fonctionnement du sous système 1
- de l'efficacité du logiciel de base et des utilitaires
- de la qualité de l'adéquation entre ces logiciels et le matériel

L'on constate que la responsabilité du bon fonctionnement commence à être dispersée : constructeurs du matériel, concepteur des logiciels, fournisseurs.

Sous système 3 : Logiciels d'application

Ce système inclut le système précédent en plus des logiciels d'application (logiciels comptables, de gestion des stocks, de gestion des immobilisations, excell, word). Les conditions de son bon fonctionnement sont les mêmes que celles vues précédemment auxquelles vient s'ajouter la qualité de ces logiciels d'application.

Sous système 4 : Les manipulateurs

C'est le premier sous système qui fait intervenir la composante humaine. Il comprend le précédent et intègre les manipulateurs. Ces derniers peuvent être définis comme étant les personnes qui ont un contact physique avec le matériel et une relation directe avec les traitements. Il peut s'agir du personnel de saisie ou de pupitrage du service informatique ou le personnel de saisie et de traitement informatisé chez les utilisateurs.

Si le système précédent fonctionne convenablement, les conditions du bon fonctionnement de ce sous système dépendent des points suivants :

- les manipulateurs sont-ils convenablement formés à l'utilisation des traitements,

du matériel qu'ils utilisent ;

- sont-ils conscients de la place de leur travail dans l'ensemble de l'application ;
- sont-ils informés et conscients des incidences de la qualité de leur travail sur d'autres travaux ;
- ont-ils une vue générale des traitements réalisés par l'application des données traitées ;
- sont-ils motivés à leur travail informatique ?

L'introduction de la composante humaine à cette étape entraîne des difficultés à retracer les zones de responsabilités. Pourtant, cette responsabilisation est primordiale pour réaliser efficacement le bon fonctionnement de ce système et par suite de l'application.

Sous système 5 : Les fournisseurs/clients internes d'informations

Ce système inclut le précédent auquel viennent se rajouter les fournisseurs/clients internes d'informations. Ce sont les personnes qui fournissent directement aux manipulateurs les informations à introduire d'une part et les personnes qui reçoivent des informations directement des manipulateurs.

Par ce fait, de nouveaux problèmes viennent s'ajouter à ceux identifiés au sous système 4 dont :

- ces personnes sont-elles conscientes du rôle joué par la qualité des informations fournies sous leur responsabilité ;
- sont-elles informées des résultats qu'elles peuvent attendre de l'application ;
- ont-elles intégré l'outil informatique à leurs tâches , l'utilisent – elles au mieux ;
- souhaitent-elles et font-elles évoluer leurs postes et leurs travaux ?

Dans ce système, on peut inclure un autre ensemble de personnes appartenant à l'organisation ne prenant qu'une part minime aux traitements et données de l'application mais jouant un rôle

important. C'est le cas des décideurs de l'organisation, des auditeurs internes examinant l'application. L'opinion des personnes sur une application peut avoir une grande importance sur le jugement de qualité de l'application dans l'organisation et entraîner des effets non négligeables.

Notons enfin que la nature des relations interpersonnelles peut influencer sur la qualité des applications et les rendre parfois inefficaces.

Ce système est considéré dans la plupart des cas comme « le système informatisé total » et celui dont on contrôle le bon fonctionnement. Toutefois, il existe d'autres personnes qui jouent un rôle dans l'application et qui peuvent présenter des contraintes importantes du système.

Sous système 6 : Les fournisseurs/clients externes d'informations

Ce système inclut le précédent et un ensemble d'entités ou de personnes n'appartenant pas à l'organisation mais qui peuvent avoir des influences sur la conception des applications. Ce sont par exemple :

- les contrôleurs externes
- les commissaires aux comptes
- les organismes sociaux
- la législation ou les règlements (ex : nouveau plan comptable, taux de TVA, ..)

L'auditeur, pour mener à bien sa mission dans un milieu informatisé, doit comprendre et évaluer les caractéristiques du Système Informatisé et ses incidences sur la conception du système comptable et de ses contrôles internes.

Ces incidences peuvent être classées (SARR, 1999) en fonction de :

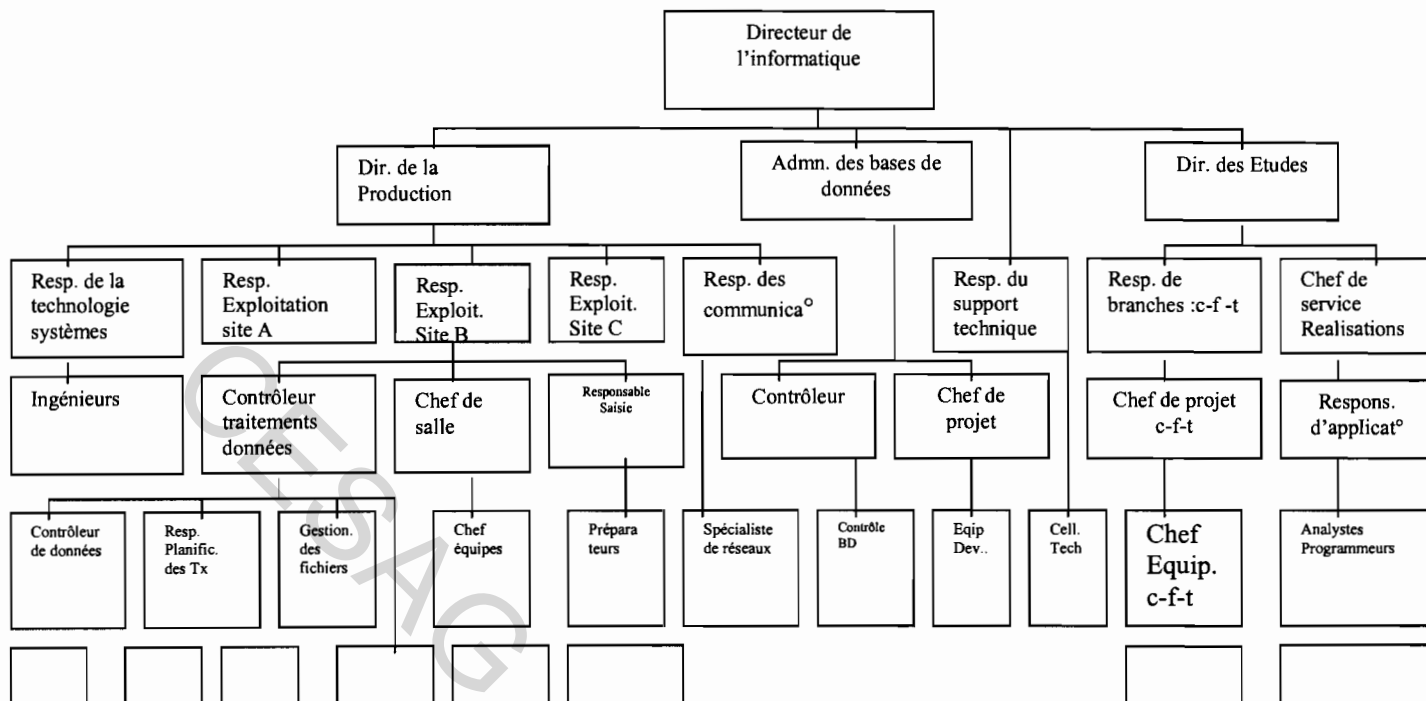
◇ La structure organisationnelle

- ◇ Les traitements
- ◇ La conception des procédures

1. INCIDENCES SUR LA STRUCTURE ORGANISATIONNELLE

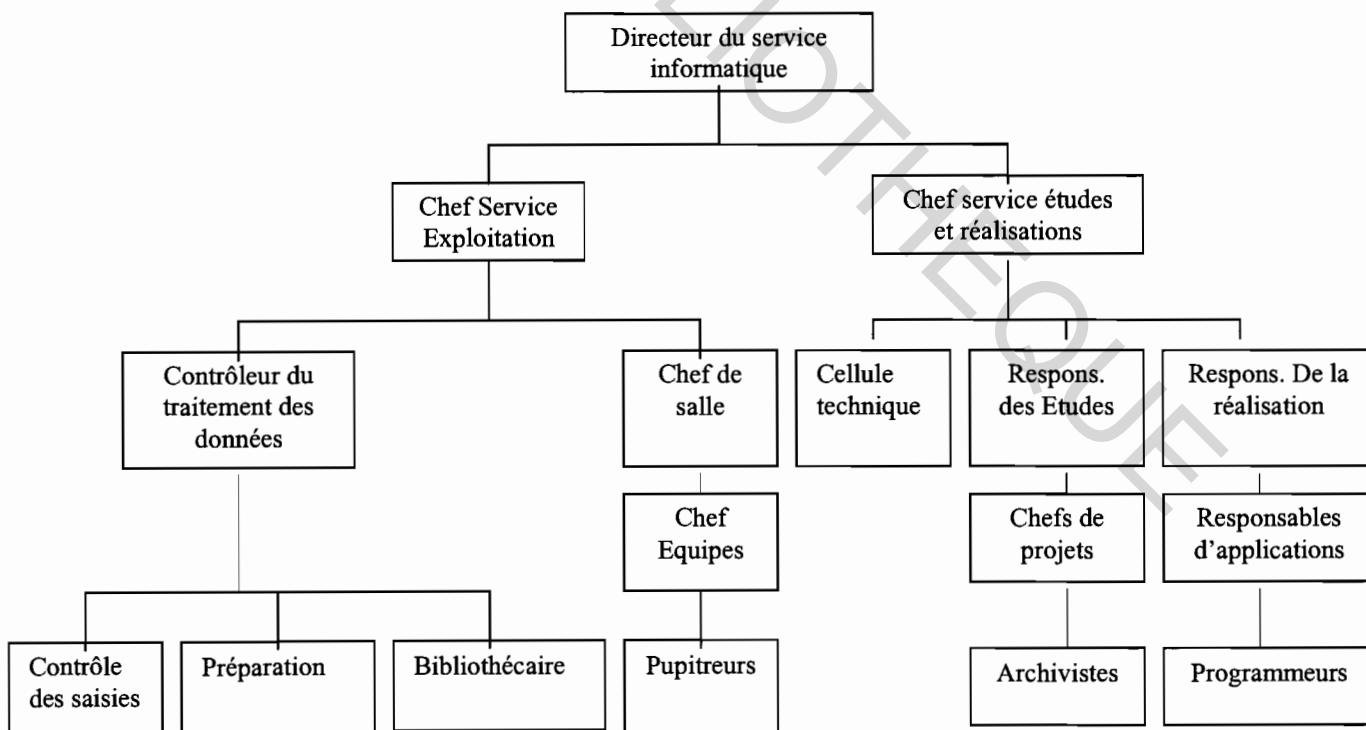
Une entreprise qui produit ses informations financières à l'aide d'un système informatisé est contrainte de repenser sa structure organisationnelle pour intégrer efficacement l'administration de ces activités informatiques. C'est ainsi que selon la complexité du système informatique et de la taille de l'entreprise, on rencontre des structures informatiques érigées en Département, Direction directement rattachés à la Direction Générale ou en Service, Division rattachés à la Direction Comptable ou Financière. De même, la configuration de ces structures diffère d'une entreprise à une autre comme le montrent les trois (3) organigrammes dans les pages ci-après.

Figure n°4 : Organigramme type d'un grand centre informatique



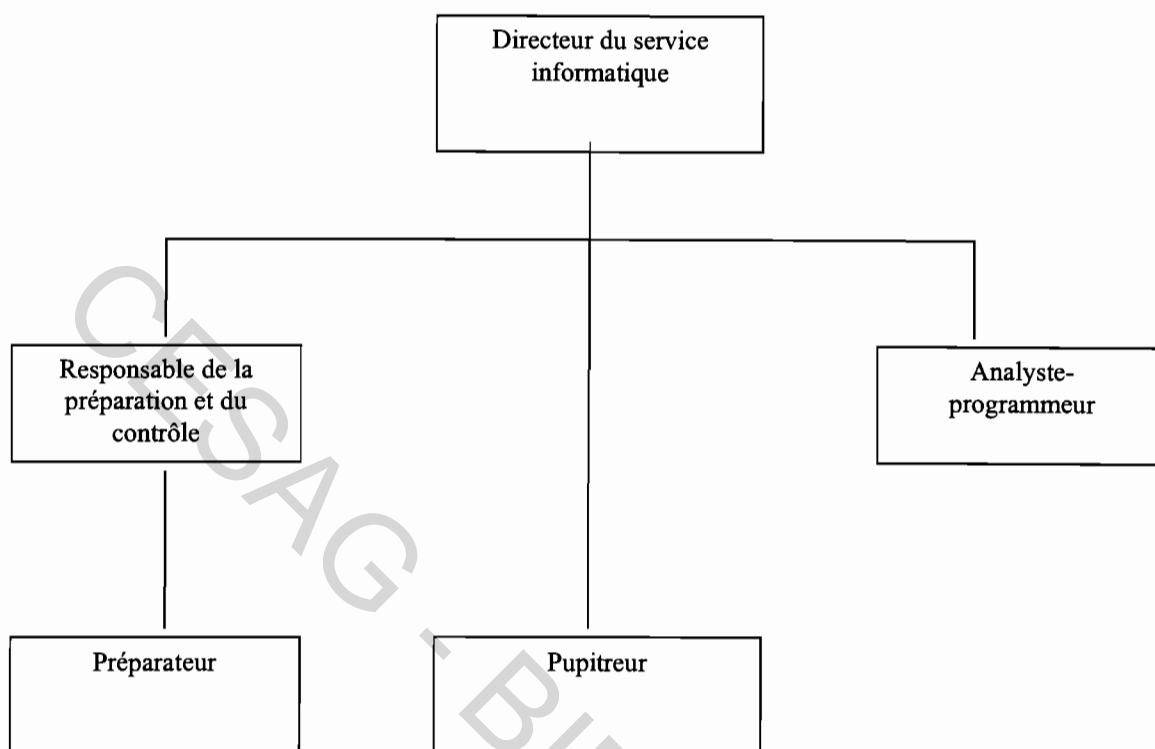
Source : Roy et Gaudron, 1984

Figure n°5 : Organigramme type d'un centre informatique moyen



Source : Roy et Gaudron, op. cit.

