CESAG

CENTRE AFRICAIN D'ETUDES SUPERIEURES EN GESTION

INSTITUT SUPERIEUR DE COMPTABILITE

DIPLÔME D'AUDIT INTERNATIONAL ET CONTRÔLE

D.E.S.S - *Diplôme de 3é cycle*

11e Promotion

MEMOIRE DE FIN D'ETUDE

Thème:
Évaluation du contrôle interne dans le cadre d'un audit légal en milieu informatisé : le cas de la SICOGI

Présenté et soutenu par:
Thomas Konan KONAN

Sous la direction de :
Monsieur Samba DIAGOLA :
Auditeur Consultant à
Continental Audit, représentant de
KPMG International

Février 2002

DEDICACES

Ce travail est particulièrement dédié à :

- DIEU, à qui toutes choses sont assujetties, qui l'a béni et m'a permis de le faire. Je lui rends grâce,
- Mes Parents ; Papa et Maman, qui m'ont appris la persévérance, la recherche de l'exception constructive;
- Mme Mariam KONE (Née COULIBALY), ma sœur, grâce à qui le financement de cette formation a été possible ;
- Jocelyne GOA, ta disponibilité, ta générosité et ton soutien ne m'ont jamais fait défaut ;
- Irène KONE (Iroo) pour tout le travail que tu as abattu pour moi.
- Mes frères et sœurs, pour votre soutien constant le long de ce parcours.

REMERCIEMENTS

Nous tenons à remercier, les dirigeants et collaborateurs du cabinet continental Audit, Ainsi que les enseignants et agents du CESAG pour nous avoir fait confiance et nous avoir permis d'apprendre à leurs côtés.

Nous remercions particulièrement

- Monsieur Fatogoma COULIBALY Expert comptable
- Monsieur Francis DESCLERS Directeur associé de continental Audit
- Monsieur Koffi AKOSSAY , directeur de la nouvelle SOCOGEC.
- Monsieur Samba DIAGOLA, Auditeur Consultant à continental Audit
- Monsieur Marius ADAGARA Auditeur à la nouvelle SOCOGEC.
- Monsieur Moussa YAZI : sous- Directeur de l'Institut Supérieur de Comptabilité au CESAG
- Monsieur Ababacar SARR, contrôleur général à la BHS et professeur associé au CESAG
- Monsieur Moustapha M'BACKE DIOP, Directeur de l'Institut Supérieur de Comptabilité au CESAG

Nos remerciements vont également à l'endroit des dirigeants et collaborateurs de nos lieux de stages et de nos amis de Dakar et en particulier :

- LA Direction de l'hôpital le DANTEC.
- La 11^{e} promotion du cycle Audit et contrôle du CESAG
- Messieurs Joël AJAKOU , Cheikh. N'DIAYE, Dacoumba SARR.et tous leurs collaborateurs de la bibliothèque du CESAG .

Nos remerciements enfin à tous ceux qui, de près ou de loin, ont contribué à la réalisation de cette formation et de ce mémoire.

FIGURES ET TABLEAUX

LISTE DES FIGURES — PAGES

LISTE DES TABLEAUX — PAGES

ANNEXES

GLOSSAIRE

A T H : association technique pour l'harmonisation des cabinets d'audit et conseil

A D P : -accession directe à la propriété

A M I : - audit en milieu informatisé

B C : -bon de commandes

C A : conseil d'administration

C A C : commissaire aux comptes

C I : -contrôle interne

C N C C : -compagnie nationale des commissaires aux comptes

C N P S : -caisse nationale de prévoyance sociale

D A F : -direction administrative et financière

D C E : -direction commerciale et de l'exploitation

D R H : -direction des ressources humaines

E D I : -échange de données informatisées

K A S : - KPMG audit servises

L V : -location vente

L S : -location simple

M I : -milieu informatisé

O D : -opérations diverses

O E C : -ordre des experts comptables de France

P I D R : provision pour indemnité de retraite

R A C I N E : -rationalisation des choix informatiques

S I C O G I : société ivoirienne de construction et de gestion immobilière

S M I M : -service des moyens informatiques et de la méthode

T I C : technologie de l'information et de la communication

V P L : -vente de patrimoine locatif

TABLE DES MATIERES

RUBRIQUES ***PAGE***

INTRODUCTION

Dans l'environnement économique, aujourd'hui sous l'emprise de la mondialisation, et de la concurrence totale, il y a urgence pour les entreprises qui veulent survivre d'améliorer leur production suivant la trilogie qualité, temps, économie. En d'autres termes, pour mieux se positionner ou même rester dans la course, les entreprises doivent produire mieux, vite et à moindre coût.

L'avènement de l'informatique a introduit dans le monde du travail tant au niveau de la production que des services, une technologie de pointe satisfaisant cette trilogie. C'est cela qu'ont compris les grandes nations industrialisées et qui justifie le développement ultra-rapide de l'informatique tant du point de vue du matériel que de ses applications, et pour une large couverture de différents domaines de l'activité économique.

En effet, parlant des technologies de l'information et de la communication (T. I. C.), D'ANDIGNE (2002 : 12) reconnaît 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. ».

Par ailleurs, BEDIN (2002 : 26), dans une description des ordinateurs portables sur le marché, donne quelques caractéristiques d'appréciation, notamment sur les éléments suivants :

- rapidité du processeur Pentium III : 700 à 850 Mhz ;
- Capacité de disque dur de 20 à 30 Go ;
- Autonomie énergique allant jusqu'à 5h-41mn.

Il va de soi que des ordinateurs de bureau (généralement plus puissants) disposent de performances plus élevées.

En plus, les applicatifs deviennent de plus en plus complexes et plus complets à l'image « des progiciels intégrés comme oracle dont on dit beaucoup de bien, et qui se vendent comme du pain (environ 1100 clients) » BIBARD (2002 : 8)

En fait, il y a une frénésie de l'industrie informatique qui gagne toutes les entreprises. Celles-ci ne résistent pas à la tentation de l'outil informatique et font parfois même de la veille technologique pour disposer, parmi les premières, des outils les plus performants.

On peut dire simplement qu'aujourd'hui toute entreprise qui se respecte est en grande partie dépendante de l'outil informatique.

C'est le cas de la SICOGI (la société ivoirienne de construction et de promotion immobilière) qui dispose d'un équipement informatique important, et parfois même au-delà de ses besoins. Les utilisateurs de l'outil informatique à la SICOGI sont dans tous les services opérationnels grâce à des logiciels d'application acquis sur le marché ou développés en interne.

La prise de conscience des risques informatiques est sans doute réelle dans les grandes multinationales ; mais en Afrique, elle est encore très timide. Et pas seulement dans les entreprises industrielles ou commerciales, mais aussi dans des cabinets d'expertise comptables, qui ne semblent pas encore réellement prendre en compte l'évaluation de la maîtrise des risques liés à l'informatique dans leurs interventions.

PROBLEMATIQUE

Obnubilées par les prouesses technologiques, mais aussi par le marketing de l'informatique, les entreprises s'adonnent (à raison sans doute) 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. Ce qui inquiète d'ailleurs le patron le plus célèbre de l'industrie informatique BILL GATES,

(2000 : 6) qui a opté de façon claire pour la fiabilité des logiciels en disant : « Dorénavant, quand il faudra choisir entre ajouter de nouvelles fonctions ou régler un problème de sécurité, nous devons préférer la sécurité ».

Nous le comprenons bien. En effet, imaginons les conséquences des quelques situations suivantes : (SARR : 2000).

- un écrasement malencontreux d'un fichier en exploitation sans sauvegarde,
- un court circuit déclenche un incendie dans la pièce des serveurs sans aucune mesure de protection,
- un pirate qui entre par un terminal non protégé dans une banque,
- etc..

Les exemples sont légions et les risques, lorsqu'ils surviennent, sont souvent ingérables.

C'est pour cela que dans le cadre de leurs misions, les auditeurs doivent de plus en plus éveiller cette conscience des risques informatiques chez leurs clients, notamment par une évaluation du C I de la fonction informatique.

C'est ROUFF (2001 : 12) qui disait : « l'objectif du CI est de maîtriser les risques (financiers essentiellement) et toutes les fonctions et processus de l'organisation ».

Alors que la SICOGI qui n'a pas pu mettre en œuvre le schéma directeur informatique dont elle s'est dotée depuis 1993 désire investir à nouveau en matière informatique sans avoir résolu les problèmes soulevés depuis cette date.

Par ailleurs, BOUANICHE, (2001 : 22) disait : « concernant l'informatique, l'évolution technologique est telle qu'elle génère de nouvelles pratiques et de nouveaux métiers. On se retrouve alors dans la situation caricaturale d'auditeur, avec un référentiel dépassé ».

D'où notre question de recherche, à savoir :

Comment peut-on évaluer le contrôle interne dans un contexte d'entreprises de plus en plus informatisées comme la SICOGI ?

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

- Comment peut-on caractériser un milieu informatisé ?
- Comment un milieu informatisé peut-il satisfaire aux objectifs du contrôle interne ?
- Quelle démarche pour apprécier le contrôle interne d'une entreprise informatisée ?

Annonce du thème

La recherche de réponses à ces interrogations nous incite à étudier comme thème : « **L'EVALUATION DU CONTROLE INTERNE DANS LE CADRE D'UN AUDIT LEGAL EN MILIEU INFORMATISE : LE CAS DE LA SICOGI** »

L'évaluation du contrôle interne, dans une entreprise informatisée ou non, est assez vaste, et nous ne pourrons la faire dans le cadre de cette étude. En effet, la méthodologie générale de l'évaluation du contrôle interne proposée par (A. T. H , 1991) et la (CNCC, 1992) commence par le choix des fonctions. Cela suppose que cette évaluation peut bien concerner toutes les fonctions de l'entreprise.

Par ce thème, nous entendons nous intéresser au C I de la fonction informatique dans le cadre d'un audit légal.

Objectifs poursuivis

La réalisation de cette étude doit nous permettre de :

- décrire les composants du contrôle interne d'un milieu informatisé
- évaluer le contrôle interne dans un milieu informatisé
- faire des recommandations

Intérêt de l'étude

- **Pour la profession d'audit**

Cette étude est d'autant plus importante qu'elle est l'avenir même de notre métier. En effet, même si, en Afrique nos entreprises ne sont généralement pas ultra-informatisées, cela ne saurait tarder du fait de la mondialisation et de l'uniformisation des systèmes de gestion des grands groupes internationaux qui s'implantent de plus en plus sur notre continent. Et l'auditeur ne saurait rester en marge de cette évolution presque naturelle des économies. Nous dirons même que c'est une obligation pour l'auditeur de « se fondre dans la peau de l'Ours » c'est-à-dire de s'adapter à son environnement de travail. C'est le cas pour les grands cabinets internationaux, mais beaucoup de cabinets africains traînent encore le pas. Il nous appartient donc de leur donner les moyens .

- **Pour la SICOGI :**

La SICOGI (la société ivoirienne de construction et de gestion immobilière) est une entreprise ambitieuse qui veut rester leader dans ses domaines d'activité (métiers, marchés etc.). Pour y arriver, elle a besoin de se doter des meilleurs moyens technologiques à la fois pour la gestion et pour la conception. Dans ces conditions, elle a aussi besoin de connaître les risques auxquels elle s'expose par l'usage de l'outil informatique, et d'en prendre les dispositions de contrôle interne nécessaires.

‣ Pour nous même

Au terme de cette formation une nouvelle carrière va commencer pour nous. Nous la voulons sous un angle "avant-gardiste" notamment pour l'Afrique. C'est pour cela que nous nous intéressons à l'audit informatique dont la qualité de service dépend de la compétence des auditeurs. Il faut alors être :

- soit un auditeur et informaticien de formation,
- soit une équipe d'audit comprenant :
  - des auditeurs de formation et de métier ;
  - des informaticiens de formation et d'expérience.

Pour notre part, nous avons choisi la première voie, et nous espérons y arriver au plus vite.

Annonce du plan

Notre travail comprendra deux grandes parties :

La 1ère partie consiste en une revue de la littérature en matière de contrôle interne dans un milieu informatisé c'est-à-dire la méthodologie de l'évaluation du contrôle interne.
La 2ème partie consiste en l'évaluation pratique du contrôle interne dans une entreprise ivoirienne, la SICOGI.

La première partie que nous traitons dans les pages suivantes comporte deux chapitres. Le premier est la synthèse de littérature relative aux composants du C I dans un milieu informatisé. Le deuxième chapitre déroule la démarche de mise en œuvre de son évaluation.

PREMIE PARTIE

CADRE THEORIQUE DE L'EVALUATION DU CONTRÔLE INTERNE EN MILIEU INFORMATISE

CHAPITRE 1 : LE CONTROLE INTERNE EN MILIEU INFORMATISE

L'appréciation du contrôle interne en milieu informatisé passe par la connaissance de ces deux éléments. C'est pour cela que ce chapitre va préciser la caractérisation du C I dans un milieu informatisé.

SECTION 1 : CARACTÉRISATION DU C I

Comme moyen permettant d'atteindre les objectifs du commissaire aux comptes, le contrôle interne n'est pas une fonction mais un ensemble de dispositions, un état, (RENARD, 1998). Nous allons dans les pages qui suivent en préciser les contours.

PARAGRAPHE 1 : DEFINITION ET OBJECTIFS DU C I

11- Définition

Selon BARRY (1994 : 9), « le contrôle interne peut être défini comme l'ensemble des sécurités qui contribuent à assurer :

- d'une part , la protection et la qualité de l'information, et la sauvegarde du patrimoine
- d'autre part, l'amélioration des performances par la mise en place d'un système d'organisation, de méthodes et de procédures garantissant la pérennité de l'entreprise ».

Cette définition ne permettant pas de percevoir le caractère dynamique et évolutif du contrôle interne, nous complétons avec celle selon KPMG (1996:52-3) : « Le contrôle interne est un processus mis en œuvre par le conseil d'administration, la direction et d'autres membres du personnel d'unc entité, destiné à assurer de manière

raisonnable la réalisation des objectifs relatifs à l'une ou l'autre des catégories suivantes :

- efficacité et optimisation des opérations;
- fiabilité des informations financières;
- conformité aux lois et réglementations en vigueur »."

Ces définitions supposent que le C I

- soit constitué d'une série de mesures intégrées dans le processus de gestion des activités de l'entité plutôt que venant s'y ajouter;
- soit mis en œuvre par le personnel;
- ne puisse fournir qu'une assurance raisonnable de la réalisation des objectifs de l'entité.

12- Les objectifs

Les définitions énoncées ci dessus dégagent trois grands objectifs du C I et qui selon (KPMG 1996 ; COLLIN & VALLIN 1992) sont :

- **Des objectifs d'ordre financier et comptable :** pour lesquels le C I doit assurer la production de comptes et d'états financiers sincères et réguliers, par référence aux normes généralement admises dans les milieux d'affaires.

- **Des objectifs opérationnels** pour sauvegarder le patrimoine et optimiser les opérations réalisées. Ces objectifs sont difficiles à réaliser puisqu'ils nécessitent la minimisation de décisions erronées, de la fraude, d'évènements extérieurs imprévus etc..

- **Des objectifs de conformité aux lois et réglementations** qui sont normalisées par des institutions, des organisations professionnelles et la direction générale.

Ces objectifs étant clarifiés, nous devons rechercher les moyens de les satisfaire. Ce

qui nous emmène à parler des principes qui soutiennent un bon C I. et des éléments qui le composent.

PARAGRAPHE 2 : PRINCIPES ET ELEMENTS DU C I

21- Principes du C I

L' O.E.C , (in OBERT 1995 : 43) en distingue sept (7), qui sont :

- l'organisation,
- l'intégration des contrôles,
- la permanence,
- l'universalité,
- l'indépendance,
- l'information,
- l'harmonie,
- auxquels (MIKOL 199) ajoute la qualité du personnel.

- **l'organisation** qui doit être

  - préalable et vérifiable ;
  - adaptée et adaptable aux différentes évolutions de l'entreprise ;
  - formalisée par un organigramme, un manuel de procédure etc..

Cette organisation doit assurer une séparation convenable des fonctions incompatibles (dont le cumul d'au moins deux , favorise les erreurs, les négligences, les fraudes et leur dissimulation) qui sont:

- les fonctions de décision;
- les fonctions de conservation;
- les fonctions d'enregistrement;
- les fonctions de contrôle;

auxquelles (RENARD, 1998) ajoute les fonctions financières (encaissements et dépenses)

- **L'intégration des contrôles** à tous les niveaux du processus de la gestion de l'entreprise ;

- **La permanence** qui veut que l'entreprise défende et protège sa pérennité ;

- **L'universalité** qui veut que le C I concerne toute personne, en tous temps et en tous lieux ;

- **L'indépendance** qui implique que les objectifs du C I soient atteints indépendamment des procédés, moyens et méthodes de l'entreprise. En particulier que l'usage de l'informatique n'élimine pas certains contrôles intermédiaires ;

- **L'information** qui se veut pertinente, utile, objective, communicative et vérifiable ;

- **L'harmonie** qui commande simplement que le C I soit adapté au fonctionnement de l'entreprise, aux sécurités recherchées et au coût du contrôle.

- **La qualité du personnel** qui doit disposer de la compétence nécessaire.

22- les composants du C I

Le C I est composé de cinq (5) éléments interdépendants et intégrés aux processus de gestion. Ce sont, (COOPERS & LYBRAND 2000 : 28) :

- l'environnement de contrôle
- l'évaluation des risques ,
- les activités de contrôle,

- l'information et la communication,
- le pilotage.

- **L'environnement de contrôle**.

Il impose discipline et organisation et est constitué de la complémentarité de :

- l'environnement matériel (secteur d'activité, culture d'entreprise etc..)
- l'individu , à travers l'éthique l'intégrité la compétence du personnel.

Il est le socle, le moteur et le fondement des autres éléments du C I .

- **L'évaluation des risques.**

Elle consiste en l'identification, en l'analyse en vue de la maîtrise des facteurs susceptibles d'affecter la réalisation des objectifs (compatibles et cohérents) de l'entreprise. C'est un processus qui doit intégrer de façon harmonieuse les activités commerciales, financières et de production de l'entreprise.

- **Les activités de contrôle.**

Elles sont menées à tous les niveaux hiérarchiques et fonctionnels de la structure. Elles comprennent des actions aussi variées qu'approuver, autoriser, vérifier et rapprocher, apprécier les performances opérationnelles, la protection des actifs ou la séparation des fonctions. Elles sont identifiées par la direction comme étant nécessaires à la réduction des risques liés à la réalisation des objectifs.

- **L'information et la communication**

Les systèmes d'information et de communication doivent être articulés autour des activités de contrôle. Ils comprennent :

- des informations internes et externes ;
- des informations ascendantes, descendantes et horizontales.

- **Le pilotage**

L'ensemble du processus doit faire l'objet d'un suivi en vue de procéder à des

modifications en cas de faiblesses constatées. Il s'agit soit :

- d'un suivi permanent par des activités courantes du management et du personnel d'encadrement ;
- d'une évaluation périodique du C I en fonction de l'évaluation des risques ;
- des deux.

SECTION 2 : ENVIRONNEMENT DE CONTROLE D'UN MILIEU INFORMATISE

L'outil Informatique est entré dans la vie de l'entreprise industrielle ou commerciale à des degrés différents. Ainsi, il existe des entreprises qui ne disposent pour tout outil informatique que quelques ordinateurs dont le seul usage est le traitement de texte. Par contre d'autres sont dotées d'équipements informatiques des plus performants dans toutes les composantes de leur structure. Entre les deux, tous les scénarios possibles existent. Comment peut-on donc caractériser un milieu informatisé ?

PARAGRAPHE 1 : CARACTERISTIQUES D'UN MILIEU INFORMATISE

11- Définition d'un milieu informatisé

Selon les recommandations internationales de l' I A S C, (in SARR 2000 : 57), « un milieu est dit informatisé lorsqu'un ordinateur, quels que soient sa taille et son type, intervient dans le traitement de l'information financière qui présente un intérêt pour l'audit, que cet ordinateur soit exploité par l'entité ou par un tiers ».

(LAMY, 1996) ne le contredit pas en expliquant qu'un milieu informatisé peut être toute entité d'une certaine importance qui dispose ou va se doter d'un système de gestion informatisé.

Plusieurs éléments liés les uns aux autres peuvent caractériser le M I. On peut citer entre autres :

- le matériel et ses consommables;
- le personnel pour son exploitation;
- une politique de sa gestion et de son développement;
- un dispositif pour sécuriser son utilisation et l'entreprise;
- etc..

12- Le matériel informatique et ses ressources spécifiques

Ils sont caractérisés par l'évolution vertigineuse que connaît la technologie qui les produit. Ils connaissent un développement extrêmement rapide qui oblige les entreprises et organisations à une veille technologique pour ne pas être dépassées. Au fur et à mesure que l'ordinateur (micro-ordinateur) se miniaturise, ses capacités mémoires et vitesses d'exécution augmentent. Il se développe de multiples logiciels de hautes performances pour tous les secteurs d'activité de l'entreprise.
Pour les entreprises, l'exception est de rester insensibles à toutes ces prouesses technologiques, et cela devient de plus en plus rare.

13- Le personnel

Dans un milieu informatisé, on peut distinguer deux types de personnels :

- le personnel informatique;
- les utilisateurs informatiques.

131- Le personnel informatique

Il est constitué de spécialistes dans les divers domaines de l'activité informatique (étude analyse et programmation, administration de réseaux ou de sécurité, développement, mise en exploitation etc..). Il est la cheville ouvrière de la fonction informatique, et constitue le lien entre producteurs de l'outil informatique et

l'entreprise. De sa compétence et de son organisation dépend la qualité de tout le système informatique de l'entreprise.

132- Les utilisateurs

Ils peuvent être dans tous les autres secteurs d'activité de l'entreprise, notamment dans les services de traitement de l'information financière et commerciale, d'analyse de données, de planification et programmation etc..
Le système informatique est un outil de travail par lequel ils entrent des informations pour en obtenir des résultats conformément aux instructions données au système. De la qualité de leur formation à utiliser le système, dépendent les résultats produits.

14- La politique de gestion et de développement du système informatique

Elle dépend de la direction générale et de l'importance de l'informatique dans les activités de l'entreprise.
Cette politique informatique sera matérialisée par un plan ou un schéma directeur informatique.

15- Le dispositif de sécurité

Le système de matériels et d'informations, appartenant au patrimoine de l'entreprise, doit être protégé.

