CENTRE AFRICAIN D'ETUDES SUPEREIURES EN GESTION
(CESAG)
BP 3802 Dakar Tél. : (221) 8397360 Boulevard du Général DE GAULLE/ SENEGAL

INSTITUT SUPERIEUR DE COMPTABILITE
(I.S.C.)

MAITRISE PROFESSIONALISEE DE TECHNIQUES COMPTABLES ET FINANCIERES MPTCF

4ème Promotion / 2004-2006

Mémoire de Fin de Formation

ANALYSE DES RISQUES LIES A LA COMPTABILITE INFORMATISEE : CAS DU CABINET SECCAPI

Présenté par :
BARRY HAMADE

Directeur de mémoire :
M. BOUGOUMA OUSSENI
Chef de Mission au Cabinet
SECCAPI

Octobre 2006

DEDICACE

Je dédie ce mémoire à :

Mon grand-père, lui qui nous a quitté prématurément ;

Ma grand-mère que je n'ai pas eu l'occasion de bien connaître ;

Qu'ils reposent en paix et qu'ils trouvent ce mémoire comme le travail d'un petit fils qui a bénéficié du soutien sans faille de leur fils **BARRY SAIDOU**.

REMERCIEMENTS

Tout d'abord nous remercions la Direction du CESAG, le corps professoral, l'ensemble du personnel pour la qualité de l'encadrement, des enseignements et des services rendus.

Nous adressons également nos sincères remerciements à Madame la Directrice Générale du cabinet SECCAPI pour nous avoir accordé ce précieux stage.

Nous adressons nos sincères remerciements également à notre oncle BARRY SAIDOU et sa famille à JEDDAH pour leur soutien sans faille, sans lequel nous ne serions pas ce que nous sommes aujourd'hui.

Je suis redevable à Mr BOUGOUMA, Chef de missions de sa disponibilité et de son soutien incessant, de son abnégation discrète et de sa chasse impitoyable à l'erreur.

Nous manifestons notre reconnaissance à la famille OUEDRAOGO à Dakar pour leur hospitalité.

Nous adressons nos sincères remerciements à l'ensemble du corps professoral du CESAG pour la qualité de la formation reçue.

Nous remercions également l'ensemble du personnel de SECCAPI pour leur esprit d'équipe.

Nous remercions l'ensemble des collègues pour la bonne ambiance qui a prévalue durant la durée de la formation.

SIGLES ET ABREVIATIONS

SYSCOA : Système Comptable Ouest Africain

OHADA : Organisation pour l'Harmonisation en Afrique du Droit des Affaires

SECCAPI : Société d'Expertise Comptable, de Conseils, d'Assistance et de Prestation Informatique.

TAFIRE : Tableau de Financement des Ressources et des Emplois

SA : Société Anonyme

SARL : Société A Responsabilité Limité

CESAG : Centre Africain d'Etudes Supérieures en Gestion

DGI : Direction Générale des Impôts

CNIL : Commission Nationale Informatique et Liberté

CNCC : Compagnie Nationale des Commissaires aux Comptes

DAF : Direction Administrative et Financière

PGI : Progiciel de Gestion Intégré

HP: Hewlett Packard

ICBM: Inter Continental Business Machines

IMMO: Immobilisations

RAM: Random Acces Memory

MO: Méga Octet

MULTI-M : Multi médicaments

GO : Giga Octet

OD : Opérations Diverses

PC: Personal Computer

STBF : Société de Gestion des Terminaux Fruitiers

TDT : Tary Dagnon Toé

LISTE DES TABLEAUX ET FIGURES

Liste des tableaux

Liste des figures

LISTE DES ANNEXES

TABLE DES MATIERES

INTRODUCTION GENERALE

Le processus d'informatisation d'une entreprise s'appuie sur la notion de délégation à l'informatique de certaines tâches, à savoir : la fonction calcul, enregistrement, édition, contrôle, gestion des informations, leur mise à disposition et leur archivage, etc, antérieurement réalisées par le personnel, qui devient utilisateur.
Mais cette délégation ne doit pas forcement signifier abandon de responsabilité. L'informatique, autrefois utilisée dans certains domaines, est de nos jours incontournable dans la tenue de la comptabilité du fait du volume très élevé des opérations à traiter et surtout de l'évolution très rapide des logiciels appropriés comme saari, ciel compta, Halley, coda financial, winner compta, etc.

L'informatique prend de plus en plus d'importance dans le processus d'information au sein de l'entreprise. L'une des conséquences de ce phénomène, est la place prépondérante qu'elle occupe dans la production de l'information financière.

La vitesse de l'innovation technologique liée aux ordinateurs et aux télécommunications, ces dernières années, et l'intégration d'opérations automatisées rendent les entreprises de plus en plus dépendantes de la fiabilité et de la continuité de leurs systèmes informatiques. Ainsi, il importe de mesurer les risques, non seulement en fonction de la probabilité ou de la fréquence de leur survenance, mais aussi en mesurant leurs effets possibles. Ces effets, selon les circonstances et le moment où ils se manifestent, peuvent avoir des conséquences non négligeables ou catastrophiques.

En effet, parlant des technologies et de la communication, DANDIGNE(2002 :12) disait que : « elles étaient supposées entraîner une baisse des prix, une amélioration de la qualité, une réduction des cycles de production, un meilleur partage de l'information, l'internationalisation des échanges, etc.)

Mais force est de constater de nos jours que l'informatique fait apparaître au sein de l'entreprise de nouveaux types de risques qui obligent les dirigeants à faire de leur maîtrise une priorité, gage de bonne réputation et autres conséquences que nous étudierons.

Tout travail scientifique pour être bien mené mérite que soit bien défini son contexte, son cadre d'étude de même que ses limites. Tous ces aspects permettent de mieux saisir la problématique afin de garantir la réussite de l'étude abordée.

I Problématique

Les entreprises hier encore uniquement soucieuses de qualité et de productivité, doivent intégrer dans leur vie quotidienne le souci de disposer d'informations fiables au temps opportun, gage d'une bonne prise de décision. Ce besoin de plus en plus croissant de disposer d'informations pousse les entreprises à devenir très dépendantes de l'outil informatique. Celui-ci est utilisé dans tous les services de l'entreprise grâce à des logiciels d'application acquis sur le marché ou développés en interne.

Obnubilées par les prouesses technologiques, mais aussi par le marketing de l'informatique, les entreprises s'adonnent à un usage sans retenue de l'outil informatique. Cette pratique entraîne irrémédiablement l'apparition de nouveaux risques potentiels et même réels dans la gestion des entreprises en général et plus particulièrement dans la comptabilité (Thomas Konan Konan ; 2002).

Cette tendance va de pair avec une sophistication de la criminalité informatique, et donc des risques auxquels sont exposés les systèmes d'informations des entreprises.

Ainsi les entreprises disposant de systèmes d'informations automatisés doivent faire face à de multitudes de problèmes liés notamment au personnel, au traitement des informations et leur transmission, aux matériels, aux logiciels et à la sécurité du système informatique.

De nombreux dirigeants d'entreprise comme SECCAPI commencent à réaliser l'impact de l'informatique sur l'aliénation des informations et de leur sécurité et admettent désormais l'existence des risques encourus et la vulnérabilité à laquelle leur entreprise est confrontée

Cette exigence informatique et organisationnelle nécessite une étude approfondie dans le but d'assurer la qualité des informations reçues et la maîtrise des risques.

En outre, ces exigences, l'un des grands problèmes des entreprises est lié à la mauvaise gestion des systèmes informatiques qui peut mettre en péril la continuité d'exploitation et aux malveillances du personnel c'est-à-dire les vols de matériels, les dégâts volontaires ou involontaires, les fraudes, les détournements d'informations discrètes et confidentielles.

Maîtriser les risques humains (maladresse, inconscience ou ignorance, espionnage) ; les risques techniques (liés aux matériels, liés aux logiciels, liés à l'environnement, et les programmes ou procédures de contrôle indépendants, les mots de passe) ; la sécurité physique des installations et des données ; la sécurité des traitements sont aujourd'hui les grandes préoccupations des dirigeants des entreprises.

La pratique de la gestion des risques, n'est pas nouvelle dans le domaine des affaires. Le milieu des banques et celui des assurances entre autres ont vite compris les bienfaits d'une

telle pratique. Les expériences relatées dans ce domaine, témoignent largement des avantages de bien gérer les risques.

Le monde de la finance n'est pas le seul cependant à gérer selon cette approche. Certaines entreprises influencées par le besoin de disposer d'informations fiables et préoccuper d'offrir des services de qualité à leur clientèle, ont même emboîté le pas.

Ainsi, nous avons convenu à cet effet d'analyser ces divers problèmes. L'analyse des divers problèmes revient à étudier leurs causes et leurs conséquences.

Ces causes sont essentiellement :

- l'absence d'une politique informatique formalisée qui se traduit par un développement anarchique du matériel et des logiciels et des acquisitions inadaptées aux besoins, des coûts excessifs et une évolution non maîtrisée ;
- la non séparation des fonctions qui génère des risques de modifications indues des programmes et des données ;
- des procédures de développement non suffisamment maîtrisées ;
- une protection insuffisante d'accès aux données et au matériel ;
- l'insécurité physique des installations, des données et des traitements.
- Le manque de documentation sur l'utilisation des programmes ;
- L'absence des procédures et une mauvaise politique de sauvegarde des données ;
- Le manque de formation ou les formations inadaptées au contexte des entreprises qui posent souvent le problème de compétence ;
- Les situations conflictuelles entre personnel ;
- Les réseaux inexistants ou difficilement interconnectable voire saturés
- Le paramétrage incorrect des logiciels
- L'insuffisance ou la passivité du contrôle interne.

Les problèmes liés à l'informatique entraînent plusieurs conséquences et entre autres, il y a :

- la perte de sa crédibilité lorsque les informations financières sont remises en cause. Cette perte de crédibilité entraîne des pertes financières énormes et une baisse du chiffre d'affaires ;

- La responsabilité pénale des dirigeants peut être engagée car il s'agit d'une infraction selon la loi informatique et liberté ;
- Ces problèmes entraînent également la remise en cause de l'intégrité du système d'information, la remise en cause de la continuité de l'exploitation ;
- entraînent des coûts d'exploitation des ressources informatiques plus élevés par rapport aux possibilités théoriques du matériel ;

- la remise en cause de la fiabilité des traitements et de l'intégrité des données.
- Impossibilité temporaire ou définitive de reprise d'activité ;
- Frais d'expertise liés aux sinistres ;
- Frais de réparation ou de remplacement des matériels ;
- Immobilisation du personnel.

Dans un souci de résolution des problèmes liés aux causes multiples, plusieurs ébauches de solutions s'offrent aux dirigeants d'entreprise. Ainsi nous pouvons mentionner celles liées au contrôle interne, celles liées à l'audit informatique et celles liées à la mise en place d'une bonne politique de sécurité informatique.

- concernant le contrôle interne, il a été démontré que dans le cadre du management des systèmes informatiques, l'efficacité du contrôle garanti :

La maîtrise des risques informatiques,

La formation adéquate du personnel,

Le contrôle de l'introduction des données,

Le contrôle de l'exploitation.

Cela vise beaucoup plus à réduire les risques d'erreurs malencontreuses, en d'autres termes, à protéger les informaticiens vis-à-vis d'eux-mêmes.

- Par contre la mise en place d'une bonne politique de sécurité informatique, qui est l'ensemble des moyens techniques, matériels, organisationnels, juridiques et humains nécessaire pour conserver ou rétablir la disponibilité, l'intégrité et la confidentialité des informations ou du système permet aux dirigeants d'entreprise d'éviter les risques en amont.

-L'audit informatique apparu dans les années 70 est utilisé comme une mission d'évaluation de conformité par rapport à une politique de sécurité ou à défaut par rapport à un ensemble de règles et de sécurité. C'est un moyen efficace pour garantir la fiabilité du système informatique. L'audit informatique devrait conduire à une réduction des risques informatiques et à une amélioration indirecte de la situation économique et financière de l'entreprise.

Partant de là, la solution qui retient notre attention et semble répondre aux problèmes exposés est celle liée au contrôle interne..

Selon Alain Desroches « al » (2003) le risque étant inhérent à l'activité humaine, toute la question est de savoir comment le découvrir, l'appréhender, l'anticiper, le quantifier, et ceci étant fait, prendre les décisions correspondantes, afin, non pas d'éliminer le risque vaine gageure et stérilisation garantis de l'initiative mais de le gérer (en éliminer certains, en réduire d'autres, et aussi, ne l'oublions pas en accepter quelques-uns mais en toute connaissance de cause)

D'où notre question de recherche, à savoir « **COMMENT MAITRISER LES RISQUES DANS LE CADRE D'UNE COMPTABILITE INFORMATISEE ?** »

En vue d'apporter une réponse, nous posons les questions spécifiques suivantes :

- Quelle organisation comptable à mettre en place dans le cadre d'une comptabilité informatisée ?
- Quelles sont les règles légales et fiscales à respecter ?
- Quels sont les différents risques possibles ?
- Quelle démarche pour apprécier le contrôle interne d'une comptabilité informatisée ?