Figure n°6 : Organigramme type d'un petit centre



Source : op. cit.

En général, le personnel informatique est le seul à connaître parfaitement l'interdépendance entre les sources des données, leur mode de traitement, leur sortie et leur utilisation. Il peut connaître par conséquent les faiblesses du contrôle interne informatique et peut-être en abuser. Ceci est surtout valable dans les structures simplifiées c'est à dire là où la séparation des fonctions incompatibles n'est pas satisfaisante.

2. INCIDENCES SUR LES TRAITEMENTS

Dans un système informatisé, certains éléments essentiels du contrôle interne peuvent disparaître. C'est le cas des pièces justificatives de certaines tâches : les écritures comptables peuvent être automatiquement générées par le système informatique sans documents de base

(par exemple : les écritures comptables relatives aux droits aux congés annuels sont générées automatiquement après 12 mois de travail).

De plus, on peut accéder à des données et des programmes sans laisser des traces.

Ainsi, s'il n'y a pas de contrôles programmés adéquats, cela présente des risques quant à la fiabilité des informations que le système produit.

3. INCIDENCES SUR LA CONCEPTION DES PROCEDURES

Dans un système informatique, la conception des procédures doit être repensée pour tenir compte de ses caractéristiques :

- l'uniformité du traitement : les systèmes informatisés exécutent leurs fonctions exactement selon le programme et de façon systématique,
- l'informatique permet d'intégrer dans le programme, des procédures du contrôle interne,
- la possibilité de mise à jour de plusieurs fichiers à partir d'une seule opération,
- l'exploitation par plusieurs personnes d'une même base de données,
- la vulnérabilité des supports de conservation des données et des programmes : vol, détérioration intentionnelle ou accidentelle.

Quel est alors l'impact d'un milieu informatisé sur le déroulement de la mission de l'auditeur.

Comment l'auditeur doit-il adapter sa démarche pour tenir compte de toutes ces caractéristiques ?

C'est l'objet du chapitre qui suit.

CHAPITRE II

DEMARCHE DE L'AUDIT INFORMATIQUE¹

Comme nous l'avons souligné ci-avant, nous entendons par Audit Informatique, l'Audit financier en milieu informatisé. Mais avant de voir la démarche que doit adopter l'auditeur, il nous paraît important d'identifier les normes d'audit en milieu informatisé.

I. NORMES D'AUDIT EN MILIEU INFORMATISE

Les normes générales d'audit sont au nombre de cinq (ATH, IFAC-1985):

- Indépendance
- Compétence
- Etendue et nature des travaux
- Planification et exécution des travaux
- Gestion du service d'audit

Par rapport à l'audit en milieu informatisé, la CNCC dans sa délibération du 7 juillet 1983 (Bulletin CNCC n°51) a fait une recommandation selon laquelle l'existence des systèmes d'information et de procédures de contrôle interne automatisés ne change pas les objectifs de la mission des auditeurs et des commissaires aux comptes. Cependant l'automatisation :

◆ appelle un complément des normes de travail de l'auditeur et plus particulièrement sur les points suivants :

- Plan d'approche de l'audit
- Nature et étendue de l'appréciation du CI

¹ Inspirée essentiellement de ROY et GAUDRON, op. cit. et A. DIARRA sur la pratique d'audit en milieu informatisé.

- Planification des travaux
- Compétence
- ◆ exige une adaptation de la démarche de l'auditeur pour prendre en compte l'ensemble des caractéristiques nouvelles.

De cette recommandation, il ressort que (DIARRA, 1994):

- Pour établir un plan d'approche en milieu informatisé, l'auditeur doit tenir compte des procédures relatives à la fonction informatique et des procédures relatives aux applications qui génèrent les informations comptables. Cela suppose une prise de connaissance de l'environnement informatisé.

- L'auditeur en milieu informatisé doit « évaluer à la fois le contrôle interne de la fonction informatique et le contrôle interne des applications ».

Pour la fonction informatique, il s'agit de s'assurer que les procédures relatives à la protection de l'intégrité des données, des programmes et du matériel, au développement et à l'exploitation des traitements garantissent de façon satisfaisante :

- la protection du patrimoine,
- la continuité des travaux du service informatique,
- la fiabilité des informations produites.

Pour les applications, l'auditeur doit s'assurer des contrôles suivants :

- contrôles des saisies,
- prévention contre les erreurs et les fraudes pendant le traitement,
- pertinence de la documentation sur les applications,
- contrôles pour s'assurer de l'exactitude et de l'autorisation des opérations ,
- disponibilité d'un fichier 'log'

- Le commissaire peut intervenir à priori. La CNCC précise que « le Commissaire aux comptes peut demander à être consulté lors de la mise en place ou lors de toute modification du système afin de s'assurer que les modalités de contrôles nécessaires ont bien été prévues ».
- L'auditeur a aussi la possibilité d'utiliser les techniques informatiques pour procéder aux travaux d'audit. C'est la notion d'audit assisté par ordinateur qu'il ne faut pas confondre avec l'audit informatique.
- Il a aussi la faculté de faire appel à un spécialiste mais la CNCC est claire sur cet aspect du point de vue responsabilité du commissaire. En effet, elle précise que « le commissaire reste seul responsable de la mission et doit garder la maîtrise du contrôle , même s'il fait appel à des collaborateurs ou des experts »

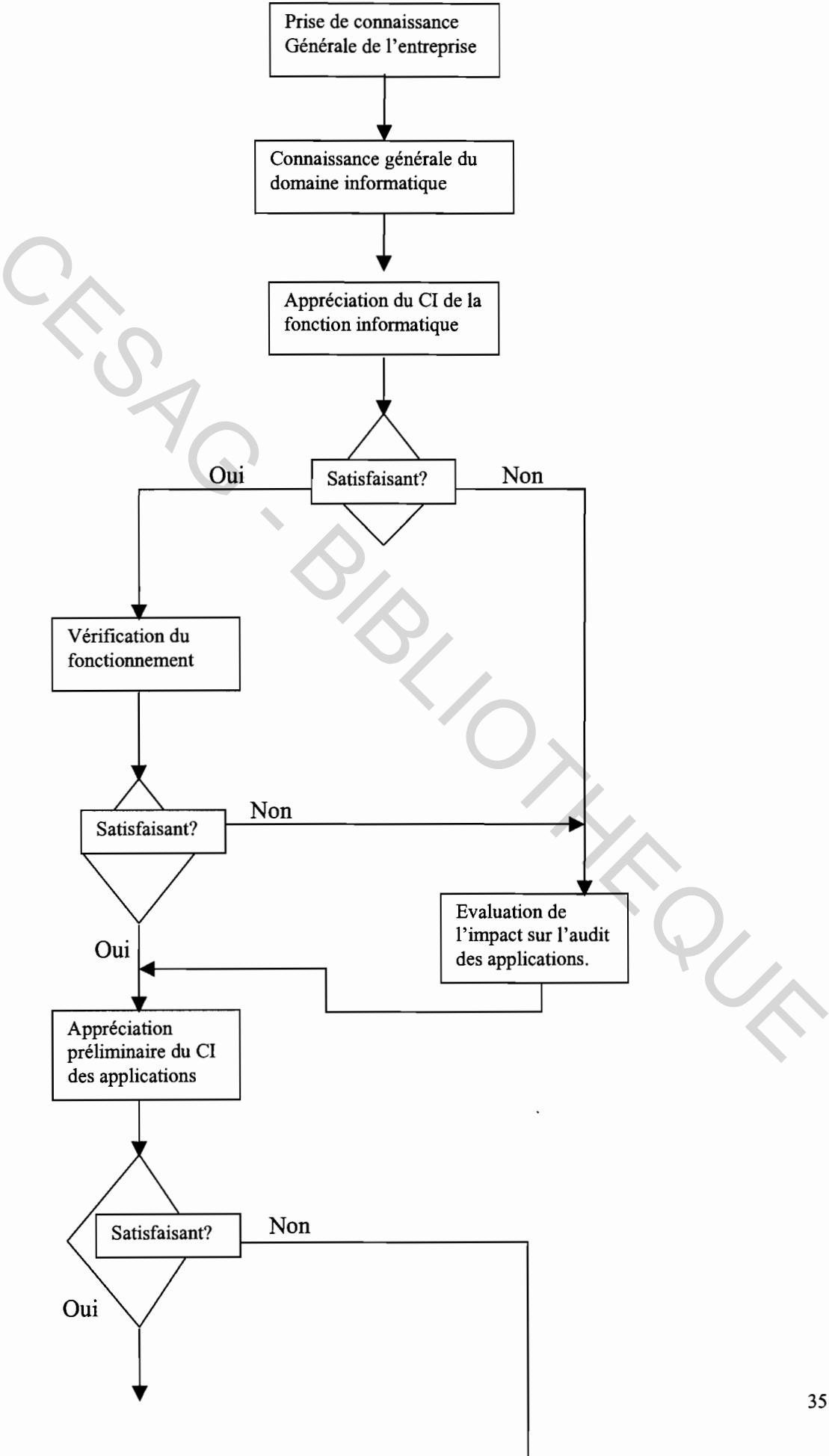
Il est intéressant de remarquer que c'est seulement en 1983 que la CNCC s'est intéressée à la question de l'audit face à l'informatique par sa recommandation vue supra.

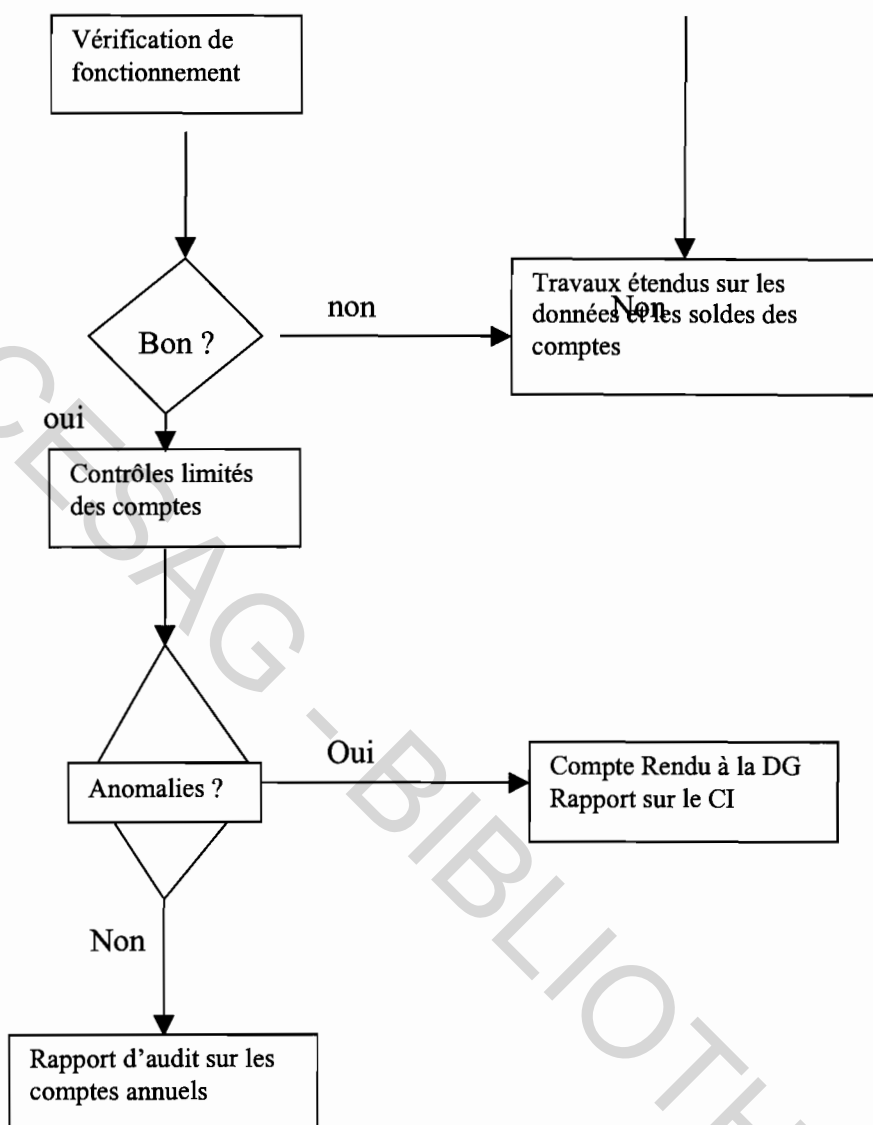
Après ces compléments et adaptations aux normes générales d'audit, quelle doit être la démarche de l'auditeur face à l'informatique ?