PARAGRAPHE 2 : ORGANISATION DE LA FONCTION INFORMATIQUE

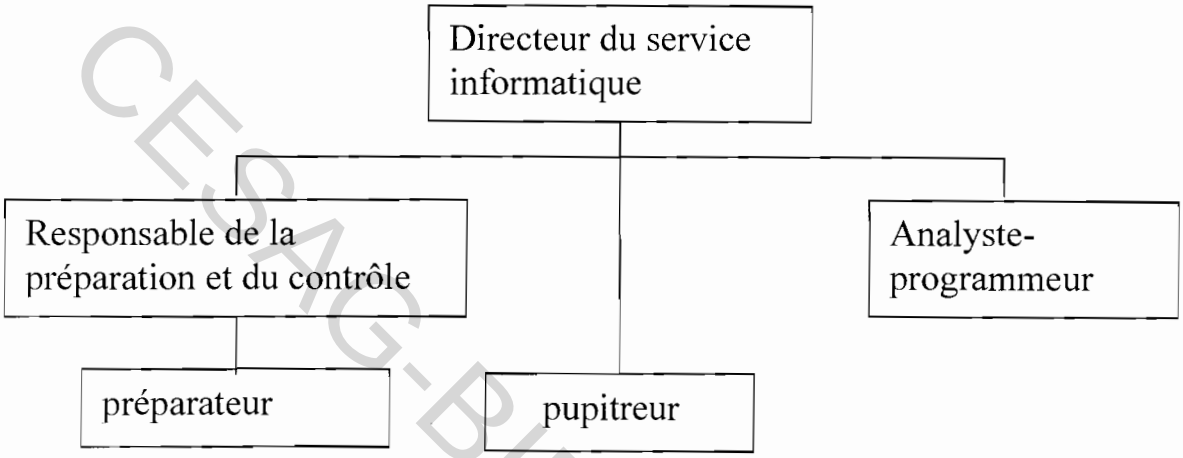
Selon le degré d'informatisation de l'entreprise et l'intensité de l'activité informatique, il sera créé un service, une direction ou un comité informatique au sein de l'entreprise.

Selon RENARD (1998 :132), l'organisation est constituée de quatre (4) éléments qui sont :

- **L'organigramme hiérarchique** pour savoir qui commande à qui ;

Nous présentons ici, un organigramme pour un petit service informatique.

FIGURE N °1 : Organigramme type d'un petit centre



Source : (JENKINS & PINKNEY 1984 : 197)

Le préparateur exerce alors la fonction d'exploitation. ce qui permet entre autre de séparer les fonctions exploitation, contrôle et développement.

- **L'analyse des postes** pour savoir qui fait quoi ;

- **Le recueil des pouvoirs et latitudes** pour connaître les limites des pouvoirs de chacun (Exemple : signer les notes de frais inférieurs à 5 000 F)
- **L'élément matériel** qui organise l'environnement. Il permet à l'organisation d'assurer sa protection (physique, logique ou contre les malversations etc…) Il comprend par exemple la sécurité dans les bureaux, le coffre du caissier, le dispositif électronique de surveillance etc…

PARAGRAPHE 3 : CARACTERISTIQUES DES APPLICATIONS INFORMATISEES

Une application informatisée est essentiellement caractérisée par :

- des fichiers permanents avec une procédure de création, de mise à jour et de maintenance de leur contenu ;
- des entrées de données ;
- des traitements ;
- des fichiers utilisés ;
- des interfaces éventuelles avec d'autres applications ;
- des sorties de résultats avec ;
- des contrôles programmés, (CNCC , 1995)

SECTION 3 : EVALUATION DES RISQUES EN M I

L'informatique, quoique présentant de nombreux avantages pour l'entreprise, lui fait courir aussi des risques physiques, logiques et aux conséquences économiques importantes.

PARAGRAPHE 1 : LES RISQUES GENERAUX INFORMATIQUES

La présence de l'outil informatique et de la micro informatique dans une entreprise entraîne nécessairement des comportements nouveaux. Ce changement part des activités opérationnelles des utilisateurs à la définition des politiques et stratégies de l'entreprise. La gestion de ce nouvel environnement entraîne des risques qui, s'ils ne sont pas maîtrisés, peuvent poser de graves difficultés à l'entreprise. Sans avoir la prétention de les traiter de façon exhaustive, nous pouvons citer entre autres :

- la carence en matière de documentation
- l'absence de politiques informatiques
- les problèmes d'insécurité,
- les cumuls de fonctions clés,

- les risques liés a la maintenance
- ect..

11- La carence en matière de documentation

La documentation relative aux logiciels (acquis ou développés), aux procédures de contrôle, de sauvegarde et de maintenance est un outil important de formation aussi bien pour les informaticiens que pour les utilisateurs finaux.

Selon FAIVRE & LOREAU (1993 : 25), « l'absence de documentation conduit inéluctablement à des atteintes à la maintenabilité des applications surtout en l'absence de la personne qui a effectué les développements».

12- L'absence de politiques informatiques

Une politique en matière informatique permet « de définir un cadre harmonieux et cohérent de développement de l'informatique dans l'organisation, en phase avec les orientations de la direction générale », (FAIVRE & LOREAU, 1993 : 28).

Le schéma directeur informatique permet d'en définir les objectifs et les moyens de sa mise en œuvre.
THORIN (2000 : 59) le confirme en disant : « l'ensemble des buts de réalisation, de leurs motivations et de leurs conditions de réalisation constituent finalement le schéma directeur », parlant ainsi de la politique informatique. Le schéma directeur aborde notamment :

- la stratégie en matière d'équipement matériel ;
- la stratégie en matière d'acquisition et / ou de développement des applications ;
- les méthodes et les procédures de développement et de maintenance des applications et du matériel ;

- la stratégie en matière de gestion des ressources humaines ;
- l'organisation fonctionnelle du service informatique et la définition des responsabilités des parties prenantes;
- etc..

Un schéma directeur informatique est donc un dispositif très important. Son absence, le non-respect des règles de son élaboration ou le non-respect de son suivi dans le temps, préfigurent d'une incohérence, d'une inadaptation du développement de l'informatique aux objectifs et finalités de l'entreprise. Ils préfigurent aussi de faiblesses des applications développées, notamment de risques de traduction comptable.

13- Les problèmes d'insécurité

Le chroniqueur masqué " yellow" (janvier 2002 : 4) explique comment il a quasiment réussi à reconstituer le réseau d'un grand cabinet de conseil en sécurité informatique, à l'aide de **l'en-tête** dans un message de ce dernier. Selon lui, l'en-tête du message contenait les traces de toutes les passerelles traversées.

Il dit : « chaque message qui sort de ce réseau constitue un véritable guide de piratage pour les indélicats qui voudraient aller voir de plus près ce que fabrique ce grand cabinet de conseil ».

Dans une enquête publiée sur les entreprises Françaises par Philippe ROSE (2001: 5), 30% des répondants ont subi les effets d'un risque informatique liés à la sécurité pour vol de matériels informatiques, 26% pour erreurs des utilisateurs, 24% pour un événement naturel, 25% pour cause non identifiée, 14% pour erreurs de conception, 13% d'accident physique, etc..

Ces exemples suffisent à comprendre les risques d'insécurité informatique.

14- Cumul de fonctions clés

D'une part la capacité de l'informatique à traiter des volumes importants d'opérations, sa rapidité d'action, sa flexibilité,
D'autre part, la méconnaissance même des risques de malveillance informatique chez certains décideurs au plus haut niveau de l'entreprise, induisent des limitations importantes de l'effectif du personnel.

Selon ASSOUMANA (2000 : 30) « En général dans les structures simplifiées, le personnel informatique est le seul à connaître parfaitement l'interdépendance entre les sources des données, leur mode de traitement, leur sortie et leur utilisation. Ils peuvent connaître par conséquent les faiblesses du C I informatique et peut être en abuser ».

La conséquence est que, des fonctions incompatibles se retrouvent souvent concentrées entre les mains d'une même personne.

15- Les risques liés à la maintenance

Selon LAMY (1996 : 32), « la maintenance consiste en L'ensemble des travaux de maintien en état opérationnel d'une application informatique ». La maintenance intervient souvent dans un environnement où l'auteur du logiciel ou du matériel est indisponible.

La difficulté première ici est la bonne compréhension du logiciel et de ses évolutions successives. Il y a en conséquence un risque de mauvaise application de la méthodologie retenue s'il y en a, ou un risque d'utilisation d'une méthodologie non adaptée.
Il y a aussi le risque d'une mise à jour non conforme aux besoins des utilisateurs s'il n'existe pas une procédure formalisée de maintenance qui les associe.

PARAGRAPHE 2- : LES RISQUES DE TRAITEMENTS INFORMATISES

Ils sont tout aussi légion. Nous pouvons citer entre autres :

- les risques de traduction comptable et financières,
- les risques liés au paramétrage des applications,
- les risques inhérents aux saisies automatisées,
- les risques liés aux traitements en temps réel,
- les risques liés aux traitements en temps différé,
- les risques liés aux systèmes intégrés,
- les risques d'opérations rétroactives,
- etc.. (LAMY 1996 ; LAMY 1997 ; FAIVRE & LOREAU 1993)

21- Le risque de traduction comptable et financière

Les informations transmises, sont-elles traitées par le système dans le strict respect des normes, des méthodes et des principes comptables et financiers ?
Exemple : le logiciel traite-t-il les informations comptables et financières conformément aux principes et règles du SYSCOA ?

22- Risques liés au paramétrage des applications

Selon LAMY (1996 : 24), « Le paramétrage d'une application, c'est un ensemble de règles qui déterminent le fonctionnement de cette application. Ce sont en réalité des codes qui lui permettent d'exécuter des tâches bien précises ».

Les erreurs de paramétrage sont courantes. Lorsqu'elles surviennent, elles ont un impact direct sur le risque de traduction comptable ou fonctionnelle et peuvent porter sur :

- des codifications ou imputations erronées (avec pour conséquence par exemple des imputations automatiques erronées) ;

- des affectations dans une mauvaise période (Taux de change se référant à une autre période) ;
- des calculs approximatifs ou faux (des calculs d'amortissement, de provision ou de rotation de stock erronés) ;
- interruption de traitements ;
- etc....

23- Les risques inhérents aux saisies automatisées

Pour les saisies automatisées, les données sont introduites dans le système grâce à des ordinateurs dédiés à des personnes étrangères, notamment des clients consommateurs des services.
C'est le cas par exemple des distributeurs automatiques de billets de banque, des cabines téléphoniques à cartes, etc.

Selon LAMY (1996 : 27), « les principaux risques de ces saisies automatisées sont la contrepartie d'un automatisme qui ne sait réagir qu'aux cas prévus ». Autrement dit :

toutes les opérations qui n'ont pas été prévues par le système sont :

- soit non comptabilisées si elles contournent le système,
- soit irréalisables si elles ne peuvent contourner le système.

Les défaillances ou dysfonctionnement du système automatisé ont des conséquences économiques souvent très graves et se présentent sous la forme :

- d'une rupture totale du service fourni à la clientèle qui se détourne automatiquement vers la concurrence car elle ne saurait faire attendre ses besoins.
- d'une fourniture de service non conforme aux besoins exprimés et la production d'informations financières et de gestions erronées.

24- Les risques liés aux traitements en temps réel

Le traitement en temps réel est caractérisé par la mise à jour immédiate des fichiers. Les risques liés aux traitements en temps réel concernent alors , (LAMY 1996 : 29):

- la non détection des doublons (qui se fait plutôt en amont de tout traitement en temps différé)
- la difficulté de reconstitution d'une situation antérieure à un instant donné, du fait de l'alimentation permanente et continue du système;
- etc.

25- Les risques liés aux traitements en temps différé

Le traitement en temps différé se caractérise généralement par :

- la mise en traitement par des pupitreurs non spécialisés dans les domaines d'utilisation
- la mise en différé de l'utilisation des résultats
- l'existence d'en-cours de traitement
- etc.

Selon LAMY (1996 : 29), " les risques du traitement en temps différé sont liés aux caractéristiques même du traitement. Nous avons entre autres :

- la non analyse, l'analyse partielle ou l'analyse erronée des en-cours de traitement (en somme la difficulté d'analyse des en-cours)
- du fait des connaissances limitées des pupitreurs dans les domaines d'utilisation des applications, le risque des traitements erronés est élevé"

26- Les risques liés aux systèmes intégrés

Un système intégré est un système dans lequel chaque opération est saisie une et une seule fois. Cette information unique est ensuite acheminée vers différentes applications informatiques afin d'être traitée. Il permet à plusieurs applications de partager les

mêmes fichiers de bases de données sans contraintes particulières (FAIVRE & LOREAU , 1993).

Le partage des mêmes fichiers de base de données, fait courir au moins des risques de manipulation sur ces données.

27- Les risques d'opérations rétroactives

Une opération peut être dite rétroactive, lorsqu'elle est effectuée pour le compte d'une période antérieure. Selon LAMY (1996 : 34) , « les techniques informatiques, quelles que soient les protections prévues, permettent toujours de modifier une situation antérieure ». Il est possible entre autres de :

- détruire un enregistrement
- modifier un enregistrement
- procéder à une insertion antidatée

Cette opération peut se faire :

- soit en repartant d'une sauvegarde antérieure ;
- soit par intervention directe sur les fichiers à l'aide de logiciel utilitaires spécialisés.

Il y a aussi des risques importants de :

- non-respect du principe d'intangibilité
- manipulation des chiffres à des fins de détournement
- trafics illicites sur des données arrêtées
- etc....

l'évaluation des risques étant faite, il faut mettre des dispositifs de contrôle en place pour les empêcher de se réaliser.

SECTION 4 : LES DISPOSITIFS DE CONTROLE EN M I

Dans un système informatisé comme dans un système manuel, les contrôles visent à assurer que seules les opérations valides (réelles, appartenant à l'entreprise, autorisées, etc..) sont enregistrées et traitées de façon complète et exacte. Pour y arriver, des dispositions de contrôle doivent être prises :

- sur les données à entrer dans le système ;
- sur les procédures programmées (traitements effectués par le système) ;
- sur les résultats produits par le système.

(COOPERS & LYBRAND, 2000) situent ces contrôles à deux niveaux

- les contrôles globaux[1] (appréciation de la fonction informatique dans son ensemble),
- l'appréciation des applications de l'entreprise ».

Nous proposons donc d'aborder les dispositifs de contrôle de ce point de vu.

PARAGRAPHE 1 : LES CONTROLES GENERAUX DE LA FONCTION INFORMATIQUE

Ils peuvent porter sur :

- l'organisation et la gestion de la fonction informatique,
- l'intégrité des systèmes,

11- Contrôles portant sur l'organisation et la gestion de la fonction informatique

Par contrôle de l'organisation et de la gestion des opérations, nous entendons ; les dispositions liées :

- à la politique informatique ;

1 : la terminologie varie dans la littérature

- aux procédures d'acquisition des applications informatiques ;
- aux règles d'application ;
- à la documentation ;
- etc..

que nous allons préciser maintenant.

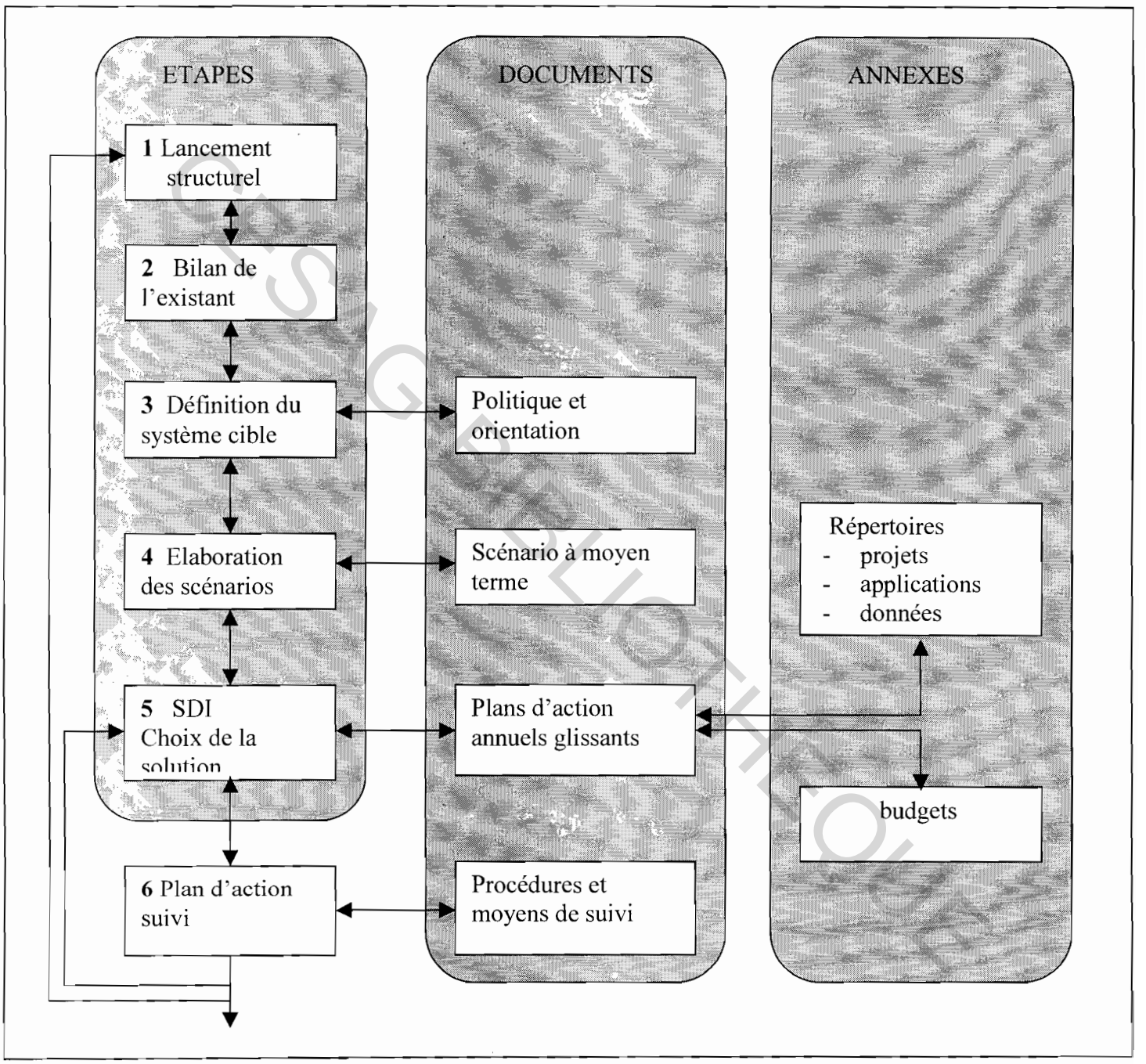
111- Contrôle portant sur la politique informatique

Parlant de la politique informatique, THORIN (2000 : 55) dit : « elle doit être définie par la direction, peut être avec l'aide d'un conseil spécialisé en organisation…Elle doit être adaptée à la finalité de l'entreprise, donc évolutive et homogène avec les objectifs de celle-ci, et documentée, donc concrétisée par écrit ».

L'existence d'un schéma directeur informatique (ou plan directeur) doit matérialiser cette politique.

En plus, l'élaboration de ce schéma directeur informatique doit respecter une procédure normalisée.
Nous présentons en conséquence, la méthode RACINES d'élaboration du schéma directeur informatique.

FIGURE N°2 : **Méthode RACINES**
Les étapes du schéma directeur informatique



Source (LAMY 1996 : 98)

1)- formation des groupes de travail et du comité de pilotage

2)- inventaire des fonctions qui donnent satisfaction, celles à améliorer, et celles à revoir ou à améliorer ;

3)- le système cible est le système idéal selon le vœu du comité de pilotage et des groupes de travail ;

4)- il y a généralement trois types scénarios chiffrés :

- un scénario de rupture qui fait table rase de l'existant;
- un scénario tendanciel qui réalise le système cible par transformation successives du système existant;
- des scénarios intermédiaires qui remplacent certaines parties de l'existant et transforment d'autres

5)- le choix d'un scénario est fait par la direction générale sur proposition du comité de pilotage

6)- un plan d'actions de suivi est mis en œuvre.

112-contrôle des procédures d'acquisition des applications

Selon la CNCC (1995 : 27), « la mise en service d'une application doit au minimum être précédée :

- d'un cahier des charges précis ;
- d'une étude de faisabilité ;
- d'une phase de test (jeux d'essais) ;
- d'une formation des utilisateurs ;
- etc.. »

Une telle procédure est un moyen pour garantir :

- une bonne coordination, un point d'accord entre utilisateurs et informaticiens,
- mais aussi la fiabilité des applications avant leur mise en service.

113- les règles d'application

JENKINS &PINKNEY (1984 : 5) définissent les règles d'application des contrôles de base comme « les dispositions du système qui sont destinées à assurer la permanence et la bonne application des contrôles de base et la protection des actifs ».

Elles sont semblables pour les systèmes informatisés et pour les systèmes manuels. Ce sont , JENKINS & ET PINKNEY , (1984 : 238) :

- les contrôles de supervision des contrôles de base ;
- la séparation des tâches ;
- la continuité du chemin de révision ;

a)- contrôles hiérarchiques

Ces contrôles hiérarchiques peuvent être matérialisés par des activités manuelles ou des procédures programmées (visa ou signature automatisé) .

Il faut donc s'assurer qu'un supérieur hiérarchique compétent vérifie de façon permanente les traitements effectués. En plus les conditions exceptionnelles d'exploitation doivent faire l'objet d'autorisations préalables.

b)- séparation des fonctions

« L'existence et l'utilisation de l'ordinateur ne dispensent pas de maintenir la division normale des tâches entre services traditionnels, en particulier entre les fonctions opérationnelles de conservation des biens, d'enregistrement des opérations, de contrôle et de décision », (OBERT, 1995 : 123).

Ce dispositif de contrôle est d'autant important pour faire des rapprochements que pour prévenir d'éventuelles erreurs, négligences, fraudes et leur dissimulation.

Dans un système informatisé, il suppose que les fonctions :

- de développement ;
- de contrôle ;
- d'exploitation ;

soient séparées (CNCC , 1995).

Par exemple, selon OBERT (1995 : 124) :

- les analystes et les programmeurs ne doivent pas avoir accès aux fichiers et programmes,
- le personnel de préparation des données et le personnel de contrôle du service informatique doivent seuls avoir accès aux données de base à traiter,
- les tests des programmes doivent, en principe, être effectués par les opérateurs et non par les programmeurs. Ils doivent donc disposer d'une instruction écrite décrivant les procédures de test.
- les analystes et programmeurs seuls doivent établir ou modifier les programmes.
- les créations et les modifications de programmes doivent être régulièrement autorisées par les responsables (utilisateur et informatique).
- les opérateurs ne doivent pas modifier les données qui leur sont fournies pour traitement.
- le ou les responsable(s) de la bibliothèque des programmes et des fichiers doivent seuls avoir accès.
- etc..

La séparation des fonctions suppose aussi que les informaticiens n'aient pas accès aux fichiers utilisateurs et réciproquement, que les utilisateurs n'aient pas accès aux programmes sources et objets.

c)- continuité du chemin de révision

« La continuité du chemin de révision d'un système informatisé correspond à la nécessité de faire le lien entre les données entrées dans ce système et les informations restituées », (DERRIEN, 1992 : 32).

Elle permet entre autres de :

- reconstituer les opérations dans un ordre chronologique,
- s'assurer de l'effectivité des contrôles intermédiaires (manuels ou électroniques),
- etc..

114- la documentation

Selon la CNCC (1995 : 33), « elle doit clairement exposer :

- le contenu des applications ;
- le contenu des programmes ;
- les instructions pour le personnel informatique ;
- les instructions utilisateurs ».

Elle est essentielle pour la pérennité du système, notamment en l'absence des personnes ayant intervenu sur celui ci. Sa mise à jour devient en conséquence impérative.

12- Contrôles de l'intégrité des systèmes

« Par contrôle d'intégrité, on désigne les contrôles exercés principalement dans la fonction informatique portant entre autres sur la création, la sécurité, l'utilisation des programmes informatiques » (JENKIN & . PINKNEY, 1984 : 65). Ce type de contrôle permet d'assurer un fonctionnement continu, régulier et correct des procédures programmées. Il concerne entre autres :

- la mise en place des systèmes (conception et modification),

- l'exploitation des systèmes,
- la sécurité, la sauvegarde et la reprise des travaux.