C'est pour répondre à toutes ces questions que nous nous proposons d'étudier comme thème : « **ANALYSE DES RISQUES LIES A LA COMPTABILITE INFORMATISEE** ».

II- Objet De L'étude

La présente étude porte sur « l'analyse des risques liés à la comptabilité informatisée ». En effet, il s'agit pour nous de contribuer à l'amélioration du système de maîtrise des risques au niveau de la comptabilité.

III- Objectifs

L'objectif principal que nous poursuivons est de contribuer à éveiller la conscience des utilisateurs sur les risques liés à la comptabilité informatisée.

Les objectifs suivants en découlent :

- Quantifier les risques le leur impact en cas de survenance,
- Décrire l'organisation comptable en milieu informatisé,
- Faire des recommandations.

Par ce thème, nous entendons nous intéresser à l'analyse des risques comptables et informatiques liés à la comptabilité informatisée

IV- Intérêt de L'étude

Aujourd'hui le besoin en matière de maîtrise des risques devient de plus en plus crucial car contrairement à ce que pensent certaines personnes, tout ce qui sort de l'ordinateur n'est pas forcement juste. L'intérêt de l'étude se trouve à trois niveaux :

► ***Pour nous-mêmes stagiaire***

Cette étude est l'occasion d'approfondir nos connaissances théoriques acquises au cours de l'année académique par la confrontation aux données de la vie de l'entreprise.
C'est également pour nous l'occasion de cerner davantage les politiques mises en place par l'entreprise pour maîtriser les risques liés à la comptabilité informatisée. Elle accroît aussi notre expérience et peut nous servir de référentiel dans l'exercice de la profession dans le cadre de notre plan de carrière.

► ***Intérêt pour la société***

Cette étude vise à lui donner une amélioration de la maîtrise des risques dans sa quête de réduire au mieux les risques dont les conséquences ne sont plus à démontrer. Elle permettrait en plus, la mise en œuvre réelle des politiques de maîtrise des risques.

► ***Intérêt pour le CESAG***

Les résultats de l'étude pourront être intéressants pour le CESAG où la recherche occupe une place de choix. Ils pourront alors servir de cadre de référence à des recherches futures. Ainsi, ils pourront servir d'étude de cas pour les besoins pédagogiques et renforcer l'expertise du centre dans ce domaine

V Démarche de L'étude

La démarche utilisée pour la mise en œuvre de cette présente étude est articulée autour des étapes suivantes :

► une recherche documentaire au niveau du CESAG, de l'Internet et des notes de cours,
► L'élaboration de guide d'entretien pour la collecte des informations,
► des entretiens avec les personnes ressources,
► une analyse des données collectées,
► une observation physique au sein de l'entreprise.

VI- Articulation De L'étude

Outre l'introduction et la conclusion générale, notre travail comprendra deux grandes parties :
La première partie consacrée en une revue de littérature en matière de risques comptables et informatiques. Elle est structurée en trois chapitres :

- L'organisation comptable,
- Les dispositions légales et règlementaires des traitements informatisés,
- Les risques liés à la fonction informatique et la méthodologie de la recherche.

La deuxième partie dans laquelle nous allons nous atteler à parler de la maîtrise des risques, le cadre pratique du mémoire. Elle comporte quatre chapitres :

- La présentation de la société
- Présentation du système comptable informatisé de la société
- Evaluation du contrôle interne de sa fonction informatique.
- Synthèses et recommandations.

PREMIERE PARTIE : CADRE THEORIQUE

CHAPITRE I : L'ORGANISATION COMPTABLE

INTRODUCTION

L'organisation comptable adoptée par l'entreprise doit permettre de traduire l'image fidèle de la situation financière, patrimoniale, et du résultat de l'entreprise et assurer la pertinence partagée.

Elle doit permettre l'établissement dans les délais requis des états financiers réguliers et sincères, donnant une image fidèle du patrimoine, de la situation financière et du résultat de l'entreprise.

Selon le corpus du SYSCOA l'organisation comptable est définie comme étant « l'ensemble des procédures comptables et administratives mises en place dans l'entreprise pour satisfaire aux exigences de régularité, de sincérité pour assurer l'authenticité des écritures de façon à ce que la comptabilité puisse servir à la fois d'instrument de mesures des droits et obligations des partenaires de l'entreprise, d'instrument de preuves et d'information des tiers et de gestion ».

L'organisation comptable optimale est décrite comme celle qui permet de faire face aux obligations indiquées dans le droit comptable en matière de tenue des livres obligatoires, de tenue et de classement des documents et pièces justificatives et en matière de traitement informatique. L'organisation porte sur les ressources humaines mais également sur les procédures (le praticien : système comptable OHADA ; 2003)

Selon l'article 16 du droit comptable, les procédures doivent être codifiées dans un document appelé manuel de procédures comptables.

Pour que l'organisation comptable puisse jouer pleinement son rôle, le respect de certaines règles est impérieux, à savoir :

- la tenue de la comptabilité dans la langue officielle et en monnaie ayant cours légal dans le pays ;
- Le respect de la technique de la partie double qui a été créée par Lucas Pacioli depuis 1494 ;
- La justification des écritures comptables par des pièces comptables et leur conservation pendant au moins 10 ans ;
- Le respect de l'enregistrement chronologique des opérations ;
- Mise en place dans l'entreprise d'un plan comptable normalisé ;
- Avoir un personnel qualifié et disposer d'un manuel de procédures comptables ;

- Et enfin tenir des livres comptables.

Dans ce chapitre, nous allons essayer d'étudier les principes comptables édictés par le SYSCOA. Il s'agit pour nous également de parler de l'image fidèle, de la pertinence partagée, des livres comptables obligatoires et enfin des systèmes et procédés comptables.

1.1 Les principes comptables

Le SYSCOA contrairement aux autres plans comptables antérieurs, a énoncé explicitement huit (08) principes comptables qui font l'unanimité des utilisateurs de la comptabilité et un neuvième qui n'est admis qu'à travers ses cinq applications. Ainsi, nous avons :

→ ***Le principe de la continuité***

La possibilité d'application des autres principes dépend de ce principe, selon lequel la comptabilité est tenue en prenant pour hypothèse que l'entité n'a pas l'intention de cesser son activité ou de la réduire sensiblement.

→ ***Le principe de la prudence***

Il se définit comme l'appréciation juste et raisonnable des faits et a pour but d'éviter de donner une image trop optimiste des résultats et de la situation financière de l'activité. En résumé ce principe recommande l'enregistrement des charges dès qu'elles sont probables et à omettre les produits probables. Ainsi selon Joël Mabudu (2003 :24-28) : « ce principe, largement lié à la fonction juridique de la comptabilité traduit le souci d'éviter une surévaluation du résultat et de la situation de l'entreprise, qui pourrait léser les tiers mis abusivement en confiance et permettre une distribution de bénéfices qui se révèleraient en partie fictifs ».

→ ***Le principe de la permanence des méthodes***

Selon ce principe, pour assurer la comparabilité de l'information comptable dans le temps, les méthodes d'évaluation du patrimoine et de présentation de l'information doivent être identiques d'un exercice à l'autre. Il n'interdit pas les changements mais les règlemente.

→ ***Le principe du coût historique***

Pour simplifier les traitements comptables, ce principe préconise l'évaluation de tout élément du patrimoine à sa valeur d'entrée qui doit demeurer inchangée. Ce principe est applicable dans les pays à inflation modérée

→ ***Le principe de correspondance bilan de clôture et bilan d'ouverture***

Encore appelé principe d'intangibilité du bilan, il garantit la continuité de l'information fournie par les états financiers et interdit l'imputation directe d'opérations sur la situation nette.

→ ***Le principe de la transparence***

Ce principe sous entend le respect des règles et la non dissimulation d'informations significatives. Il exige le respect du plan comptable et de sa terminologie, le respect de la présentation des états financiers et le respect de la non compensation.

→ ***Le principe de la séparation ou spécialisation des exercices***

Il est à l'origine du découpage de la vie de l'entreprise en exercices, et selon ce principe les charges et les produits d'un exercice donné ne doivent pas être transférés sur d'autres exercices.

→ ***le principe de l'importance significative***

Principe d'application difficile car très subjectif, il préconise la prise en compte dans les états financiers tous les éléments susceptibles d'influencer le jugement que les destinataires de ces états financiers de l'entreprise peuvent porter sur le patrimoine, la situation financière et le résultat de l'entreprise.

→ ***Le principe de la prééminence de la réalité sur l'apparence juridique***

Principe d'origine anglo-saxonne, il est partiellement adopté par le SYSCOA. Il préconise une interprétation plus économique des faits car certains éléments bien qu'ils n'appartiennent pas à l'entreprise ont participé à la réalisation des résultats ainsi obtenus.

Il faut noter que ces principes peuvent faire l'objet d'une dérogation si l'entreprise trouve une nécessité légitime. L'objectif final recherché par l'application de tous ces principes est l'image fidèle.

1.2 L'image fidèle et la pertinence partagée

1.2.1 L'image fidèle

Elle est obtenue par l'application de bonne foi des règles du SYSCOA, sans souci de dissimuler la réalité derrière l'apparence : il y a présomption d'image fidèle. Mais pour les cas exceptionnels, cette présomption est obtenue, soit en mentionnant les informations complémentaires dans l'état annexé, soit il s'agit des dérogations aux règles du SYSCOA

Elle est héritée des pratiques anglo-saxonnes sous le nom « true and fair view ». L'image fidèle ne constitue pas un principe supplémentaire mais plutôt une résultante des principes comptables précédemment étudiés.

En effet, l'image fidèle donnée par les états financiers doit refléter la situation patrimoniale, financière et du résultat de l'entreprise. Cette image fidèle doit être donnée à travers tous les états financiers qui sont indissociables. Le bilan éclaire particulièrement le lecteur sur le patrimoine, le compte de résultat sur les éléments concourant à la formation de ce résultat et le TAFIRE, en liaison avec le bilan de l'année précédente et avec le compte de résultat, éclaire sur l'évolution de la situation financière. Mais l'état annexé vient compléter et expliciter « l'image » donnée par les trois autres états.

1.2.2 La pertinence partagée

Elle est l'un des objectifs assignés à la comptabilité : l'information multiple. A la différence des nomes anglo-saxonnes (américaines principalement) qui privilégient l'information à destination boursière et dans laquelle les états financiers sont conçus comme un instrument de transparence d'un capitalisme boursier, la présente norme comptable entend répondre au mieux aux besoins d'informations de tous les agents d'une économie marchande dont le centre est la libre entreprise (SYSCOA, plan comptable général des entreprises ; 1996)

La pertinence partagée poursuit trois principaux objectifs : l'information comptable pour qui ? Pour quoi ? Et de quelle nature ?

L'information comptable qui est véhiculée par les états financiers annuels : le bilan, le compte de résultat, le TAFIRE, l'état annexé et l'état complémentaire, doit servir d'éclairage à des prises de décisions à l'ensemble des partenaires de l'entreprise (Etat, investisseurs, fournisseurs, clients, personnel, la centrale des bilans et l'extérieur) et à l'entreprise elle-même.

Cependant cette pertinence partagée est relative car ce qui est pertinent pour l'un ne l'est pas forcement pour l'autre. Ce qui constitue en même temps une faiblesse parce que les seuls documents de synthèse ne peuvent pas satisfaire tous les partenaires de l'entreprise qui ont souvent des intérêts divergents.

1.3 Les systèmes et procédés comptables

Une bonne organisation comptable repose sur la mise en place d'un bon système comptable et de procédé permettant d'enregistrer et de traiter les informations comptables.

1.3.1 Les systèmes comptables

Un système comptable est défini comme étant l'organisation générale d'une comptabilité, c'est-à-dire l'ensemble des supports permettant d'agencer et de traiter les informations jusqu'aux états financiers. Il existe principalement deux types de systèmes comptables :

► **Le système classique** :

C'est le système le plus ancien mais le moins usité de nos jours. Il est basé sur l'utilisation d'un journal unique dans lequel toutes les opérations sont enregistrées chronologiquement. Avec l'avènement de l'informatique et le développement sans cesse croissant du volume des opérations à traiter, il est abandonné au profit du système centralisateur.