II. DEMARCHE DE L'AUDITEUR FACE A L'INFORMATIQUE

Nous rappelons que face à un milieu informatisé, l'auditeur doit évaluer à la fois le contrôle interne de la fonction informatique et le contrôle interne des applications.

Figure n°7 : Démarche générale de l’audit informatique





PHASE N°1: PRISE DE CONNAISSANCE GENERALE DE L'ENTREPRISE

Dans toute démarche d'audit, il importe en premier lieu de collecter des informations sur l'entreprise et son environnement afin de permettre à l'auditeur d'identifier les risques généraux qu'encourt l'entreprise. Il prend connaissance de ces informations à travers les entretiens avec les responsables ou en consultant la documentation aussi bien interne qu'externe.

PHASE N°2 : EVALUATION DU CONTROLE INTERNE DE LA FONCTION INFORMATIQUE

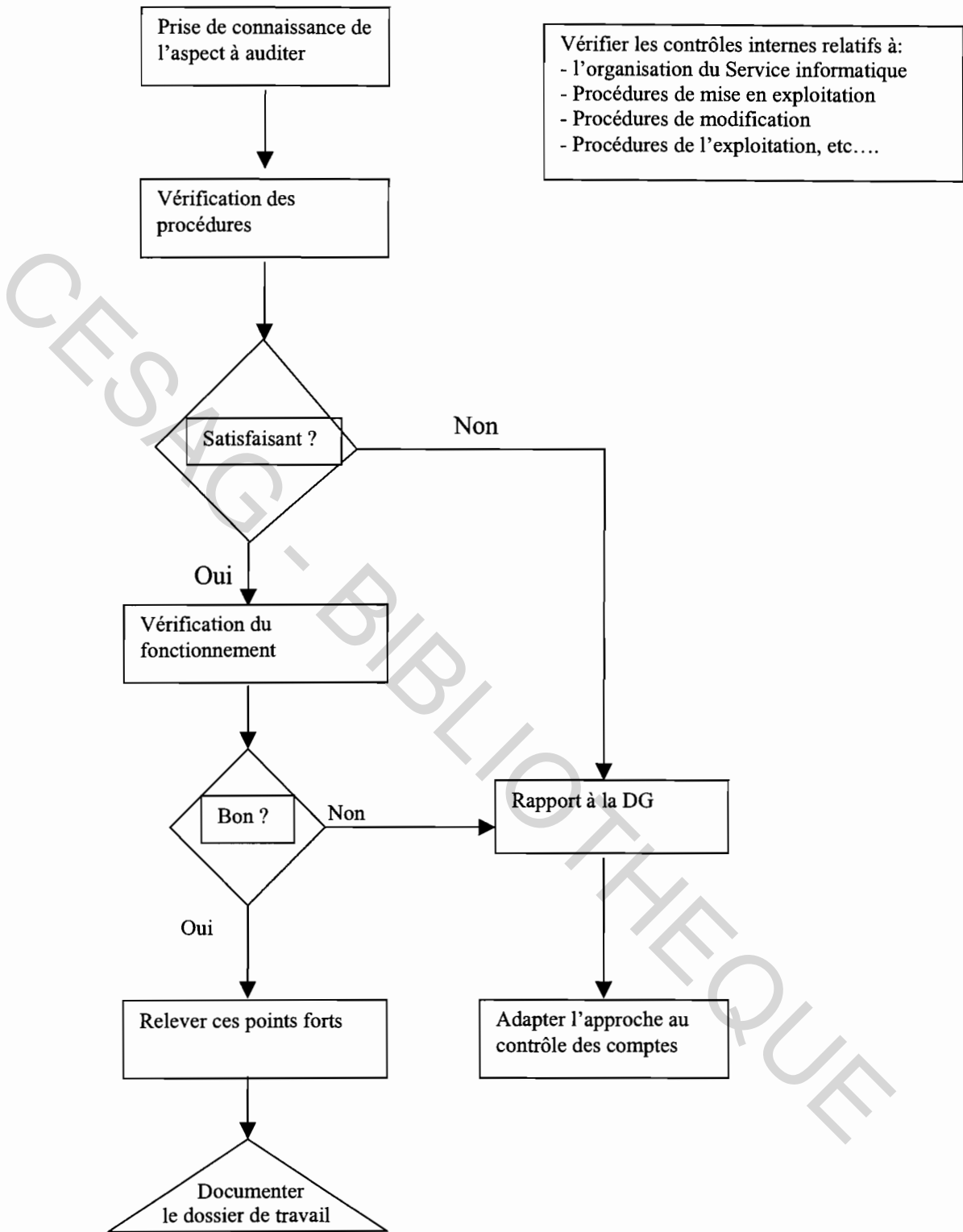
Comme au niveau général de l'entreprise, il faut procéder à une prise de connaissance spécifiquement informatique avant d'apprécier le contrôle interne de la fonction informatique.

Ceci est important car la performance d'un service informatique peut dépendre de :

- sa position dans l'organisation,
- des rapports interpersonnels plus ou moins satisfaisants entre les informaticiens et les utilisateurs,
- de l'existence d'un schéma directeur,
- de l'existence d'organes de supervision : comité informatique, comités ad hoc...,
- du matériel,
- des applications,
- de la maintenance.

Après cette prise de connaissance, l'auditeur procède à l'évaluation du contrôle interne. Pour ce faire, il doit s'assurer (suivant schéma ci-dessous) que les contrôles mis en place au niveau de tous les aspects de la fonction informatique permettent de garantir la fiabilité des informations produites, la protection du patrimoine et la sécurité des programmes et des fichiers.

Figure No 8: Appréciation du contrôle interne de la fonction informatique



Source: A. DIARRA (1994).

L’insuffisance des contrôles au niveau de la fonction informatique fait courir des risques importants à l’entreprise comme l’indique le tableau ci-dessous :

Tableau n°2 : Insuffisances des contrôles et risques potentiels

Insuffisances	Risques	Techniques d'audit pour identifier les risques
Rapports tendus entre informaticiens et utilisateurs	Développement des programmes sans relation avec les besoins des utilisateurs ; Informatisation 'sauvage' Configuration mal adaptée aux besoins ; Insuffisance de contrôles programmés.	Entretiens avec les utilisateurs et les informaticiens ; Examen des PV des réunions du comité informatique et des correspondances entre les informaticiens et les utilisateurs.
Insuffisance dans la séparation des tâches	Malversations, atteinte à la confidentialité, détournement des ressources, fraudes,...	Prise de connaissance des organigrammes et des fiches de fonction, Procédures de gestion de personnel.
Insuffisances dans les procédures de gestion du personnel informatique	IDEM + incompetence et inefficacité	Prise de connaissance des procédures de gestion du personnel informatique
Mauvaise procédure de développement	Non fiabilité des applications Insuffisance de contrôles programmés et de sécurité	Entretiens, observations, manuels de procédure sur la méthodologie de développement
Mauvaise procédure de mise en exploitation	Non exhaustivité des données transférées Pertes de données Anomalies en raison d'erreurs latentes Erreurs d'interprétation des instructions nouvelles	IDEM + examen des procès verbaux de transfert
Non respect des procédures de modification des applications ou inexistence de ces procédures	Fraude, malveillance, non fiabilité des applications	IDEM + Examen des correspondances entre le chef de projet et les utilisateurs
Mauvaise procédure pour le maintien de l'intégrité des systèmes.	Modifications non autorisées	IDEM + Tests par impression : - des tables d'accès aux données - des tables d'accès aux programmes Examen des rapports de gestionnaire de sécurité

Cette évaluation permet à l’auditeur d’apprécier si la réalisation des objectifs ci-dessous est garantie :

- objectifs de fiabilité des traitements ;
- objectifs de protection de patrimoine ;
- objectifs d’efficacité.

Les insuffisances éventuelles sont systématiquement présentées à la Direction générale avec des suggestions d’axes d’améliorations.

L’auditeur doit aussi évaluer les procédures de contrôle d’accès dont les risques sont présentés ci-dessous :

Tableau n°3 : insuffisances et risques

Insuffisances	Risques	Techniques d’audit pour identifier ces risques
Absence de stratégie de sécurité écrite Absence de procédures écrites limitant l’accès physique	Destruction des actifs entraînant une rupture de la continuité des traitements. Transfert d’informations commerciales à la concurrence. Chantage sur le contenu confidentiel d’un support informatique volé.	Visites des locaux ; Entretiens ; Se faire transmettre le plan de sécurité incendie et de sauvegarde; Observations des entrées/sorties à la salle informatique .
Absence de procédures de sauvegarde Climatisation défailante. Absence de procédures écrites pour la reprise à froid quotidienne. Manque de plan de Sauvegarde	Destruction des actifs entraînant une rupture de la continuité des traitements.	Observations ; Entretiens ; Visites des locaux ; Prise de connaissance des procédures de sauvegarde.

PHASE N°3 : EVALUATION DU CONTROLE INTERNE DES APPLICATIONS

Il faut préciser que dans le cadre d'une application, il existe deux types de contrôles : les contrôles utilisateurs et les contrôles programmés (ROY et GAUDRON , 1992).

Contrôles utilisateurs :

Ce sont des contrôles manuels effectués sur les données à traiter et sur les restitutions informatiques. Ils sont effectués soit par les utilisateurs qui n'ont pas de rapport direct avec le service informatique, soit par le personnel de contrôle dans ce service. Par exemple

- vérification de la pré-comptabilisation avant la saisie des bordereaux comptables,
- Pointage des éditions informatiques avec les documents de base ou des totaux préétablis.

Contrôles programmés :

Certaines procédures programmées remplacent des fonctions de contrôle manuel (par exemple les contrôles des séquences). D'autres remplacent des contrôles de nature comptable. Par exemple, le contrôle de l'équilibre débit/crédit des bordereaux de saisie comptable.

Ce sont donc ces deux procédures de contrôle que l'auditeur doit examiner pour apprécier le contrôle interne d'une application. En effet, l'objectif de ces contrôles est d'assurer que les données valides sont traitées de façon complète et correcte.

L'auditeur doit ainsi s'assurer que :

- des procédures manuelles et informatiques sont mises en place pour prévenir l'introduction de données fictives.
- des procédures sont mises en place pour prévenir l'omission de l'enregistrement de données réelles.

- des procédures existent pour assurer l'enregistrement des données réelles dans la bonne période.
- des procédures existent pour assurer une correcte évaluation des données.
- des procédures existent pour s'assurer que les données sont bien enregistrées et bien comptabilisées dans les journaux, le grand livre.

De façon plus spécifique, l'auditeur doit s'assurer de l'existence des procédures programmées ci-dessous :

1. Contrôle par appariement

Ce contrôle par rapprochement soumet à condition préalable l'acceptation d'une saisie.

Par exemple :

- enregistrement dans un compte seulement si ce dernier existe dans le plan comptable de l'entreprise,
- enregistrement d'un règlement seulement si la facture correspondante est préalablement enregistrée dans un compte fournisseur.

2. Contrôle d'accès

Ce contrôle consiste à verrouiller le système de façon que seules les personnes autorisées peuvent avoir accès aux programmes ou fichiers. Cela s'effectue généralement sous forme de mot de passe. L'auditeur doit s'assurer que ce dernier n'est pas facile à découvrir (il est déconseillé de choisir des mots de passe de moins de 5 caractères car facilement décelable par analyse combinatoire).

3. Contrôle de l'intégrité des données

Il consiste à contrôler par exemple si les montants dans la base de données correspondent à ceux issus d'une application différente.

4. Contrôle sur l'exécution préalable d'une règle

Il s'agit des contrôles conditionnant l'acceptation de la saisie d'une opération à l'existence de certaines données. Par exemple, le taux d'amortissement pour la saisie d'une immobilisation.

5. Contrôle sur les rejets

En cas de traitement par lot, le système doit rejeter les données erronées dans un fichier d'anomalies en attente de régularisation afin qu'elles puissent être recyclées.

6. Contrôles sur la séparation des périodes comptables

Ces contrôles permettent d'interdire la possibilité de modifier une écriture comptable après sa validation. Il s'agit d'assurer l'irréversibilité des écritures comptables.