121- Contrôle de mise en place des systèmes

- **Mise en place des nouveaux systèmes**

Un nouveau système est toujours source de beaucoup de faiblesses par manque de maîtrise. Généralement, l'auditeur ne peut se fier à sa mise en place. Il préférera attendre qu'il soit opérationnel avant de l'évaluer. Toute fois, lorsqu'il décide de l'évaluer, il s'intéresse à ,:

- son analyse fonctionnelle pour s'assurer que les utilisateurs comprennent et acceptent les procédures programmées, mais aussi que les informaticiens peuvent concevoir des contrôles efficaces.
- son analyse organique (si possible) pour s'assurer de la logique et de la cohérence des programmes, s'ils sont conçus par l'entreprise (JENKINS & PINKNEY , 1984)

- **Modification des programmes**

Des normes existent pour une évaluation fiable de celles ci, notamment sur la validité des programmes.

Elle doit respecter une procédure rigoureuse comportant les éléments suivants [1] :

- une demande formalisée exprimée par les utilisateurs et approuvée à un niveau hiérarchique autorisé,
- une analyse par le service informatique (analyste et programmeurs) pour sa réalisation,

- une modification de la documentation relative.
- des tests de validation

1 : ces tests sont aussi valables pour la mise en place des nouveaux systèmes

122- Contrôle de l'exploitation du système

« Ce sont des contrôles mis en place pour s'assurer que les procédures programmées fonctionnent correctement pendant le traitement des données comptable », (JENKINS & PINKNEY , 1984 :216). Ces contrôles s'inscrivent dans un processus qu'on peut énumérer en deux étapes :

- préparation et exécution des travaux,
- reprise après un incident de traitement.

- **Contrôle de préparation et d'exécution de travaux informatiques**

Il porte entre autres sur :

- les instructions d'exploitation
- des programmes pour les pupitreurs
- des traitements particuliers sur les détails de fichiers à utiliser
- de standards qui s'appliquent à tous traitements informatiques.
- les paramètres qui adaptent l'application à des utilisations spécifiques (création de factures, bulletin de solde, etc).

- **Contrôle des procédures de reprise**

Selon (JENKINS & PINKNEY , 1984 : 223), « ces contrôles sont nécessaires pour qu'en cas de panne des procédures, la reprise concernant des programmes d'exploitation , les logiciels de base et les fichiers de données n'introduisent pas des erreurs dans le système ». Il faut donc s'assurer qu'un responsable accrédité examine et entérine de telles procédures avant leur mise en œuvre.

123- Contrôle des sécurités et sauvegardes des systèmes

Les problèmes de sécurité constituent l'une des plus grandes préoccupations de l'auditeur dans un milieu informatisé.

Pour l'auditeur, la sécurité est abordée sous deux aspects :

- la sécurité physique ;
- la sécurité logique

- **La sécurité physique;**

Elle vise le matériel et les consommables informatiques. Son objectif est d'assurer qu'un contrôle des accès physiques aux locaux d'exploitation est effectué, que des dispositions de relais et de substitution sont prises (alimentation électrique, réseau de substitution etc..). En général il s'agit de s'assurer que des protections sont prises contre les dommages physiques quelles que soient leurs origines.

- **La sécurité logique ;**

Elle est évaluée essentiellement par l'utilisation de moyens d'accès tels que les identifiants et mots de passe régulièrement modifiés. Elle l'est aussi par l'enregistrement et l'analyse des tentatives d'accès non autorisées.

Selon MAURY (2002 : 34), « sécuriser les systèmes nécessite d'analyser les techniques employées par les pirates, de connaître leur outillage et d'étudier leur profil ». Il recommande alors les systèmes de sécurité fondés sur des leurres (appelés aussi honeypots ou pots de miel), c'est à dire destinés à attirer et occuper les HACKERS.

PARAGRAPHE 2 LES CONTROLES D'APPLICATIONS INFORMATISEES

« Ils sont destinés à mettre en place des procédures de contrôle spécifiques sur les programmes, en vue d'apporter un degré raisonnable de certitude que toutes les opérations sont autorisées, enregistrées et traitées de façon exhaustive, correcte et dans les délais » (SARR 2000 : 60).

Selon SARR (2000 : 60) « ces contrôles visent à :

- minimiser les risques d'erreurs de malveillance, de fraudes et de diffusion

à des personnes non autorisées;

- maximiser la satisfaction des besoins utilisateurs, notamment, la conformité des fonctionnalités aux besoins opérationnels, la confidentialité des fichiers de données ».

21- Contrôle des entrées de documents sources

Ces contrôles sont d'une importance capitale. En effet, quelle que soit la qualité des traitements informatiques, si les données entrées dans le système ne sont pas exactes et conformes aux règles, il ne peut en sortir qu'un résultat erroné.

Selon OBERT (1995:134), "ces contrôles portent notamment sur :

- l'autorisation des opérations à entrer dans le système;
- la saisie correcte;
- l'enregistrement correct des données dans les fichiers adéquats;
- la validation des opérations entrées dans le système;
- le rejet des anomalies pour correction et recyclage".

Les entrées de données peuvent se faire par transactions, par interface (traduction et transmission de données entre deux systèmes) ou par lot.
Selon SARR (2000:51)

« Les entrées par transactions nécessitent une sécurité d'accès aux terminaux, une sécurité d'accès au système et une sécurité d'accès à l'application.
Celles par interface nécessitent des moyens automatiques qui vérifient le bon fonctionnement des interfaces (version correcte du fichier, détection d'erreur de transmission, etc..).
Et celles par lots nécessitent des moyens automatiques qui vérifient particulièrement que toutes les données qui devaient être introduites l'ont été effectivement (par comptage des enregistrements, totalisation par lot) et que la totalisation avant saisie est conforme au résultat de l'ordinateur après saisie ».

22- Contrôles des procédures programmées

Selon COOPERS & LYBRAND (2000 : 78), « la plupart des contrôles applicatifs s'appuient sur des procédures automatiques qui comprennent des contrôles sur le format, l'existence, la vraisemblance des données. … Si ces vérifications sont correctement conçues, elles contribuent à garantir le contrôle des données entrées dans le système ».

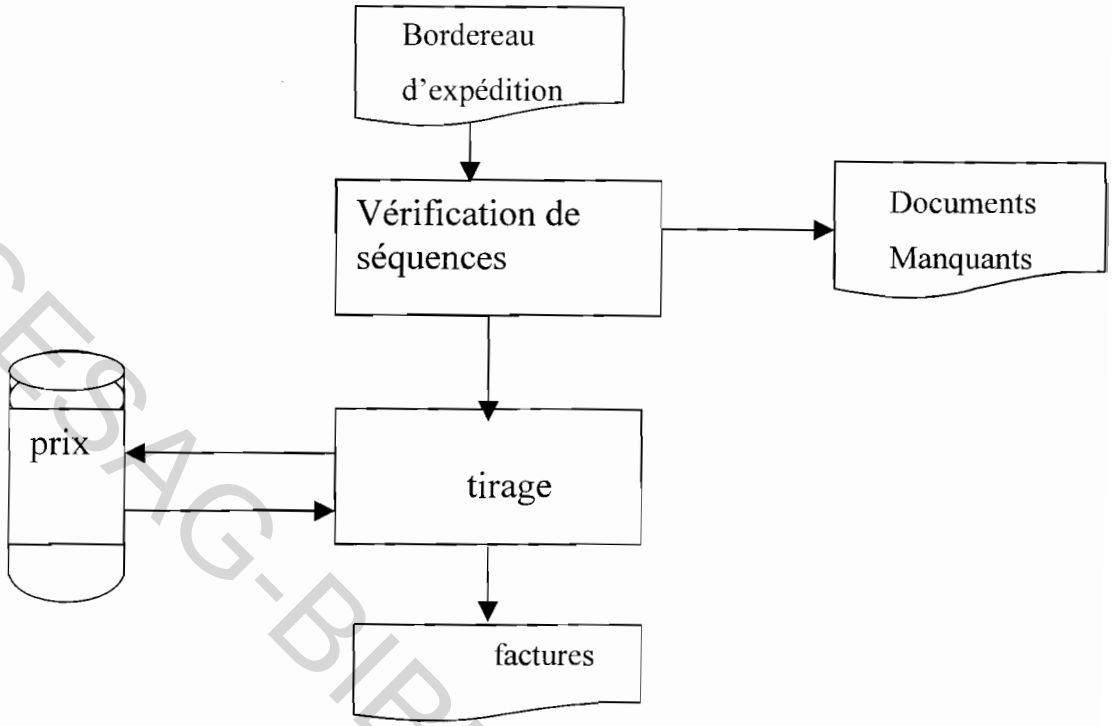
Pour JENKINS & PINKNEY (1984), ce type de contrôles porte sur deux aspects essentiellement:

- les fonctions de contrôle réalisées automatiquement;
- les activités opérationnelles programmées;

221- Procédures programmées des fonctions de contrôle

Il s'agit de s'assurer que le système vérifie que les traitements qui lui sont soumis sont complets exacts et valides. Ces contrôles doivent aussi assurer que les anomalies sont mises en évidence, par des tests d'épuration, des rapprochements des données traitées avec d'autres fichiers, l'édition des données manquantes, exceptionnelles ou incorrectes.

FIGURE N°3 : Schéma d'une procédure de contrôles programmés



Source : JENKINS & A PINKNEY

222- Procédures programmées des activités opérationnelles

Ces contrôles visent à donner une assurance raisonnable que les activités opérationnelles programmées s'exécutent conformément aux règles. C'est à dire qu'il n'y a pas de perte, de modifications, d'éditions ou de calculs irréguliers (sur des factures, B C, Bulletins de salaires, etc..).

23 Contrôles sur les sorties et les résultats

Ils portent notamment sur :

- l'exactitude et l'exhaustivité des sorties d'informations
- l'autorisation des diffusions

Selon SARR (2000 : 52), « il a pour but de donner l'assurance que les résultats transmis sont exacts, exhaustifs et adressés aux destinataires autorisés dans le respect des règles de sécurité ».

Conclusion

Dans un milieu informatisé, les principes fondateurs du CI ne changent pas ; notamment les objectifs et les éléments sont globalement identiques. Cependant les systèmes informatisés appellent à des risques spécifiques auxquels il faut apporter des contrôles adaptés. Ils se situent à deux niveaux essentiellement :

- Les contrôles globaux (ou généraux)
- Les contrôles des applications informatisées.

Par quels outils et quelle démarche peut-on effectuer l'évaluation de telles contrôles ?

CHAPITRE 2 MISE EN ŒUVRE DE L'EVALUATION DU C.I. DANS UN M.I

Mettre en œuvre l'évaluation du C I dans un M I nécessite des outils et une méthodologie propre à l'audit.

Les objectifs poursuivis par l'auditeur demeurent identiques à ceux qui guident ses missions dans d'autres environnements. Cependant, la complexité et l'accélération des processus informatiques imposent le recours à des diligences techniques spécifiques, (LAMY, 1997)

Ce chapitre se propose d'étudier les outils les plus courants et de décrire la méthodologie.

SECTION 1 : CARACTERISTIQUES DE L'AUDIT EN MILIEU INFORMATISE

Dans les paragraphes suivantes, nous prenons connaissance avec L'AMI et ses objectifs.

PARAGRAPHE 1 : LA DEFINITION DE L'AUDIT EN MILIEU INFORMATISE

Par audit en milieu informatisé, nous entendons, la réalisation des objectifs traditionnels d'audit financier et comptable dans un environnement utilisant l'ordinateur comme outil de travail.

PARAGRAPHE 2 : LES OBJECTIFS DE L'A.M.I

21- Les objectifs de fait d'entreprise

L'audit d'une entreprise ou d'une organisation vise des objectifs clairement

définis au préalable dont le niveau de réalisation forge l'opinion du professionnel. (KPMG 1996 ; LAMY 1997) résument ses objectifs en :

- la réalité des opérations
- l'appartenance à l'entreprise auditée
- l'exhaustivité des enregistrements
- l'unicité d'enregistrement de chaque opération
- la comptabilisation dans la bonne période
- la comptabilisation dans le bon compte
- la comptabilisation du bon montant

22- Les objectifs liés à la gestion par l'informatique

Même si le C A C n'a pas d'obligation légale concernant le système informatique de son client, il en a une obligation professionnelle comme le précise le commentaire 09 de la norme 2102 (in CNCC 1995 : 15), et qui décrit l'évaluation de son C I en deux parties.

- **Au niveau de la fonction informatique,** avec pour objectifs :
  - La fiabilité des informations produites,
  - La protection du patrimoine,
  - La sécurité et la continuité des travaux ;

- **Au niveau d'un système ou d'une application** avec pour objectifs :
  - Les contrôles sur la préparation et la saisie des données , aussi bien au niveau des services utilisateurs qu'au niveau informatique,
  - Les contrôles sur l'exploitation : prévention contre des erreurs et des fraudes pendant le traitement.
  - Les contrôles destinés à s'assurer de l'intégrité, de l'exactitude et de l'autorisation des opérations à enregistrer,
  - Le maintien du chemin de révision (ou système de référence)

- La qualité de la documentation,
- Les modifications intervenues d'un exercice à l'autre dans les programmes, notamment pour les méthodes d'enregistrement et d'évaluation.

SECTION 2 : LES OUTILS DE L'EVALUATION

De nombreux outils de l'évaluation du C.I. sont bien connus des auditeurs.
Avec l'entrée massive de l'informatique dans les entreprises, on peut imaginer sans risque de se tromper qu'ils ont pu évoluer pour s'adapter à chaque évolution de l'environnement . C'est pourquoi, nous nous proposons de les apprécier sous deux angles :

- Les outils traditionnels ; qui sont les outils indépendants de l'informatisation des structures de gestion ;
- Les outils informatiques, évidemment liés à l'usage de l'informatique dans les entreprises.

PARAGRAPHE 1 : LES OUTILS TRADITIONNELS DE L'EVALUATION DU C I

Ils sont nombreux, et nous ne saurions les traiter de façon exhaustive. Nous allons donc analyser ceux qui nous paraissent le plus couramment utilisés. (ROUFF 2001 ; RENARD 1998) les classes en 5 catégories :

- les outils de collecte de l'information
- les outils de description
- les outils de diagnostic
- les outils de validation
- les outils de formalisation

11- les outils de collecte de l'information

111- Le questionnaire de prise de connaissance (QPC)

Selon ROUFF (2001 ; 14), « en audit, lorsqu'on parle de questionnaire, il s'agit de questions que l'auditeur doit se poser et non celles qu'il doit poser. Les questionnaires ont pour but d'appréhender l'organisation, les faits et les processus ; de détecter les dysfonctionnements potentiels et d'en déterminer la cause ; de standardiser les méthodes ; de ne pas omettre les points importants à analyser ».

Le QPC permet de conduire les interviews et entretiens divers, notamment sur la prise de connaissance. Il porte souvent sur la connaissance du contexte socio-économique, du contexte organisationnel et du fonctionnement.
Le QPC est constitué de questions ouvertes, c'est-à-dire qui donnent lieu à des commentaires puisqu'il sert à la description des systèmes.

112- L'Interview :

« C'est un échange verbal, au cours duquel , un auditeur pose des questions à son interlocuteur, tout en s'interdisant le plus possible d'exprimer ses propres opinions » (ROUFF, 2001 : 14). Pour le réussir, J. RENARD, (1998 : 182) propose 5 règles

- respecter la voie hiérarchique ; en d'autres termes, informer le supérieur hiérarchique de son interlocuteur.
- rappeler clairement la mission et ses objectifs, pour des raisons de transparence et dissiper toute suspicion chez l'interviewé.
- évoquer avant tout, les difficultés, les points faibles, et les anomalies rencontrées.
- les conclusions doivent recueillir une adhésion réciproque des interlocuteurs avant toute communication avec son supérieur hiérarchique.
- se garder de toute question subjective et mettant en cause les personnes.

Pour réussir donc une interview constructive, il faut bien la préparer

113- L'observation physique

Utilisée à la fois pour la collecte de l'information et la validation,

« l'observation physique est un outil, à haut niveau de force probante qui est utilisé pour confirmer l'existence d'un actif, (stock, immobilisations corporelles, effets, espèces de caisse…) selon ATH (1991 : 206), mais aussi pour valider un dispositif (de sécurité physique par exemple). Il consiste à aller observer ce qui se passe sur le terrain.

La démarche peut être globalement la suivante.

- collecte des procédures ;
- évaluation des procédures
- observation physique (contrôle de l'application des procédures, tests de fiabilité etc..)

Selon ROUFF (2001 : 14), « la pratique de l'observation physique exige trois conditions :

- elle ne doit pas être clandestine
- elle ne doit pas être ponctuelle
- elle doit toujours être validée, sauf le cas où elle est elle même une validation ».

12- Les outils de description

121- Le Diagramme de circulation

« Il permet de représenter la circulation des documents entre les différentes fonctions et centres de responsabilités…de décrire une vision complète du cheminement des informations et de leurs supports » (RENARD, 1998 : 200).

Selon ATH (1991 : 188),

- chaque système (ensemble d'opérations homogènes, généralement représentées par une fonction) doit pour cela être subdivisé en opérations principales ;
- chaque opération principale sera décrite dans un tracé distinct pouvant comporter un ou plusieurs folios ;

- les services (ou personnes) intervenants dans les procédures sont matérialisés par des colonnes (tous les services intervenants étant matérialisés).
- la dernière colonne à droite pourra servir pour les éventuels commentaires (par exemple lorsque le symbole « contrôle » est utilisé, on peut préciser la nature du contrôle).
- la circulation des documents est matérialisée par des flèches
- etc.

Il est souvent recommandé pour ; ATH (1991 : 142)

- son langage commun à tous ses utilisateurs par entreprise
- une meilleure visualisation des opérations
- sa capacité de synthèse et de précision

122- La Narration

La technique de narration consiste à transcrire littéralement et de façon synthétique la procédure d'exécution des opérations. Elle utilise le style personnel d'écriture de son auteur et présente les inconvénients suivants selon la CNCC (1992 : 89) :

- de n'être compréhensible que par son auteur (abréviations, etc..)
- de rendre difficile la vision d'ensemble du système et la chronologie des opérations ;
- de ne permettre que difficilement de s'assurer que le dispositif est complet .

En définitive elle présente le risque d'interprétations divergentes par un autre auditeur à charge du même dossier au cours de contrôles ultérieurs.
Elle est plus particulièrement adaptée aux systèmes simples et à certains aspects du système qu'il est difficile de schématiser.

123- Le chemin d'audit (ou piste d'audit)

Selon ROUFF (2001 ; 15), « il permet de retracer un document, une action en partant du point d'arrivée et en remontant à la source ».

Ses caractéristiques sont : .RENARD, (1998 : 206)

- il ne concerne qu'une seule opération à la fois
- il part du document ou résultat final pour remonter à la source
- il permet de contrôler pour les stades intermédiaires, leurs justificatifs et justifications.
- il rend possible à cette occasion le test de toutes les interfaces et donc la vérification des points spécifiques de raccordement dans le cheminement des opérations.

Par exemple, il permet de vérifier la logique d'un traitement informatique lorsque les données traversent des chaînes informatisées ou de retracer toutes les opérations relatives au paiement d'un salaire.

124- L'organigramme fonctionnel

Contrairement à l'organigramme hiérarchique, celui-ci est élaboré par l'auditeur sur la base des informations recueillies par la mise en œuvre des autres outils (observations interviews, narrations etc.…).

Selon RENARD, (1998 : 195), « il se caractérise par le fait que, dans les cases, sont inscrits des verbes désignant des fonctions et non des noms de personnes ». En plus, dans cet organigramme ;

- une même personne peut avoir plusieurs fonctions
- une même fonction peut être partagée par plusieurs personnes
- une fonction peut ne pas être attribuée.
- une personne peut se trouver sans fonction.

Son intérêt est qu'il permet d'enrichir ses connaissances sur l'organigramme hiérarchique analysé par poste de responsabilité. Et un croisement des deux organigrammes est une source de force probante.

13- Les Outils de diagnostic

131- Le questionnaire de contrôle Interne (QCI)

Il peut être aussi outil de description. Selon ROUFF (2001 : 15), « les (QCI), ont pour objectifs de guider l'auditeur dans son travail d'analyse afin de lui permettre, en toute objectivité, de déceler les dysfonctionnements, et d'en discerner les causes réelles ».
Ici, il s'agit de concevoir un référentiel , en vue d'évaluer le dispositif de CI de l'entreprise. Cependant, pour être efficace le Q C I doit être adapté aux caractéristiques spécifiques de chaque entreprise. C'est ainsi par exemple qu'un comité informatique sera exigé comme dispositif de CI dans une banque multinationale où l'informatique est le moyen des transactions par excellence et passé sous silence dans une PME locale de vente de peau à Tambacounda qui n'a que quelques ordinateurs de direction.

Selon la CNCC (1992 : 96) le QCI doit respecter les principes suivants :

- être conçu par fonction significative (achat, vente, informatique etc.…)
- être classé par objectifs pour chaque fonction (exhaustivité des traitements, fiabilité du système informatique, sécurité etc.…)
- être rédigé de façon à ce qu'une réponse **'OUI'** corresponde à une bonne conception du système et une réponse ' **NON'** à un risque.

Exemple en annexe N°1

132- Le tableau des forces et faiblesses (tableau d'identification des contrôles)

« Il donne une vue d'ensemble des forces et faiblesses apparentes ou réelles par rapport aux procédures et règles existantes et aux résultats attendus », (ROUFF 2001 ; 15) .
Cette technique garantie une identification spécifique des risques pour chaque système de l'entreprise. En effet son élaboration se fait en suivant la description du système.

Cependant, selon la CNCC ; (1992 : 95)

- elle exige une grande expérience pour ne rien omettre ;
- elle est consommatrice de temps ;
- elle est difficile à superviser.

14 - Les outils de validation

141- Le sondage (échantillonnage statistique)

« C'est une technique qui permet, à partir d'un échantillon prélevé aléatoirement dans une population de référence, d'extrapoler à la population les observations effectuées sur l'échantillon, avec une certitude spécifiée et une précision désirée », (IFACI, 1995 : 215).

La norme 2103, (in ATH, 1991 : 224) donne le droit au commissaire au compte d'utiliser cet outil en disant : « sauf cas exceptionnels, le CAC ne peut examiner l'ensemble des documents justificatifs et des écritures comptables. Il sélectionne l'échantillon sur lequel il va appliquer ses procédures de vérification, selon la technique de sondage la mieux adaptée aux circonstances (prélèvements au hasard basés sur le jugement professionnel ou échantillonnage statistique) ».

Il y a plusieurs types de sondages applicables selon les objectifs recherchés. Pour la validation du fonctionnement du CI, ATH, (1991 : 240) préconise le sondage sur les attributs qui consiste à vérifier l'existence (ou l'absence) d'anomalies de fonctionnement des systèmes. Lors de la prise de décision de sa réalisation, l'auditeur doit s'interroger sur :

- le choix d'un risque de surestimation raisonnable de la fiabilité de ses résultats, bien sur en fonction de sa confiance préalable dans l'environnement de l'entreprise ;
- l'utilité de procéder à un tel sondage, au delà d'un certain taux (ou nombre) d'anomalies acceptables ;

142- L'examen de l'évidence des contrôles :

Il consiste à vérifier la matérialité des contrôles effectués au cours de la gestion des opérations. Exemple, le contrôle de l'existence des signatures et visas électroniques ou manuels apposés par les personnes habilitées à les réaliser (CNCC 1992).