► **Le système centralisateur** :

Il présente des similitudes avec le système classique. Leur différence réside du fait de l'éclatement du journal unique en plusieurs journaux appelés journaux auxiliaires. Les opérations sont d'abord enregistrées dans les journaux auxiliaires avant d'être centralisées dans le journal central avec souvent l'utilisation des comptes de virement interne pour éviter les doubles enregistrements. C'est le système le mieux adapté à l'ordinateur. Il facilite la répartition des tâches au niveau de la comptabilité, donne des comptes plus analytiques et permet une utilisation multiple au même moment.

1.3.2 Les procédés comptables

La comptabilité peut être tenue par tout procédé technique approprié à condition que le procédé et les méthodes utilisés confèrent par eux-mêmes un caractère d'authenticité aux écritures comptables, et permettent tous les rapprochements utiles et nécessaires à un contrôle.

On entend par procédé comptable, tout support matériel d'un document comptable. De la même manière que les systèmes comptables ont évolué du système classique, au système centralisateur, les procédés comptables ont également connu cette évolution. Ainsi, on a :

► **Le procédé de traitement manuel** :

Ce procédé consiste à reporter manuellement les opérations comptables effectuées dans le journal ou dans les journaux auxiliaires (avec comme support le papier). De nos jours il n'existe que dans les très petites entreprises dans lesquelles le volume des opérations à traiter n'est pas élevé ;

► **Le procédé de traitement informatisé**

Il utilise comme support la machine (généralement l'ordinateur) en combinaison avec un logiciel comptable. Contrairement au procédé manuel, l'intervention de l'homme ici se situe à un seul niveau, qui est la préparation des imputations comptables et leur saisie. Ce procédé n'est applicable que grâce à l'utilisation de logiciel. Ainsi le logiciel comptable utilisé doit permettre de générer à tout moment une balance de contrôle assurant l'égalité des totaux des mouvements des comptes individuels des opérations avec les totaux des journaux auxiliaires. Un bon logiciel doit respecter les principes suivants :

- il doit être fiable ;
- Ses données doivent être infalsifiables, mais puisque le risque zéro n'existe pas, elles devront être protégées ;
- Les opérations doivent être traçables.

Ce procédé constitue le champ de notre étude puisqu'il s'agit de la comptabilité informatisée.

1.4 Les livres comptables

La loi fait obligation aux entreprises de disposer de quatre types de livres comptables (le livre journal, le grand livre, la balance générale des comptes et le livre d'inventaire).

► Le livre journal :

C'est le livre dans lequel doit être enregistrés tous le mouvements relatifs à l'exercice. L'enregistrement doit être exhaustif et chronologique opérations par opérations et dans l'ordre de leur valeur comptable qui est la date d'émission pour les opérations internes et la date de réception pour celles externes. Les mouvements sont récapitulés par période préalablement déterminée qui ne peut excéder un mois.

Il regroupe tous les comptes ouverts par l'entreprise. Ces comptes sont reportés simultanément dans le journal et dans le grand livre.

► La balance générale des comptes

C'est l'état récapitulatif de tous les comptes faisant apparaître leur solde débiteur ou créditeur de l'ouverture de l'exercice, le cumul des mouvements au débit et/ou au crédit depuis l'ouverture pour chaque compte et les soldes créditeurs ou débiteurs de chaque compte à la date considérée (généralement à la clôture de l'exercice).

► Le livre d'inventaire :

Il constitue le document dans lequel sont transcrits les documents de synthèse (bilan, compte de résultat) de chaque exercice, ainsi que le résumé de l'opération d'inventaire.

Ces documents doivent être tenus sans blanc, ni altération d'aucune sorte et toute correction d'erreur doit être effectuée exclusivement par inscription en négatif des éléments erronée et l'enregistrement exact est ensuite effectué.

1.5 Organisation d'une comptabilité informatisée

L'informatique, traditionnellement gérée comme une fonction interne de l'entreprise, est désormais marquée à la fois par des pratiques fréquentes d'externalisation surtout la fonction informatique comptable, par la généralisation des solutions de type PGI (Progiciel de Gestion Intégré, globalisant fonctions comptables et financières et autres fonctions de l'entreprise), ce qui nécessite la mise en place ou l'adaptation des organisations à ces nouveaux environnements.

L'environnement informatique en comptabilité existe lorsqu'un ordinateur est utilisé pour le traitement des informations financières concourant à l'établissement des comptes, que cet ordinateur soit exploité par l'entité ou par un tiers.

Ainsi dans un souci de recherche de transparence financière, les conséquences de la généralisation de l'informatique dans l'entreprise et la complexité croissante, les systèmes d'information automatisés doivent être parfaitement identifiées, tout particulièrement sur l'organisation de la comptabilité, source de l'information financière.

A cet effet l'organisation d'une comptabilité informatisée, du fait que le traitement d'une comptabilité par informatique se caractérise notamment par la raréfaction voire l'absence de trace matérielle justifiant les opérations, nécessite la mise en place des processus suivants :

► Un système de traitement

Par système de traitement, il faut entendre l'ensemble devant permettre à la fois :

- d'atteindre les objectifs fixés par les dirigeants de l'entreprise pour les besoins de la gestion interne (gestion des stocks, facturation…) ;
- d'obtenir les états et renseignements de la comptabilité générale dans le respect des dispositions légales et règlementaires en la matière.

Le système de traitement est constitué par d'une part , des matériels comme les organes périphériques d'entrée et de sortie, les mémoires auxiliaires connectés à l'organe central de traitement en fonctionnant sous son contrôle ; et d'autre part, des logiciels utilisés pour la mise en œuvre de toutes les applications.

► Une procédure de validation

Cette procédure de validation doit permettre de rendre définitif les enregistrements effectués dans le livre journal et dans le livre inventaire et doit rendre toutes modifications ou suppressions de l'enregistrement impossible. Autrement dit il s'agit d'une phase de traitement informatique qui consiste à figer les différents éléments de l'écriture de façon à ce que toute modification ultérieure de l'un de ses éléments soit impossible.

Avant la validation comptable d'une écriture, l'utilisateur peut modifier tout élément comptable qu'il désire modifier. En effet, tant que la validation n'est pas demandée par l'utilisateur, les écritures, parfois conservées dans un fichier intermédiaire, ne font en fait pas partie du système comptable.

Les éditions faites à partir de ce fichier intermédiaire constituent seulement des listes de contrôle appelées couramment brouillard de saisie, procès-verbal d'entrée, accusé de réception de saisie, etc. En conséquence, il n'y a pas lieu d'apprécier la régularité du système pendant cette phase.

C'est ainsi après la validation comptable qu'on peut commencer à apprécier la régularité du système comptable.

► Une procédure de clôture

Cette procédure de clôture est destinée à figer la chronologie et à garantir l'intangibilité des enregistrements. Elle est appliquée au total des mouvements enregistrés. Lorsque la date d'une opération correspond à une période déjà figée par la clôture, l'opération concernée est enregistrée à la date du premier jour de la période non encore clôturée, avec mention expresse de sa date de survenance.

► Les mentions minimales d'un enregistrement comptable

Tout enregistrement comptable doit préciser l'origine, le contenu et l'imputation de chaque donnée, ainsi que les références de la pièce justificative qui l'appui.

CONCLUSION

Ce premier chapitre de la revue de la littérature, nous a permis de montrer à travers les documents que nous avons eu à lire, l'organisation comptable tant dans un environnement manuel que dans un environnement informatisé.

La comptabilité pour qu'elle puisse jouer pleinement son rôle doit être organisée. Mais cette organisation ne peut se faire sans tenir en compte les aspects légaux et règlementaires que nous essayerons de traiter dans le deuxième chapitre de notre revue de la littérature.

CHAPITRE II : LES DISPOSITIONS REGLEMENTAIRES ET JURIDIQUES DES TRAITEMENTS INFORMATISES

INTRODUCTION

L'existence de règles précises et formalisées relatives à l'appréciation de la qualité du système d'information de l'entreprise informatisée est primordiale, dans la mesure où ces règles sont appelées à servir de référence. Ainsi, progressivement, doctrine, jurisprudence, et législation essayent d'apporter des éléments de réponse aux multiples interrogations que suscite l'automatisation grandissante des processus de production de l'information financière dans l'entreprise.

Ainsi, en matière de textes qui régissent les traitements automatisés dont fait partie la comptabilité informatisée, nous avons les dispositions de l'article 22 du droit comptable OHADA, les textes fiscaux, la loi informatique et liberté, la loi relative à la protection littéraire et artistique, la loi relative à la fraude informatique.

2.1 Les Sources Juridiques Et Fiscales

2.1.1 Les obligations du droit comptable OHADA.

Selon l'article 22 du droit comptable lorsque l'organisation comptable repose sur un traitement informatique, elle doit recourir à des procédures qui permettent de satisfaire aux exigences de régularité et de sécurité requises en la manière de telle sorte que :

— Les données relatives à toute opération donnant lieu à enregistrement comptable comprennent, lors de leur entrée dans le système de traitement comptable, l'indication de l'origine, du contenu et de l'imputation de ladite opération et puissent être restituées sur papier ou sous une forme directement intelligible ;

— L'irréversibilité des traitements effectués interdise toute suppression, addition ou modification ultérieure d'enregistrement ; toute entrée doit faire l'objet d'une validation, afin de garantir le caractère définitif de l'enregistrement comptable correspondant ; cette procédure de validation doit être mise en œuvre au terme de chaque période qui ne peut excéder un mois ;

— La chronologie des opérations écarte toute possibilité d'insertion intercalaire ou d'addition ultérieure ; pour figer cette chronologie le système de traitement comptable doit

prévoir une procédure périodique (dite « clôture informatique ») au moins trimestrielle et mise en œuvre au plus tard à la fin du trimestre qui suit la fin de chaque période considérée ;

— Les enregistrements comptables d'une période clôturée soient classées dans l'ordre chronologique de la date de valeur comptable des opérations auxquelles ils se rapportent ; toutefois lorsque la date de valeur comptable correspond à une période déjà clôturée, l'opération concernée est enregistrée au premier jour de la période non clôturée ; dans ce cas, la date de valeur comptable de l'opération est mentionnée distinctement.

— La durabilité des données enregistrées offre des conditions de garantie et de conservation conformes à la réglementation en vigueur. Sera notamment réputée durable toute transcription indélébile des données qui entraîne une modification irréversible du support.

— L'organisation comptable garantie toute possibilité d'un contrôle éventuel en permettant la reconstitution ou la restitution du chemin de révision et en donnant droit d'accès à la documentation relative aux analyses, à la programmation et aux procédures des traitements en vue notamment de procéder aux tests nécessaires à l'exécution d'un tel contrôle ;

— Les états financiers périodiques fournis par le système de traitement soient numérotés et datés. Chaque enregistrement doit s'appuyer sur une pièce justificative établie sur papier ou sur un support assurant la fiabilité, la conservation et la restitution en clair de son contenu pendant les délais requis. Chaque donnée, entrée dans le système de traitement par transmission d'un autre système de traitement, doit être appuyée d'une pièce justificative probante.

Du point de vue fiscal, les traitements informatisés pour garantir leur fiabilité doivent respecter un certain nombre de règles, notamment disposer d'une documentation, le respect de formats des fichiers et les délais de conservation.

— La documentation qui doit être présentée à l'administration lors de contrôle fiscal notamment doit comporter au minimum le dossier de conception du système, le dossier de réalisation et de maintenance et le dossier d'utilisation et d'exploitation. Cette documentation joue un rôle très important car elle doit décrire les solutions techniques et organisationnelles qui permettent d'insérer des applications dans le système, elle permet également de définir de façon précise les entrées et les sorties de système, les règles de fonctionnement.

Enfin, c'est grâce à cette documentation, qui constitue un mode d'emploi du système ; que le fisc ou les nouveaux employés peuvent comprendre le fonctionnement du système.

— Les formats de fichiers, selon l'administration fiscale sont libres pour l'entreprise.

2.1.2 Les obligations de sources fiscales

La Direction Générale des Impôts (DGI) a la possibilité d'effectuer une vérification fiscale « à travers l'ordinateur », et peut étendre ses vérifications à l'examen de la documentation relative aux analyses, au respect des délais de conservation et au format des fichiers. Les vérificateurs, pour s'assurer de la fiabilité des procédures de traitements, peuvent procéder à des tests de contrôle sur le matériel utilisé par l'entreprise. Ainsi nous examinerons élément par élément dans les lignes qui suivent :

- Parlant des obligations relatives aux tests informatisés, le Code Général des Impôts (CGI) recommande : « à l'entreprise de conserver sur support magnétique, les fichiers, les procédures et les programmes susceptibles de permettre de tester a posteriori la fiabilité de traitements concourant, directement ou indirectement, à la formation des résultats comptables et fiscaux de la période vérifiée, ou à la confection des documents ou des déclarations rendues obligatoires ».