7. Contrôle par équivalence

Ce type de contrôle est possible surtout dans un système intégré, c'est à dire dans le cas de plusieurs applications qui s'échangent des données. Dans ce cas, une sortie de données d'une application engendre des entrées dans une autre application. On peut en ce moment prévoir une procédure qui effectue un contrôle par équivalence entre ces sorties et ces entrées.

8. Autres contrôles

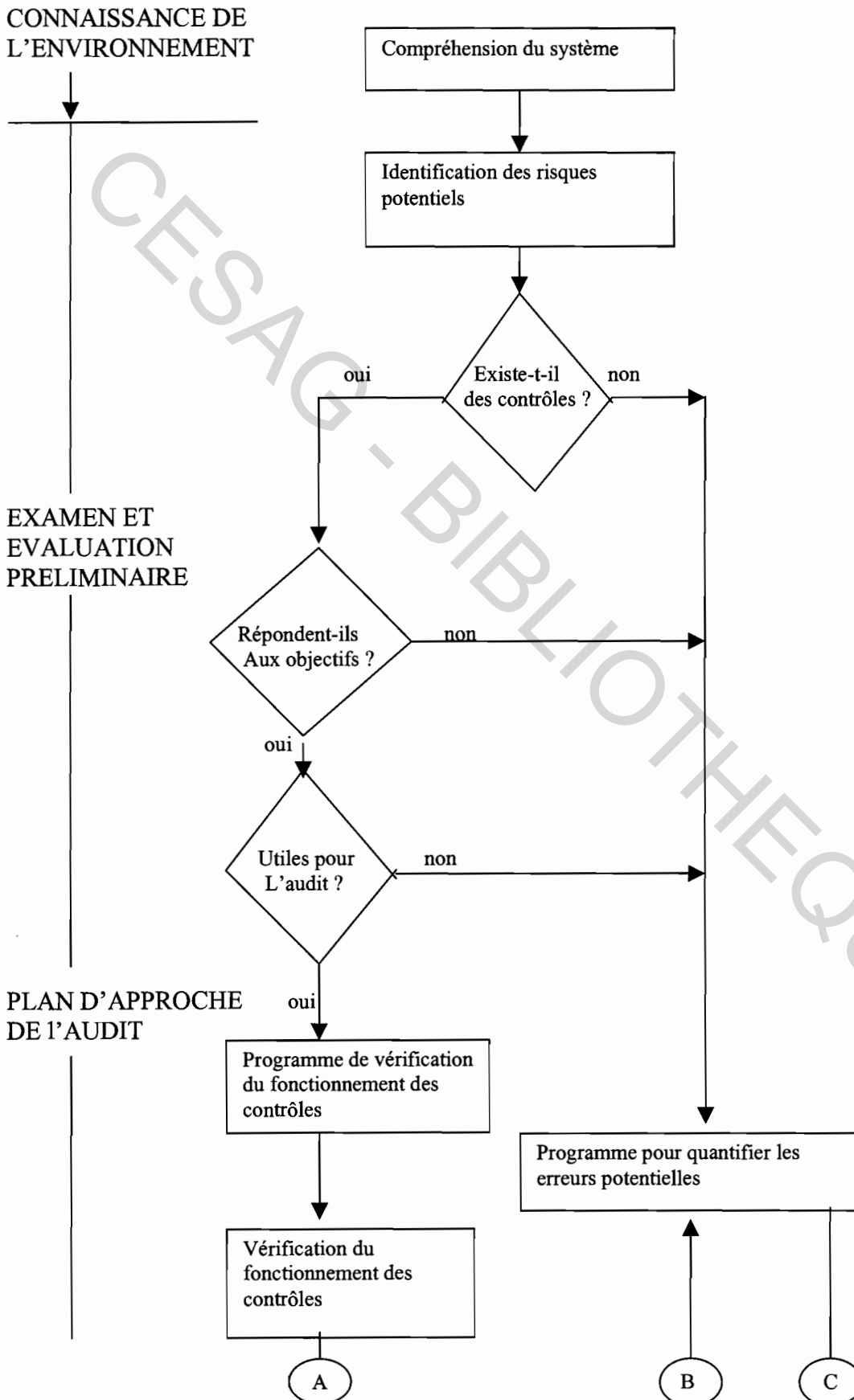
Sur le plan de l'exhaustivité, un contrôle programmé imprimant « dernière page » par exemple peut être utile.

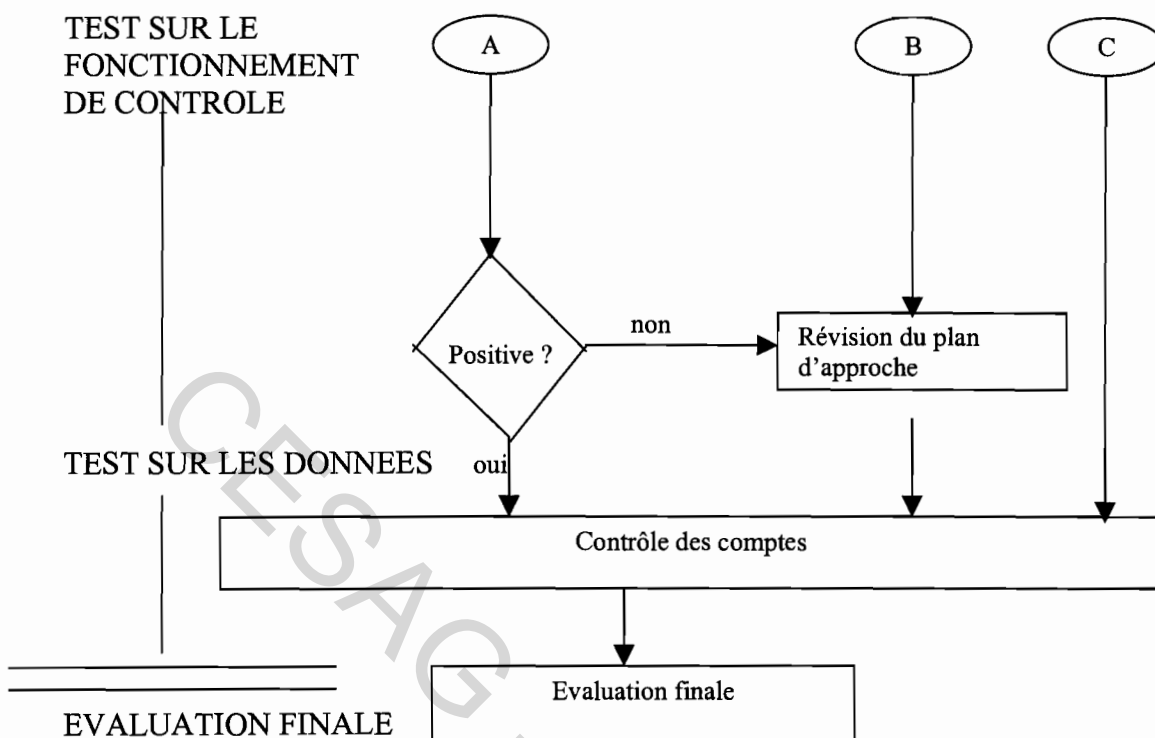
L'existence de ces contrôles programmés ne constitue pas une condition suffisante pour un contrôle interne efficace de l'application. En effet, ces contrôles peuvent être facilement battus en brèche par les informaticiens. C'est pourquoi, il faut adopter une démarche spécifique aux applications.

Démarche d'audit des applications

Cette démarche est celle recommandée par la CNCC (Recommandation N°2, 25-10-1980).

Figure n°9 : Démarche d'audit des applications





L'analyse des différentes phases nous donne ce qui suit :

Phase n°1 : Connaissance de l'environnement

L'objet de cette prise de connaissance est d'avoir une vue générale de l'application.

Cela consiste à juger de la complexité de la partie informatisée de l'application et de sa place dans le système d'information de l'entreprise prise globalement. Pour cela, il faut évaluer l'impact sur l'application :

- des contrôles généraux,
- des contrôles de la fonction informatique,
- des procédures d'autorisation permettant d'intervenir dans le flux manuel et informatisé des données et apprécier les modifications apportées à l'application susceptibles d'avoir un impact sur les données significatives pour l'audit.

Il faut remarquer que l'insuffisance des contrôles de la fonction informatique et des procédures d'accès a de fortes chances d'accentuer l'insuffisance des contrôles programmés.

A contrario, un bon contrôle interne de la fonction informatique peut laisser présupposer de l'existence de contrôles programmés efficaces.

Après cette prise de connaissance, l'auditeur doit procéder à l'examen et évaluation préliminaires.

Phase n°2 : Evaluation préliminaire

Avant l'évaluation proprement dite, l'auditeur doit :

- procéder à la description des étapes de traitements (à l'aide de flow chart ou description narrative),
- identifier les procédures de contrôles mises en place par l'entreprise et celles nécessaires,
- puis, les risques liés à l'application étant identifiés, procéder à des tests d'existence pour être sûr d'avoir bien compris les procédures . Par exemple pour les opérations d'achat :
 - partir du grand livre centralisé des fournisseurs,
 - demander la facture et les documents connexes,
 - rapprocher avec le compte individuel du fournisseur en question,
 - rapprocher avec le journal des achats,
 - puis avec le bordereau de saisie
 - et ensuite avec la procédure de comptabilisation.

A chaque étape, l'auditeur identifie sur les documents, la matérialisation des contrôles effectués, l'enchaînement des phases de traitement et les services intervenants.

Après cet examen préalable, l'auditeur doit pouvoir appréhender :

- les risques potentiels d'erreurs,
- les procédures de contrôles développées par l'entreprise pour prévenir et détecter les erreurs potentielles,
- l'impact théorique des procédures de contrôles ou de leur absence sur la probabilité de survenance des erreurs,
- l'impact des problèmes liés à l'organisation des tâches (grille de séparations des tâches)
- l'impact des procédures d'organisation et de contrôle de la fonction informatique sur le fonctionnement des procédures de contrôles de l'application,

Sur la base de toutes ces informations, l'auditeur peut répondre à deux questions essentielles :

1. les procédures de contrôles de l'application permettent-elles d'atteindre les objectifs d'audit ? Si oui, procéder aux tests de bon fonctionnement. Si non, évaluer l'incidence potentielle de cette défaillance en décrivant les contrôles inefficaces dans une feuille de travail 'incidence des risques identifiés' ainsi que l'impact des risques .
2. Les procédures de contrôles de l'application peuvent-elles être utiles à l'audit ? Si non, évaluer l'incidence potentielle de l'absence de contrôles

Phase n° 3: Plan d'approche

L'évaluation permet de mieux planifier l'organisation des tests :

- Tests de vérification du bon fonctionnement des contrôles : lorsque les contrôles de l'application sont satisfaisants et que l'auditeur veuille s'appuyer sur eux pour limiter ses travaux sur les comptes.

- Tests étendus sur les données pour quantifier les risques d'erreurs potentielles : lorsque les contrôles de l'application sont inexistants, inefficaces ou insuffisants et que l'auditeur ne peut pas s'appuyer sur eux.
- Tests limités sur les soldes des comptes : lorsque les tests précédents se sont avérés satisfaisants.
- Tests étendus sur les soldes des comptes : si les tests précédents dénotent l'existence de risques significatifs.

Phase n° 4 : Tests de fonctionnement

Comme souligné précédemment, ces tests ont pour objet de s'assurer que les procédures de contrôle fonctionnent bien comme décrit par l'entreprise et comme l'a compris l'auditeur. Les techniques d'audit pour les tests de vérification de fonctionnement consistent généralement en l'observation et l'examen de la matérialisation des contrôles.

Si les tests de fonctionnement ne révèlent pas d'anomalies, les conclusions de l'évaluation préliminaire sont confirmées et l'auditeur peut préparer son programme de contrôle des comptes selon le plan d'approche qu'il a établi.

Si par contre ces tests révèlent des anomalies, l'auditeur doit évaluer l'incidence des faiblesses des procédures de contrôle et modifier le plan initial d'approche.

Phase n°5 : Tests sur les données et/ou comptes

Ces tests consistent à vérifier si l'application a généré des erreurs et si ces erreurs ont un impact significatif sur les états financiers. Ils peuvent être effectués des à l'aide des outils informatiques (Audit assisté par l'ordinateur).

Phase n°5 : Evaluation finale

L'évaluation finale est faite à l'issue des tests planifiés à la phase ⁴~~3~~. Elle consiste à se prononcer sur les traitements informatiques quant à leur capacité à satisfaire les objectifs de régularité, de sincérité et d'image fidèle du patrimoine, de la situation financière et du résultat. Parallèlement et conformément à la recommandation de la CNCC, l'auditeur « signale aux dirigeants les observations qu'appelle de sa part le contrôle interne. Cette communication prendra une forme appropriée, orale ou écrite, en fonction de l'importance relative des observations. » (CNCC Recommandation N°2-29, octobre 1980).

Il nous semble incomplet de parler de l'audit informatique sans souligner l'appui que l'ordinateur peut apporter à l'auditeur. C'est pourquoi nous consacrerons le chapitre qui suit à cette question.