143- La répétition des contrôles :

Elle consiste à refaire par l'auditeur, le travail de contrôle effectué par le personnel de l'entreprise. Il se fait par sondage. Exemple : l'auditeur refait des calculs ou des rapprochements de fichiers de données.

144- le test de conformité

Le test de conformité est le moyen utilisé en vue de rapprocher la description du processus de C I de la réalité pratiquée dans l'entreprise, c'est à dire de confirmer que la description faite est correcte, sinon la corriger.

« Il consiste à sélectionner une transaction appartenant au circuit décrit et à suivre son exécution du début à la fin, afin de vérifier qu'il correspond à la description faite » (CNCC, 1992 : 48).

145- Le test de permanence

Il consiste à répéter le test de conformité pour un niveau de sondage acceptable. Il permet de valider les points forts théoriques du C. I.
En cas de non-conformité, il y a deux possibilités :

- ou bien la description est mal faite (aucun test de transactions du même circuit n'est conforme au même stade du traitement) et il faut la corriger,
- ou bien la pratique décrite n'est pas permanente, et il s'agit de déviations ponctuelles à fustiger.

15- Les outils de formalisation des travaux

151- Le papier de travail

Selon ROUFF « il est le support obligatoire de tout constat, de toute observation etc. ».

Il a une présentation spécifique pour chaque cabinet, mais présente toujours des référencements obligatoires préconisés par (la CNCC, 1988) :

- dénomination de l'entité
- type de mission
- date d'intervention
- rubrique (application) analysée
- signature des intervenants (auditeur, chef de mission etc.)
- référencement de pièces jointes
- etc…

152- La FRAP

La FRAP se présente comme suit (IFACI 1995 : 97):

TABLEAU N°1 : Représentation de FRAP

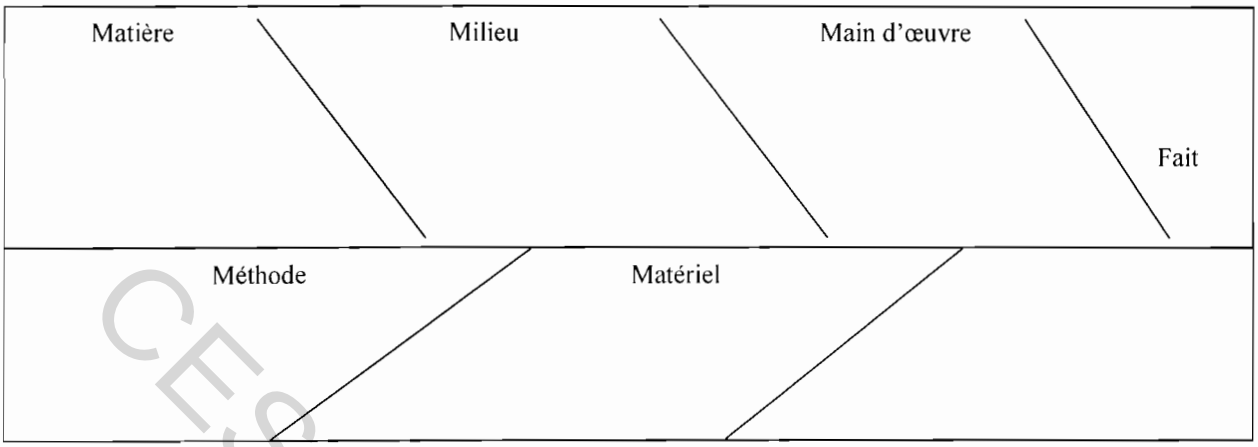
A Modèle de FRAP Feuille de révélation et d'analyse des problèmes Référence papier de travail : FRAP N°
Problème :
Constat : (finding)
Causes :
Conséquences :
Recommandations :
Etabli par : Approuvé par :

Source : IFACI

Constat : pour énoncer de façon synthétique l'erreur, l'anomalie, le dysfonctionnement constaté

Causes : L'IFACI recommande le diagramme d'Ishikawa appelé aussi diagramme d'arrête de poisson ou encore méthode des 5 M, pour l'analyse causale.

FIGURE N°4 : Le diagramme d'Ishakawa



Conséquences :

On évalue sous cette rubrique l'impact du constat (finding). Ces conséquences peuvent être d'ordre

- financières
- juridique
- économiques
- mais aussi techniques quand l'auditeur a les moyens objectifs de les apprécier.

Recommandation :

« La recommandation est impérativement l'exacte contre partie de la cause », . RENARD (1998-171).

Problème :

Son énoncé tardif permet de mieux le cerner et de l'exprimer.

PARAGRAPHE 2 : LES OUTILS INFORMATIQUES

Les besoins des auditeurs en matière d'outils informatiques sont de plus en plus marqués. Cela est dû, non seulement à l'informatisation des entreprises, mais aussi à l'efficacité, la rapidité et la pertinence qu'ils apportent aux travaux.

Une enquête de l'IFACI (2001 : 17) a révélé « qu'environ la moitié des répondants estime « très important » dans les trois (3) années à venir, les outils de communication, les outils de gestion des référentiels d'audit et d'analyse des risques ainsi que les outils d'extraction, d'analyse et de tests, … mais aussi que 79 % utilise déjà les utilitaires (cryptage, anti-virus…) »

Ces résultats démontrent clairement, l'importance significative des besoins des auditeurs en outils informatiques. Les fonctionnalités recherchées sont nombreuses, et répertoriées par VIDAUX (2001 : 19) dont nous empruntons celles-ci :

- le suivi des recommandations et des plans d'action ;
- l'extraction des données utiles à la mission
- la possibilité d'analyser toute application informatique
- la capitalisation des expériences acquises
- le fait de ne pas être « stoppé » par des problèmes de volume d'information
- la modélisation des procédures, des modes opératoires et des diagrammes
- la conservation des informations avec accès rapide et simple …
- etc…

Nous allons nous intéresser de façon spécifique à quelques outils. Il faut préciser que ces outils informatiques ne sont pas utilisés de façon spécifique à chaque étape de la méthodologie d'évaluation du CI, mais sont utilisés souvent de façon transversale.

21- Outils d'analyse des risques

Selon VIDAUX (2001 : 20), pour analyser les risques il convient de procéder comme suit :

- représenter l'ensemble des flux de l'entreprise modélisés ou non
- ensuite, comparer la représentation obtenue au périmètre organisationnel pour en déduire des fiches d'évaluation des risques par entité opérationnelle.
- dans la mesure où on ne peut procéder ainsi, en raison de la complexité ou de la charge de travail , on peut constituer un catalogue des bonnes pratiques. La représentation obtenue est à comparer au périmètre organisationnel pour en déduire des fiches d'évaluation des risques par entité opérationnelle.

Il propose des logiciels comme SPHYNX ou HORUS qui permettent une analyse complète et une cartographie des risques.

Ces logiciels peuvent notamment :

- recenser les principaux processus
- décrire les entités et leurs activités fonctionnelles ou opérationnelles
- évaluer les risques potentiels par processus et (ou) entité.
- décrire les moyens mis en œuvre pour couvrir les risques
- récupérer des informations au travers d'interfaces avec des outils d'auto évaluation des audités.
- prendre en compte l'impact des recommandations effectuées lors des missions.
- effectuer des consolidations par type d'agrégat (type ou niveau de risques, métiers ou entités, processus),
- mettre en évidence les risques à couvrir et identifier les missions à planifier.

22- Le jeu d'essai

La CNCC (1992 : 100) le définit comme « une technique qui consiste à injecter dans la chaîne de traitement, des données préparées par le CAC, destinées à tester l'existence et le fonctionnement des contrôles programmés ».

En pratique, il s'agit de comparer les résultats d'un tel traitement aux résultats attendus.

OBERT précise, (1991 : 138) que : « ce type de méthode de contrôle est plus spécialement utilisé lorsque :

- une partie importante du CI est incorporée dans les programmes de l'entreprise ;
- il y a des lacunes dans les systèmes de référence ; (perte du chemin de révision) ;
- le volume des enregistrements est important ».

Pour donner un résultat fortement probant, le jeu d'essai d'audit doit s'exécuter dans un environnement identique à l'environnement réel de l'entreprise. En d'autres termes :

- sur les programmes réellement utilisés par l'entreprise ;
- s'il est exécuté sur des copies de programmes, le CAC (l'auditeur) doit s'assurer par tout moyen que ces copies correspondent bien aux programmes qui sont en exploitation » CNCC (1992 : 100).

23- Les progiciels d'interrogation et/ ou d'extraction de données

Ce sont des outils spécialisés pour explorer les fichiers ou interroger une base de donnée.

Selon LAMY (1996 : 68), «il n'est pas possible d'interroger une base de données avec d'autres outils que les programmes d'interrogation associés ».

Ils permettent selon LAMY (1997 : 50)

- de vérifier l'intégrité et l'exhaustivité des données à posteriori
- de vérifier les traitements informatiques et la bonne application des contrôles identifiés par l'auditeur.
- de réaliser des tests sur de gros volumes de données
- des recherches d'exception
- etc…

Par exemple, un tel progiciel peut extraire.

- des soldes clients pour lesquels aucun plafond de crédit n'est défini.
- des soldes clients supérieurs à un certain montant ;
- des soldes fournisseurs débiteurs
- etc..

« Un autre avantage et non des moindres, est qu'il n'est point besoin d'être informaticien pour les utiliser comme les logiciels ACL ; FDEA ; SAS » selon MORRISSEY.(2001)

24- Les logiciels utilitaires

Des logiciels utilitaires, fournis par le constructeur notamment dans les systèmes d'exploitation, tout comme ceux installés pour des besoins d'ordre général peuvent être aussi utilisés par les auditeurs.
Selon OBERT (1991 : 137), ils permettent entre autres de :

- faire de l'extraction de données ou de fichiers, des tris ou de l'impression.
- faire des tableaux ou des traitements de texte.
- servir de dispositif de sécurité (cryptage, anti-virus…)
- etc …

25- Les outils micro informatiques

Les outils micro informatiques sont utiles à plusieurs niveaux dans le déroulement de la mission, par exemple pour la préparation des rapports du CI.
Selon LAMY (1996 : 70), « dans la mesure où ils peuvent être connectés sur des ordinateurs centraux de l'entreprise, il est possible de rapatrier sur les disques des micro ordinateurs, les fichiers désirés pour y être traités avec les outils de celui-ci (qui peuvent être en particulier des outils spécifiques au cabinet) ».

26- Les outils d'aide à la mission

Les logiciels utilitaires servent pour la plupart à la gestion des missions d'audit, notamment pour l'élaboration de programme de travail, la construction de diagramme ou de tableaux. Mais il existe aussi des logiciels spécifiques d'aide à la mission. Selon MORRISSEY (2001 : 25) on peut citer entre autres :

261- Des logiciels de planification et de suivi des missions.

Ils permettent de mener l'équipe d'audit selon les directives reçues et de planifier la mission dans le temps ; (par exemple PSN HORUS, LOTUS, NOTES).

262- Des logiciels qui traitent les référentiels d'audit.

Ces référentiels constituent la base de réflexion des auditeurs pour leur travail y compris les points de contrôles.
Certains sont obligatoires (plan comptable) ou sont un recueil de normes d'audit (ISO) ou encore de bonnes pratiques acceptées dans la profession. Les logiciels qui les traitent ont pour objectifs de présenter les différents domaines, leurs risques et de proposer des points de contrôle. Ils sont souvent capables d'éditer un tableau des forces et faiblesses pour orienter les efforts de la mission. En outre, les résultats de ces investigations sont sauvegardés de façon à pouvoir les comparer à d'autres missions.

263- Les logiciels de présentation

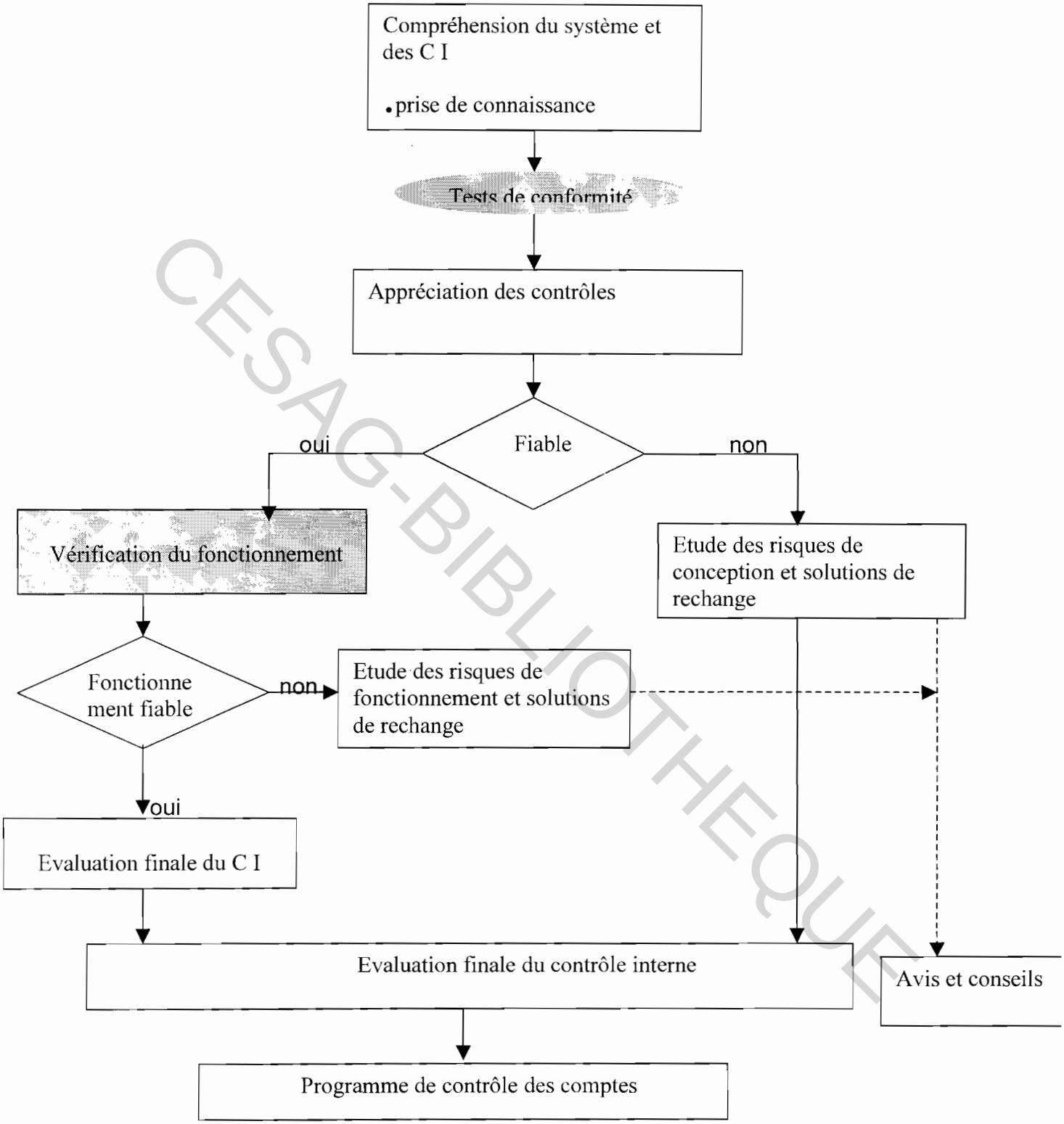
L'école de Chicago (in Audit ; 2001 : 26) a longuement démontré qu'un dessin vaut mieux qu'un long discours. D'où l'importance d'une présentation synthétique, schématique, graphique, pour un rapport d'audit, notamment en conseil d'administration. Et POWER POINT excelle dans ce domaine, en concurrence avec FREELAND selon (MORRISEY , 2001).

SECTION 3 : LA METHODOLOGIE DE L'EVALUATION DU C. I

Selon le commentaire 09 de la norme 2102 (in CNCC 1995 : 15) « l'évaluation du contrôle interne d'un système de traitement informatisé de l'information financière est effectuée selon la même démarche que celle décrite ci dessus[1] ».

1 : la démarche est celle décrite ci dessous

FIGURE N°5 : Schéma de la méthodologie d'évaluation du C I



Source : (CNCC : 1995)

L'existence d'une fonction informatique ne change pas la démarche générale, mais influe sur toutes ses étapes. L'auditeur doit ainsi :

- comprendre les caractéristiques générales de l'informatique de l'entreprise lors de la prise de connaissance, afin d'apprécier son incidence sur la mission ;
- apprécier le C I spécifique à l'organisation de la fonction informatique et de certaines applications critiques ;
- adapter la nature et l'étendue du contrôle à réaliser lors du contrôle des comptes , (CNCC : 1995)

Pour une meilleure compréhension de la démarche, nous allons en préciser les différents points.

PARAGRAPHE 1 : COMPREHENSION DU SYSTEME ET DES C I

La compréhension du système existant doit requérir la plus grande rigueur et couvrir tout élément permettant de se familiariser avec l'environnement informatique de l'entreprise. Nous pouvons énumérer quelques-uns des points importants à prendre en compte sur :

- les dispositions générales informatiques ;
- les applications utilisées ;
- les conditions de mise en place de tests auditeurs.

11- Sur le dispositions générales informatiques ,

LAMY (1996 : 38) propose de connaître :

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

Il complète (1997 : 15) par :

- l'organisation de la fonction informatique ;
- les matériels opérationnels ;
- l'organisation retenue pour les fichiers (base de données etc..) ;
- les logiciels utilisés ;
- les applications existantes.

l'auditeur doit aussi demander ou faire établir les documents suivants pour analyse :

- le schéma général du système informatique ;
- le schéma générale des applications informatiques en service ;
- les listes de documents et informations saisies dans le système ;
- les listes de transactions proposées aux utilisateurs ;
- la liste des principaux fichiers utilisés ;
- les manuels opératoires (informatiques et utilisateurs) ;

12- Sur les principales applications utilisées,

LAMY recommande (1996 : 40) que l'auditeur se fasse décrire de façon macroscopique ,

Pour les aspects fonctionnels :

- les données en entrée ;
- l'acheminement de ces données ;
- les traitements essentiels
- les principaux fichiers utilisés en amont ;
- les incidences des traitements sur les fichiers en aval ;
- les états et les résultats produits les plus significatifs ;
- les principaux contrôles prévus ;
- le suivi de la correction des anomalies;
- les déversements en comptabilité ;
- etc..

sur le plan technique, l'auditeur devra s'intéresser :

- aux normes et techniques de développement ;
- aux tests de mise en œuvre par les utilisateurs ;
- aux conditions de réalisation de la maintenance ;
- aux difficultés rencontrées au plan informatique
- etc..

13- sur les conditions de mise en place de tests auditeurs.

LAMY (1996 : 40) propose de connaître :

- la nature des bases de données ou la structure des fichiers ;
- l'existence d'outils d'interrogations propre aux systèmes vérifiés ;
- les possibilités de connecter un micro-ordinateur ;
- etc..

Cette prise de connaissance pourra permettre à l'auditeur de cerner les zones à risque.

L'on peut utiliser pour cela les moyens de description.

PARAGRAPHE 2 : LES TESTS DE CONFORMITE (vérification de l'existence)

La vérification de l'existence des systèmes répond à des inquiétudes précises. La première année d'intervention, dans la formalisation de la compréhension des systèmes, l'auditeur peut avoir :
(CNCC 1992 : 48)

- omis des informations ;
- mal compris ou déformé certaines informations ;
- mal transcrit des informations.

Au cours des missions suivantes, l'auditeur doit s'assurer que les

procédures n'ont pas été modifiées et que sa description reste toujours valable.

En ce qui concerne la fonction informatique, l'évolution technologique et des systèmes est que cette vérification devient indispensable.

La technique utilisée est le test de conformité. Il consiste à rapprocher la description faite, du système existant par la répétition d'une transaction appartenant au processus décrit.

PARAGRAPHE 3 : APPRECIATION DES CONTROLES

Il s'agit ici de s'assurer que le processus satisfait aux objectifs de C I selon un référentiel conçu au préalable.

Un questionnaire de contrôle interne (Q C I) est le moyen le plus souvent utilisé pour cette évaluation en précisant pour chaque section les objectifs de C I . Pour être efficace le questionnaire doit être adapté au contexte spécifique de chaque entité.

« Le Q C I est en principe rempli par celui qui a décrit le système, mais doit être revu par le responsable de la mission », (A. T. H. 1991 146).

Parfois plusieurs réponses semblent nécessaires à une même question :

- ou bien il faut choisir le point de contrôle le plus utile pour la mission,
- ou bien il faut référer chaque situation (transaction, site, niveau, etc..) dans la question.

Cette évaluation porte autant sur les questions de sécurité, les conditions d'exploitation, les procédures de sauvegarde, la satisfaction des besoins utilisateurs, la contrôlabilité des applications, etc..

La rigueur de cette évaluation veut que l'auditeur expose les faiblesses constatées

aux responsables concernés et les interroge sur l'existence éventuelle de contrôles alternatifs compensatoires.

Les outils utilisés sont ceux de diagnostic.

PARAGRAPHE 4 : VERIFICATION DU FONCTIONNEMENT DES SYSTEMES (tests de permanence des points forts)

A l'issue de l'appréciation des contrôles, l'auditeur détermine les points forts du C I sur lesquels il souhaite s'appuyer pour orienter son contrôle. Les points forts théoriques sont définis par l'existence effective de points de contrôles (prévus ou alternatifs compensatoires) dans le système de gestion des procédures écrites ou décrites. Mais à ce stade, il n'a que des présomptions qu'il doit confirmer par des tests de fonctionnement et de permanence du système.

Selon la C.N.C.C. (1992 : 53),

D'une part, ces contrôles portent sur le fonctionnement des contrôles qui allient forces probantes maximum et facilité de vérification parmi ceux qui contribuent aux mêmes objectifs , en priorité sur ceux qui ont un objectif de fiabilité sur les comptes annuels;

D'autre part, ils peuvent être classés en deux catégories :

Les contrôles à priori. Ceux qui sont exécutés au jour le jour sur les transactions individuelles, et réalisés avant de passer à une phase suivante. Ils sont surtout destinés à éviter que des erreurs soient introduites dans le système. C'est le cas par exemple des vérifications arithmétiques ou des autorisations d'imputation dans les comptes à l'aide de visas ou encore les opérations de validation des traitements effectués par l'ordinateur.

Les contrôles de supervision et de détection. Ils sont faits à posteriori par un superviseur, sur un groupe d'opérations de même nature pour déceler des anomalies éventuelles qui auraient échappé aux contrôles à priori. C'est le cas par exemple des contrôles sur les résultats des traitements, et en particulier on peut citer les rapprochements bancaires mensuels

Les tests ont pour objectifs de justifier que ces contrôles sont :

- réellement et régulièrement faits ;
- correctement effectués ;
- réalisés par des personnes habilitées.

Selon A.T.H. (1991 : 149) trois techniques permettent d'effectuer ces tests.

- l'examen de l'évidence des contrôles
- la répétition des contrôles
- l'observation physique

auxquels on peut ajouter,

- les jeux d'essais
- des logiciels d'audit

De façon particulière pour les systèmes informatisés ; la vérification du fonctionnement se situe à quatre (4) niveaux.
Ce sont , selon JENKINS & PINKNEY (1984 : 238) :

- les règles d'application,
- les contrôles utilisateurs ,
- les contrôles d'intégrité ,
- les procédures programmées.