Cependant, lorsque l'entreprise a recours, pour tout ou partie de ses traitements automatisés, aux services d'un façonnier, elle est tenue de mettre les vérificateurs en mesure d'effectuer chez le façonnier les tests qu'ils estiment nécessaires à l'exercice du droit de vérification. Ces tests sont effectués dans les conditions définies dans le décret[1], y compris la possibilité pour le façonnier de fournir les copies des informations et des logiciels. Donc, il est dans l'intérêt du chef d'entreprise de prévoir, dans le contrat qui le lie au façonnier, la possibilité pour l'administration de procéder à des investigations.

- L'entreprise doit disposer d'une documentation qui doit être présentée à l'administration lors de contrôle fiscal et elle doit comporter au minimum le dossier de conception, de réalisation et de maintenance, et le dossier d'utilisation et d'exploitation.

- Pour ce qui est du format des fichiers, il est, selon l'administration fiscale, libre pour l'entreprise. Mais toutefois, si l'entreprise opte pour le contrôle sur le matériel, elle doit présenter des fichiers « à plat ».

- Le délai de conservation avant d'être une exigence fiscale constitue une nécessité pour l'entreprise (les données conservées peuvent servir de preuves, possibilité d'effectuer des

[1] Article 54, alinéa 4 du CGI et du décret du 29 décembre 1982

comparaisons temporelles, etc.). L'entreprise a l'obligation de conserver ses données sur supports informatiques pendant les trois (03) années puis sur tout autre support laissé à son choix pour les années restantes. Elle a aussi l'obligation d'assurer la conversion et la compatibilité des fichiers avec les matériels et logiciels existant lors du contrôle, lorsque son environnement informatique a été modifié avant la fin du délai légal.

2.1.3 La loi relative à la fraude informatique

Cette loi, contenue dans le code pénal, a essayé d'énumérer les faits qu'on peut qualifier de fraudes informatiques et a prévu des sanctions. Ainsi peuvent être considérées comme fraudes informatiques, les infractions suivantes :

- Accès où maintient frauduleux des données dans un système de traitement automatisé ;
- La suppression ou la modification des données contenues dans un système ou l'altération du fonctionnement du système ;
- La falsification des documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui ;
- Entravé ou faussé intentionnellement ou au mépris des droits d'auteurs, le fonctionnement d'un système de traitement automatisé.

Toutefois il faut noter que la tentative de ces délits est punie des mêmes peines que le délit lui-même.

2.1.4 La loi relative à la protection artistique et littéraire

Les dispositions de cette loi sont étendues aux auteurs des logiciels. En effet, l'article 45 stipule que : « sauf stipulation contraire, le logiciel créé par un ou plusieurs employés dans l'exercice de leurs fonctions, appartient à l'employeur auquel sont dévolus tous les droits reconnus aux auteurs et que son auteur ne peut s'opposer à l'adaptation du logiciel dans la limite des droits qu'il a cédés, ni exercer son droit de repentir ou de retrait ». Cette loi protège également les auteurs des logiciels contre les contrefaçons qui sont légions. A cet effet, l'article 47 stipule que : « toute reproduction autre que l'établissement d'une copie de sauvegarde par l'utilisateur ainsi que toute utilisation d'un logiciel non expressément autorisée par l'auteur ou ses ayants droit, est passible de sanctions prévues par ladite loi ». Mais cette protection s'éteigne à l'expiration d'une période de vingt-cinq (25) ans à compter de la date de création du logiciel.

2.2 Les règles et principes liés aux logiciels

Un logiciel peut être défini comme l'ensemble de programmes, de procédés, de règles, et de documentation, relatifs au fonctionnement d'un ensemble de traitement de données.

Il s'agit pour nous, dans cette partie de répondre à la question suivante : le logiciel utilisé pour le traitement de la comptabilité permet-il de garantir que les faits économiques intervenant dans l'entreprise se retrouvent traduits fidèlement et complètement dans la comptabilité ?

L'organisation d'une comptabilité informatisée suit pratiquement les mêmes règles que le système manuel. Toutefois certains principes et règles lui sont propres.

2.2.1. Règle de continuité d'exploitation et de régularité de la tenue des écritures.

Parlant de continuité d'exploitation et de régularité, GARNIER (1984 :532)disait que : « les écritures créées doivent être sans doublon et sans manquement, traduisant ainsi la continuité de l'exploitation, une continuité qui tient compte de l'inaltérabilité des écritures ». La continuité et la régularité interviennent que suite à la création des écritures et leur numérotation correcte.

2.2.2. Règle d'irréversibilité et d'inaltérabilité des écritures

Selon ANGOT « al »,1995 :59 « l'inaltérabilité suppose l'interdiction de modifier la composante légale d'une écriture c'est-à-dire ce qui appartient aux données constitutives des documents légaux (numéro d'écritures, date d'imputation, code journal préparation ». Selon cette règle, tous les enregistrements doivent apparaître clairement et doit demeurer inchangés.

2.2.3. Règle de conservation des supports informatiques

La conservation des supports informatiques doit se faire conformément aux règles fiscales en vigueur. Comme l'environnement des traitements automatisés ne garantit pas l'inaltérabilité des données de chaque période clôturée, la conservation doit se faire sur un support intelligible tels que les fiches les microfilms, les disques optiques, etc. La société peut choisir le support qu'elle désire mais doit s'assurer de la disponibilité des données pendant le délai de prescription.

2.2.4 Structure physique de l'organisation d'un logiciel

Le matériel essentiel pour la tenue d'une comptabilité informatisée est l'ordinateur, mais seul il ne pourra pleinement jouer son rôle, il doit être associé à un logiciel.

Depuis l'avènement de la bureautique, le logiciel, est au cœur du système d'information dont aucune entreprise ne pourrait plus se passer. Sa fiabilité est mesurée par sa probabilité à accomplir l'ensemble des fonctions spécifiées dans son document de référence, dans un environnement donné et pour un temps de fonctionnement donné.

Pour ce qui est de son organisation, ANGOT « al » disait que : « elle doit garantir deux types de contrôles : le contrôle à priori et le contrôle à posteriori ».

Le contrôle à priori est relatif au processus d'imputation qui veut qu'en principe qu'une fois l'information introduite exactement qu'il y ait peu de risques de la voir altérer.

Tandis que le contrôle à posteriori doit permettre de garantir une bonne sécurité quant à l'adéquation de l'instrument comptable.

Ainsi la structure de l'organisation du logiciel utilisé doit assurer la tenue de la comptabilité de manière à confirmer le caractère fiable et légal de l'information comptable fournie. L'organisation du logiciel doit également donner à son utilisateur les possibilités en terme de fonctionnalités tels que les besoins normaux de saine gestion tant sur le plan comptable qu'extracomptable.

CONCLUSION

Ce chapitre nous a permis à travers ses deux sections de comprendre tous les textes réglementaires, fiscaux et même juridiques qui gouvernent les comptabilités tenues par le procédé informatique. Ces textes sont de sources différentes mais poursuivent les mêmes objectifs : permettre à la comptabilité informatisée de produire des informations financières sincères et réguliers.

Cette sincérité de l'information ne peut être obtenue dans un système comptable informatisé qui présente des risques non maîtrisés.

CHAPITRE III LES RISQUES LIES À LA COMPTABILITE INFORMATISEE ET METHODOLOGIE DE RECHERCHE

INTRODUCTION

Selon la CNCC : « la qualité de l'organisation d'ensemble de la fonction informatique est pour l'entreprise, un élément de sécurité qui affecte l'ensemble du processus d'information financière quelle que soit la qualité des applications, leur fiabilité peut être remise en cause par un environnement d'utilisation inappropriée ».

La bonne organisation de la fonction informatique est celle qui cherche à limiter les conséquences des risques encourus par l'ensemble en mettant des procédures de natures différentes qui sont réparties entre le « service informatique » et les utilisateurs.

Avant d'étudier les risques liés à la fonction informatique à proprement parler, il nous semble important d'étudier son organisation.

3.1 L'organisation de la fonction informatique

Il n'existe pas à proprement parler de structure type d'un service informatique car la structure doit non seulement être adaptée en fonction de l'importance de service informatique, du nombre de personnes qui le composent mais tenir aussi compte de l'évolution rapide des structures en fonction du progrès des technologies.

Mais néanmoins une bonne organisation est celle qui assure le respect du principe de la séparation des fonctions incompatibles (développement, exécution et contrôle). Ainsi elle peut être structurée comme suit :

- Service développement et maintenance encore appelé fonction études, elle représente l'ensemble du personnel informatique dont le rôle est de développer de nouvelles applications et d'assurer leur maintenance. Organisé sous forme d'équipes, il écrit et teste les programmes qui seront validés par l'utilisateur par le jeu d'essai. Il doit assurer une bonne coordination entre le service informatique et les utilisateurs et aussi la fiabilité des applications avant leur mise en exploitation.

Pour atteindre ses objectifs une bonne définition des besoins (formats de saisie et des éditions, le traitement, le contrôle), la réalisation de tests garantissant la bonne programmation et une actualisation régulière en fonction de l'évolution des besoins des utilisateurs s'impose ;

- Service exploitation dont le rôle principal est d'empêcher et de détecter rapidement les anomalies (utilisation de programmes par des personnes non autorisées, utilisation des programmes non autorisés, les modifications non autorisées de programmes ou de données, les défaillances techniques du matériel, etc.)

Elle permet de prévenir ou de déceler les erreurs accidentelles durant les traitements informatiques et lors de la saisie des données.

- Service traitement : il est étroitement lié aux procédures d'exploitation et doit assurer le bon fonctionnement de chaque opération. Il a pour rôle la création des données, leur saisie exhaustive, leur validité, leur traitement, la centralisation des données dans les bons fichiers, le contrôle des sorties et des résultats obtenus ;
- Service sécurité : il conditionne les autres services car il est destiné à protéger l'intégrité physique des installations et des données, la confidentialité d'accès, la gestion des sauvegardes, etc. Il a connu un développement considérable au cours des dernières années à cause de la recrudescence de la criminologie informatique.

Nous ne saurons parler d'organisation de la fonction informatique sans se prononcer sur son rattachement hiérarchique. Ainsi, deux grandes tendances coexistent :

- Elle peut être rattachée soit à la direction générale : ce type de rattachement procure une indépendance à la fonction informatique vis-à-vis des autres services et directions qui lui permet de participer à la définition des priorités. Mais en revanche, le principal inconvénient réside dans le fait que la direction générale, par manque de temps ou compétence pour exercer un contrôle réel sur elle. Ainsi le responsable pourrait orienter les choix stratégiques en fonction de ses propres intérêts plutôt qu'en fonction de l'intérêt de l'entreprise.
- Elle peut être soit rattachée à la direction administrative et financière : selon **YANN DERRIEN** « ce rattachement devrait permettre dans son principe un meilleur contrôle de l'activité informatique ». Mais des conflits peuvent naître entre le directeur administratifs et financier et le responsable de la fonction informatique du fait de l'insuffisance de formations des premiers dans ce domaine et surtout de la forte technicité de la fonction informatique. En plus il peut provoquer une orientation du budget au développement de logiciels à caractère administratif ou financier, au détriment d'autres secteurs d'activités.

3.2 Les risques liés à la comptabilité informatisée.

Le risque est une notion complexe qui naît de l'existence de menaces et d'impacts, c'est-à-dire la conséquence de la réalisation de la menace et la probabilité qu'elle se réalise.

Ainsi le risque est représenté par l'équation suivante : risque =menace*impact. Si l'un des membres est nul, le risque n'existe pas mais par contre il sera autant grave que l'un des membres (facteurs) ou les deux seront élevés.

Selon Angot « al » les risques liés aux comptabilités informatisées n'est pas liés au piratage du système comme le pensent certains mais surtout à leur mauvaise conception.

Il ne s'agit pas pour nous dans ce paragraphe d'établir une liste exhaustive des risques liés à la comptabilité informatique mais de faire ressortir les plus récurrents.

Il existe selon nous trois grandes catégories de risques : les risques informatiques, les risques liés à l'organisation comptable proprement dite et les risques liés à l'organisation de la fonction informatique.

3.2.1 Les risques informatiques.

Les risques informatiques comprennent essentiellement les risques humains et les risques techniques.

→ Les risques humains.

Ils sont les plus fréquents même s'ils sont le plus souvent ignorés ou minimisés et concernent les utilisateurs et les informaticiens eux-mêmes. Ainsi il peut s'agir de :

-La maladresse : selon Caspard & Enselme (2002 :35) il faut entendre par maladresse, la commission des erreurs par les hommes. Il leur arrive donc plus ou moins fréquemment d'exécuter un traitement non souhaité, d'effacer involontairement des données ou des programmes. Ainsi donc nous avons les erreurs de saisie qui peuvent survenir lors de la saisie des numéros de comptes, de leur intitulé ou le montant. Elles sont les plus fréquentes et difficile à détecter surtout si les comptes sont équilibrés ;

-La malveillance : elle se définit comme étant l'introduction volontaire dans le système en connaissance de cause des virus, de mauvaises informations dans la base de données ou d'ajouter de façon délibérée des fonctions cachées lui permettant, directement avec surtout l'aide de complices, de détourner à son profit d'information confidentielle ou de fonds.