CHAPITRE III: L'ORDINATEUR : UN OUTIL POUR L'AUDITEUR

Pour l'auditeur, l'informatique n'est pas seulement un objet d'audit ; elle est aussi un outil d'audit. En effet, l'auditeur peut utiliser l'ordinateur pour accroître la qualité et la productivité de ses missions (GAUTHIER, 1992).

I. L'ORDINATEUR POUR ACCROITRE LA QUALITE

Dans un système intégré, il est difficile, voire impossible, de vérifier certains contrôles, autrement que par l'utilisation de logiciels d'extraction de données. C'est le cas par exemple, de la vérification de la correcte centralisation des écritures des sous-systèmes vers l'interface comptable.

De plus, ces logiciels permettent d'étendre le niveau de sondage. Par exemple, on peut extraire toutes les données relatives aux immobilisations et recalculer les dotations aux amortissements dans leur intégralité à des fins de validation des soldes annoncés par le client mais aussi de contrôles de la logique du programme.

La sélection de transactions qui méritent une attention particulière peut être systématisée en spécifiant des critères de valeurs ou de date. Par exemple, à partir des dates échéances des factures-clients, on opère une sélection pour reconstituer la balance âgée en vue de vérifier la pertinence et la réalité des provisions pour créances douteuses.

Les logiciels d'échantillonnage aussi augmentent la qualité du travail de l'auditeur par une détermination et une quantification précises des échantillons et du niveau de confiance.

Les tableurs sont de même largement utilisés dans le cadre de revues analytique pour les calculs des ratios et le benchmarking (dans le temps, l'espace,...).

Les logiciels graphiques, de flow chart, de traitement de texte améliorent la documentation des travaux de l'auditeur.

II. L'ORDINATEUR POUR ACCROITRE LA PRODUCTIVITE

Il existe de nos jours, des logiciels de planification et de suivi des budgets des missions d'audit facilitant la gestion des ressources disponibles. COLLINS (1992) signale que « la CNCC tient à la disposition des auditeurs des logiciels de gestion du dossier permanent Dp et de logiciels de rédaction du programme de contrôle des comptes Pcc ».

Les Systèmes Experts quant à eux, aident l'auditeur à affiner sa stratégie d'audit en cernant les erreurs potentielles puis en produisant les programmes de travail. Ce sont des véritables outils d'aide à la décision. A PROBST (1983) dit de ces Systèmes Experts : « qu'ils se comportent effectivement comme des experts humains raisonnant sur des faits établis. Ils sont constitués d'une base de connaissances (comprenant aussi bien une base de données et de faits qu'une base de règles logiques) et d'un programme de contrôles utilisant la base de connaissances pour effectuer des déductions logiques ».

Les principaux Systèmes Experts d'audit comptable connus selon F. FRERY (1992) sont :

- TICOM (Bailey et Whinston, 1983)
- AUDIT SMARTER (Arthur Young, 1984)
- AUDITOR (Dungan et Chandler, 1985)
- LOAN PROBE (Peat Marwick, 1985)
- HSD EXPERT (Arthur Young, 1989)

Ces Systèmes Experts, à partir des comptes que l'auditeur considère comme significatifs, sélectionnent les applications comptables concernées (ventes, encaissements, paie, gestion des immobilisations,...) et demandent une évaluation des contrôles internes effectués. Ils déterminent alors automatiquement les zones à risque sur lesquelles l'auditeur doit se focaliser ainsi que les procédures qui doivent être utilisées. Ce diagnostic est présenté dans deux documents directement exploitables : le plan d'approche destiné au responsable de la mission et les programmes de travail destinés aux membres de l'équipe.

Ces quelques lignes nous ont montré combien l'auditeur peut profiter des bienfaits de l'ordinateur pour mieux planifier ses missions, mieux effectuer ses contrôles et enfin, mieux rentabiliser ses activités.

Les pages qui suivent constituent la dernière partie de notre travail et portent sur l'audit d'un logiciel comptable où nous avons tenté de mettre en application les éléments théoriques développés dans les parties précédentes.

CESAG - BIBLIOTHEQUE

TROISIEME PARTIE : CAS D'AUDIT DU LOGICIEL

'COMPTAB' DE LA SOCIETE X

AUDIT DU LOGICIEL 'COMPTAB' DE LA SOCIETE X

Dans la deuxième partie, nous avons développé une méthodologie d'audit dans un milieu informatisé. Dans la troisième partie, nous abordons un cas relatif à l'audit d'une application de comptabilité.

Le logiciel 'COMPTAB' qui fait l'objet de notre audit est un logiciel 'maison' conçu par les informaticiens de l'entreprise appuyés par une Société de Services en ingénierie informatique (SSII). Cela fait deux (2) ans qu'il fonctionne mais les utilisateurs ne semblent pas satisfaits de ses performances et ne sont pas compris par les informaticiens. La Direction Générale avait donc voulu l'examen par un œil extérieur avant de prendre la décision de remplacer ou non ce logiciel. De plus, le passage au plan SYSCOA requiert des adaptations à ce logiciel.

Sous la responsabilité du chef du service « Contrôle de Gestion » qui tient lieu en même temps de service d'audit, nous avons donc procédé à cet examen.

Compte tenu du contexte ci-dessus, nous avons jugé nécessaire d'examiner quelque peu la fonction informatique avant d'auditer l'application proprement dite. En effet, les griefs portés au service informatique laisse croire que de sérieux problèmes existent à ce niveau qui, s'ils ne sont réglés, risquent de compromettre les adaptations envisagées d'autant qu'il s'agit de la même équipe d'informaticiens qui va faire ces adaptations.

Ainsi, nous avons procédé à une prise de connaissance et à l'évaluation des contrôles internes de tous les aspects du service informatique ci-après avant d'auditer l'application COMPTAB:

- Audit de l'organisation du service
- Audit des procédures de développement
- Audit des procédures de mise en exploitation

- Audit des procédures de modification
- Audit des contrôles de l'intégrité
- Audit de l'exploitation

Dans les pages qui suivent, nous présenterons :

I Le programme de travail

II Le Questionnaire du contrôle interne qui nous a permis d'évaluer la fonction informatique et le logiciel « Compta »

III Les notes de conclusion (portant uniquement sur les faiblesses constatées) et l'appréciation globale

IV L'avis sur l'appréciation et recommandations

I PROGRAMME DE TRAVAIL

SCG/SOCIETE X	Tâche : PROGRAMME DE TRAVAIL	Cde :
Collab : Assoumana H.		F° :

1. PRISE DE CONNAISSANCE GENERALE DE L'ENTREPRISE

a) Objectifs

L'objectif à ce niveau est de nous permettre d'avoir une compréhension d'ensemble de l'entreprise pour mieux adopter la mission aux spécificités de l'entreprise.

b) Travail à faire

Pour avoir une vue d'ensemble des particularités de l'entreprise, procéder par :

- visite des locaux ;
- entretiens ;
- exploitation de la documentation ;
- analyse des états financiers.

Il s'agira de collecter des informations relatives :

- au secteur d'activité de l'entreprise ;
- à la structure organisationnelle de l'entreprise ; organigramme, attributions, compétences des dirigeants ;
- au niveau de la culture de contrôle dans l'entreprise ;
- à l'intérêt porté à l'informatique par les dirigeants.

2. PRISE DE CONNAISSANCE DU SERVICE INFORMATIQUE

a) Objectifs

Il s'agit d'avoir une compréhension d'ensemble du service informatique, ses particularités, sa place dans l'organisation générale, l'intérêt qu'il suscite dans l'entreprise.

b) Travail à faire

▪ Faire une synthèse de toute la documentation relative au service informatique notamment :

- Organisation du service ;
 - Description des fonctions ;
 - Caractéristiques du matériel ;
 - Caractéristiques des logiciels.
- Lister les états informatiques de sortie et d'entrée, leurs émetteurs et leurs destinataires.

Ce travail doit se faire par entretiens et consultation de la documentation.

3. AUDIT DE LA FONCTION INFORMATIQUE

L'objectif est de s'assurer que le Service Informatique fonctionne de façon à garantir :

- la fiabilité des informations produites ;
- la protection du patrimoine ;
- la sécurité et la continuité des travaux.

3.1. Audit de l'organisation générale de la fonction

a) Objectifs

Il s'agit de s'assurer qu'il existe :

- un intérêt pour le contrôle ;
- un climat serein de travail au sein de l'équipe des informaticiens ;
- une séparation satisfaisante des tâches incompatibles ;
- un souci de dialogue franc entre utilisateurs et informaticiens.

b) Travail à faire

Il faut, à l'aide d'entretiens, de consultation de la documentation et d'observations, chercher à comprendre :

- l'histoire de la fonction informatique,
- l'évolution prévue de la configuration (existence ou non d'un schéma directeur, développements prévus ou en cours,...),
- L'organigramme du SI et les descriptions de fonctions,
- Les procédures propres à la fonction informatique,
- Examen des PV du comité et autres organes de supervision le cas échéant,
- Gestion du personnel informatique s'il constitue une spécificité dans l'entreprise,
- Le degré de satisfaction des utilisateurs.

3.2. Audit des procédures de développement

a) Objectifs

S'assurer que les applications sont développées avec professionnalisme de façon à limiter les dysfonctionnements, les erreurs de chaînes de calculs, des anomalies dans les états restitués par l'informatique (objectifs de fiabilité des traitements).

b) Travail à faire

- Par entretiens et examen des manuels de procédures, prendre connaissance de la méthodologie de développement des programmes et les compétences des personnes impliquées.
- Par tests, apprécier l'application de la procédure en examinant les documents afférents aux derniers développements.
- Examiner les PV de mise en exploitation des derniers développements.

3.3. Audit des procédures de mise en exploitation

a) Objectifs

S'assurer que les applications présentent toutes les fonctionnalités nécessaires pour s'intégrer de façon efficace dans le système global de l'entreprise (objectif d'efficacité).

b) Travail à faire

- Prendre connaissance des procédures de transfert par entretiens, observations et examen des procédures.
- Tests par l'examen de la documentation et des documents de contrôle.

3.4 Audit des procédures de modification des applications

a) Objectifs

S'assurer que les applications ne peuvent être modifiées à l'insu des utilisateurs (objectifs de fiabilité des traitements et de protection du patrimoine).

b) Travail à faire

- Examen des correspondances du service informatique avec les utilisateurs ;
- Prise de connaissance des procédures de modification par entretiens ;
- Tests sur les modifications observées.

3.5. Audit des procédures de l'intégrité

a) Objectifs

S'assurer que les accès aux matériels, aux données et aux applications font l'objet d'un contrôle rigoureux et que seules les personnes autorisées peuvent toucher à la substance des fichiers et des programmes.

b) Travail à faire

- Prise de connaissance des procédures de protection de l'intégrité des systèmes par entretiens, examen du manuel de procédures,
- Tests de pénétration.

3.6. Audit de l'exploitation

a) objectifs

S'assurer que les procédures de contrôle permettent de détecter les traitements incomplets, voire des anomalies (objectifs d'exhaustivité et d'exactitude).

S'assurer que seuls les traitements autorisés sont exécutés par l'exploitation.

b) Travail à faire

Examen du planning d'exploitation et du manuel de l'exploitation s'ils existent.

Tests pour vérifier si les procédures sont appliquées.

A l'issue de ces différents audits, il faut :

- relever les insuffisances et faire des recommandations d'amélioration.
- identifier les risques encourus par l'entreprise.
- apprécier leur impact sur l'évaluation du logiciel COMPTAB.

4. AUDIT DU LOGICIEL 'COMPTAB'

a) Objectifs

S'assurer que :

- toutes les données saisies et traitées sont réelles (réalité).
- des procédures existent pour prévenir l'introduction de données fictives (existence).
- toutes les données sont saisies, enregistrées et traitées (exhaustivité).

- des procédures existent pour prévenir l'omission d'enregistrement de données réelles (exhaustivité).
- des procédures existent pour assurer l'enregistrement des données dans la bonne période.
- Toutes les donnée enregistrées sont correctement comptabilisées, correctement centralisées au journal et au grand-livre.

b) Travail à faire

b-1) Evaluation préliminaire

Avant l'évaluation proprement dite, il faut :

- procéder à la description des étapes de traitements (à l'aide de flow chart ou description narrative),
- identifier les procédures de contrôles mises en place par l'entreprise et celles nécessaires,
- puis, les risques liés à l'application étant identifiés, procéder à des tests d'existence pour être sûr d'avoir bien compris les procédures .

A chaque étape, identifier sur les documents, la matérialisation des contrôles effectués, l'enchaînement des phases de traitement et les services intervenants.

Après cet examen préalable, appréhender :

- les risques potentiels d'erreurs,
- les procédures de contrôles développées par l'entreprise pour prévenir et détecter les erreurs potentielles,
- l'impact théorique des procédures de contrôles ou de leur absence sur la

probabilité de survenance des erreurs,

- l'impact des problèmes liés à l'organisation des tâches (grille de séparations des tâches),
- l'impact des procédures d'organisation et de contrôle de la fonction informatique sur le fonctionnement des procédures de contrôles de l'application.