Ces contrôles sont effectués par les outils de validation et / ou :

Des contrôles de la matérialité des contrôles ; par exemple : les états d'anomalies ou de rejets doivent être **visés** pour attester de leur retraitement satisfaisant,

l'examen de l'organigramme du service informatique et du manuel des procédures pour attester de la séparation des tâches, etc..

La répétition des contrôles dans la mesure du possible. En effet, l'auditeur ne dispose pas toujours du savoir-faire et de l'expérience du personnel pour répéter ces contrôles à sa place.

PARAGRAPHE 5 : ETUDE DES RISQUES DE CONCEPTION, DE FONCTIONNEMENT ET SOLUTIONS DE COMPENSATION

La vérification du fonctionnement devrait révéler des zones à risque non couvertes par des points forts. Elles sont les points faibles de fonctionnement, et constituent avec les points faibles de conception, l'ensemble des faiblesses du C I . L'auditeur doit alors analyser les solutions de substitution proposées par le client . Il évaluera enfin l'impact de ces points faibles sur les traitements effectués, sur leurs résultats, et sur les comptes et états financiers.

(RENARD 1998 & L'IFACI 1995) proposent dans le cadre de la feuille de révélation et d'analyse des problèmes (FRAP), de voir notamment :

- les problèmes,
- les constats,
- les causes,
- les conséquences.

Pour leur appréciation, voir la page 51 de ce document.

PARAGRAPHE 6 : RECOMMANDATIONS

Parlant des faiblesses, A.T.H. (1991 : 151) dit :

« En cas d'incidence significative sur le contrôle des comptes, elles seront reportées sur la feuille d'évaluation du système ;

En cas d'incidences non significatives, elles peuvent être portées à la connaissance du

client dans les recommandations en vue de lui permettre d'améliorer les performances de son système ».

Les recommandations de l'évaluation sur le C I constituent la contribution personnelle de l'auditeur à l'amélioration du système de l'entreprise et elles sont bien appréciées du client.

SECTION 4 : MODELE D'ANALYSE ET APPROCHE PRATIQUE DE L'EVALUATION

Le modèle (méthodologie de l'évaluation) est posé selon notre revue de littérature. Il constitue donc le modèle de synthèse. Quant à notre modèle d'analyse, il va tenir compte des caractéristiques particulières de l'environnement de notre travail..

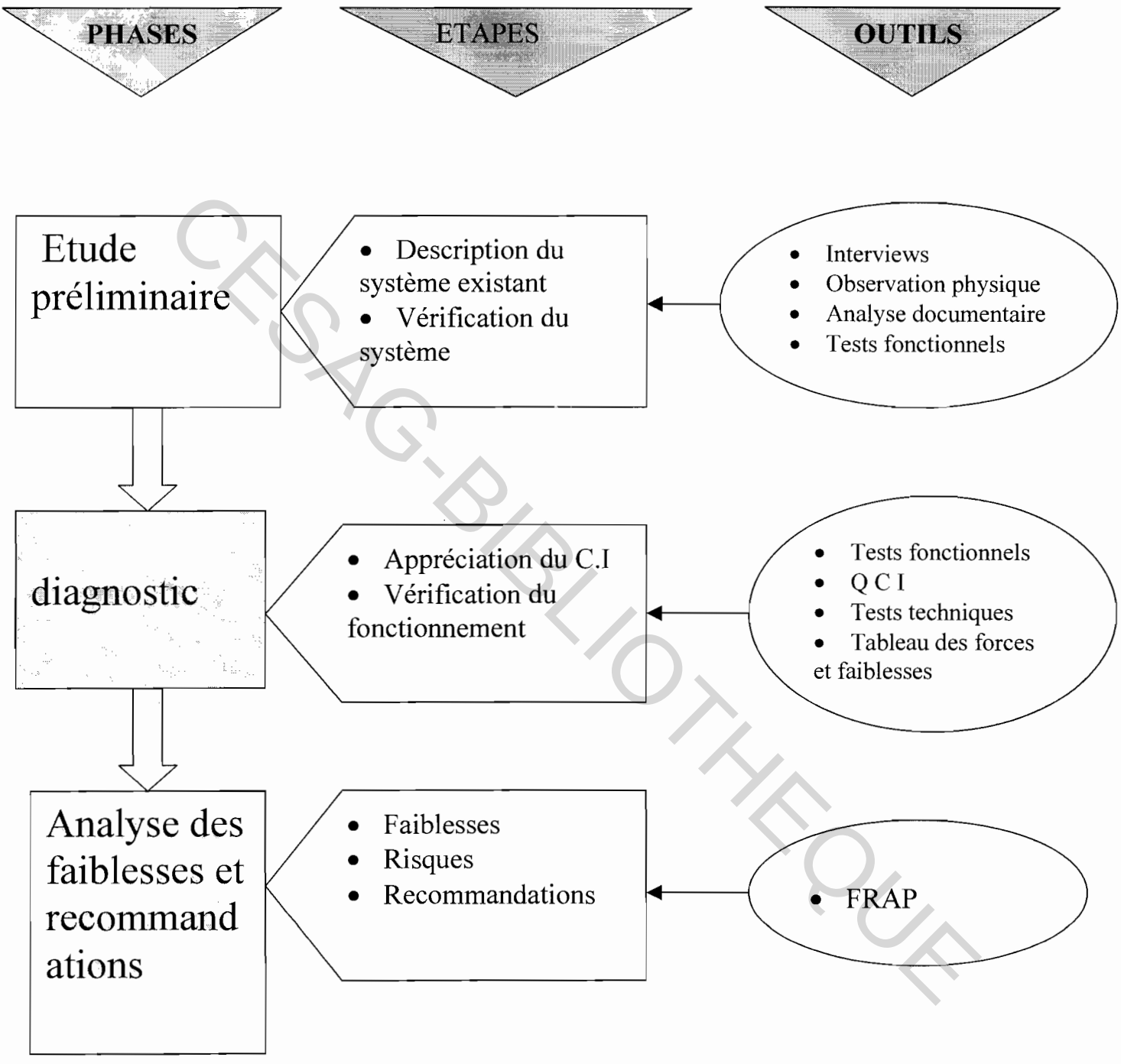
PARAGRAPHE 1 : CONSTRUCTION DU MODELE D'ANALYSE

Le modèle de synthèse, posé par la revue de littérature, fait ressortir cinq (5) grandes étapes successives dans une démarche cohérente. Notre modèle d'analyse est une démarche en trois grandes phases :

- une phase d'étude préliminaire,
- une phase de diagnostic,
- une phase d'analyse des faiblesses du C I et recommandations.

Il utilise alors les outils effectivement à notre disposition. Il est décrit dans le schéma ci dessous.

FIGURE N°6 : Le modèle d'analyse



Source : nous même

- **Phase d'étude préliminaire** (compréhension du système et du C.I)

Cette première phase nous a permis de prendre connaissance des activités et du fonctionnement général de la SICOGI et plus spécifiquement de la fonction informatique. Au cours de cette étape, nous avons également circonscrit les zones à risques et par conséquent le périmètre de notre intervention.

- **Phase de diagnostic**

Cette phase correspond aux étapes suivantes :

- appréciation des contrôles ;
- vérification du fonctionnement des points forts .

Au cours de cette phase, nous avons procédé à :

- La revue technique, comprenant l'analyse du système d'information , ainsi que le niveau de sécurité physique, logistique et opérationnelle associé.
- L'analyse de la fonction informatique

- **Phase d'analyse des faiblesses et recommandations**

Cette phase nous a permis d'élaborer des recommandations à l'issue de l'analyse des faiblesses du C I .

Nous présentons dans le tableau suivant, la décomposition des variables d'évaluation auxquelles nous allons appliquer notre modèle d'analyse.

TABLEAU N°2 : Décomposition des variables d'évaluation

VARIABLES	DIMENSIONS	INDICATEURS	MESURES
L'organisation générale de la fonction informatique	▸ Organisation du service informatique	▪ Organigramme	- existence
		▪ séparation des fonctions	- effectivité
	▸ Contrôles hiérarchiques	▪ Procédures de supervision des tâches	- Existence et application
	▸ Mise en place des systèmes	▪ Procédures	- Existence et application
La sécurité informatique	▸ Sécurité physique	▪ Procédures de prévention	- Existence et application
		▪ procédures de restauration	- existence et tests de simulation
	▸ Sécurité logique	▪ Mots de passe	- Existence
		▪ historique des tentatives d'accès illicites	- journalisation et analyse
		▪ sauvegardes des programmes et des fichiers	- effectivité
Applications informatisées	▸ Adéquation fonctionnelle	▪ Prise en compte des besoins opérationnels	- Exhaustivité
	▸ Fiabilité des traitements	▪ Traitements erronés	- Non-existence
		▪ contrôles programmés	- existence et effectivité
	▸ Satisfaction des utilisateurs	▪ Prise en compte des besoins opérationnels	- Exhaustivité
		▪ disponibilité des systèmes	- durée d'indisponibilité par jour

Source :nous même

PARAGRAPHE 2 : LA COLLECTE DES DONNEES

21- procédure d'échantillonnage

211- les interlocuteurs des interviews

Ils ont été sélectionnés selon des convenances basées sur :

- leur implication à la gestion informatique,
- leur intérêt pour les applications étudiées,
- leur appartenance à l'audit interne.

Nous avons ainsi interrogé les personnes suivantes :

- le D A F,
- le chef du service financier,
- le chef du service comptabilité
- le D C E,
- le chef du service commercial,
- le chef du service recouvrement,
- le chef du SMIM,
- le chef de la section étude du SMIM,
- le chef du service audit interne.

L'ensemble de ses personnes couvre la supervision des services utilisateurs, la mise en exploitation des applications étudiées, l'organisation de la fonction informatique, et les activités de contrôle au second degré.

212- les applications étudiées

A la suite d'une appréciation globale de la fonction informatique, nous avons ciblé nos investigations sur les applications informatisées qui présentent des risques financiers importants, à savoir :

- les applications qui font l'objet de flux financiers diversifiés et importants ;
- les applications spécifiques aux transactions commerciales.

Nous avons en conséquence choisi les applications suivantes :

- application Gestion de la Facturation,
- application Saari Négoce,
- application Paie Personnel,
- application Comptabilité 500 et Tiers.

22- méthodes de collecte des données

La collecte des données a été effectuée au moyen de :

- **Interviews** réalisées auprès de différents directeurs de la SICOGI, les responsables de services, le service des moyens informatiques et de la méthode, (SMIM °) et des utilisateurs (voir 21- procédure d'échantillonnage).

Sur la base d'un guide dont les questions ont pour objectif de nous donner une description du contrôle interne de la fonction informatique.

- **Analyses documentaires** : elle a consisté à nous assurer de l'existence et de la prise en compte effective d'un schéma directeur informatique dans une politique cohérente de développement informatique. Nous nous sommes aussi intéressé à l'existence de procédures formalisées de développement, de maintenance, de mise en exploitation et d'utilisation des applications, mais aussi la documentation des fournisseurs pour les besoins éventuels de formation.

- **Observations physiques**. Elle a consisté à valider les procédures de sécurité physiques décrites, notamment les accès physiques, l'isolement des serveurs et des systèmes sensibles. En effet, ayant travaillé constamment avec le personnel du SMIM et notamment avec son chef, nous avons pu constater le respect des procédures d'accès

aux systèmes sensibles.

- **Questionnaire de contrôle interne**

D'une part, les entretiens que nous avons eus avec les différents directeurs, chefs de services et les utilisateurs ;

D'autre part, nos connaissances du système de C.I de la SICOGI ;

nous ont permis de documenter un questionnaire de contrôle interne (Q.C.I). Pour le réaliser nous nous sommes appuyé sur un référentiel de K.P.M.G (l'environnement de contrôle des systèmes d'information I et II) et un autre de la CNCC .

Nous avons ainsi formulé des questions satisfaisant aux objectifs de C.I recherchés dans le cadre de notre évaluation. L'on y aborde notamment les questions suivantes :

- la politique informatique ;
- l'organisation de la fonction informatique ;
- la sécurité du matériel et des logiciels ;
- les capacités du matériel ;
- les fonctionnalités de logiciels ;
- la fiabilité de logiciels ;
- la convivialité ;
- etc..

A la suite des entretiens, des analyses documentaires, des observations et les tests fonctionnels, nous avons rempli le QCI que nous avons par la suite validé au cours d'autres entretiens avec le chef du SMIM et les utilisateurs.

- **Tests fonctionnels** (extraction de données, interrogation de fichiers)

Les tests fonctionnels ont consisté à effectuer des contrôles croisés entre des utilisateurs (services financiers, comptables commercial et d'exploitation) de l'outil informatique d'une part et les informaticiens d'autre part afin d'en ressortir les forces et faiblesses fonctionnelles des systèmes informatiques. Sur ces bases, nous avons procédé au contrôle des collectes et restitutions des systèmes à savoir :

- les supports de saisie,
- les états,

- les écrans et la documentation utilisée.

A l'issue de cette étape, nous avons établi les différentes fiches d'analyse suivantes :

- description des applicatifs
- diagnostic des applicatifs
- description du matériel
- de la documentation : des applications, du Schéma Directeur, etc.

- **jeux d'essais (tests techniques)**

Ces jeux d'essai ont consisté en des traitements effectifs d'opérations par les applications de notre échantillon.
Les résultats de notre analyse figurent au chapitre 2 section 2

Conclusion

La démarche de l'évaluation du CI n'est pas différente de celle globalement connue. Cependant l'informatique va influencer les différentes étapes de celle- ci à travers les outils d'évaluations en particulier.
C'est ainsi qu'il y a des outils traditionnels, mais aussi des outils informatiques qui sont indispensables par endroit, notamment sur les applications informatisées.

2ème PARTIE

L'EVALUATION DU C. I. DE LA SICOGI DANS LE CADRE D' UN AUDIT LEGAL

Introduction

Le C I d'un système informatisé a des particularités dont nous avons exposé dans le cadre théorique quelques aspects. La deuxième partie qui suit vise à permettre de nous faire une opinion sur le CI de la fonction informatique de la SICOGI tant du point de vu organisationnel que du point de vu de ses applications.

Pour ce faire, notre évaluation porte sur

- les contrôles du système organisationnel de la fonction informatique
- puis sur des contrôles spécifiques d'un échantillon d'applications jugées sensibles.

Mais notre opinion ne peut être établie que sur ce que nous connaissons. C'est pourquoi nous présentons la SICOGI et son système informatique dans le premier chapitre sur les deux que compte cette deuxième partie.
Dans un deuxième chapitre, nous présentons notre diagnostic et les recommandations nécessaires.

CHAPITRE 1 : PRESENTATION DE LA SICOGI ET DE SA FONCTION INFORMATIQUE

En matière de promotion et de gestion immobilière, l'espace économique ivoirien a suscité beaucoup d'intérêt , en raison d'un accroissement rapide de sa population et donc des besoins en logement . Une dizaine d'entreprises se partagent le marché dans une concurrence qui ne laisse pas de place à l'amateurisme.

Dans le lot, une société fait figure de pionnière. La SICOGI, dont l'expérience, le savoir faire et la connaissance du marché ivoirien, lui permettent de demeurer leader, est toujours ambitieuse. Elle modernise sa gestion autant que ses moyens lui permettent, pour garder une longueur d'avance sur ses concurrents.

SECTION 1 : PRESENTATION DE LA SICOGI

Dès son accession à la souveraineté nationale en 1960 l'état ivoirien a compris la nécessité de promouvoir l'habitat social. Il a donc suscité la création de plusieurs sociétés immobilières dont la SICOGI.

PARAGRAPHE 1 : CONSTITUTION DE LA SOCIETE

La SICOGI a été créée le 22 mars 1962 par la fusion de deux sociétés :

- la SIHCI (Société Immobilière des Habitations (à bon marché) de la Côte d'Ivoire (1952) ;
- la SUCCI (Société Urbaine et de Construction de Cote d'Ivoire (1959).

Elle a été créée sous le régime de société d'économie Mixte qu'elle est restée jusqu'à maintenant.

Son capital, de 2 milliards de FCFA depuis 1977, est réparti comme suit :

- Etat de Côte d'Ivoire 79,72%
- CNPS (Caisse Nationale de Prévoyance Sociale) : 11,78%
- Divers autres actionnaires privés : 8,5%

PARAGRAPHE 2 : LES ACTIVITES DE LA SICOGI

Les activités de la SICOGI peuvent être regroupées en deux grandes familles

- La promotion immobilière
- La gestion du patrimoine

21- La promotion immobilière

Elle consiste en la réalisation d'opérations immobilières de quatre types essentiellement :

- les locations simples (L S),
- les locations vente (L V) ;
- les accessions directes à la propriété (A D P) ;
- les opérations pour le compte de tiers.

211- Les opérations de types location simple (L S)

Elles constituent la fonction première de la société. Elles consistent en la mise à la disposition des populations ou des organismes, des bâtiments à usage domestique en location simple, la SICOGI restant la seule et unique propriétaire.

212-Les opérations de type location vente (L V).

Elles concernent les logements dont la SICOGI est copropriétaire avec des clients et qui sont entièrement cédés au terme de l'exécution du contrat qui peut courir jusqu'à vingt ans selon les cas.

213- Les opérations de type accession directe à la propriété (ADP).

Elles concernent des immeubles entièrement cédés par la SICOGI à la signature du contrat.

214- Les opérations pour le compte de tiers.

La SICOGI agit alors en qualité de maître d'ouvrage délégué.

2.2 La Gestion du Patrimoine

Elle comprend : deux activités :

- l'exploitation du patrimoine immobilier
- la maintenance.

221- L'exploitation du patrimoine

Elle consiste , notamment :

- au recouvrement des loyers et charges locatives
- à la vente de logements (A D P , V P L)

222-La maintenance qui concerne :

elle concerne notamment :

- l'entretien des logements construits pour son propre compte tel que le patrimoine immobilier (locatif ou non).
- l'entretien des équipements annexes et du parc automobile.

Le patrimoine immobilier de la SICOGI est constitué comme suit :

- location simple (LS) : 8 506 logements

- patrimoine locatif à vendre (V P L) : 22 308 logements
- accession directe à la propriété (ADP) 1 419 logements

Au total nous estimons le nombre de logements de la SICOGI à 42 028 logements que nous avons obtenu par analyse des fichiers règlement, client, et logement sur lesquels nous avons effectué des tris.

PARAGRAPHE 3 : L'ORGANISATION DE LA SICOGI

Elle est schématisée par l'organigramme ci-dessous.

3.1 au niveau stratégique

Un directeur général coordonne les activités de la société et est coiffé par un conseil d'administration dont le président est nommé par décret présidentiel

Un staff de direction est composé :

- d'un conseiller financier
- de sept (7) services dont le service d'audit interne et le service des moyens informatiques et de la méthode (S M I M)

3.2 Au niveau hiérarchique

Nous avons :

- Deux directions opérationnelles
  - la direction commerciale et de l'exploitation (CDE)
  - la direction des travaux neufs (DTN)

- Deux directions fonctionnelles
  - la direction administrative et financière (DAF)
  - le service formation et communication

PARAGRAPHE 4 : LE CONTEXTE GENERAL DES TRAVAUX

L'évaluation du C I s'est déroulée dans un contexte qui présentait les caractéristiques spécifiques suivantes :

D'une part, le cabinet a exprimé le nécessaire besoin d'approfondir sa connaissance des mécanismes de gestion transactionnelle de la SICOGI. En particulier, il souhaitait se faire une opinion précise sur les transactions informatisées à la suite

- d'insuffisances de justification sur des opérations financières de la D.A.F et de la D.C.E ;

- d'une insatisfaction manifeste des utilisateurs de la D.C.E.

D'autre part, la direction générale de la SICOGI a affiché une volonté :

- de disposer d'une évaluation des systèmes informatiques depuis l'élaboration du schéma directeur ;
- d'acquérir de nouveaux équipements (matériels et logiciels) ;
- de résoudre la problématique de l'interface entre certains systèmes.

Dans ce contexte, il a été convenu avec la SICOGI d'entreprendre l'évaluation globale de son système d'information avec pour principaux objectifs :

- l'évaluation de la qualité des applications mises en exploitation ;
- l'évaluation de l'adéquation des choix matériels ;
- l'évaluation de l'organisation et des ressources humaines du service informatique ;
- l'évaluation des procédures de gestion et d'exploitation des systèmes informatiques, (sécurité, fiabilité, efficacité).

SECTION 2 : DESCRIPTION DE LA FONCTION INFORMATIQUE

La fonction informatique de la SICOGI dans son ensemble, est l'objet de la présentation dans les pages suivantes. Elle comprend notamment :

- l'organisation du service,
- la description du matériel,
- le fonctionnement des applications.

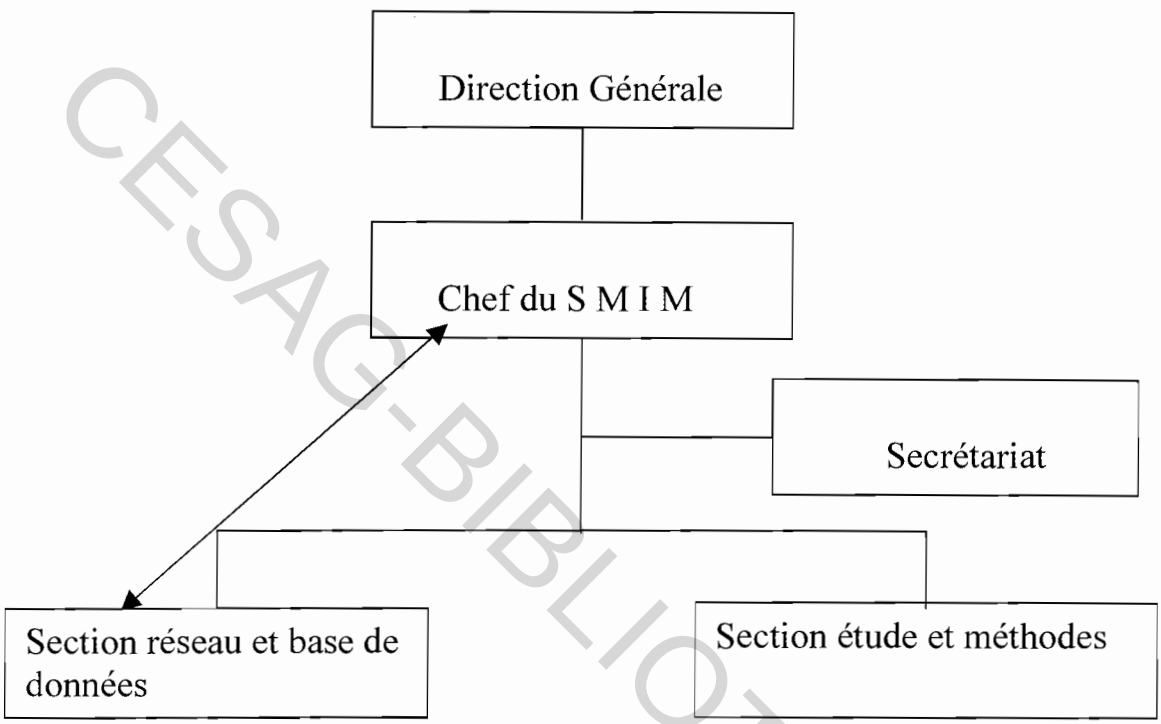
PARAGRAPHE 1 : ORGANISATION ET GESTION DU SMIM

11- présentation du SMIM

Le service informatique ici est dénommé SMIM (service de moyens informatiques

et méthodes). Il est organisé selon la présentation de son organigramme mis à notre disposition.