-L'ingénierie sociale : c'est une méthode par laquelle une personne obtient des informations confidentielles, qu'elle n'est pas normalement autorisée à obtenir, en vue de les exploiter à d'autres fins. Elle se manifeste par le vol d'informations confidentielles qui peuvent être des données de la comptabilité pour les divulguer aux concurrents directs de l'entreprise.

-Vol de mots de passe : Le mot de passe permet à l'utilisateur, ou à un groupe d'utilisateurs d'être authentifier puis autorisé par l'intermédiaire d'une table d'accès, à accéder soit à une ressource logique, soit à un profil d'accès.

Les mots de passe doivent faire l'objet d'une gestion et doivent respecter les critères suivants : être composés de quatre caractères au minimum. Cela permet d'éviter de retrouver facilement les mots de passe par l'analyse combinatoire, ils ne doivent pas s'afficher sur l'écran lorsque l'opération les frappe au clavier, ils doivent faire l'objet de changement permanent : tous les mois par exemple. Le changement est nécessaire pour décourager les personnes qui cherchent à forcer les règles d'accès. Ainsi les autorisations d'accès accordées à un utilisateur doivent être supprimées lorsque ce dernier quitte l'entreprise, qu'il s'agisse d'un licenciement ou d'une démission.

L'entreprise qui gère inefficacement ses mots de passe court le risque de perdre la confidentialité de ses données comptables, le risque de modification ou de suppression, voire d'ajout de données.

→ Les risques techniques

Par risques techniques, il faut entendre ceux liés aux défauts et pannes inévitables que connaissent tous les systèmes. Ces risques sont plus ou moins fréquents selon le soin apporté lors de la fabrication et des tests effectués avant que les ordinateurs et les programmes ne soient mis en service. Au titre de ces risques, nous allons étudier trois (03) types, il s'agit essentiellement :

-Les risques liés aux matériels (ordinateurs essentiellement). On néglige souvent la probabilité d'une erreur d'exécution par un processeur, pourtant la plupart des composants électroniques, produits en grandes séries peuvent comporter des défauts et bien entendu finissent un jour ou l'autre par tomber en panne (site : Wikipédia). La rareté et l'intermittence de certaines de ces pannes les rendent assez difficile à déceler. En cas de survenance de ces pannes l'entreprise courre le risque de produire des informations non sincères, blocage partiel ou intégral de travailler.

-Les risques liés aux logiciels : selon YANN DERRIEN : « la complexité croissante des systèmes d'exploitation et des programmes nécessite l'effort conjoint de dizaines, de centaines, voire de milliers de programmeurs, mais individuellement ou collectivement, ils font inévitablement des erreurs que les meilleures méthodes de travail et les meilleurs outils de contrôle ou de test ne peuvent pas éliminer en totalité ». Ces risques sont de loin les plus fréquents. Mais lorsqu'ils interviennent, ils rendent non fiables les informations financières que les logiciels contiennent. Les risques liés aux logiciels sont les plus

difficiles à déceler car il est quasiment impossible de tester d'une manière exhaustive la fiabilité d'un logiciel. Cela s'explique par le fait que la méthode à priori utilisée consiste à relire chaque programme pour vérifier qu'il ne contient pas d'erreur. Toute chose qui est dans la pratique inapplicable, dans la mesure où la relecture et la compréhension d'un seul programmes peut nécessité plusieurs jours de travail, sans pourtant qu'on ait la certitude de déceler d'éventuelles anomalies.

- Les risques liés à l'exploitation : comme nous l'avons dit plus haut l'exploitation permet de détecter rapidement les anomalies. Ainsi si elle est mal maîtrisée, le système ne pourra plus prévenir les erreurs, les fraudes, les atteintes à la confidentialité. Ainsi donc il sera difficile d'éviter ces risques suscités.

3.2.2 Les risques liés à l'organisation de la fonction informatique

→ Les risques liés au cumul de fonctions incompatibles

Selon la CNCC : « le cumul des fonctions incompatibles (exploitation, développement, contrôle) au sein de l'informatique génère des risques de modification indues des programmes et des données. » Ainsi l'entreprise doit songer dans l'organisation de la fonction informatique à assurer la séparation de ces fonctions.

→ Les risques liés à la documentation

Selon YANN DERRIEN (1991 :213) le manque de documentation (qui est le plus fréquent) liée à un logiciel, ou à un quelconque matériel informatique peut entraîner la non continuité de l'exploitation lorsque les premiers utilisateurs sont appelés à quitter l'entreprise soit pour cause de licenciement soit pour cause de démission soit la fermeture de la société qui les a conçus.

→ Les risques liés au paramétrage :

Un mauvais paramétrage d'un logiciel comptable peut conduire à l'entreprise à produire des informations financières non sincères.

Le bon paramétrage est la condition sine qua non pour assurer la sincérité et la régularité des informations financières.

3.2.3 Les risques liés à l'organisation comptable

.Nous avons vu plus haut que l'organisation comptable en milieu informatisé doit respecter certaines conditions telles que les conditions de validité,de validation, les mentions minimales que doit comporter une écritures comptables et enfin le respect du chemin de révision. Ainsi lorsque l'organisation comptable ne garantit pas le respect de ces règles, cela a pour effet la remise en cause de la force probante de la comptabilité, et par voie de conséquence celle des comptes annuels.

De même lorsque les principes comptables émis par le SYSCOA ne sont pas respectés dans sa rigueur l'entreprise court le risque de présenter des documents de systèmes qui ne sont pas fiables.

Ainsi, selon Caspard & Enselme (2002 :35), en comptabilité informatisée, les livres sont pour la plupart incorporés aux procédures programmées. Le logiciel comptable incapable de produire des documents comptables sincères et réguliers expose l'entreprise à des litiges avec l'administration fiscale et les auditeurs externes.

Il en est ainsi lorsqu'une entreprise en dispose pas d'un manuel de procédures comptables ou lorsque celui-ci n'est pas efficace. Le manuel de procédure qui est un document qui décrit les procédures d'enregistrement, de contrôle et d'organisation comptables, est une prescription de la loi, faisant partie des exigences à satisfaire pour garantir la fiabilité de l'information comptable et financière.

Dans le même ordre d'idée, lorsque le système n'assure pas l'irréversibilité et l'inaltérabilité des écritures, l'entreprise en plus de se voir refuser la certification de ses comptes par son commissaire aux comptes, court le risque de fraude, de manipulation, de malversation, de destruction volontaire des données, etc.

Une mauvaise organisation comptable entraîne aussi la non concordance de la comptabilité auxiliaire à la comptabilité générale, des écritures comptables inadéquates mais aussi n'assure pas l'intangibilité du bilan, qui est l'un des principes comptables du SYSCOA.

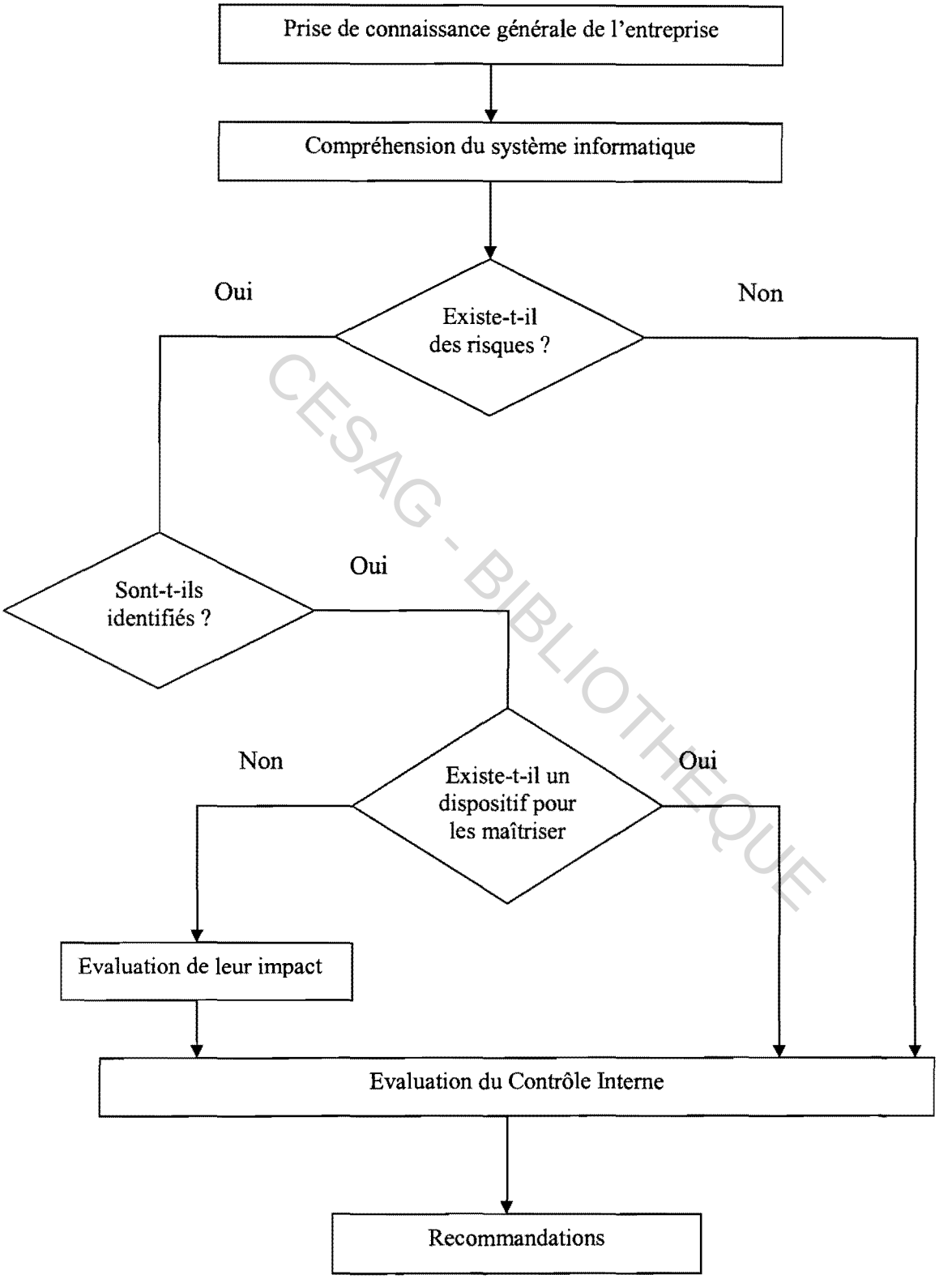
En dehors des risques suscités, il existe d'autres risques telle que la destruction partielle ou totale des actifs informatiques liés aux facteurs environnementaux (les inondations, les coupures d'électricité, le vent, autres catastrophes naturelles...) que l'entreprise doit se doter les moyens pour les éviter.

3.3 Méthodologie de la recherche

Dans cette section, il s'agit pour nous de construire notre modèle d'analyse et présenter les outils utilisés pour collecter les données.

3.3.1 Construction d'un modèle d'analyse

Figures n°1 : Construction d'un modèle d'analyse



Source : Nous-mêmes

► la prise de connaissance générale de l'entreprise

La prise de connaissance générale de l'entreprise est le préalable. Elle doit permettre de connaître les particularités de l'entreprise, pour déterminer les risques généraux (les zones à risques) et identifier les systèmes significatifs. Ainsi, lors de cette prise de connaissance, on cherche à collecter le maximum d'informations sur l'entreprise et son environnement informatique afin de détecter l'existence de risques.

L'objectif de la prise de connaissance est de collecter et d'analyser les informations en s'assurant toutefois qu'elles ne semblent pas incohérentes.

A cette étape les outils utilisés pour collecter les informations sont essentiellement :

-l'entretien avec les différentes personnes qui sont susceptibles de fournir une information appropriées ;

-l'analyse documentaire interne et externe obtenu ;

- la visite des locaux.

Cette prise de connaissance doit permettre d'avoir des informations sur la structure de la fonction information, le matériel utilisé.

► La compréhension du système

Après la connaissance générale de l'entreprise, nous allons chercher à comprendre son système informatique dans tout son ensemble. Elle doit permettre de mieux comprendre les aspects liés à l'informatique et aux circuits d'informations qui ont un impact sur les comptes.

Selon la CNCC pour pouvoir apprécier l'impact de l'informatique sur les comptes, il est nécessaire d'avoir une connaissance préalable suffisante du système informatique de l'entreprise dans son ensemble. La compréhension du système a pour objectif principal de comprendre le fonctionnement de tout le système d'information comptable.