Sur la base de toutes ces informations, répondre à la question essentielle: les procédures de contrôles de l'application permettent-elles d'atteindre les objectifs d'audit ?

Si oui, procéder aux tests de bon fonctionnement. Si non, apprécier l'incidence potentielle de cette défaillance en décrivant les contrôles inefficaces dans une feuille de travail 'incidence des risques identifiés' ainsi que l'impact des risques .

b-2) Tests de fonctionnement

S'assurer que les procédures de contrôle fonctionnent bien comme décrit par l'entreprise et comme l'a compris l'auditeur. Les techniques d'audit pour les tests de vérification de fonctionnement consistent généralement en l'observation et l'examen de la matérialisation des contrôles.

Si les tests de fonctionnement ne révèlent pas d'anomalies, les conclusions de l'évaluation préliminaire sont confirmées.

Si par contre ces tests révèlent des anomalies, évaluer l'incidence des faiblesses des procédures de contrôle.

b-3) Evaluation finale

L'évaluation finale est faite à l'issue des tests planifiés à la phase 3. Elle consiste à se prononcer sur les traitements informatiques quant à leur capacité à satisfaire les objectifs de régularité, de sincérité et d'image fidèle du patrimoine, de la situation financière et du résultat.

Faire un rapport soulignant les insuffisances relevées et les recommandations pour l'amélioration du logiciel.

Ce Programme de travail nous a conduit à l'élaboration d'un questionnaire que nous présentons dans les pages qui suivent.

CESAG - BIBLIOTHEQUE

II. QUESTIONNAIRE DE CONTROLE INTERNE

SCG/Sté X	Taches : QCI pour l'évaluation du Logiciel COMPTAB	Réf. :
Collab. : Assoumana H.		F° :

QUESTIONS	Réponses Oui/Non	Pondération			Commentaires
		A ²	S	I	
COMPREHENSION DE L'ORGANISATION GENERALE DE LA FONCTION INFORMATIQUE 1. La fonction informatique obéit – t – elle aux règles les plus usuelles du management : - Détermination des objectifs ? - Planification ? - Sélection et formation du personnel ? - Supervision et motivation du personnel ? - Description de fonction ? - Existence de procédures formalisées ? - Comparaison des résultats avec les objectifs ?					
2. Le service informatique est – t – il hiérarchiquement rattaché à un niveau lui donnant l'autorité nécessaire à l'exécution de ses objectifs ?					
3. Existe – t – il un comité informatique ? si oui fonctionne – t – il de façon satisfaisante ?					

² A :Acceptable S: Souhaitable I: Indispensable

4. Les procédures de séparations de fonctions sont - elles satisfaisantes ?					
5. Les ingénieurs systèmes sont – ils soumis à un minimum de procédures : - Documentation de leurs travaux ? - Compte rendu d'activité à la Direction ?					
6. L'implantation de la micro informatique est – elle coordonnée et supervisée par le service informatique ?					
COMPREHENSION DES PROCEDURES DE DEVELOPPEMENT					
7. Les développements sont – ils effectués selon une méthodologie formalisée?					
8. Cette méthodologie implique – t - elle suffisamment les utilisateurs au niveau : - Etude de faisabilité? - Etude fonctionnelle ? - Transfert en exploitation ?					
9. L'étude de faisabilité est – elle approuvée par le comité informatique ?					

10. La phase étude fonctionnelle prend – elle en compte : - La philosophie des contrôles manuels et informatisés au niveau du système ? - Les procédures de sauvegarde, de reprise ? - La formation nécessaire des informaticiens ? - La formation nécessaire des utilisateurs ?					
11. La phase étude fonctionnelle est – elle approuvée par les utilisateurs ?					
12. Les phases d’analyse sont – elles effectuées Selon des méthodes standardisées ?					
13. Pour la phase réception provisoire, les utilisateurs sont – ils impliqués à la mise au point des jeux d’essai ?					
14. La réception des utilisateurs fait – elle l’objet d’un PV entre informaticiens et utilisateurs ?					

15. En cas de développement confiés à une SSII, les éléments fondamentaux suivants sont – ils respectés : - Cahier des charges définies conjointement avec l’entreprise ? - Période d’essai en exploitation normale ? - Fourniture d’une documentation ? - Protection suffisante en cas de fourniture de programme limitée aux programmes-objets ?					
COMPREHENSION DES PROCEDURES DE MISE EN EXPLOITATION					
16. Existe – t –il un contrôle sur l’intégralité du transfert des programmes de l’environnement de tests à l’environnement de production ?					
17. En cas de reprise de fichiers ou l’installation d’une base de données, existe – t – il un contrôle pour s’assurer que les données sont : - exhaustives : toutes enregistrées ? toutes enregistrées dans la bonne période ? - Exactes : validation suffisante sur l’exactitude des données ?					

18. La réception finale donne – t – elle lieu à un PV ?					
COMPREHENSION DES PROCEDURES DE MODIFICATIONS					
19. Toute modification fait – elle l’objet d’une demande écrite des utilisateurs ?					
20. Toute modification n’est - elle testée qu’avec des jeux d’essai de l’environnement de tests ou avec des copies autorisées de fichiers réels ?					
21. La mise en production des programmes modifiés est – elle précédée de l’accord du responsable hiérarchique du programmeur et de l’utilisateur ?					
COMPREHENSION DES PROCEDURES D’INTEGRITE					
22. Existe – t – il des procédures assurant l’intégrité des systèmes mis en production ?					
23. Ces procédures permettent – elles un contrôle satisfaisant dans les domaines suivants : - Protection contre les accès non autorisés ? - Correspondance entre programme d’exploitation sources et objets ?					

COMPREHENSION DES PROCEDURES DE LA SECURITE DES ACCES LOGIQUES ET PHYSIQUES					
24. Existe – t – il une stratégie de la sécurité des accès logiques dans l’entreprise ?					
25. Les fichiers et programmes sont – ils stockés hors site, en dehors des périodes de traitement ?					
26. Les commandes et les programmes utilitaires auxquels peuvent accéder les informaticiens par terminaux ou consoles sont – ils affectés en accord avec les règles de séparation des fonctions nécessaires à un bon contrôle interne ?					
27. Les commandes et les programmes utilitaires auxquels peuvent accéder les utilisateurs par terminaux ou consoles sont – ils affectés en accord avec les règles de séparation des fonctions nécessaires à un bon contrôle interne ?					

28. Existe – t – il des mots de passe ? Si oui, les règles suivantes sont – elles respectées : - Gestion des mots de passe par une personne suffisamment indépendante ? - Le responsable des mots de passe procède – t – il régulièrement aux tâches suivantes : contrôle de la diffusion des mots de passe, contrôle sur les forçages ? - Les procédures relatives aux mots de passe assurent – elles une protection suffisante : - Quatre caractères alphanumériques minimum ? - Pas d’affichage à l’écran ? - Changement au moins tous les mois ? - Déconnexion automatique des terminaux après forçage ou déclenchement d’une procédure bloquante ?					
29. Existe – t –il des procédures de comptabilisation des accès ? Permettent– ils d’analyser les éléments suivants : - Autorisation des sollicitations (fichier programme, transaction) ? - Localisation et fréquence des forçages ? - Changement de profils d’accès ?					

30. Existe – il des procédures permettant de contrôler a posteriori l'intégrité du système ?					
31. Existe – t – il une stratégie de la sécurité portant sur la protection : - des accès physiques ? - des procédures de sauvegarde et reprise ? - un plan de sauvegarde en cas de destruction du patrimoine informatique ?					
32. Existe – t – il des procédures limitant l'accès physique aux actifs informatiques : - les utilisateurs ne sont pas admis dans les locaux informatiques ? - les tiers accédant aux locaux informatiques font l'objet d'une autorisation préalable ? - Les documents ne sont accessibles qu'aux personnes autorisées ?					
33. Les procédures d'accès physiques sont – elles renforcées par des systèmes de badges, de cartes magnétiques ?					

34. La gestion du système est – elle satisfaisante pour traiter les problèmes suivants : - Vols ? - Démission, licenciement ?					
35. En cas de crise (mouvements sociaux, par exemple), les locaux informatiques peuvent – ils être fermés rapidement ?					
36. L'entreprise a – t – elle mis en place un système de détection de : - Fumée ? - Chaleur ?					
37. Existe - t – il des instructions incendie suffisamment connues du personnel informatique : - Interdiction de fumer ? - Volume de papier maximal acceptable à la salle machine ? - Nettoyage périodique, y compris dans les faux planchers ? - Actions à suivre en cas d'incendie ?					
38. Existe – t – il des procédures suffisantes permettant de prévenir ou de limiter les dégâts des eaux ?					

39. Le système d'alimentation électrique est – il conforme aux règlements et normes en vigueur ?					
40. L'installation électrique permet – elle la continuité de l'exploitation en cas de coupure : - Onduleur + batteries + groupe électrogène ?					
41. Existe – t – il un plan de sauvegarde ?					
COMPREHENSION DES PROCEDURES D'EXPLOITATION					
42. Les règles d'administration de l'activité exploitation sont – elles consignées dans un manuel de procédures ?					
43. Ce manuel prévoit – il notamment : – Une séparation entre les activités développement et exploitation ? – Une séparation des tâches d'exploitation et de contrôle au sein de l'activité exploitation ? – Une interdiction absolue aux équipes d'exploitation de modifier des programmes et le contenu des fichiers ? – Des consignes en cas d'incidents ?					
44. Les travaux sont – ils lancés selon un planning strict ?					

45. La gestion du planning est - elle accessible aux équipes d'exploitation ?					
46. Existe – t – il une fonction de gestion des supports magnétiques ?					
47. Existe – t – il des procédures suffisantes de contrôle de l'exhaustivité des traitements ?					
48. Les procédures de distribution des informations produites par la fonction informatique sont – elles adéquates ?					
49. Un programme complémentaire est – il utilisé à des fins de contrôle (fichier LOG) a posteriori : - temps d'exécution ? - l'utilisation des programmes ? - l'utilisation des fichiers ? - contrôle des traitements finissant anormalement ?					
50. La périodicité des visites de maintenance est – elle suffisante pour une prévention efficace ?					

QCI DE L'APPLICATION 'COMPTAB'					
CARACTERISTIQUES FONCTIONNELLES 1. Y- a – t- il un langage de paramétrage (programmation utilisateurs) ? 2. Le langage est – il de types questions – réponses ? 3. Les fonctions ci-dessous sont – elles Inaccessibles à certaines catégories de personnel (mots de passe hiérarchisés) ? - Création - Modification - Suppression - Consultation					
4. L'utilisateur dispose – t – il à l'écran d'un guide genre « AIDE » ?					
5. Existe – t – il des fichiers : - des paramètres utilisateurs ? - plan comptable ? - des journaux ? - des cumuls ? - historiques ?					

6. Fichier des paramètres utilisateurs. L'utilisateur peut – il décider du nombre de périodes comptables par exercice?					
7. A chaque modification de paramètres, y – a – t – il édition d'un journal de modification ?					
9. L'utilisateur peut – il – définir lui - même différentes règles de contrôle et de sécurité ?					
10. Le logiciel permet – t – il une arborescence des Comptes ?					
11. Peut-on créer des comptes à vocation spécifique : - comptes de comptabilité analytique ? - Comptes de tiers ? - Comptes budgétaires ?					
12. En cours de saisie, l'utilisateur peut – t - il : - changer la structure des comptes ? - créer de nouveaux comptes ? - supprimer des comptes ?					
13. Quelle est la longueur maximale d'un intitulé de compte (en nombre de caractères) ?					

14. Les sous comptes peuvent - t – ils être créés ou supprimés ?					
15. Peut – on à tout moment consulter les totaux des comptes ?					
16. Le comptable peut – il à tout moment demander l'édition des comptes et des journaux ?					
17. Peut – on connaître le nombre d'écritures que l'on peut encore passer sur le même support ?					
18. L'identification du journal comprend –elle : - un code journal ? - un intitulé ?					
19. Combien de journaux auxiliaires peuvent être reliés au journal général ?					
20. Peut – on à tout moment visualiser les journaux ainsi que le solde d'un compte ?					
21. Sur combien d'exercices peuvent s'étendre les Fichiers historiques ?					
22. Comment s'opère, lors de la clôture, le transfert en fichier historique ?					

SAISIE					
23. Les grilles de saisie comportent – elles des zones optionnelles et des zones obligatoires ?					
24. Peut – on, à partir de plusieurs écrans , faire de la saisie simultanément : - Pour un même journal ? - Pour un même compte ?					
25. Comment est distingué un débit d'un crédit ? Un signe apparaît –il à l'écran ?					
26. Le logiciel comporte – t – il un système de libellé automatique ?					
27. Peut – on supprimer une écriture saisie et validée ?					
28. Le solde du compte est – il mis à jour progressivement ?					
29. Les contreparties peuvent – elles être imputées automatiquement ?					
30. En cas de coupure de courant ou d'arrêt inopiné, l'utilisateur est – il tenu de reprendre la saisie depuis le début ?					