FIGURE N°8 : Organigramme du service des moyens informatiques et de la méthode (S M I M)



Source : SICOGI

Le SMIM dispose d'un effectif de sept (7) personnes.

- le chef du SMIM, qui gère aussi la section réseau et base de données ;
- cinq (5) personnes pour la section étude et méthode ;
- une secrétaire.

L'organisation actuelle de l'informatique prévoit que l'exploitation des applications soit assurées par les services utilisateurs, ainsi :

- les systèmes de comptabilité et de paie par la direction administrative et financière (D.A.F) ;
- les systèmes de facturation (L.V, L.S., V.P.L.) et gestion des A.D.P. par la direction commerciale et de l'exploitation.

12- description des tâches du SMIM

Nous donnons une description des tâches du SMIM selon les fiches signalétiques qui nous ont été remises par son chef. Nous la présentons dans le tableau suivant.

TABLEAU N°4 : Fiches signalétiques du personnel informatique

Nom et prénoms	fonction	Ancienneté dans la fonction	Ancienneté à la SICOGI	formation	Compétences techniques	Description des tâches effectuées	Besoins exprimés
SAMON Sylvain	Chef du SMIM	16 mois	3 ans	- MERISE - Administration réseau Netware 3.12 et 4.10 - Sécurité et qualité d'un système d'information - Efficacité du cadre dirigeant et la gestion du temps - Dynamique de la communication à la SICOGI	- Conception des systèmes d'information - Conception et intégration des systèmes hétérogènes	- Administration et gestion des ressources (humaines, matérielles et logicielles) du service des moyens informatiques et de la méthode - Participation à l'élaboration des stratégies de l'entreprise.	- Management - Certificat CNE des réseaux Novell Netware - Certificat système des réseaux Microsolft Windows NT
SANOGO Anliyou	Chef section étude et méthode	2ans 1/2	2ans 1/2	**Diplômes :** - Maîtrise en droit et affaires - Ingénieur concepteur des systèmes informatiques de gestion - Audit international et contrôle **Formation professionnelles :** - Organisation, gestion et conduite de projet informatique - Systèmes et organisations des bases de données - Administrateur de réseau (Novell Netware)	- Méthode d'analyse : MERISE - AGL , AMC , DESIGNOR - Développement : langages, Cobol, Oracle 7, Clipper, Access - Administrateur réseau Netware	- Gestion des projets informatiques - Etudes préalables - Recherche de solution logiciel - Rédaction de dossiers techniques - Organisation, mise en place de procédures	- Mise à niveau Oracle
KOBOU Adou	Chef de projet		14 ans	- Ingénieur Analyste Programmeur - Administrateur réseau	- Réseau Windows NT , Novell 4.X - Cobol / Gcos4, Clipper 5	- Ecriture et test de programmes - Analyse et études - Installation et paramétrage de	- Formation et pratique sur les aspects approfondis du réseau / programmation

				NETWARE , Windows NT - Méthodologie MERISE - Assurance des risques en informatique - Organisation et informatique	- MERISE	cartes réseaux - Assistance aux utilisateurs	objer - Acquisition d'un génie logiciel)
AMICHIA Niamkey	informaticien	14ans	15ans	- Analyste Programmeur - Méthodologie MERISE	- Programmation - Analyse	- Ecriture et test de programmes - Analyse et études - Assistance aux utilisateurs	- Formation MERISE - Recyclage (Windows NT , Novell, atelier de génie logiciel)
ADJA Emile	Analyste programmeur	13 ans	13 ans	- Administrateur réseau (NT , Netware) - Méthodologie de programmation LCP - Système d'exploitation UNIX - Méthodologie MERISE	Compétences techniques : - Programmeur : langages Cobol, Clipper, C++ , Visual basic, RG II, Turbo pascal - Administrateur réseau	Description des tâches effectuées : - Suivi et encadrement des stagiaires en informatique - Adjoint au chef de projet technique - Adjoint et l'administrateur réseau	Besoins exprimés : - Formation en M.C.P/SE, Windows/NT - Formation C.N.E. NOVELL 4.11 - Formation Windev 5 (PC solf)
WATTARA	Analyste programmeur	2ans 8mois.	1ans 2mois	**Diplômes :** - Brevet de Technicien Supérieur **Formation professionnelles** : - Informatique de gestion	- Méthode d'analyse : MERISE - Développement : langages, Clipper, Cobol, Access, Dbase, C - Assistance spéciale aux produits SAARI - Environnement : Windows 95, MS-DOS , Netware, Windows NT	- Analyse et développement - Assistance aux utilisateurs - Rédaction de guide utilisateur - Formation des utilisateurs	- Formation Windows NT 4 , Novell Netware 4.11 - Nouvel outil de développement - Nouvelle base de données

Source : nous même

PARAGRAPHE 2 : DESCRIPTION DU SYSTEME INFORMATIQUE DE LA SICOGI

21-historique et évolution

211- Historique

L'informatique a véritablement été introduite à la SICOGI au début des années 80. Le premier système automatisé fut la gestion de la paie en janvier 1984 sur un ordinateur BULL DPS 4. L'architecture matérielle (système centralisé) était bâtie autour de cette machine. A partir de cette date, des systèmes ont été installés sans véritables études de ses activités, la SICOGI s'est vue confrontée à plusieurs problèmes tels que l'adéquation, la fiabilité et l'obsolescence de ses systèmes informatiques.
Ainsi, elle a décidé de se faire assister par un cabinet externe pour l'élaboration d'un Schéma Directeur Informatique en vue de définir la stratégie de ses systèmes informatiques à court, moyen et long terme.
Le Schéma Directeur a été élaboré en 1993. Ses objectifs principaux étaient de :

- faire un état des lieux des systèmes informatiques de la SICOGI
- définir la nature et l'organisation des futurs systèmes
- définir le plan de mise en œuvre
- établir un bilan économique des futurs investissements.

212- Revue succincte du Schéma Directeur Informatique et de sa mise en œuvre

- **Le Schéma Directeur**

Si le Schéma Directeur a de façon globale dressé les principaux besoins de la SICOGI, on peut néanmoins noter qu'il a privilégié le bilan économique. Des points importants tels que :

- l'analyse des orientations stratégiques de la SICOGI
- la définition de la stratégie en matière de systèmes matériels et logiciels
- l'organisation de la fonction informatique

n'ont pas été abordés.

La mise en œuvre du schéma directeur était prévue sur une durée de quatre années (de 1994 à 1998). Dans le cadre du schéma directeur, le système d'information de la SICOGI a été découpé en six sous systèmes :

- le système d'informations générales et administratives (SIGA)
- le système d'informations commerciales (SIC)
- le système d'informations techniques (SIT)
- le système d'informations financières et Comptables (SIFC)
- le système d'informations statistiques (SIS)
- le système d'informations immobilières (SII)

- **La mise en œuvre**

L'ensemble de ces systèmes représente près de 70 modules. A ce jour, seulement une dizaine de modules concernant la gestion administrative, financière et comptable ont été mis en œuvre.

L'important projet relatif au système d'informations commerciales (SIC) n'a pu être réalisé. Ceci n'a pas permis de tirer les avantages prévus par le schéma directeur.

Le budget initial du schéma directeur était de 623 millions de Francs CFA (1994). Ce budget a été ramené à 330 millions de Francs CFA en 1995 du fait des difficultés financières de l'entreprise.

Face à cette situation le schéma directeur n'a pas été réorienté.

Normalement, dans un tel cas, une revue du schéma directeur aurait dû être effectuée pour coller avec le nouveau budget en respectant les orientations stratégiques et les priorités. Aucune mise à jour n'a été faite.

Cette situation est d'autant plus gênante que les projets informatiques sont réalisés

sans véritable planification. Ce qui a un impact sur l'efficacité de la mise en place des systèmes informatiques.

22- Cartographie du matériel et des logiciels

221- description du matériel

L'ensemble des applicatifs de la SICOGI fonctionne dans un environnement matériel composé de :

- 4 serveurs interconnectés entre eux.
- 68 mico-ordinateurs
- 3 portables pour les directeurs
- 2 imprimantes matricielles grande vitesse
- 6 imprimantes matricielles
- 13 imprimantes à jet d'encre
- 2 imprimantes laser
- 37 onduleurs (dont 1 onduleur central de 6 Kva)

Nous en présentons ci-dessous une cartographie.

SICOGI
Service des Moyens Informatiques

NOUVELLE REPARTITION DU MATERIEL

DIRECTION	Service	MICRO-ORDINATEURS					IMPRIMANTE
		MARQUE	MODELE	DESCRIPTION	UTILISATION	OBSERVATIONS	
Conseil d'Administration	*Secrétariat*	DIGITAL	VENTURIS 4100	- 486 DX4 100 Mhz - RAM : 8 Mo - DD : 540 Mo	- Bureautique	- Bon état - Poste en mono	- Jet d'encre - 300 cps
Direction Générale	*DG*	COMPAQ	LT LITE 209	- 486 SL 25 Mhz - RAM : 4 Mo - DD : 200 Mo	- Bureautique - SAARI - Facturation	- Bon état	- Jet d'encre - 330 cps
	Secrétariat	DIGITAL	VENTURIS 4100	- 486 DX4 100 Mhz - RAM : 8 Mo - DD : 540 Mo	- Bureautique	- Bon état	
Audit & Contrôles	*Directeur*	DIGITAL	VENTURIS 4100	- 486 DX4 100 Mhz - RAM : 8 Mo - DD : 540 Mo	- Bureautique - SAARI - Facturation	- Bon état	
	Secrétariat	DIGITAL	VENTURIS 4100	- 486 DX4 100 Mhz - RAM : 8 Mo - DD : 540 Mo	- Bureautique	- Bon état - ***Pool Impres.***	- Jet d'encre - 330 cps
	Section Contrôle	DIGITAL	DECpcLpv+ 466D2	- 486 DX2 66 Mhz - RAM : 8 Mo - DD : 340 Mo	- Bureautique - SAARI	- Bon état - ***Pool Bureaut.***	
Service Communication	*Directeur*	DIGITAL	VENTURIS 4100	- 486 DX4 100 Mhz - RAM : 8 Mo - DD : 540 Mo	- Bureautique	- Bon état	
Services Généraux	*Section courrier & reprographie*	COMPAQ	DESKPRO XE 433S	- 486 SX 33 Mhz - RAM : 4 Mo - DD : 270 Mo	- Courrier général - Bureautique	- Bon état - Poste en mono	- Matricielle - 240 cps - 136 colonnes

	Section Achats	DIGITAL	DECpcLpv+ 466D2	- 486 DX2 66 Mhz - RAM : 8 Mo - DD : 340 Mo	- Bureautique - NEGOCE	- Bon état	
Service des Moyens Informatiques & de la Méthode	*Secrétariat*	DIGITAL	DECpcLpv+ 466D2	- 486 DX2 66 Mhz - RAM : 8 Mo - DD : 340 Mo	- Bureautique	- Bon état ***- Pool Bureaut.*** ***- Pool Impres.***	- Jet d'encre - 230 cps
	Chef de service	DIGITAL	HiNote	- 486 DX2 50 Mhz - RAM : 8 Mo - DD : 340 Mo	- Bureautique	- Bon état	
	Bureau Production	DIGITAL	DECpcLpv+ 466D2	- 486 DX2 66 Mhz - RAM : 8 Mo - DD : 340 Mo	- Facturation - Traitement des des cassettes	- Bon état - Poste maître	
		DATA GENERAL	466V	- 486 DX2 66 Mhz - RAM : 16 Mo - DD : 2 Go	- Serveur de développement	- Bon état - non connecté	
DIRECTION	**Service**	**MICRO-ORDINATEURS**					**IMPRIMANTE**
		MARQUE	**MODELE**	**DESCRIPTION**	**UTILISATION**	**OBSERVATIONS**	
Service des Moyens Informatiques & de la Méthode	*Section Etudes & Méthode*	DIGITAL	VENTURIS 4100	- 486 DX4 100 Mhz - RAM : 8 Mo - DD : 540 Mo	- Bureautique - Dév. - Adm. réseau	- Bon état	
		DIGITAL	VENTURIS 4100	- 486 DX4 100 Mhz - RAM : 8 Mo - DD : 540 Mo	- Bureautique - Dév.	- Bon état	
		OPUS	433	- 486 SX 33 Mhz - RAM : 8 Mo	- Bureautique - Dév.	- Bon état ***- Pool Dev.*** ***- Pool Impres.***	- Matricielle - 330 cps - 136 colonnes
		DIGITAL	VENTURIS 4100	- 486 DX4 100 Mhz - RAM : 8 Mo - DD : 540 Mo	- Bureautique - Dév.	- Bon état	
		DIGITAL	DECpcLpv+ 466D2	- 486 DX2 66 Mhz - RAM : 8 Mo - DD : 340 Mo	- Bureautique - Dév.	- Bon état	
	Section Réseaux & Base de données	DIGITAL	VENTURIS 4100	- 486 DX4 100 Mhz - RAM : 8 Mo	- Bureautique - Dév.	- Bon état	

				- DD : 540 Mo	- Adm. réseau		
DTM	*DTM*	DIGITAL	VENTURIS 4100	- 486 DX4 100 Mhz - RAM : 8 Mo - DD : 540 Mo	- Bureautique - Win Projet	- Micro de démo. **- Propriété de DIGITAL**	
	Secrétariat	COMPAQ	DESKPRO XE 433S	- 486 SX 33 Mhz - RAM : 4 Mo - DD : 270 Mo	- Bureautique	- Bon état	- Jet d'encre - 330 cps
	Service Opérations	DIGITAL	VENTURIS 4100	- 486 DX4 100 Mhz - RAM : 8 Mo - DD : 540 Mo	- Bureautique	- Bon état	
	Service foncier	ACER	AST 900N	- 486 DX4 70 Mhz - RAM : 8 Mo - DD : 327 Mo	- Bureautique	- Bon état	
	Pool Bureautique	DIGITAL	VENTURIS 4100	- 486 DX4 100 Mhz - RAM : 8 Mo - DD : 540 Mo	- Bureautique	- Bon état ***- Pool Bureaut.*** ***- Pool Impres.***	- Jet d'encre - 230 cps
DAF	*DAF*	DIGITAL	VENTURIS 4100	- 486 DX4 100 Mhz - RAM : 8 Mo - DD : 540 Mo	- Bureautique - SAARI	- Bon état	- Jet d'encre - 330 cps
	Secrétariat DAF	DATA GENERAL	433SG	- 486 SX 33 Mhz - RAM : 8 Mo - DD : 327 Mo	- Bureautique	- Bon état	
	Service Comptabilité	DIGITAL	DECpcLpv+ 466D2	- 486 DX2 66 Mhz - RAM : 8 Mo - DD : 340 Mo	- Bureautique - SAARI	- Bon état	
		DIGITAL	DECpcLpv+ 466D2	- 486 DX2 66 Mhz - RAM : 8 Mo - DD : 340 Mo	- Bureautique - SAARI	- Bon état ***- Pool Impres.***	- Matricielle - 300 lpm - 136 colonnes
		DATA GENERAL	433SG	- 486 SX 33 Mhz - RAM : 8 Mo - DD : 327 Mo	- Bureautique - SAARI	- Bon état ***- Pool Bureaut.*** ***- Pool Impres.***	- Jet d'encre - 330 cps
		DIGITAL	DECpcLpv+ 466D2	- 486 DX2 66 Mhz - RAM : 8 Mo - DD : 340 Mo	- Bureautique - SAARI	- Bon état	

		COMPAQ	PROLINEA 433	- 486 SX 33 Mhz - RAM : 4 Mo - DD : 270 Mo	- Bureautique - SAARI	- Bon état	
DIRECTION	**Service**	**MICRO-ORDINATEURS**					**IMPRIMANTE**
		MARQUE	**MODELE**	**DESCRIPTION**	**UTILISATION**	**OBSERVATIONS**	
DAF	*Service Comptabilité*	COMPAQ	DESKPRO XE 433S	- 486 SX 33 Mhz - RAM : 4 Mo - DD : 270 Mo	- Bureautique - SAARI	- Bon état	
		DIGITAL	DECpcLpv+ 466D2	- 486 DX2 66 Mhz - RAM : 8 Mo - DD : 340 Mo	- Bureautique - SAARI	- Bon état	
		DIGITAL	DECpcLpv+ 466D2	- 486 DX2 66 Mhz - RAM : 8 Mo - DD : 340 Mo	- Bureautique - SAARI	- Bon état	
	Chef du Service ad. & des ressources Humaines	DIGITAL	DECpcLpv+ 466D2	- 486 DX2 66 Mhz - RAM : 8 Mo - DD : 340 Mo	- Bureautique - Suivi Frais M.	- Bon état	
	Pool Bureautique	COMPAQ	DESKPRO XE 433S	- 486 SX 33 Mhz - RAM : 8 Mo - DD : 270 Mo	- Bureautique ***- Pool Bureaut.*** ***- Pool Impres.***	- Bon état	- Jet d'encre - 230 cps
	Section Paie	COMPAQ	DESKPRO XE 433S	- 486 SX 33 Mhz - RAM : 4 Mo - DD : 270 Mo	- Paie	- Bon état	- Matricielle - 330 cps - 136 colonnes
	Bureau Production (SMIM)	UNISYS	SVI 5907	- Pentium 90 Mhz - RAM : 16 Mo - DD : 1 Go	- Serveur DAF Tous les logi. SAARI	- Bon état ***- Serveur DAF***	- Matricielle - 800 lpm - 132 colonnes
DCE	*Secrétariat*	DIGITAL	DECpcLpv+ 466D2	- 486 DX2 66 Mhz - RAM : 8 Mo - DD : 340 Mo	- Bureautique - Gestion Commerciale	- Bon état ***- Pool Bureaut.*** ***- Pool Impres.***	- Jet d'encre - 330 cps
	Secrétariat Administratif	COMPAQ	DESKPRO XE 433S	- 486 SX 33 Mhz - RAM : 8 Mo - DD : 270 Mo	- Bureautique - Courrier DCE	- Bon état	
	Service Commercial	DIGITAL	VENTURIS 4100	- 486 DX4 100 Mhz - RAM : 8 Mo	- Bureautique - Gestion	- Bon état	

				- DD : 540 Mo	Commerciale		
		DIGITAL	VENTURIS 4100	- 486 DX4 100 Mhz - RAM : 8 Mo - DD : 540 Mo	- Bureautique - Gestion Commerciale	- Bon état	
		COMPAQ	DESKPRO XL 5100	- Pentium 90 Mhz - RAM : 16 Mo - DD : 1 Go	- Bureautique - CorelDraw	- Bon état ***- Pool Bureaut.*** ***- Pool Impres.***	- Jet d'encre - 330 cps
	Service Juridique & Contentieux	DIGITAL	VENTURIS 4100	- 486 DX4 100 Mhz - RAM : 8 Mo - DD : 540 Mo	- Bon état	- Bon état	- Laser - 8 ppm
	Service Copropriété	ZENITH	386SX	- 386 SX 20 Mhz - RAM : 4 Mo - DD : 40 Mo	- Bon état - Poste de saisie	- Bon état	
	Bureau Assistance Clientèle	ZENITH	386SX	- 386 SX 20 Mhz - RAM : 4 Mo - DD : 80 Mo	- Bon état - Poste de saisie	- Bon état	
	Service Exploitation	OLIVETTI	486DX66	- 486 DX2 66 Mhz - RAM : 8 Mo - DD : 256 Mo	- Bon état - Poste de Cons.	- Bon état ***- Pool Impres.***	- Matricielle - 330 cps - 136 colonnes
		DATA GENERAL	433SV	- 486 SX 33 Mhz - RAM : 8 Mo - DD : 327 Mo	- Bon état - Poste de saisie	- Bon état	
				- 486 SX 33 Mhz - RAM : 8 Mo - DD : 327 Mo	- Bon état - Poste de saisie	- Bon état	
		ZENITH	386SX	- 386 SX 20 Mhz - RAM : 4 Mo - DD : 40 Mo	- Bon état - Poste de saisie	- Bon état	
		DIGITAL	CELEBRIS XL 590	- Pentium 90 Mhz - RAM : 32 Mo - DD : 1 Go	- Serveur DCE Gestion Commerciale	- Bon état ***- Serveur DCE***	- Matricielle - 800 lpm - 132 colonnes

222- Cartographie des systèmes logiciels

Les logiciels systèmes utilisés sur les différents serveurs sont :

- Novell Netware 4.10. pour le serveur DCE.
- Windows NT Server 4.0. pour le serveur DAF
- Windows NT Server 3.51. pour le serveur de développement.
- Windows NT Server 4.0 avec MS Exchange Server pour le serveur de Messagerie
- Convertisseur de données SAARI :
- Logiciel de sauvegarde des données : ARCSERVE.

Du côté applicatif, on note d'une part, les progiciels suivants :

- Immobilisations SAARI V2.04
- Comptabilité 500 et tiers de Sage Sybel
- Saari NOGOCE (Gestion des Achats et des ADP)
- Paie CS
- la suite bureautique (MS Office 95 et 91), des produits WinPhone et WinProject

(voir annexe 2)

Et d'autre part, des logiciels spécifiques suivants, (développement interne) :

- Gestion de la Facturation
- Gestion des Prospects
- Gestion des Courriers (Secrétariat Administratif et Services Généraux)
- Suivi du tableau d'amortissement des logements VPL
- Calcul du remboursement d'un prêt

(Voir annexe 2)

On note également l'existence des applications qui ont été acquises mais non utilisées :

- Paie Saari Major
- Budget de trésorerie Saari Major
- Rapprochement bancaire Saari Major
- Immobilisation Saari Maestria
- Paie 500 Sage Sybel
- Trésorerie 500 et Budget
- Rapprochement bancaire 500
- Etat financier 500
- Gestions des Réclamations

La comptabilité Saari Major a été remplacée par la Comptabilité 500 et Tiers de sage Sybel.

(Voir annexe 3)

223- Logiciels applicatifs

A ce jour, les applications en exploitation ne sont pas intégrées. En effet, aucune interface n'existe. Le transfert de données entre elles s'effectue par ressaisie.

Dans les pages suivantes, nous avons effectué une revue des applications de notre échantillonnage.