Ainsi les techniques de collecte des informations sont principalement :

- l'entretien,
- L'observation physique,
- L'analyse documentaire (manuel de procédure comptable, documentation liée à l'informatique).

►L'évaluation du contrôle interne

L'évaluation du contrôle interne est une méthodologie importante pour la collecte d'information et pour l'appréciation du niveau de fonctionnement, de contrôle de sécurité.

Plutôt que de revenir sur une définition du contrôle interne, nous mettons ici un accent sur l'intérêt de son évaluation. Ainsi les procédures internes seront évaluées afin d'appréhender

les responsabilités définies et de s'assurer de l'efficacité de la séparation des fonctions incompatibles en informatique.

Cette évaluation du contrôle interne devra permettre de faire ressortir ses forces et ses faiblesses afin de mieux cerner les zones à forts risques.

Les outils utilisés sont :

-les tests de conformité,

-les tests d'existence

-les tests de pertinence.

3.3.2 Les outils de collecte des données

Comme outils de collecte de données, nous allons utiliser l'entretien, l'analyse documentaire, l'observation physiques, et le questionnaire.

► L'entretien

L'entretien permet d'illustrer des résultats, de les rendre vivants ou de les nuancer soit par un exemple, soit par un contre exemple, soit par un cas particulier. L'entretien comme son nom l'indique est un échange verbal entre un auditeur et un audité au cour duquel le premier pose des questions au dernier. Il existe trois (03) types d'entretien :

- Les entretiens directifs, pour lesquels les questions posées demandent des réponses très concises, fermées (entretien quasi-questionnaire) ;
- Les entretiens ouverts, pour lesquels une question générale laisse libre court au récit de la personne interrogée ;
- Et enfin les entretiens entre les deux, pour lesquels les réponses aux questions sont plus libres, plus développées, contrairement à l'entretien directif.

L'entretien permet une meilleure maîtrise de l'entrevue.

►Le questionnaire

Contrairement à l'entretien, le questionnaire peut être administré à l'audité en l'absence de l'auditeur. Le questionnaire doit nous permettre d'avoir des informations suffisantes sur l'organisation de la fonction informatique, la sécurité du matériel et des logiciels, la fonctionnalité des logiciels et leur fiabilité.

Pour élaborer ce questionnaire, nous nous sommes inspiré du référentiel de la CNCC.

► L'observation physique

L'observation physique est la constatation de la réalité instantanée de l'existence et du fonctionnement d'un processus, d'un bien, d'une transaction, d'une valeur (LEMANT,

1995 :201). Elle peut être menée de deux manières : l'observation directe et l'observation indirecte.

L'observation est un mode fiable de collecte d'informations car selon OBERT (2000 :91) :« le moyen le plus sûr de vérifier la véracité et l'existence de certains éléments est de se les faire présenter »

CONCLUSION PARTIELLE

Le cadre théorique nous a permis de mieux cerner les contours de notre étude. La maîtrise des risques occupe une place essentielle dans une organisation au vue des avantages qu'elle procure à l'entreprise.

De nos jours nombreuses sont les entreprises qui ignorent encore que les comptabilités informatisées présentent tout comme la comptabilité manuelle des risques dont les conséquences sont multiples.

Mais ce gap est loin d'être atteint si on ajoute à cela, le fait que l'auditeur externe, pas manque de temps, ou de compétences suffisantes, mais surtout de la complexité des systèmes informatiques, ne prend pas cet aspect en compte dans la planification de sa mission.

Ainsi donc, de part la revue de la littérature que nous avons eu à faire et qui constitue la première parie de notre étude, l'on serait tenté de poser plusieurs questions :

- Quelle est l'organisation de la comptabilité informatisée ?
- Quels sont les matériels utilisés pour la tenue de cette comptabilité ?
- Quels sont les outils de maîtrise des risques ?

La deuxième partie de notre étude, appelée cadre pratique nous emmènera à trouver des réponses à nos préoccupations pour ce qui est de la société SECCAPI, objet de notre étude.

Ce cadre consistera à travers un questionnaire (voir annexe) et des interviews à faire ressortir la pratique de la maîtrise des risques liés à la comptabilité informatisée appliquée par la société.

DEUXIEME PARTIE : ANALYSE DES RISQUES LIES A LA COMPTABILITE INFORMATISEE DE SECCAPI

CHAPITRE IV PRESENTATION DE SECCAPI

4.1 ACTIVITES ET CAPITAL SOCIAL

Le cabinet SECCAPI, est une société à responsabilité limité (SARL) au capital social de 3 000 000 FCFA. Il fait partie du groupement TDT Associé qui réunit trois (03) cabinets africains : Fiduciaire Conseil et Audit (FCA) au Niger, Fiduciaire d'Afrique au Bénin (FAB) et SECCAPI au Burkina Faso Créé en 1972, le cabinet SECCAPI occupe une place de choix dans ce domaine avec une clientèle très diversifiée composée d'entreprises commerciales, d'associations, de banques, etc. Actuellement, le cabinet intervient dans certains pays de la sous région comme le Mali, le Niger, le Togo, donc s'internationalise. Comme atouts majeurs, le cabinet dispose en son sein une équipe de collaborateurs expérimentés et évolutifs, dirigée par un expert comptable diplômée d'Etat. Ils disposent d'une expérience professionnelle diversifiée et pour certains d'une expertise spécifique, acquise dans des missions exécutées au profit d'administrations de projets financés par les bailleurs de fonds internationaux. Ses collaborateurs bénéficient d'une formation continue aux techniques comptables, financières, juridiques, fiscales... dans le cadre des séminaires internes organisés par le cabinet, de la préparation des diplômes suivie par la plupart des collaborateurs professionnels.

SECCAPI a pour activités de réaliser pour les entreprises, les projets financés par les bailleurs de fonds, les institutions, les administrations... des missions d'audit, de commissariat aux comptes, d'expertise comptable et de conseil....

Les missions d'audit et de commissariat aux comptes concernent essentiellement les investigations, les évaluations, les audits opérationnels et de gestion, les audits informatiques, les audits des marchés publics, des circonscriptions urbaines, la certification et l'attestation.

L'activité conseil- expertise comptable couvre quant à elle le diagnostic d'entreprise, le conseil de gestion et recommandations au profit des dirigeants, la révision comptable, l'élaboration des états financiers, les déclarations administratives, etc.

L'activité conseil fiscal et social couvre des domaines très variés. Il s'agit notamment des consultations fiscales et sociales, d'audit fiscal et social, de conseil et d'assistance en droit social et de formation dans le domaine fiscal et social.

4.2 Organisation et fonctionnement de SECCAPI

→ La direction générale

La direction générale du cabinet est assurée par l'expert comptable. Elle s'occupe de la gestion quotidienne du cabinet, de la planification, bien entendu avec le chef de mission.

Elle tient régulièrement des réunions avec l'ensemble de ses collaborateurs pour fixer les prochaines missions, pour constituer les équipes qui vont intervenir, et pour s'imprégner de l'état d'avancement des missions déjà entamées.

→ Le secrétariat

Le secrétariat assiste la direction générale dans toutes ses tâches. A cet effet, il s'occupe de la gestion du courrier ordinaire, du courrier électronique, et confidentiel, de la saisie et l'envoi aux clients des rapports des missions réalisées par les auditeurs.

→ Le chef de mission

Il est chargé d'assurer la bonne exécution des missions qui sont sous son contrôle. De ce fait, il constitue un intermédiaire entre les auditeurs (ses collaborateurs) et le comptable de la société auditée.

→ Le service des auditeurs

Les auditeurs constituent les professionnels du cabinet. Ils sont chargés de réaliser les missions d'audit, de commissariat aux comptes, d'assistance comptables sous la supervision du chef de mission.

→ Le service juridique et fiscal

Ce service est chargé d'assurer les missions de conseil juridique et fiscal. Il est animé par des juristes de formation.

Cette tâche est confiée à un autre cabinet « émergence juridique et fiscale » qui fait partie du groupe SECCAPI

→ Le service informatique

Ce service a pour mission principale de faire des prestations informatiques. Ces prestations informations sont de divers ordres : audit informatique, installation et paramétrage logiciels, etc. il assiste les auditeurs pour des missions qui demandent des connaissances particulières en informatique.

→ Le directeur des ressources humaines

Il a pour tâche principale de gérer la carrière administrative et d'assurer la formation continue du personnel. Pour se faire, il définit les besoins en formation au sein du cabinet et établit un

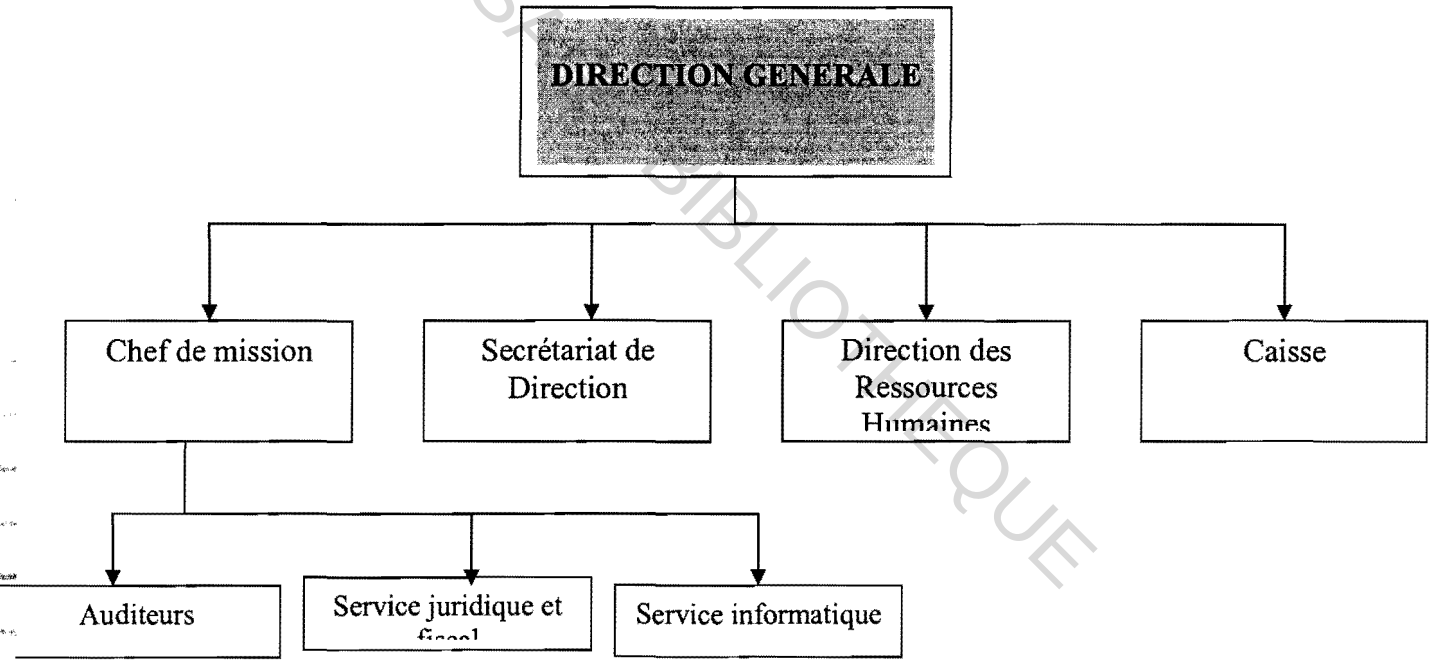
programme de formation. Le DRH a aussi la lourde tâche de gérer toutes les situations conflictuelles nées au sein du cabinet en interne.

→ La caisse

Elle a pour fonction de gérer les fonds du cabinet. De ce fait, la caissière sur ordre du Directeur s'occupe du règlement des factures fournisseurs des virements ou paiement des salaires.

Elle s'occupe également de l'encaissement des règlements effectués par les clients. Cette présentation très succincte, nous permet de construire pour conclure l'organigramme du cabinet SECCAPI

Figure n°2 Organigramme de SECCAPI



CHAPITRE V : PRESENTATION DU SYSTEME COMPTABLE INFORMATISE DE SECCAPI

INTRODUCTION

Après avoir présenté la société SECCAPI à travers ses activités, son organisation, il nous semble opportun de présenter sa comptabilité informatisée à travers le matériel utilisé, son système et procédé comptable et la répartition des tâches au sein de la comptabilité.

Cette présentation, à notre humble avis nous permettra de mieux comprendre l'organisation comptable de la société.

5.1 Description du système comptable informatisé de SECCAPI

5.1.1 Le matériel utilisé

Le rôle des ordinateurs n'est plus d'assurer les travaux bureautiques (saisies et traitements des correspondances), mais ce rôle a évolué et l'ordinateur occupe une place très importante dans la tenue de la comptabilité.