31. A chaque fin de saisie d'un écran, quelle est la procédure de validation des écritures.					
CONTROLES ET PROCEDURES DE CORRECTION					
32. Des contrôles de cohérence existent – ils lors de la mise à jour d'un fichier ?					
33. L'accès de certains fichiers peut – il être limité à certaines personnes ?					
34. Y – a – t – il un contrôle sur l'identité de l'utilisateur ?					
35. Y – a -- t – il un contrôle sur la nature de la zone (zone numérique ou alphanumérique) ?					
36. Peut – on saisir des écritures non équilibrées ?					
37. L'utilisateur est – il obligé de corriger tout de suite après constatation de l'erreur ?					
38. Dans le cas d'une anomalie, apparaît –il à l'écran un message sur la nature et l'objet de l'anomalie ?					
39. Les erreurs et les anomalies sont – elles versées automatiquement dans un fichier d'attente ?					

40. Deux numéros de comptes peuvent – ils avoir le même libellé ?					
41.Des contrôles existent – ils sur la cohérence des informations saisies avec celles connues par le système ?					
42. Une correction est – elle soumise aux mêmes contrôles qu’une écriture de premier jet ?					
43. Pour corriger une zone faut –il : - effacer l’existant et frapper les nouvelles données ? - refrapper directement sur l’existant ?					
44. Les écritures saisies peuvent – elles être Accessibles sur papier et sur écran pour Vérification systématique par un comptable ?					
45. Dans un journal, un signe distingue – t – il les écritures définitives de celles qui sont en attente ?					

TRAITEMENTS					
46. Existe des interfaces de liaison avec : - le progiciel de paie ? - le progiciel de facturation ? - des tableurs ? - des traitements de texte ?					
47. Les regroupements des comptes peuvent – ils être progressifs afin d’obtenir différents niveaux d’analyse ?					
48. Les différents regroupements sont – ils Accessibles à l’écran ?					
49. Le chevauchement sur deux exercices est – il possible ?					
50. A l’écran, l’opérateur peut – il contrôler que l’imputation a bien eu lieu dans le bon exercice ?					
51. Peut – on obtenir des états provisoires partiels : - chaque mois ? si oui, lesquels ? - chaque trimestre ? si oui, lesquels ?					
52. Peut – on supprimer un compte soldé ?					

53. Le progiciel permet – il des clôtures Provisoires ?					
54. Certains états peuvent – ils être protégés afin d'en limiter la diffusion ?					
55. Le solde des comptes s'effectue – t – il de façon Automatique ?					
56. Certains traitements comptables s'effectuent – ils automatiquement ?					
COMPTABILITE GENERALE					
Le plan comptable					
57. Est – il visualisable à l'écran à tout moment ?					
58. La définition des états est – elle imposée ? Optionnelle ? paramétrable ?					
Les journaux					
59. Quel type de journal peut – on choisir : - Journal unique avec la liste des écritures introduites ? - Journaux auxiliaires avec journal centralisateur ? - Journaux particuliers de contrôles ?					

60. Combien de journaux auxiliaires le système peut – il gérer au maximum ?					
61. Les écritures sont – elles classées Chronologiquement ?					
62. Y – a – t – il regroupement par classe de comptes ?					
63. Tous les journaux sont – ils accessibles à l'écran ? Sur papier ?					
64. Pour chaque journal, les informations suivantes sont – elles précisées en fin de page : - le total des mouvements du mois ? - l'état antérieur ? - le total à reprendre pour le mois suivant ?					
65. Pour une information trouve – t – on : - le numéro du compte débité ? - le numéro du compte crédité ? - le montant débité ? - le montant crédité ?					

Le grand Livre					
66. En début de compte, trouve – t – on la reprise de l'ancien du début de la période ?					
67. Pour chaque ligne, y – a – t – il identification de l'écriture ?					
68. Le numéro de la pièce est – il présent ?					
69. Trouve – t – on : - la date de l'écriture ? - le libellé de l'écriture ? - le montant ? - le compte de contrepartie ?					
70. En fin de compte, les cumuls des écritures débitées et créditées et le solde du compte sont – ils présents ?					
Le bilan					
71. A – t – on la possibilité d'avoir un bilan simplifié et un bilan synthétique ?					

Le compte de résultat					
72. A – t – on la possibilité d’obtenir un compte de résultats détaillé et un autre synthétique ?					
La balance générale					
73. La balance renseigne t – elle sur le détail des comptes et fournit – elle des sous totaux ?					
74. Fournit – elle le solde pour chaque compte ?					
75. Donne – t – elle le récapitulatif à la date d’arrêté de tous les comptes du grand livre ?					
76. Peut – on la consulter à l’écran ?					
Les comptabilités auxiliaires					
77. Les traitements effectués sur la comptabilité générale ont – ils une influence sur les comptabilités auxiliaires et vice versa ?					
78. Les comptes clients ou fournisseurs sont – ils intégrés ou séparés de ceux de la comptabilité générale ?					

79. Les dates d'échéances peuvent – elles être prises en compte et le progiciel peut – il faire un inventaire ?					
80. Quelles sont les opérations réalisables grâce à ces comptabilités auxiliaires : – échéancier ? – relance automatique ? – suivi des règlements ?					
81. Comment s'effectue à l'écran le rapprochement entre l'émission et le règlement : - par numéro d'écriture ? - par date d'échéance ?					
82. Le rapprochement est – il visible à l'écran ?					
83. Le progiciel permet – il de distinguer les clients douteux des autres clients ?					

III NOTES DE SYNTHESE ET APPRECIATION GENERALE

III-1 NOTES DE SYNTHESE

Nous ne présentons ici que la synthèse des travaux sur le logiciel COMPTAB, les points soulevés, la synthèse globale et les recommandations proposées.

1 TRAVAUX EFFECTUES

Nous avons procédé à la prise de connaissance générale de l'entreprise et de la fonction informatique puis analysé tous les documents relatifs au logiciel COMPTAB, notamment les divers états de sortie et d'entrée, les états d'avancements des travaux de développement, les PV de réunion du comité informatique.

nous avons élaboré un questionnaire d'évaluation du contrôle interne (voir point II) que nous avons administré.

nous avons exécuté l'ensemble des points figurant dans le programme de travail à l'aide d'entretiens, d'observations et parfois des tests directement sur l'application.

2 POINTS SOULEVES

A l'issue de nos travaux, nous avons retenu ce qui suit :

2 .1 Prise de connaissance générale de l'entreprise

Les résultats relatifs à cette phase ne sont pas exposés dans les détails dans le cadre de ce mémoire car la prise de connaissance générale de l'entreprise dans le déroulement d'une mission d'audit est identique que cela soit dans un milieu Informatisé ou non. Toutefois, nous retiendrons que c'est une société de transport et de distribution d'eau qui dessert une cinquantaine de centres d'exploitation, qui fait un Chiffre d'affaires d'environ 3 milliards fcfa

avec un effectif de plus de 300 personnes.

La société comprend :

- Une Direction d'exploitation ;
- Une Direction d'études ;
- Une Direction comptable et financière ;
- Une Direction des ressources humaines ;
- Un Service contrôle de gestion ;
- Un Service informatique.

Cette prise de connaissance est essentielle; elle nous a permis d'appréhender :

- le manque de culture de contrôle dans l'entreprise et
- le peu d'intérêt porté au service informatique par les dirigeants.

2.2 Prise de connaissance générale de la fonction informatique

A) Organisation générale

Le service informatique est rattaché à la Direction générale mais c'est une Structure très simple où la séparation des tâches n'est pas formalisée compte Tenu de l'effectif très réduit du personnel (4 informaticiens). Et le plus haut Grade est Ingénieur des travaux (BAC + 4).

Le service est équipé d'un AS Unisys et de 5 terminaux intelligents 3 Zenith 386 et 2 DELL 386 selon nos entretiens. D'autre part, il existe une Multitude d'autres micro ordinateurs de marques différentes disséminés dans l'entreprise dont la gestion échappe au service informatique.

Les faiblesses essentielles sont :

- ◆ Beaucoup d'utilisateurs n'ont pas été formés à l'utilisation du COMPTAB.

- ◆ Les utilisateurs n'ont pas été impliqués comme il se doit dans la conception
- ◆ du logiciel, l'assistant (SSII) n'étant pas basé sur place.
- ◆ Les rapports entre informaticiens et utilisateurs sont tendus. Les derniers sont traités d'incompétents par les premiers.
- ◆ Il n'existe pas de Comité informatique.
- ◆ Les travaux des informaticiens ne sont pas suffisamment documentés.
- ◆ Nous n'avons pas pu disposer des compte rendus des travaux du service ce qui confirme le peu d'intérêt porté à la fonction informatique.

B) Procédures de développement

- ◆ Il n'existe pas de méthodologie formalisée de développement.
- ◆ Les utilisateurs ne sont pas suffisamment impliqués dans les développement.
- ◆ Il n'y a pas eu de cahier de charges spécifique au logiciel comptab.

C) Procédures de mise en exploitation

Nous n'avons pas pu nous assurer des contrôles effectués lors des mises en exploitation car il n'y a pas de manuel de procédures y afférentes.

D) Procédures de modifications

La séparation des tâches n'est pas être satisfaisante car le chef de service fait les modifications, teste et met en production les programmes modifiés.

E) Procédures d'intégrité et de sécurité des accès

Tous les informaticiens sans distinction peuvent accéder aux programmes existants (gestion clientèle, comptab, paie, facturation). Il n'existe pas de séparation des tâches compte tenu de la simplicité de la structure.

Les mots de passe sont composés du N° Matricule précédé d'une lettre ce qui ne garantit pas une protection suffisante.

Il n'existe pas une procédure bloquante en cas de forçage.

L'accès à la salle informatique n'est pas suffisamment contrôlé malgré

l'existence d'un système de badges.

Il n'existe pas de système de détection de fumée ni d'extincteurs dans la salle informatique.

Il n'y a pas de groupe électrogène en cas de rupture d'électricité. Cependant, un onduleur Merlin Gérin dispose d'une autonomie de 30 minutes selon le chef du service.

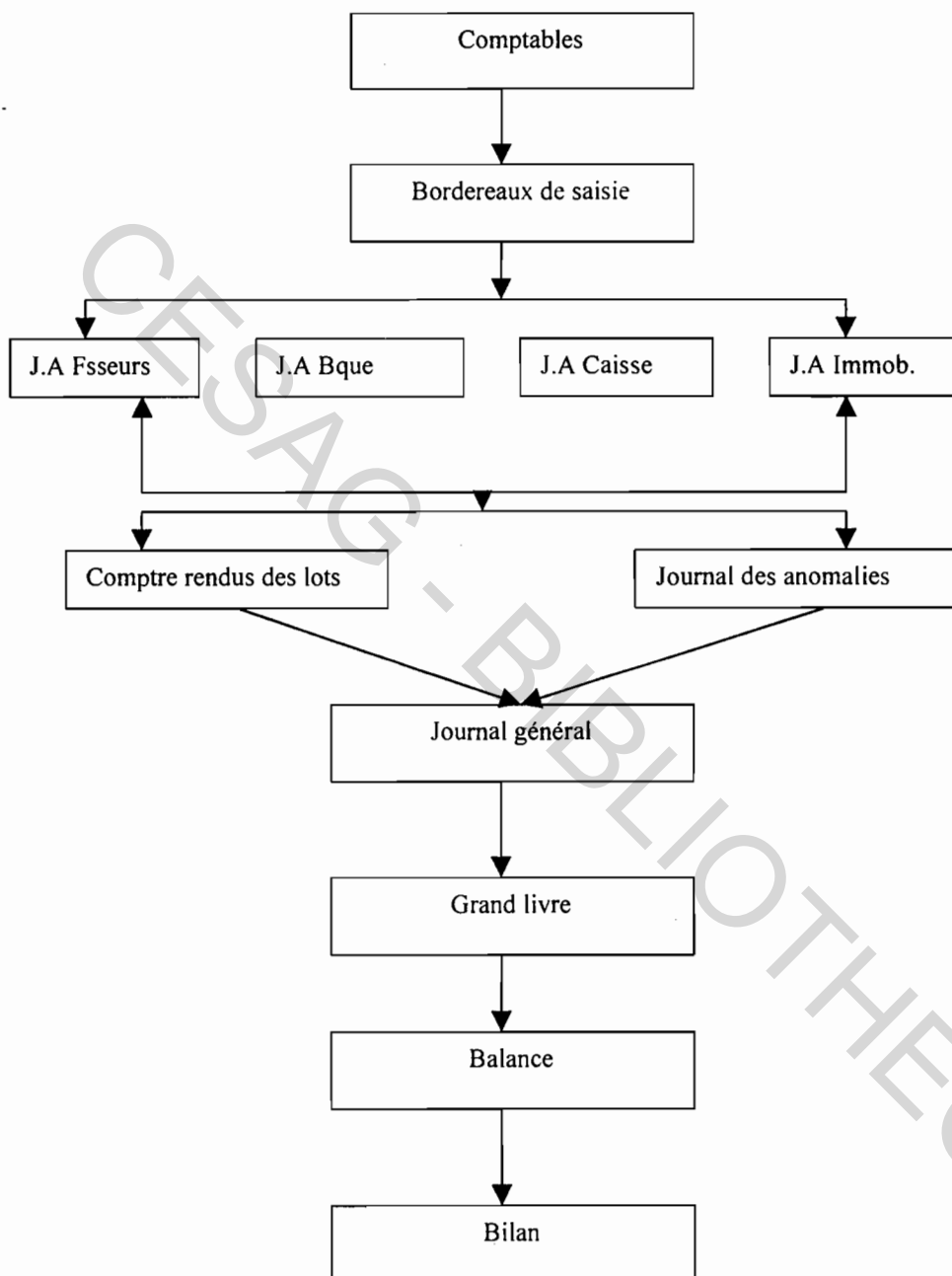
F) Procédures d'exploitation

La seule lacune observée à ce niveau est le manque de séparation des tâches.