TABLEAU N°7 : Cartographie des applications de l'échantillon de contrôle

Applications	Fonctionnalités utilisées	Nature de développements	Durée d'exploitation	Matériel de support	Applications interfacées	Nombre d'utilisateurs	Volume estimé d'activité
Gestion de la facturation	- Gestion de tables - Gestion des logements - Gestion des contrats - Gestion de la facturation et du recouvrement	Interne	6 ans	Serveur compaq proliant 3000 R	aucune	12	- Nbre de logements : 38 000 environ - Nbre de locataires : 40 874 (partis et présents - Nbre de quittances mensuelles : 19 000 environ - Nbre de versements mensuels : 19 000 environ - Nbre d'opérations diverses âr mois : 100 environ
Saari négoce	- Gestion des clients (mise à jour, suivi es comptes - Gestion des fsseurs (mise à jour, suivi des comptes - Gest°des articles (contrôle de stock, inventaire) - Edition de stock - Suivi des encaissements	progiciel	4 ans	Serveur compact proliant 3000 R	aucune	11	- Opération Djibi maison basses : 683 logements - Opération Djibi commerce :48 logements - Opération Djibi duplexes 220 logements - Opération Latrille : 192 logements - Opération Adjamé sud : 80 logements - Nombre d'articles (fournitures) : 763 - Nombre de clients (directions et services) : 17
Comptabilité 500 et Tiers (Sage Sybel)	- Enregistrements comptables - Lettrage, rapprochements - Edition des états comptables (	progiciel	En cours d'installation	Serveur compaq proliant	aucune	10	- Nombre de comptes généraux et tiers : 1300 - Nombre de comptes analytiques : 24 - Nombres de journaux : 35

	balance, grands livres etc..) - Suivi des tiers (gestion, gestion des fournisseurs)			3000R			- Nombre d'écritures : environ 1000 par jour
Paie C. S	- Gestion du personnel, des départs (licenciement, retraite) - Gestion des prêts, calcul des salaires édition des bulletins - Edition des états de déclaration mensuelles et annuelles des impots et CNPS - Transmission des états sur disquette à la CNPS	progiciel	5 ans	Compaq deskpro XE 433S	aucune	2	Nombre d'employés : 210

Source : nous même

23- description des fichiers

231- les fichiers des acquéreurs

Il ressort des différents entretiens que nous avons eus avec les différents services aussi bien informatiques qu'utilisateurs, que certains renseignements concernant les locataires sont obligatoires. Ce sont :

- le matricule et le nom du locataire,
- son indicateur de présence qui ne peut prendre que les valeurs « 0 » s'il est présent et « 1 » s'il est parti,
- le prix de vente pour les VPL (vente et d'échéance pour les VPL) ;
- le loyer, la mensualité pour les L. S ;
- les totaux débit et crédit qui permettent d'obtenir le solde du locataire (total débit total crédit),
- la valeur initiale si le locataire est passé de la location simple en VPL ,
- la date correspondante à la reprise de cette dette initiale) ;
- le numéro et la date d'inscription de la fiche VPL.

232- Le fichier des logements

. Un logement doit obligatoirement comporter les renseignements suivants :

- codes secteurs et géographiques,
- numéro du logement,
- indicateur du patrimoine,
- le standing ;
- le type de logement ;
- le nombre de pièces.

233- le fichier historique des mouvements

En principe, il ne devrait pas avoir de mouvements dont les références (codes

secteur et géographique, numéro logement et matricule) sont inconnues de ces deux fichiers.

Un compte locataire ne devrait pas présenter un solde créditeur d'un montant assez important.

24- vérification du fonctionnement des applications

Nous avons procédé à des contrôles informatiques sur la base d'extraction des fichiers QUI00002 (logements), VPL00003 (locataires) et VPL00004 (historiques mouvements locataires). Nous avons récupéré une copie de ces fichiers avant et après la facturation Les informations extraites ont été rapatriées sur un micro-ordinateur puis traitées à l'aide d'un progiciel de gestion des bases de données.

Nous avons axé les tests sur la cohérence des informations recueillies. (si elles sont correctement renseignées) dans les fichiers. Ainsi, on ne devrait pas retrouver des locataires sans matricule dans la base

Nous avons alors procédé entre autres aux interrogations suivantes :

241- les fichiers acquéreurs

- Locataires dont le matricule est nul (matricules =0)
- Locataires dont le nom est effacé de la base
- Locataires dont l'indicateur de présence n'est pas renseigné
- Locataires en VPL (Vente de Patrimoine Locatif) ou LV (Location Vente) dont les dates de contrat de vente et d'échanges ne sont pas renseignés.
- Locataire en VPL (Vente de Patrimoine Locatif) pour lesquels il n'existe pas de numéro et de date d'inscription de fiche
- Locataires dont le total crédit est nul
- Locataires débiteurs en Location Simple dont la dette initiale n'a pas été reprise en VPL

242-les fichiers des logements

Nous avons interrogé les fichiers sur :

- les codes secteurs non renseignés,
- les numéros de logement nul ,
- les indicateurs du patrimoine non renseignés,
- le nombre de pièces nul ou non renseigné,
- etc..

243- le fichier historique des mouvements

Nous avons interrogé le fichier sur :

- les mouvements des locataires en double,
- les mouvements du compte de régularisation,
- les locataires partis (L S) dont le solde est créditeur,
- les locataires à contrats échus dont le solde est créditeur.

25- les résultats du test

Les tests ont révélé les faiblesses suivantes.

251- les fichiers des acquéreurs

- **Locataires dont le matricule égal à zéro**

Nous en avons identifié 9 dont le matricule est nul.

Nous verrons par la suite qu'il existe des mouvements sur ces comptes locataires.

- **Locataires dont le nom est effacé de la base**

Il existe 7 locataires sans nom dans le fichier. Ces locataires ont leur indicateur de présence égal à «.1 », donc, supposé parti.

secteur et géographique, numéro logement et matricule) sont inconnues de ces deux fichiers.

Un compte locataire ne devrait pas présenter un solde créditeur d'un montant assez important.

24- vérification du fonctionnement des applications

Nous avons procédé à des contrôles informatiques sur la base d'extraction des fichiers QUI00002 (logements), VPL00003 (locataires) et VPL00004 (historiques mouvements locataires). Nous avons récupéré une copie de ces fichiers avant et après la facturation Les informations extraites ont été rapatriées sur un micro-ordinateur puis traitées à l'aide d'un progiciel de gestion des bases de données.

Nous avons axé les tests sur la cohérence des informations recueillies. (si elles sont correctement renseignées) dans les fichiers. Ainsi, on ne devrait pas retrouver des locataires sans matricule dans la base

Nous avons alors procédé entre autres aux interrogations suivantes :

241- les fichiers acquéreurs

- Locataires dont le matricule est nul (matricules =0)
- Locataires dont le nom est effacé de la base
- Locataires dont l'indicateur de présence n'est pas renseigné
- Locataires en VPL (Vente de Patrimoine Locatif) ou LV (Location Vente) dont les dates de contrat de vente et d'échanges ne sont pas renseignés.
- Locataire en VPL (Vente de Patrimoine Locatif) pour lesquels il n'existe pas de numéro et de date d'inscription de fiche
- Locataires dont le total crédit est nul
- Locataires débiteurs en Location Simple dont la dette initiale n'a pas été reprise en VPL

242-les fichiers des logements

Nous avons interrogé les fichiers sur :

- les codes secteurs non renseignés,
- les numéros de logement nul ,
- les indicateurs du patrimoine non renseignés,
- le nombre de pièces nul ou non renseigné,
- etc..

243- le fichier historique des mouvements

Nous avons interrogé le fichier sur :

- les mouvements des locataires en double,
- les mouvements du compte de régularisation,
- les locataires partis (L S) dont le solde est créditeur,
- les locataires à contrats échus dont le solde est créditeur.

25- les résultats du test

Les tests ont révélé les faiblesses suivantes.

251- les fichiers des acquéreurs

- **Locataires dont le matricule égal à zéro**

Nous en avons identifié 9 dont le matricule est nul.

Nous verrons par la suite qu'il existe des mouvements sur ces comptes locataires.

- **Locataires dont le nom est effacé de la base**

Il existe 7 locataires sans nom dans le fichier. Ces locataires ont leur indicateur de présence égal à «.1 », donc, supposé parti.

- **Locataires à indicateur de présence non renseigné**

Il existe 1207 locataires dont l'indicateur de présence n'est pas renseigné. (ni .«0», ni(«1»). Certains de ces locataires sont présents, tandis que d'autres sont partis.
D'autres locataires ont leur indicateur de présence à «1», et sont présents.

Cette situation ne permet pas de déterminer les nombres exacts de locataires partis et présents.
Cet indicateur ne donne finalement aucun renseignement sur l'état de présence d'un locataire.

- **Locataires dont le compte existe en double**

Nous avons identifié 11 locataires dont les comptes sont en double (code secteur, codes géographiques et codes logements, matricules et noms identiques). La différence entre les deux comptes se situe au niveau des indicateurs de présence qui prennent les valeurs (1.1) ; (0.1) ; (blanc, 0) .

- **Dates de contrat de vente ou d'échéances non renseignées correctement**

Nous avons trouvé dans la base, des locataires dont la date de contrat ou de vente est [0/0/0], [0/0/1900], et la date d'échéance est 30 janvier ou 31 avril ou simplement des dates d'échéance nulles ([0/0/0]).

- **Contrat VPL n'ayant pas de numéro de fiche d'inscription**

Chaque contrat VPL s'identifie par une fiche d'inscription portant un numéro d'ordre. Nous avons relevé plusieurs contrats dont le numéro de fiche d'inscription est égal à zéro.

- **Locataires dont les totaux débit et crédit sont nuls**

Les rubriques total débit et total crédit représentent les cumuls des quittancements et des paiements d'un locataire. Ainsi, le solde de celui-ci se déterminerait par la différence entre le total débit et le total crédit. Il est donc difficile d'admettre que ces

totaux soient égaux à zéro.

Nous avons décompté plusieurs locataires quittancés dont les totaux établis de crédit sont nuls.

Cette situation ne permet pas de donner avec exactitude le solde d'un locataire qui désire effectuer un paiement par anticipation.

- **Locataires débiteurs en (L.S) passant en (V.P.L)**

Les dettes de certains locataires en location simple ne sont pas reprises lors de la signature de leurs contrats V.P.L elles seraient incorporées au coût d'acquisition

252- les fichiers des logements

Les tests effectués à ce niveau ont consisté à déterminer aussi la cohérence des informations relatives aux logements

Nous avons recensé 1328 logements dont le nombre de pièces est égal à zéro.

253- Le fichier historique des mouvements

Au niveau de ce fichier, nous avons procédé :

- d'une part, à des tests croisés avec le fichier des logements ;
- d'autre part, à des tests croisés avec celui des locataires.

- **Mouvement de locataires en double**

Nous avons fait ressortir que les comptes qui existent en double sont mouvementés parallèlement. Cette situation altère considérablement la fiabilité de l'application de la facturation.

- **Mouvement du compte de régularisation**

Le Compte de Régularisation présente un solde créditeur de 42. 978. 538 francs CFA.. Malgré les efforts entrepris par le chef du service exploitation pour l'apurer, aucune évolution de ce compte qui enregistre en moyenne 40 écritures par mois n'est

constatée. La régularisation des écritures passées sur ce compte semble difficile, car aucune référence du locataire n'est disponible au moment de la passation de l'écriture (quittances oubliées, compte non encore crée, etc.). Les utilisateurs n'ayant pas non plus la possibilité d'insérer une indication sur le locataire dans le libellé qui s'affiche automatiquement.

- **Locataires partis (Location Simple) dont le solde est créditeur**

Certains locataires au titre de la location simple présentent, dans la base, des reports à nouveau créditeurs alors qu'ils sont supposés partis. Il s'agirait d'écritures de régularisation non encore passées.

- **Locataires à contrats échus dont le solde est créditeur**

Il apparaît dans la base, des locataires qui, ayant payé au comptant, par anticipation ou dont le contrat est échu, présentent un solde créditeur.

Les écritures de régularisations correspondantes n'auraient pas été passées. Cette situation ne donne pas une image fiable des comptes locataires

Remarques générales sur les différents résultats obtenus

Les incohérences relevées ici, sont loin d'être exhaustives. Nous avons fait apparaître celles qui témoignent du manque de fiabilité de l'application et des comptes locataires ainsi gérés.

Conclusion

La SICOGI dispose d'un service informatique qui exerce des fonctions d'étude, d'analyse et de développement, d'exploitation, de contrôle. Elle dispose aussi d'un personnel informatique de qualification satisfaisante, d'équipement matériel et logiciel important dont certains de ces derniers sont développés en interne.

Cependant elle présente une organisation insuffisante et des applications dont le fonctionnement donnent lieu à des faiblesses à ne pas négliger

CHAPITRE 2 : DIAGNOSTIC ET ANALYSE DES RESULTATS

Notre diagnostic du CI de la SICOGI nous a conduit à analyser de façon plus spécifique :

- les contrôles généraux de la fonction informatique (contrôles globaux) ;
- le contrôle des applications informatisées .

SECTION 1 : ANALYSE DES CONTROLES GENERAUX DE LA FONCTION INFORMATIQUE

Nous rappelons que ces contrôles ont été effectués aux moyens d'analyses documentaires, l'observation physique, d'interviews et de tests d'intrusion sans autorisation.

Concernant les contrôles généraux de la fonction informatique, nous mettons l'accent :

- sur les contrôles organisationnels ;
- sur la sécurité informatique.

PARAGRAPHE 1 : LES CONTROLES ORGANISATIONNELS

Pour les contrôles organisationnels, nous avons porté notre appréciation, notamment sur :

- l'organisation du service informatique ;
- les contrôles hiérarchiques ;
- les contrôles de mise en place des systèmes

11- Evaluation de l'organisation du service informatique

Nous avons effectué une analyse des tâches du service des moyens informatiques et de la méthode. Nous la présentons dans le tableau suivant :

TABLEAU N°6 : Grille d'analyse des tâches du SMIM

N°	Nature des opérations	TACHES / INTERVENANTS	SAMON	SANOGO	KOBOU	AMICHIA	ADJA	OUATTARA	UTILISATEURS
1	Co	Politique et stratégie de l'entreprise	X						
2	Co	Administration et gestion des ressources (hum. , mat., Log)	X						
3	Co	Administration du réseau	X				X		
4	De	Etude		X	X	X			
5	De	Recherche de solution logiciel (analyse)		X	X	X		X	
6	De	Gestion de projets informatiques		X			X		
7	De	Rédaction de dossiers techniques		X					
8	Co	Organisation et mise en place des procédures		X					
9	De	Installation et paramétrage des cartes réseaux			X				
10	De	Ecriture (développement)			X	X		X	
11	Ex	Assistance aux utilisateurs			X	X		X	
12	Co	Suivi et encadrement des stagiaires					X		
13	Ex	Test des programmes			X	X			
14	Ex	Rédaction de guides utilisateurs						X	
15	Ex	Formation des utilisateurs						X	
16	Ex	Exploitation	X		X	X		X	X

Légende : Co : tâches destinées au contrôle ; De : tâches destinées à l'étude et au développement ; Ex : tâches destinées à l'exploitation

Source : nous même

Le tableau présente de toute évidence des cumuls de fonctions. Le résultat de notre analyse est présenté au chapitre suivant.

111- Points forts

- L'organigramme est formalisé et les attributions de chacun des membres du service sont connues. Les responsabilités de chacun sont donc situées d'avance.

- L'organisation du SMIM prévoit la séparation des fonctions entre informaticiens et les utilisateurs qui sont par conséquent chargés de l'exploitation des applications par :
  - le DAF pour les systèmes de comptabilité et de paie.
  - le DCE pour les systèmes de facturation (LS, LV, VPL) et la gestion des ADP.

112- Points faibles

- La séparation des fonctions énoncées en théorie n'est pas respectée en pratique. En effet,
  - des agents de la section étude et méthodes (conception et maintenance des applications) interviennent dans les charges d'exploitation et d'administration du réseau :
    - ➢ deux agents pour la gestion des ADP (Négoce Saari)
    - ➢ un agent pour l'application paie.
  - le chef du SMIM et un agent de la section étude et méthodes interviennent dans l'exploitation de l'application facturation (LS, LV, VPL) prévu à la charge de la DCE.
  - la section réseau et base de données, supposé gérée par le chef du SMIM reçoit les interventions d'un agent du service étude et méthode.

Nous avons alors un cumul de fonctions d'exploitation et d'étude et développement et / ou d'exploitation et de contrôle.

- L'historique du réseau, des incidents d'exploitation, des interventions de maintenance et de développement n'est pas tenue dans une documentation.

Il est donc difficile voire impossible d'établir une relation de cause à effet entre les pannes du réseau ou les difficultés d'exploitation et leurs antécédents.

- Le personnel informatique n'est pas très motivé car les perspectives de carrière sont limitées du fait de leur concentration quasi totale au service étude et méthode. Trois d'entre eux souhaitent partir. Cela constituerait un manque de personnes qui connaissent bien le système informatique de la SICOGI et ses problèmes.

- Les utilisateurs estiment ne pas tirer tout le profit espéré de l'existence du S M I M qui du reste ne répondrait pas à la plupart de leurs demandes d'intervention, conséquence de la démotivation du personnel informatique.

113- Risques

- Les problèmes significatifs liés à l'équipement ou aux performances et susceptibles d'échapper à la surveillance en temps réel peuvent être ignorés.
- Des références permettant d'effectuer des comparaisons avec les données les plus récentes peuvent ne pas être disponibles.
- Des futurs administrateurs auraient des difficultés sur l'exploitation du réseau.
- La séparation des fonctions incompatibles n'étant pas respectée, il y a risque de manipulations erronées ou malveillantes sur des fichiers de données ou de programmes.
- Le personnel informatique risque de ne pas atteindre les objectifs à lui assignés.
- Les utilisateurs risquent de se décourager des systèmes informatiques et de revenir à des traitements rétrogrades.

114- Recommandations

- Il faut tenir et mettre à jour un historique du réseau et des interventions.
- Il faut faire respecter de façon stricte la séparation des fonctions incompatibles

entre :

- Sections du service informatique
- Services informatiques et utilisateurs

- Il faut créer une section exploitation au niveau du SMIM à charge de :
  - contrôler l'accès à la bibliothèque des programmes ;
  - tester périodiquement la performance des équipements
  - vérifier l'utilisation de bonnes versions de fichiers ou de programmes ;
  - d'examiner les temps d'exploitation des systèmes.

12- Evaluation des contrôles hiérarchiques

121- points forts

- L'accès aux différentes fonctionnalités des applications est défini par niveaux variant de 1 à 9. On ne peut accéder aux différentes fonctionnalités que si l'on a le niveau requis. Cela contribue à la séparation des fonctions et à la protection des données et des informations.

- L'utilisateur ayant un niveau donné peut accéder aux fonctionnalités de niveaux inférieurs. L'utilisateur de niveau 9 est le directeur de département pour chaque application. Les contrôles de supervision sont prévus dans ces conditions.

- Il existe un service d'audit interne rattaché directement à la direction générale. Des contrôles du second degré sont possibles avec une autorité suffisante.

122- points faibles

- les informaticiens en charge du réseau peuvent accéder aux fichiers des mots de passe utilisateur qui ne sont pas cryptés. Les opérateurs de saisie de la D C E peuvent

en faire autant. Ils peuvent les utiliser ou les communiquer à des tiers.

- l'audit interne ne fait pas l'évaluation du systèmes informatique. Il se limite aux aspects comptables . le système informatique n'est donc pas connu et apprécié de ce service important de contrôle dans la société.

123- risques

- il existe des possibilités de traitements malveillants avec la complicité d'informaticiens

124- recommandations

- Il faut développer un programme ou paramétrer les applications en vue de crypter les mots de passe.
- Il faut créer une responsabilité, audit informatique , dans le service audit.

13- Contrôles de mise en place des systèmes

131- Points forts

- Un schéma directeur existe qui a été mis en place avec l'assistance d'un cabinet. La SICOGI dispose donc d'un conducteur pour sa politique informatique.
- La formation au paramétrage des applications a été faite pour les informaticiens. Ils peuvent donc effectuer des paramétrages correctes de ses applications.
- Les utilisateurs ont bénéficié de séminaires de formation auprès des fournisseurs pour certains progiciels. Ils s'y familiarisent plus facilement et les utilisent mieux.
- Des tests sont effectués sur les applications développées avant leur mise en service. Sur les fonctionnalités qui ont été commandées, un minimum d'accord est effectué sur les résultats avant leur exploitation.

132- Points faibles

- Il n'existe pas de manuel des procédures formalisées , notamment au niveau de la D C E et de la D A F. Un important outil de gestion fait ainsi défaut. En plus des procédures sont liées à des personnes qui deviennent irremplaçables.
- Le schéma directeur élaboré depuis 1993 est dépassé. Il ne permet plus de conduire la politique informatique de façon efficace.
- Il n'existe pas de cahier de charges pour l'acquisition des matériels et des logiciels applicatifs. Il n'est donc pas fait une analyse des capacités mémoires, des spécifications techniques, de la conformité des spécifications fonctionnelles avec les besoins utilisateurs, etc..
- Les utilisateurs n'ont pas été formés, ni même associés au paramétrage de certaines applications. Ils sont donc trop dépendants des informaticiens.
- Les utilisateurs n'ont pas été suffisamment formés à l'utilisation de certaines applications importantes (gestion des A D P). Ils ont beaucoup de difficultés à les maîtriser.

133- Risques

- Le manque de manuel des procédures peut entraîner une insuffisance de rigueur et de contrôle dans le processus de gestion, mais aussi des comportements de gestion incohérents et même des erreurs.
- Des investissements lourds et coûteux peuvent s'avérer inadaptés aux besoins actuels de l'entreprise. D'ailleurs du matériel et des logiciels applicatifs acquis à grands frais et non utilisés existent.
- Le paramétrage réalisé par les informaticiens risque de ne pas satisfaire à tous les besoins des utilisateurs.
- Des applications risquent de n'être utilisées que partiellement.

134- Recommandations

- L'élaboration d'un manuel des procédures s'impose à l'entreprise.
- Il faut actualiser le schéma directeur informatique en tenant compte de la stratégie de développement et des moyens de l'entreprise.
- Une analyse des offres et des choix doit être effectuée pour toute acquisition de matériels et de logiciels applicatifs pour une meilleure adéquation avec les besoins utilisateurs.
- Il faut former les utilisateurs au paramétrage de toutes les applications et les impliquer à leur réalisation en vue de réduire les fréquentes interventions des informaticiens auprès d'eux.
- Toutes les applications doivent faire l'objet d'une formation pour les utilisateurs.

PARAGRAPHE 2 : LE CONTROLE DES SECURITES INFORMATIQUES

21- tests d'évaluation des sécurités

211-sécurité physique

Nous avons interrogé le chef du SMIM ; chargé de la sécurité du matériel, des logiciels et du réseau.
Il ressort de cet entretien que des dispositions sont prises pour isoler des serveurs, les contacts avec des personnes hors du service. Il est aussi pris des dispositions pour Le conditionnement à basse température et la prévention contre les atteintes à l'intégrité physique des systèmes.

Nous avons alors demandé à prendre connaissance des procédures relatives aux comportements en cas d'incendie ou d'accidents, mais aussi des conditions de conservation des sauvegardes amovibles.

212- la sécurité logique

La sécurité logique à la SICOGI consiste à l'attribution des autorisations d'accès aux fichiers de données et de programmes, en l'empêchement d'intrusions externes, en la protection contre les virus et en la sauvegarde des fichiers.

Nous avons alors effectué des tentatives d'accès au réseau à partir d'un poste de la comptabilité pour entrer dans le système de facturation de la DCE. Nous n'avons pas pu y accéder.
Nous avons vérifié trois fois en arrivant parmi les premiers chez le client que les sauvegardes de la nuit sont effectives. Nous avons alors procédé à une lecture des bandes magnétiques et vérifié que des traitements de la veille sont dans les sauvegardes.

Cependant la régularité des procédures manuelles de sauvegardes et de sécurité en général n'est pas acquise.