Pour tenir une comptabilité informatisée l'outil indispensable est l'ordinateur. Ainsi SECCAPI ne dérogeant pas à ce principe dispose pour la tenue de sa comptabilité un certain nombre d'ordinateurs de marques et de capacités très différentes.

Ainsi nous avons pu noter au cours de notre passage près de deux (02) machines PC et quatre (04) portatifs et un serveur qui concourent au bon fonctionnement de la comptabilité.

Tableau 1 : Environnement physique (matériel)

Machines utilisées	Nombre	Caractéristiques	
		Disque dur (en Go)	RAM (en Mo)
Machines PC	2	5	128
Machines portables	4	60	256
Serveur	1	20	256

Le cabinet SECCAPI utilise plusieurs imprimantes classées aussi par catégorie. Ainsi l'on peut retrouver :

- Brother HL-1240
- CCMX Fichier PDF compatible

- HP laser jet 6L
- Lexmark
- Brother Model HL-14.

5.1.2 Le logiciel

L'ordinateur à lui seul ne saurait être suffisant pour une tenue normale d'une comptabilité. Ainsi comme logiciel comptable, la SECCAPI utilise le CMXX WINNER COMPTA. Il s'agit d'un logiciel comptable qui donne des fonctionnalités similaires au logiciel SAARI.

Le logiciel est installé dans tous les ordinateurs, toute chose qui permet aux comptables de pouvoir travailler en toute indépendance.

En plus de ce logiciel, SECCAPI dispose d'un autre logiciel développé en interne à partir de l'application EXCEL appelé « LEADS ET BILAN » qui permet une fois la balance saisie de générer automatiquement les états financiers. Il est utilisé uniquement pour établir les états financiers. Le logiciel CMXX WINNER COMPTA est par excellence celui réservé à la saisie comptable des opérations. La saisie est assurée par une secrétaire mais la validation comptable est faite par un comptable qui doit s'assurer d'abord que les opérations qui ont fait l'objet d'une saisie sont faites dans les comptes appropriés.

Le logiciel CMXX WINNER COMPTA dispose d'autres spécificités comme CMXX WINNER IMMO qui permet de gérer les immobilisations à travers les tableaux d'immobilisations et leur amortissement.

Ainsi l'environnement logiciel de SECCAPI est essentiellement composé de système d'exploitation, de logiciel bureautique, de logiciel comptable que nous résumons dans un tableau.

Tableau n°2 : Environnement logiciel de SECCAPI

Types de logiciels	Désignations
Système d'exploitation	Windows
Logiciels bureautiques	Microsoft office (Word, Excel, power point, Access)
Logiciels comptables	Cmxx winner compta, leads et bilan, Cmxx winner immo
Antivirus	F.secure, e.trust

5.2 L'organisation comptable

→ La répartition des tâches

Les auditeurs, en dehors des missions d'audit qui sont la plupart périodiques, qu'ils doivent assurer, s'occupent également de l'assistance comptable demandée par les clients du cabinet. Ainsi donc, chacun en ce qui le concerne tient la comptabilité d'un ou plusieurs clients. Cette tenue comptable consiste à recevoir les pièces comptables du client, procéder à leur imputation, leur saisie dans le logiciel comptable susnommé, leur traitement et l'édition des états financiers annuels.

Cette assistance comptable couvre également le classement, l'archivage des pièces comptables mais également des déclarations fiscales et sociales.

Chaque client possède un compte dans le logiciel avec un code d'accès qui permet au comptable une fois le code introduit dans le logiciel d'afficher la comptabilité du client.

Nous résumons dans le tableau qui suit les principaux clients avec l'agent comptable approprié :

Tableau n°3 : Répartition des clients pour chaque comptable

Agent comptable	Client
Mr TOE	Alcatel, Impricolor
Mr PARE	STBF, Emergence Burkina
Mlle KERE	ICBM
Mr SAWADOGO	MULTI-M, Laboratoire du Centre

→ Système et procédé comptables

L'évolution de la technologie et la multitude des opérations dont réalisent les entreprises comme SECCAPI ont pour conséquences l'abandon des anciens systèmes (le système classique) au profit des plus récents (le système centralisateur).

Le cabinet SECCAPI pour la tenue de la comptabilité de ses clients, a opté pour le système centralisateur pour diverses raisons : il permet d'avoir des comptes plus analytiques, le volume très important des opérations des clients à traiter, mais aussi ce choix est guidé par le fait que le système centralisateur est le système par excellence le mieux adapté à la comptabilité par l'intermédiaire de l'ordinateur.

Pour le bon fonctionnement du système et comme il l'exige, le cabinet crée divers journaux auxiliaires en fonction de l'activité de son client. Ainsi les plus couramment utilisé sont : le

journal banque, journal caisse, journal des achats, journal des ventes et le journal des opérations diverses (OD).

CHAPITRE VI : EVALUATION DU CONTROLE INTERNE DE LA FONCION INFORMATION

Introduction

L'évaluation du CI de la fonction informatique poursuit comme objectif, au moyen d'outils appropriés, de vérifier qu'un certain nombre de règles propres à un bon contrôle interne sont bien respectées. Selon YANN DERRIEN : « Même si l'examen du contrôle interne ne permet pas de déceler toutes les erreurs dans la réalisation, l'exploitation ou l'utilisation des logiciels, l'analyse du CI fournit de bonnes présomptions quant à la fréquence et à l'ampleur de telles erreurs ».

Dans ce chapitre, nous allons essayer d'analyser les sources des risques liées à la comptabilité informatisée du cabinet SECCAPI.

6.1 Le logiciel comptable

Nous avons vu un peu plus haut que le cabinet SECCAPI utilise comme logiciel comptable CMXX WINNER. Notre observation physique nous a permis de constater que le logiciel n'admet pas la correction en négatif comme préconisée par l'OHADA. Ce logiciel également ne reconnaît pas les comptes de la classe huit (8). C'est un logiciel conçu sur la base du système français.

Les clients par l'intermédiaire du cabinet courant le risque de se voir refuser la certification de leur compte conforme aux exigences de l'OHADA.

En ce qui concerne les comptes de la classe huit (08) , la solution suivante a été retenue : leur enregistrement dans les comptes de la classe six ou sept selon qu'il s'agit d'une charge ou d'un produit, ce qui dans une certaine mesure, ne permet pas de donner des comptes de charges et de produits fiables.

6.2 La gestion des mots de passe

Il existe une séparation claire entre les mots de passe de saisie et les mots de passe de validation comptable dans la mesure où celui qui s'occupe de la saisie et celui qui s'occupe de la validation sont différents.

Le risque de modification des données introduites est seulement possible avant la validation car avant de procéder à la validation, le comptable doit s'assurer de la bonne saisie des imputations effectuées sur les pièces comptables.

Il n'existe pas une table de mots de passe ou un gestionnaire de mots de passe. Chacun gère son mot de passe à sa guise. Le risque de vol de mots de passe est élevé même si selon nos renseignements, le risque ne s'est pas encore matérialisé, car les mots de passe ne sont pas renouvelés fréquemment. Mais il faut noter aussi que les prêts de mot de passe n'existent.

6.3 Les locaux et le personnel intervenant dans la comptabilité informatisée

Une analyse sur les possibilités d'évacuation du matériel informatique mais aussi des personnes en cas d'incendie ou de catastrophe naturelle nous permet de dire qu'aucune disposition sécuritaire n'a été prise dans ce sens, pourtant, elle constitue une condition préalable pour assurer la continuité d'exploitation.

Mais en analysant l'emplacement des locaux, il nous a été donné de constater une très faible probabilité (voire nulle) d'inondation, de tremblement de terre, d'inaccessibilité en cas de mauvais temps.

Il existe également des possibilités de vol des actifs informatiques surtout que le cabinet utilise beaucoup d'ordinateurs portatifs. Au niveau de la prévention contre les incendies, nous avons noté un dispositif inexistant, même pas de petites bouteilles d'extincteurs, ni un détecteur de fumée. Au niveau du personnel, dans l'optique de nous assurer de la qualité (compétente) des personnes qui participent au fonctionnement et à la bonne marche de la comptabilité informatisée, nous avons effectué une vérification au niveau du fichier du personnel. Ainsi tous les quatre (04) personnes qui s'occupent de l'assistance comptable, ont au moins un niveau universitaire en comptabilité, ce qui est à notre avis suffisant pour assurer convenablement la tenue d'une comptabilité.

6.4 La gestion des risques

SECCAPI dans son système de gestion des risques liés à la comptabilité informatisée ne dispose d'aucune procédure de reprise du système en cas de sinistre. Le cabinet ne pratique pas un stockage des informations hors site, ce qui en cas de survenance d'un sinistre, pourrait entraver la continuité de l'exploitation

Pour ce qui est de la documentation relative à l'informatique dont son existence peut en cas de départ des premiers utilisateurs du logiciel ou d'un quelconque matériel, la société essaie de combler ce vide par l'organisation des formations sous forme de séminaire. Ce qui permet au cabinet de limiter un temps soit peu le risque de non continuité de l'exploitation qu'il encourt.

6.5 Le système de sauvegarde mis en place

La sauvegarde est l'opération qui consiste à mettre en sécurité les données contenues dans un système informatique. La sauvegarde permet de faire des copies de données pour les stocker. Mais il est important de ne pas stocker ces copies de sauvegarde à côté du matériel informatique voire dans la même pièce car en cas d'incendie, de dégât des eaux, il serait difficile voire impossible de récupérer les données.

Cette sauvegarde peut être faite dans l'entreprise ou en dehors de l'entreprise.

Le système de sauvegarde actuel du cabinet ne garanti pas la continuité de l'exploitation autrement dit ne garantie pas la récupération des données de la comptabilité. La sauvegarde est faite directement sur la machine. Aucune sauvegarde hors site n'est pratiquée.

Le risque de perte des données est d'autant plus élevé dans la mesure où le serveur n'est pas disponible permanemment, ce qui oblige les comptables à travailler en local. Ce risque est également amplifié par le fait du risque élevé de perte de matériel.

6.6 La documentation

La documentation est définie comme étant l'ensemble documentaire qui décrit l'ensemble du système informatique utilisé par l'entreprise. Elle doit être classée et complète et mise à jour à chaque modification.

Le manque de cette documentation fait courir à l'entreprise le risque de blocage du travail, ou encore la non maîtrise du système mis en place dans l'entreprise en cas de départ massif de son personnel. Ce manque de documentation crée également une dépendance de l'entreprise vis-à-vis du concepteur du logiciel, car en cas de problème, elle est obligée de lui faire appel.

CONCLUSION

Ce chapitre nous a permis de passer en revue quelques risques encourus par le cabinet. Ces risques sont essentiellement liés au logiciel que utilise le cabinet pour la tenue de sa comptabilité, au manque de documentation relative aux programmes.

Un contrôle interne efficace est celui qui permet à l'entreprise de prévenir les risques et de les maîtriser.

Cette évaluation nous a permis de faire certains que nous allons essayer d'aborder dans le prochain chapitre. Ces constats seront suivis de recommandations dans le but de renforcer les acquis et 'améliorer un temps soit peu les insuffisances.

CHAPITRE VII : SYNTHESES ET RECOMMANDATIONS

7.1 Les synthèses

Après avoir présenter dans le chapitre précédent, les risques auxquels le cabinet court, ce chapitre sera l'occasion pour nous de faire une synthèse des forces et des faiblesses du système.

Dans l'optique de permettre aux dirigeants d'améliorer la qualité dans ce domaine pour être encore plus efficace, nous nous permettrons par la suite de faire des recommandations.

7.1.1 Les principales forces

- Bonne compétence du personnel, ce qui entraîne une bonne exécution de leur tâche ;
- Existence d'Une installation électrique sécurisée, d'un groupe électrogène de secours pour une relève immédiate de l'alimentation électrique en cas de coupure d'électricité ;
- Le logiciel d'exploitation adéquat car facilement utilisable ;
- Le logiciel disposant un degré de fiabilité satisfaisante ;
- Existence de contrôle des points de sortie des traitements afin de s'assurer de la réalité des données saisies ;
- Non sauvegarde des données hors site pour permettre une reprise des données en cas d'accident ;
- Bonne organisation comptable ;
- Mis à jour des antivirus permettant d'éviter les attaques des virus ;
- Tout accès aux applications (logiciels) est protégé par un mot de passe ;
- Formation régulière du personnel en informatique
- Existence d'un budget informatique pour le renouvellement du matériel existant ;
- un logiciel assurant l'irréversibilité et l'inaltérabilité des données validées ;
- un logiciel n'admettant pas d'import en Excel ce qui pourrait être sources de modifications.