2.3. PRISE DE CONNAISSANCE DU LOGICIEL « COMPTAB »

La prise de connaissance générale du logiciel nous a permis de comprendre qu'il est conçu suivant le système centralisateur de la comptabilité générale.

Nous le schématisons ci-dessous tel que nous l'avons compris.



Il ressort de ce schéma que :

- les comptables (parfois des stagiaires) font la saisie sur la base de bordereaux de saisie ;
- Les saisies sont faites par type de journal ;

- Après la saisie, des compte rendus de lots saisis et un journal des anomalies sont édités. Les écritures erronées sont ensuite recyclées.
- Après toutes les corrections, le grand livre et la balance sont édités trimestriellement pour la justification des comptes ;
- Le bilan est édité seulement à la demande du Directeur financier ou son représentant.

Nous avons retenus les problèmes ci-dessous :

A) Caractéristiques fonctionnelles

- ◆ Le logiciel se plante parfois quand plusieurs personnes saisissent simultanément ;
- ◆ L'accès à l'application n'est pas hiérarchisé: les comptables se prêtent même les mots de passe ;
- ◆ Le logiciel ne dispose pas de guide à l'écran ce qui fait qu'à chaque anomalie, il faut demander l'assistance des informaticiens.
- ◆ Le comptable ne peut pas à tout moment éditer des comptes ou des journaux.

B) Saisie

- ◆ Absence de contrôles programmés sur la séquence des bordereaux de saisie.
- ◆ Une écriture validée peut être supprimée.
- ◆ Le journal n'est qu'une liste d'écritures sans contreparties.
- ◆ Il n'existe pas de génération automatique des libellés de comptes.
- ◆ Il n'existe pas de contrôles sur la nature des zones.
- ◆ Pour corriger une erreur, il faut d'abord effacer l'existant avant de ressaisir.

C) Contrôles et procédures de correction

- ♦ Le journal reprend les écritures même celles déséquilibrées.
- ♦ Il n'existe pas de contrôles d'accès aux fichiers.
- ♦ Le logiciel accepte des écritures non équilibrées.

D) Traitements

- ♦ Il n'existe pas d'interface avec le logiciel de paie ni avec la facturation.
- ♦ Important volume d'anomalies après chaque saisie impliquant plusieurs tentatives du recyclage.

E) Comptabilité générale

- ♦ Les comptes soldés n'apparaissent pas dans la balance.
- ♦ Le logiciel ne fournit pas un bilan en grandes masses.
- ♦ Tout comptable a accès à toutes les opérations.
- ♦ Absence de contrôles hiérarchiques au niveau des comptables.
- ♦ Le masque de saisie ne présente pas tous les contrôles nécessaires à une saisie correcte.

III-2 FICHE D'APPRECIATION GLOBALE

Notation sur 5					
1	2	3	4	5	
	X				
X					
X					
	X				
		X			
	X				
	X				
	X				
X					
X					
		X			
	X				
	X				
	X				
	X				
	X				
X					
	X				
APPRECIATION GLOBALE					
	X				

A l'aide d'entretiens, observations et consultation de la documentation, nous avons noté sur 5 chacune des réponses aux questions contenues dans le QCI. La fiche ci-dessus constitue l'ultime synthèse de notre appréciation de logiciel COMPTAB qui se trouve alors, en dessous de la moyenne (2/5).

Dans les pages qui vont suivre, nous proposons notre synthèse de recommandations.

IV RECOMMANDATIONS

La prise de connaissance générale de l'entreprise et de la fonction informatique révèle que :

- la société X est une grande société compte tenu de son aire de gestion, l'effectif de son personnel, le chiffre d'affaires annuel;
- son secteur d'activité est très stratégique;
- la fonction informatique est une structure très simple comparativement à la taille de l'entreprise. Cela dénote le peu d'intérêt porté par les dirigeants à l'informatique et à la comptabilité qui est apparemment considérée comme une obligation légale uniquement et non comme un outil de gestion. En effet, il ne nous paraît pas normal qu'un logiciel comme « COMPTAB » qui présente tant de faiblesses ne soit pas remplacé dès ses premiers jours;
- la comptabilité semble être une activité accessoire du service informatique. Le logiciel de gestion « CLIENTS » fait l'objet de plus d'attention par les informaticiens ;
- compte tenu de l'effectif du personnel informatique, la séparation des tâches incompatibles ne peut se réaliser ;
- les contrôles des accès aussi bien physiques que logiques ne sont pas fiables.

Au vu de ce qui précède, nous recommandons :

1. Que la Direction Générale s'intéresse davantage à la fonction informatique et à la comptabilité ;
2. De créer un comité informatique qui sera chargé en premier lieu de la restructuration du service informatique (effectif, profil du personnel, organigramme , manuel des procédures à mettre en place) et ensuite du suivi des activités de celui-ci ;
3. D'impliquer les utilisateurs à toutes les phases d'acquisitions ou de développements futurs des applications ;

4. De procéder à des actions de formation et de sensibilisation des utilisateurs et des informaticiens pour améliorer les prestations du service informatique ;
5. Au lieu d'un développement à l'interne, l'achat pur et simple d'un progiciel de comptabilité qui a fait ses preuves dans les entreprises de la place ou à défaut procéder à une analyse comparative des progiciels existants sur le marché ;
6. Enfin, en cas de prestations de service par une Société de Services en Ingénierie informatique, nous recommandons de bien rédiger le contrat (pour éviter des surprises) notamment :
 - décrire l'objet du contrat avec précision ;
 - rédiger un cahier de charges ;
 - prévoir la procédure de la recette des prestations de la SSII et des conditions de modifications futures.

CONCLUSION GENERALE

« FAUT – T – IL ADOPTER LA MEME DEMARCHE D'AUDIT DANS UNE ORGANISATION INFORMATISEE QUE DANS UNE ORGANISATION où LA PRODUCTION DES INFORMATIONS FINANCIERES EST MANUELLE ? », telle est la question qui constitue la quintessence de notre travail.

Nos différents développements nous permettent de ne pas répondre, aujourd'hui, par l'affirmative à cette question. Cela ne serait pas objectif car l'ordinateur présente de nouveaux risques pour l'auditeur.

En effet, les documents qu'il génère ne sont toujours pas fiables car les programmes sont des œuvres humaines donc sujets à des dysfonctionnements. De plus, les informaticiens n'ont pas toujours les mêmes objectifs que les auditeurs ; certains contrôles indispensables à l'auditeur ne présentent pas d'intérêt particulier pour les informaticiens (cas des contrôles d'accès aux fichiers des données par exemple). La séparation des tâches incompatibles - chère à l'auditeur - au niveau du service informatique n'est pas toujours satisfaisante car ces tâches sont souvent méconnues du management pour pouvoir les clarifier.

La fonction informatique ne peut être auditée comme n'importe quelle autre fonction dans l'entreprise car l'ordinateur y vient remplacer l'homme dans certaines tâches et certains contrôles.

Dans ces conditions, il est clair que faire l'audit financier « autour de l'ordinateur » dans un milieu informatisé serait très risqué pour l'auditeur. Et la question de savoir s'il faut avoir des connaissances solides en informatique pour faire l'audit « à travers l'informatique » ne se pose pas d'autant que les normes d'audit stipulent qu'on peut avoir recours à des travaux d'autres experts, les informaticiens en l'occurrence.

Malheureusement, force est de constater que ce recours à des spécialistes n'est pas systématique dans les cabinets alors que la plupart d'entreprises sont aujourd'hui informatisées.

Dans nos développements, nous avons montré qu'il est nécessaire, pour l'auditeur qui veut donner une opinion avec un minimum de risques sur les états financiers produits par l'informatique, d'adopter dans un milieu informatisé une démarche à deux niveaux :

- Audit de la fonction informatique
- Audit des applications

Nous osons espérer que cette étude suscitera l'intérêt des professionnels d'audit pour mieux adapter leur démarche en vue d'une plus grande pertinence d'appréciation du contrôle interne des milieux informatisés dont les configurations deviennent d'ailleurs de plus en plus complexes pour l'auditeur.

Enfin, nous n'ignorons pas que notre travail présente des limites dont les principales sont :

- nos stages en cabinets ne nous ont pas permis de tester nos acquis en matière d'audit informatique ; ce qui veut dire que dans le cadre de notre cas d'application, nous n'avons pas bénéficié de la supervision d'un professionnel d'audit expérimenté en la matière.
- nous avons centré notre travail sur un seul aspect de l'audit informatique alors que nous avons souligné que la notion d'audit informatique est très vaste et recouvre plusieurs aspects de la gestion de l'entreprise.

Ce faisant, notre souhait est d'avoir ouvert la voie aux futurs stagiaires pour approfondir d'une part la question de l'audit en milieu informatisé et d'autre part, pour aborder les autres aspects de l'audit informatique à savoir : l'audit du schéma directeur, l'audit des projets informatiques, l'audit des SGBD, l'audit du réseau, etc.



Cependant, nous pensons que ces nouvelles perspectives qui s'ouvrent aux auditeurs requièrent un préalable important qui est celui de la refonte des cours d'informatique et d'audit informatique pour que plus jamais on ne parle « d'auditeurs financiers vs auditeurs informatiques mais d'auditeurs tout court ».

Dakar, le 5 janvier 2000

CESAG - BIBLIOTHEQUE

BIBLIOGRAPHIE

LIVRES

COLLINS, VALIN (1992), Audit et Contrôle Interne

DANIEL, JOCELYN et PETIT (1985), Guide pour l'audit financier des entreprises informatisées (ATH-CLET)

DERRIEN Y. : Les Techniques de l'audit informatique

JENKINS, PINKNEY (1984), Audit des systèmes et comptes gérés sur informatique, traduction et adaptation ROY J. et GAUDRON P.

LEGER M.,(1989): Compétences financières

RITZ R. J., (1986), Audit et Informatique

RUBIELLO, (1986), Progiciels de comptabilité

THORIN M., (1984), L'Audit informatique

ARTICLES

COLLINS, Lionel (1990), Evolution de l'audit, *Cahiers français*, n°248: 3-9

FRERY, Frédéric, (1990), Les systèmes Experts et l'Audit, *Cahiers français*, n°248 :54

GAUTHIER, Gauthier (1992), L'Informatique: un outil pour l'audit, *Cahiers français*

JOLY Daniel, (1999), Les progiciels intégrés et les nouveaux outils informatiques vont-ils changer l'approche d'audit ?, *Revue Française de Comptabilité*, n°316 :32-35

LAPORTE et PRUDHOMME, (1999), Audit informatique dans les entreprises : évaluation du contrôle interne et contrôle des comptes, *RFC*, n°316 :26-31

LIPSKI, Stéphane, (1999), Le commissariat aux comptes et l'évolution de l'informatique, *RFC*, n°316 :19-20

PETIT, Gérard (1997), Le contrôle interne est encore le meilleur moyen d'enrayer la fraude, *Revue Française de l'Audit interne*, N°135 : 20-22

POMPER, Gérard (1990), L'Audit informatique, *Cahiers Français*, N°248 : 34-37

STOLOWY, Hervé (1990), Les Flow-Charts, *Cahiers Français*, N°248 : 66-67

TROUCHAUD Philippe, (1999), Appréciation du contrôle interne informatique des grandes entreprises et impact sur le contrôle des comptes, *RFC*, n°316 :21-25

AUTRES

Séminaire d'informatique (BASSENE J., CESAG, 1999)

Séminaire de méthodologie d'audit (FALILOU D., CESAG, 1999)

Séminaire d'audit informatique (SARR B., CESAG, 1999)

Mémoire sur la Pratique d'audit dans les systèmes informatisés (A. DIARRA, CESAG, 1994)

Mémoire sur l'Enseignement Assisté par Ordinateur (sur l'aspect Systèmes Experts, H.

ASSOUMANA, HEC Liège, 1984)