7.1.2 Principale faiblesses

- insuffisance de documentation et de guides utilisateurs pour permettre à tout le personnel de s'imprégner des procédures et de maîtriser les fonctionnalités des logiciels ;
- un logiciel non conforme aux exigences du système comptable en vigueur ;
- inexistence de table de mots de passe chacun gère son mot de passe comme bon le semble ;
- aucun calendrier de maintenance préventive et des entretiens physiques des machines n'est effectué (absence totale de maintenance des machines) ;
- les mots de passe ne sont pas régulièrement modifiés ;
- il n'existe pas de procédure de suppression et de non validation des mots de passe en cas de démission, licenciement ou congés d'un utilisateur ;
- absence de procédure d'évacuation en cas d'incendie ou de catastrophe (même si leur probabilité de survenance est faible) ;
- absence de bouteilles d'extincteurs ;
- câblage réseau local inadéquat et caduc entraînant des difficultés de travail en réseau, ce qui oblige le personnel à travailler en indépendance ;
- absence de police d'assurance la sécurité informatique.

7.2 RECOMMANDATIONS

Après avoir analysé les forces et les faiblesses de la fonction informatique, du reste pour ce qui concerne la comptabilité, il nous semble primordial de procéder à des recommandations. Ces recommandations n'ont pas pour objectifs de corriger toutes les éventuelles erreurs mais doivent contribuer à améliorer la pratique actuellement en vigueur.

→ Recommandations concernant les mots de passe

La pratique actuelle en ce qui concerne la gestion des mots de passe, à notre avis ne permet pas d'assurer pleinement leur rôle d'éviter une intrusion dans le logiciel. Ainsi nous suggérons la mise en place d'un système efficace de gestion des mots de passe, par leur renouvellement permanent, par leur annulation ou par leur non validation en cas de démission, ou congé, ou licenciement d'un utilisateur.

→ Recommandations concernant le logiciel

Le logiciel, nous l'avons dit précédemment n'admet pas les corrections en négatif et n'admet pas les comptes de la classe huit (08). Il nous semble plus que impérieux, pour résoudre ce problème, préconiser l'acquisition d'un nouveau logiciel qui respecte les prescriptions du système comptable en vigueur. Cela permet également d'avoir des comptes plus sincères.

→ Recommandations concernant les procédures comptables

Nous suggérons la mise en place de procédures spécifiques à chaque clients car les clients n'ont pas forcement les mêmes caractéristiques et leur mise à jour.

→ Recommandations concernant le matériel utilisé

Le parc informatique du cabinet est vieillissant et en nombre insuffisant car les ordinateurs portatifs servent en même temps des outils de travail en cas de missions d'audit ou CAC ce qui réduit considérablement le nombre du matériel et constitue de ce fait un blocage

Pour remedier ce probleme, nous preconisons l acquisition de nouveaux ordinateurs. La question que nous nous posons est d ou viendra les moyens autrement dit quelles sont les sources de financements et quelles les consequences liees a cette acquisition. Nous pensons sans doute que la meilleure source de financement reste lautofinancement qui permet a la societe d eviter certaines charges liees a l operation de financement, et surtout de garder son autonomie financiere et avoir une bonne capacite d endettement, mais son inconvenient majeur est qu il limite les possibilites de la societe du fait de son montant parfois faible.

A defaut de cette source interne de financement, la societe pourra faire recours a un emprunt bancaire.

→ Recommandations concernant le réseau

.Nous avons remarqué durant notre séjour que le réseau est fréquemment en panne, ce qui oblige le personnel concerné à travailler en local, toute chose qui ne permet pas de centraliser les informations dans le serveur.

Ainsi nous suggerons la mise en place d un reseau fonctionnel mais surtout la mise en place d un systeme de prevention des pannes en confiant l entretien du reseau a une maison specialisee. Les couts lies a une telle decision sont essentiellement les frais d entretien du reseau qui sont consideres comme les charges courantes et sont deductibles de l impot sur les benefices.

→ Recommandations concernant la sauvegarde

Nous préconisons, pour assurer la continuité d'exploitation de ses clients et surtout pour éviter de payer de grosses sommes d'argent pour dommages et intérêts, une politique de sauvegarde hors site des informations comptables.

→ Recommandations concernant la documentation

Vu la fréquence des formations et surtout des thèmes abordés au cours de ces formations qui ne concernent pas les risques liés à l'informatique, il nous semble pour permet aux arrivants éventuels de mieux comprendre les procédures, que le cabinet doit disposer la documentation relative à l'utilisation du logiciel.

7.3 MISE EN ŒUVRE DES RECOMMANDATIONS

Le plan de mise en œuvre des recommandations diffère vis-à-vis des coûts et des délais selon qu'il provienne d'un auditeur interne ou un auditeur externe.

Nous préciser qu'il s'agit pour en intervenant comme auditeur externe, de déterminer les modalités pratiques de mise en application effective des recommandations formulées.

Les caractéristiques d'une bonne recommandation étant sa faisabilité et son coût mais aussi de son degré de résolution du problème, la direction générale du cabinet, pour assurer la continuité d'exploitation et présenter des comptes exacts de ses clients, devra prendre les mesures qui s'imposent.

CONCLUSION DE LA DEUXIEME PARTIE

Dans la perspective de comprendre au mieux et d'évaluer l'organisation comptable notamment l'aspect informatique, nous avons entrepris au cours de notre mission, les démarches et investigations suivantes :

— Questionnaire soumis aux utilisateurs

— Entretien avec la direction générale

—Entretien avec les différents utilisateurs

Ces diligences nous ont permis de présenter les résultats. En définitive, malgré la présence de quelques défaillances liées surtout à l'environnement informatique notamment le logiciel, nous avons constaté qu'elles n'avaient pas de répercussions importantes sur la fiabilité des comptes.

CONCLUSION GENERALE

L'existence des risques liés à la comptabilité informatisée nous semble vraiment inconnue dans nos organisations car pour certaines personnes, tout ce qui vient de l'ordinateur est juste. La complexité des systèmes informatiques, ajoutée à la multitude formes des risques possibles, rendent leur maîtrise très difficile. Pourtant l'entreprise a intérêt à les maîtriser, condition sine qua non pour présenter des comptes sincères et réguliers.

Cette difficulté est surtout due au manque de spécialistes en la matière. L'auditeur doit avant l'examen des comptes de la société, examiner sa fonction informatique qui est le support de la comptabilité qui a permis de produire ces comptes. Cette prise en compte dans la mission ne modifie en rien la démarche de l'auditeur mais lui permet d'évaluer d'une part le contrôle interne de la fonction informatique de la société et d'autre part de s'assurer de la qualité de la documentation .

BIBLIOGRAPHIE

Ouvrages

♣ ANGOT Hugues FISCHER Christian, THEUNISSEN Baudouin (1994), Audit comptable, Audit informatique, Boeck université, p 253 ;

♣ CNCC Audit réalisé en environnement informatisé, Juin 1998, p 239 ;

♣ CNCC (1995), Démarche du Commissaire aux Comptes en milieu informatisé,

♣ CNCC Prise en compte de l'environnement informatique sur la démarche d'Audit, Avril 2003, p 129 ;

♣ Comptable (2005) : Mémento Pratique, édition Francis Lefebvre, p 1791 ;

♣ DERRIEN Yann (1992), Les techniques de l'audit informatique, édition Dunod, p 238 ;

♣ KPMG (1998), Audit informatique, collection comptable, p 316 ;

♣ IFACI (1993), Audit et contrôle des systèmes d'informations, module 8 : Sécurité, p 126

♣ IFACI (1993), Audit et contrôle des systèmes d'informations, module 3 : Gestion des ressources informatiques, p 126 ;

♣ MOR Niang (2002), Comptabilité des sociétés commerciales, comptabilité approfondie, 2ème éditions, Dakar, p 438.

♣ SYSCOA (1998) Plan Comptable Général des Entreprises, édition Foucher, p 831 ;

♣ THORIN Marc (2000), l'Audit informatique, édition Hermès, p 184 ;

Mémoires et supports de cours

♣ MARIO Barboza (2005) Analyse des risques liés à la comptabilité informatisée : cas de HALD ;

♣ NGUESSAN David Parfait (2003), Audit informatique dans une entreprise pétrolière : Oxygaz Sénégal, p 132 ;

♣ SARR Abacar (2003), Audit informatique, p 63 ;

♣ TALL Mamadou (2003), Audit de la sécurité informatique, p 100 ;

Articles

- AWT (2000) La sécurité informatique, fiche p 6
- DGI la tribune de l'impôt N°006 du 15 Janvier au 15 Avril 2006
- La revue française de l'Audit Interne N°81 et N°93 de Janvier Février 1989

Sites Internet

- www. lemonde.fr
- www. lemondeinformatique.fr
- www. lesechos.fr
- www. sécurité. teamlog.com
- www. wikipédia.fr

QUESTIONNAIRE N°1 : LES RISQUES LIES AUX MOTS DE PASSE

1. Les mots de passe sont-ils affectés individuellement à chaque utilisateur ?
2. Les mots de passe sont-ils modifiés assez régulièrement ?
3. Les mots de passe sont-ils assez sophistiqués ?
4. Existe-t-il des mots de passe pour entrer dans le système ?
5. La table des mots de passe est-elle protégée ?
6. Existe-t-il un gestionnaire des mots de passe ?
7. Est-il possible de détecter les tentatives d'accès non autorisée ?
8. Les utilisateurs sont-ils sensibilisés aux risques qui peuvent découler au prêt de leur mot de passe ?
9. Existe-t-il d'autres systèmes d'identification au sein de l'entreprise ?
10. Existe-t-il un système de suppression ou de non validation de mot de passe en cas de démission, de licenciement ou de congé d'un utilisateur ?
11. Toute intrusion est-elle détectée immédiatement ?

QUESTIONNAIRE N°2 : LES RISQUES LIES AUX LOGICIELS

1. Comment se fait la validation comptable ?
2. Les procédures de reprise sur un site extérieur sont-elles régulièrement testées ?
3. L'accès aux logiciels comptables est-il réglementé ?
4. Quelle est la procédure de validation ?
5. Est-ce possible de supprimer ou modifier après la validation ?
6. Existe-t-il des périodes de clôtures ?
7. Procède-t-il d'abord à la révision comptable avant la validation ?
8. Quelle est la qualification des opérateurs de saisie ?
9. Le logiciel utilisé assure-t-il l'irréversibilité et l'inaltérabilité des données contenues ?
10. Quel est le degré de fiabilité du logiciel ?
11. Le logiciel garantit-il le chemin d'audit ?
12. Le logiciel utilisé accepte-t-il la correction en négatif préconisée par le SYSCOA. ?
13. Le logiciel utilisé reconnaît-il la monnaie ayant cours légal dans la zone UEMOA (Le FCFA) ?
14. Les programmes de détection des virus sont-ils exécutés régulièrement ?
15. L'anti-virus est-il mis à jour régulièrement ?
16. Le logiciel fourni est-il accompagné par la documentation nécessaire permettant son utilisation adéquate ?

QUESTIONNAIRE N°3 : LES RISQUES LIES AU NON RESPECT DE LA REGLEMENTATION.

1. Les dirigeants respectent-ils les dispositions légales relatives à la comptabilité informatisée ?
2. L'accès à la salle du serveur est-il règlementé ?
3. Qui est autorisé d'accéder à la salle du serveur ?
4. Quels sont les risques qui se sont déjà survenus dans l'entreprise ?
5. Les procédures et l'organisation comptables sont-elles suffisamment documentées ?
6. L'identification des pièces comptables satisfait-elle les obligations réglementaires ?
7. Le système comptable permet-il un contrôle a priori par les organes de contrôles ?
8. Les entrées dans le système comptable font-elle l'objet d'édition sur papier pour archivage ?
9. Chaque donnée imputée dans le système fait-elle l'objet d'un justificatif constitué par un document écrit ?
10. L'entreprise effectue-t-elle des enquêtes sur les forçages ?
11. Existe-t-il une politique informatique formalisée ?

QUESTIONNAIRE N°4 : LES RISQUES LIES AUX MATERIELS

Quelle est la capacité du serveur ?

Quelle est la date d'acquisition des ordinateurs servant à la tenue de la comptabilité ?

Existe-t-il une prévision de renouvellement permanent ?

Existe-t-il une police d'assurance pour couvrir les pertes de matériel ?

Quelles sont les mesures mises en place pour sécuriser le matériel informatique ?

Existe-t-il de contrat de maintenance avec une maison spécialisée ?

Le système de sauvegarde des données est-il fiable ?

Existe-t-il un plan de sécurité informatique ?

Existe-t-il un plan de sécurité informatique ?

Peut-on réellement éviter le vol ou la destruction du matériel et des données par le système de sécurité actuel?

Le plan de secours est-il testé ? Si oui, à quand remonte le dernier test ?

Les fichiers comptables vitaux sont-ils stockés hors site ?

L'humidité et la température de la salle sont-elles surveillées ?