22- Evaluation de la sécurité physique

211- Points forts

- Les serveurs et onduleurs sont dans une salle fermée à clé détenue par le chef du SMIM. Un contrôle d'accès est donc effectué sur ces éléments.
- Les onduleurs sont suppléés par un groupe électrogène de secours. Il y a donc une continuité d'alimentation électrique du système et une possibilité d'arrêt dans les bonnes conditions le cas échéant.
- Les salles sont climatisées. Le conditionnement des ordinateurs favorable.
- Il existe un détecteur d'incendie et un système manuel d'extinction. Le risque incendie est donc minimisé.
- Le câblage est protégé par une goulotte. Les câbles de transmission sont donc isolés et protégés des accidents.

212- Points faibles

- Il n'existe pas de procédure formelle indiquant la conduite à tenir en cas d'accidents. La gestion d'un accident sera difficile voire impossible.
- Il n'existe pas d'armoire ignifuge, pour la conservation de supports et consommables amovibles. Ces supports ne sont donc pas protégés selon les normes.
- La porte d'entrée du serveur n'est pas blindée. En cas d'accident (incendie par exemple) la propagation du feu peut atteindre la salle des serveurs.
- Les sauvegardes hors site se font à domicile. Elles peuvent donc être à la porté de personnes non professionnelles et donc faire l'objet de manipulations inadaptées.

213- Risques

- En cas d'accident, il pourrait y avoir une panique générale, et une mauvaise utilisation des ressources et des secours éventuels.
- En cas d'incendie et des propagations du feu, les postes sensibles ne sont plus protégés (serveurs).
- Les sauvegardes à domicile ne garantissent pas une bonne protection et un niveau de confidentialité acceptable.

214- Recommandations

- Une procédure formelle de sécurité doit être élaborée et diffusée au personnel.
- Il faut à l'entreprise un coffre fort ignifuge pour ses besoins de conservations et de sauvegarde.
- La salle des serveurs doit être isolée et sécurisée à tout point de vue.
- Les sauvegardes hors site doivent être le fait d'entreprises spécialisées, assurées et pérennes.

22- Evaluation des sécurités logiques

221- Points forts

- L'accès aux fichiers de données se fait par mot de passe et identifiant personnels. L'accès est donc contrôlé et réservé aux gestionnaires de ces fichiers.
- Les identifiants sont invalidés après cinq tentatives d'accès illicites. Cela permet de contrôler les tentatives d'accès illicites.
- Il existe des sauvegardes des données et des programmes. Chaque jour, à partir de une heure du matin, une sauvegarde différentielle automatique du contenu des disques des serveurs de la DAF et de la DCE est effectuée sur cartouche (trois cartouches par semaine). Les bases de facturations sont sauvegardées manuellement chaque soir par le chef du bureau production. Une autre sauvegarde est effectuée avant chaque mise à jour des comptes clients. Il est ainsi possible de restaurer ces données en cas d'accident.

- Il existe un logiciel antivirus mis à jour chaque deux mois. Le risque d'attaques par virus est limité.
- Des mouchards sont générés en cas de tentative d'accès illicite pour ainsi signifier les intrusions indésirables.

222- Points Faibles

- Il n'existe pas une politique de mise à jour régulière des mots de passe dont certains ne sont pas cryptés. Ils peuvent donc passer entre les mains de personnes autres que leurs destinataires .
- Le renouvellement des mots de passe ne se fait pas automatiquement. Les délais de renouvellement sont donc décidés façon subjective.
- Les tentatives d'accès illicites, ne sont pas journalisées et revues. Les cause, les origines et les motivations ne sont donc pas connues et analysées, et les solutions pour

les combattre ont moins de chances d'être efficaces.

- Les sauvegardes de certains fichiers et de programmes ne sont pas automatiques. Souvent, elles ne sont pas faites par oublie ou par indisponibilité du responsable en charge.
- Il n'existe pas de procédures formelles de restauration des fichiers et des données en cas de catastrophes. Une telle restauration est, soit fortement liée à une personne, soit faite par tâtonnement.

223- Risques

- La protection et la confidentialité des fichiers et données ne sont pas garanties.
- Certains utilisateurs malveillants peuvent utiliser les mots de passe de leurs collaborateurs en vue de modifier le contenu de certains fichiers.
- Pour les tentatives d'accès illicites il est impossible de les analyser en vue d'en déterminer les causes, les origines et les objectifs.
- Il est possible qu'il y ait des omissions de sauvegardes du fait que celles ci se font manuellement.
- En cas d'incendie grave, la restauration des fichiers et des données peut s'avérer difficile.

224- Recommandations

- Les mots de passe doivent être tous cryptés, renouvelés périodiquement et de façon automatique.
- Il doit être mis en place un registre de journalisation des tentatives d'accès illicites.
- Les sauvegardes de fichiers de données doivent être automatisées.
- Une procédure formelle, de restauration de fichiers de données doit être élaborée et régulièrement mise à jour.

SECTION 2 : ANALYSE DES APPLICATIONS INFORMATISEES

Cette analyse à été obtenue à la suite :

- Des évaluations faites sur les descriptions du fonctionnement des applications. En effet, nous avons effectué des tests de conformité grâce à des extractions et analyses de fichiers de données dont les résultats ont été exposés plus haut.

- De l'administration d'un questionnaire de contrôle interne dont un extrait est présenté en annexe 1.

- Mais surtout des tests techniques qui ont consisté à l'exploitation en réel des systèmes afin d'identifier des dysfonctionnements éventuels. De manière générale, ces tests ont consisté à vérifier :

  - la fiabilité des traitements (par le suivi de certains traitements) ;
  - la sécurité des accès et de l'utilisation des applications (par des tentatives d'accès non autorisées) ;
  - l'adéquation fonctionnelle aux besoins spécifiques de la SICOGI
  - etc.

Nous avons donc regroupé nos résultats sous les rubriques suivantes :

- adéquation fonctionnelle,
- fiabilité de l'application , étant entendu que la fiabilité des traitements et la sécurité y concourent tous les deux ;
- satisfaction des utilisateurs sur la base des entretiens effectués avec eux.

PARAGRAPHE 1 : TESTS D'EVALUATION

11-adéquation fonctionnelle :

Nous avons recensé les besoins opérationnels des utilisateurs d'un côté, et de l'autre côté, nous nous sommes fait établir par le SIMM une cartographie des applications qui retrace leurs fonctionnalités respectives.

Nous avons alors rencontré les utilisateurs pour confirmer que ces fonctionnalités sont effectives sur les applications.

Nous avons enfin procédé à quelques vérifications comme par exemple :

- La classification des locataires par zone géographique qui nous a par ailleurs permis un rapprochement avec le nombre de locataires (LS, LV et VPL).
- Nous avons pu assister à la génération des factures du mois de juin 2001 qui se fait par type de contrat (LS, LV, VPL)
- Il est prévu une édition des états de déclarations mensuelles et annuelles pour les impôts et la CNPS qui n'est pas effective.
- etc..

12-la fiabilité des applications

Nous avons pour cela suivi le traitement de certaines opérations.

Au service commercial, bureau gestion des A D P , nous avons pu simuler l'ouverture d'un compte pour l'achat d'un appartement quatre (4) pièces. Nous avons remarqué qu'il était possible de changer le nombre de pièces par cinq, trois ou deux sans modifier le montant d'ouverture du compte. Inversement, nous avons modifié le montant de l'apport initial, cela modifie le code mais pas le nombre de pièces.

Nous avons effectué notamment le calcul de la PIDR. Après avoir exporté les données sur micro ordinateur nous les avons introduit selon le programme de référence dont dispose le cabinet. Nos résultats étaient supérieurs d'au moins ¼ de la valeur calculée par la SICOGI.

Etc…

PARAGRAPHE 2 : APPLICATION GESTION DE LA FACTURATION

Il faut avant tout remarquer que cette application est un produit spécifique de la maison. Elle a été développée par le SMIM pour les besoins spécifiques de l'entreprise. Elle a pour objectif de gérer, les logements, la facturation et le recouvrement.

21- adéquation fonctionnelle

211- points forts

- l'application est dotée des fonctionnalités suivantes :
  - Gestion des logements.
  - Gestion de la facturation.
  - Gestion des recouvrements.
  - L'application permet une classification des locataires par zone géographique.
  - Elle donne le nombre de logement que gère la SICOGI

Ces fonctionnalités sont spécifiques à la gestion immobilière

- Le quittancement est généré automatiquement par l'application mensuellement. Les erreurs et les malversations sur les quittances de loyer sont ainsi réduites.

212- points faibles

- L'application ne gère pas les opérations relatives aux anciens ayants

droit pour environ 210 logements. Le suivi de ces opérations s'effectue manuellement.

- Certains états importants pour le suivi des opérations du service exploitation et de la comptabilité ne sont pas édités par l'application. Ce sont :
  - bilan des comptes locataires par catégorie et nature de contrat ;
  - ventilation du quittancement par catégorie de logement ;
  - ventilation du quittancement par catégorie et par produit ;
  - analyse des versements par Banque.

Il faut noter que ces états étaient édités par l'application précédente.
Certains contrôles de premier niveau ne peuvent être effectués sur ces états.

- L'application ne permet pas d'établir la balance des reports à nouveau et un grand livre de fin d'exercice.

- L'application ne permet pas de connaître l'historique d'un contrat locataire. Ce qui entraîne au besoin un recours au dossier papier. Des contrôles sur Le suivi des statuts locataires et leur changement sont difficiles et non exhaustifs.
- L'application ne permet pas de saisir des échéances de remboursement avec des mensualités variables. Les recouvrements des arriérés manquent de souplesses et font l'objet de rejet de la part des associations de locataires.
- L'application ne gère pas les pénalités de retard qui ont en conséquence été officiellement abandonnées, mais sont presque régulièrement perçues par les agents.

213- Risque

- La gestion des opérations relatives aux anciens ayants droit se faisant manuellement, les risques de manipulation et d'erreurs sont élevés.
- La non édition des états cités risque de laisser passer des erreurs, et même d'inciter à des actions malveillantes.
- Les analyses et contrôles des reports générés et des balances auxiliaires clients et comptes rattachés peuvent être erronés ou biaisés.

214- Recommandations

- L'application ayant été développée par l'entreprise, une modification par le SMIM s'impose pour prendre en compte les faiblesses révélées. Ce sont :
  - la gestion des opérations relatives aux anciens ayants droit
  - l'édition des états cités et même davantage pour couvrir les besoins des utilisateurs ;
  - l'établissement d'une balance des reports à nouveau et d'un grand livre de fin d'exercice.
  - la saisie des échéances de remboursement avec des mensualités variables.
  - La prévision de pénalités de retard.

- Un Cahier des charges doit être rédigé par les utilisateurs pour prendre en compte tous leurs besoins fonctionnels.

22- fiabilité de l'application

221- Points faibles

- Les dates d'échéances des contrats sont saisies manuellement par les utilisateurs, suite à l'opération transfert des données de l'ancien système vers le nouveau.
- L'application ne s'adapte pas au changement du mode de paiement (espèce à virement et vice-versa). En effet, lorsqu'un client qui règle en espèces décide de le faire par virement, le système continue de le quittancer en espèces, malgré le changement effectif du mode de paiement, et vice-versa. Ces cas sont donc traités manuellement.
- Le passage d'un client ordinaire en gros clients engendre parfois des problèmes, comme cet employé d'Air Afrique référence 6101021890 qui se trouve actuellement avec deux comptes dans la base de facturation, avec les mêmes mouvements, mais présentant des soldes différents.

- La mutation entre deux employés d'un gros client pose également des problèmes de suivi des deux comptes. En effet le gros client étant identifié par un seul numéro de compte, le système n'arrive pas à distinguer le nouvel employé de l'ancien. Ainsi tous les versements effectués par l'un, passent sur son ancien compte donc au profit de son copermutant, de sorte qu'il est difficile d'établir la situation exacte des deux employés séparément.

- L'application ne produit pas d'états de synthèse des comptes locataires (situation des OD, situation des versements, état de répartition des quittances) des contrôles ne sont donc pas effectués à ce niveau.
- Les reports à nouveaux sont générés par un traitement automatique lancé par le service informatique après l'autorisation de la D C E. Cependant, Il n'existe aucune trace (balance des à nouveaux), après la génération de ces écritures pour d'éventuels contrôles.
- Les états et documents (décision d'arrêt de quittancement, avis de vacance, début de location, mutations etc..) sont transmis en retard entre les services exploitation et commercial. Des contrôles ne sont fait qu'à posteriori.

222- risques

- Compte tenu du fait que les dates d'échéance des contrats déterminent le critère d'arrêt de quittancement, leur traitement manuel ne garanti pas la fiabilité des fins de contrats.
- La non adaptation du système au changement du mode de paiement peut entraîner des doubles emplois tout comme le passage d'un client ordinaire en gros client.
- Le traitement des mutations entre les employés d'un gros client peut entraîner des confusions au niveau des comptes individuels, et peut faire perdre de l'argent.
- Des écarts significatifs existent entre les états mensuels de réparation des quittances émis par le service exploitation, enregistrés par la comptabilité et les états manuels de synthèse établis par le même service exploitation en fin d'année.

- Le traitement manuel des états de synthèse des comptes locataires peut entraîner des écarts significatifs par rapport aux états de synthèse programmés. C'est d'ailleurs le cas entre les états mensuels de répartition des quittances émises par le service d'exploitation, enregistré par le service comptabilité et les états manuels établis par le même service exploitation.

- Le traitement des reports à nouveau empêche tout contrôle de l'exactitude des soldes clients reportés sur l'exercice suivant.
- Les retards de transmission des états et documents, peut entraîner des traitements erronés des comptes. Comme c'est le cas du compte de régularisation qui traîne depuis plusieurs années un solde créditeur de 42.918.538 F.

223-Recommandations

- Le SMIM devrait programmer les dates de fin de contrat pour éviter les manipulations éventuelles.
- Une revue de l'application s'impose, qui devrait la rendre plus souple en vue de l'adapter aux différents changements de comportements de la clientèle :
    - mode de paiement (espèce à virement et vice versa)
    - type de client (client ordinaire à gros client et vice versa)
    - mutation entre clients, employés de gros clients.
    - etc..

- Les états de synthèse nécessaires à l'analyse et au contrôle doivent être automatisés (situation des OD, situation des versements, états de répartition des quittances, balance des à nouveaux etc..)
- Une procédure de développement des applications doit être mise en place et rigoureusement respectée.

23- Satisfaction des utilisateurs

231-Points forts

- L'installation de l'application a été relativement facile, les transferts de données ont été effectués de façon satisfaisante.
- L'application n'est pas trop gourmande en ressources (30 MO de disque), il reste assez de capacité pour les traitements.

232- Points faibles

- Lors du lancement de certains traitements, l'utilisateur perd le contrôle du système. C'est le cas pour le traitement des éditions des locataires copropriétaires par ordre alphabétique, qui bloque le système et entraîne des suspensions du système.
- En consultation, le système n'affiche pas le solde global du client par rapport aux versements qu'il a effectués et au montant de vente. Le contrôle de la situation nette du client n'est pas fait.
- L'application manque de convivialité et de souplesse. En effet, lors des tests fonctionnels, il est apparu des messages d'erreurs.

Exemple : l'édition du retrait de gros clients génère une erreur d'ouverture de fichier ou des blocages systématiques, obligeant les utilisateurs à sortir de manière inopinée de l'application en perdant les données non enregistrées.

- De nombreux traitements et contrôles sont effectués manuellement compte tenu de l'absence de certaines fonctionnalités et états avec leurs corollaires d'erreurs. Cette situation amène les utilisateurs à se désintéresser de l'application.

233- Risques

- La rigidité de l'application et / ou la perte de contrôle du système peuvent entraîner

des manipulations aux conséquences imprévisibles en cas de panique d'un utilisateur.

- Le traitement peut recouvrir des erreurs, notamment sur le solde global du client et ses inducteurs, par rapport aux versements qu'il a effectués.
- Cela peut aussi inciter à des détournements de recouvrements et de règlements de clients.
- Les traitements et contrôles manuellement effectués peuvent recouvrir des erreurs ou faire l'objet de manipulations.

234- Recommandations

- Les causes des différents blocages du système évoqués doivent être recherchées et corrigées.
- Pour chaque client engagé dans les opérations de vente, il est important de connaître à tout moment le solde de son compte et la date d'échéance et d'en apprécier le respect de son contrat.

- L'affichage systématique du solde client à chaque consultation doit être programmé dans l'application.

PARAGRAPHE 3 : APPLICATION SAARI NEGOCE

Ce progiciel acheté permet de gérer les ADP (accession directe à la propriété) et les achats.

31- Adéquation fonctionnelle

311- Points forts

L'application est dotée des principales fonctionnalités suivantes :

- Gestion des clients (mise à jour, suivi des comptes)

- Suivi des encaissements
- Gestion des fournisseurs (mise à jour, suivi des comptes)
- Gestion des articles (inventaire, contrôle de stock)
- Edition des stocks

C'est une application de gestion des stocks qui a été paramétrée pour la gestion immobilière,

312- Points faibles

- L'application ne prend pas en compte le numéro du chèque lors de la saisie des règlements . il est donc impossible de faire des vérifications et des rapprochements avec les chèques d'origine.
- Il est impossible d'éditer un reçu de paiement, ainsi que la liste des règlements par banque. Il est donc impossible de faire certains contrôles sur pièces .
- Les opérations suivantes :
  - désistements,
  - remboursements ;
  - transfert ou mutation ;
  - complément sur apport initial (crédit bancaire) ;
  - etc..

ne sont pas gérées par le système.
Ils sont donc faits manuellement avec leurs corollaires d'erreurs et de malversation

- Il est impossible de déterminer directement le prix d'achat moyen pondéré sur le prix toutes taxes comprises. (gestion des stocks). Des erreurs figurent donc dans le traitement de ces achats.

313- Risques

- Les contrôles éventuels sur les règlements par chèque sont difficiles. Ces

règlements peuvent faire l'objet de traitements erronés ou malveillants.

- Un reçu de paiement et la liste des règlements par banque sont des éléments importants sans lesquels subsiste une insuffisance de contrôle ou d'analyse.
- Les traitements fastidieux (suppression, création et modification de données) des opérations ci-dessus cités et sur les achats, les assujettissent à des erreurs ou des manipulations.

314- Recommandations

- Le programme de l'application doit prendre en compte davantage de paramètres fonctionnels pour une plus grande efficacité . notamment :
    - les numéros des chèques saisis,
    - les éditions de reçu de paiement, de liste des règlements par banque,
    - la gestion automatisée des opérations de
        - désistements
        - remboursements
        - transfert ou mutation
        - complément sur apport initial
        - etc..
- Calcul du prix moyen pondéré sur prix d'achat toutes taxes comprises.

32- Fiabilité de l'application

321- Points forts

- La documentation nous paraît acceptable qui prend en compte la maintenance, l'exploitation, l'utilisation, les sauvegardes, etc.. elle permet la formation et le recours en cas de nécessité.

322- Points faibles

- Sur la fiche client, des zones texte sont utilisées pour la saisie des montants ou des dates. Cette utilisation n'est pas conforme aux spécifications techniques .

- En saisie des décomptes, le système n'effectue aucun contrôle entre le code saisi (qui engendre automatiquement l'apport initial sur logement) et le nombre de pièces du logement qui justifie cet apport.

323- Risques

- Le système prédispose à des risques d'erreur ou de manipulation car, Il n'effectue aucun contrôle de conformité et de cohérence sur les zones textes.

324- Recommandations

- Le système doit établir des contrôles sur les traitements cités ci-dessus :
- En rejetant ou signalant par toutes sortes de moyens, les caractéristiques spécifiques à la monnaie et aux dates,
- En établissant une correspondance entre le code, l'apport initial et le nombre de pièces du logement.

33- satisfaction des utilisateurs

331- Points forts

- L'application est d'une utilisation conviviale.
- La documentation relative est fournie et est d'une lecture aisée.

332- Points faibles

- Les utilisateurs procèdent à des traitements lourds en lieu et place des traitements

automatisés qui font défaut pour les opérations de

- désistement
- remboursement,
- transfert ou mutation,
- complément sur apport initial.

- La situation détaillée des consommations de fournitures par service pour le compte de la direction générale est faite manuellement et avec difficulté par manque d'états statistiques automatisés classés par rayon, famille, sous-famille. Des erreurs subsistent.

- Les prix d'achat moyen pondérés sont calculés manuellement avant d'être saisis dans le système. Ils manquent de précision et sont sujets à des erreurs.

333- Risques

- Les traitements manuels et lourds effectués sont sources d'erreurs et de manipulation. Par exemple, il est courant d'avoir :
  - un logement déclaré vacant alors qu'il est occupé
  - un faux montant d'apport initial sur le décompte.
  - la non prise en compte de frais de dossiers
  - etc..

334- Recommandations

- Les traitements manuels doivent être automatisés, et les utilisateurs formés à les exploiter.

- Les états statistiques doivent être programmés pour les besoins.

PARAGRAPHE 4 : APPLICATION PAIE CS

41- Adéquation fonctionnelle

411- Points forts

- L'application est active pour les fonctionnalités suivantes :
  - gestion du personnel, des départs (licenciement, retraite…)
  - gestion des prêts, calcul des salaires, édition des bulletins ;
- Edition des états de déclarations mensuelles et annuelles des impôts et CNPS ;
- L'application édite les bulletins de salaires conformément aux réglementations en vigueur.
- Les départs à la retraite sont automatiquement versés dans un fichier à la date d'échéance
- Les éditions de bulletins de salaire cessent à la date du départ.

Ces spécifications sont demandées par la comptabilité .

412- Points faibles

- L'application ne gère pas automatiquement le calcul des départs en congés et à la retraite. Le programme nécessite des sous calculs manuels.
- Les contractuels (en moyenne 50 / mois) ne sont pas gérés par le système. Ils font l'objet de traitements irréguliers.
- L'application ne permet pas l'édition des états de déclarations mensuelles et annuelles pour les impôts de la CNPS. Il sont traité manuellement, en retard et de façon irrégulière.

413- Risques

- Les calculs et contractuels non gérés par le système sont prédisposés à des erreurs

ou à des actes malveillants.

- Les états non édités risquent d'être assujettis à un contrôle insuffisant.

414- Recommandations

- Les calculs des provisions pour indemnité de départ en congé ou à la retraite doivent être programmés correctement.
- La gestion des contractuels doit être introduite dans le système.
- Les éditions des déclarations fiscales doivent être corrigées.

42- Fiabilité de l'application

421- Points forts

- Une documentation relative à l'application est disponible pour les éventuels recours..
- Les traitements des salaires courants sont conformes aux réglementations en vigueur.
- Les dates de départ à la retraite prises en compte par l'application sont conformes à la réglementation en vigueur .

422- Points faibles

- Le calcul des droits de départ (licenciement, retraite) par le système n'est pas correct en regard à nos calculs référentiels.

423- Risques

- Le calcul des droits de départs étant manuel, il n'est pas à l'abri d'erreur et de

manipulations malveillantes.

424- Recommandations

- Le programme de calcul des droits de départ doit être corrigé et adapté aux conditions en Côte d'Ivoire.

43- Satisfaction des utilisateurs.

431- Points forts

- L'utilisation de l'application est conviviale,
- Une documentation utilisateur est disponible pour les recours éventuels.

432- Points faibles

- Les utilisateurs sont obligés de faire les calculs de départ en congé, départ à la retraite et licenciement, manuellement pour une bonne part et les erreurs ne manquent pas.
- Les bulletins et les dates de fin de contrat des contractuels sont gérés manuellement, avec leur lot d'irrégularité.
- Les états de déclaration pour les impôts et la CNPS sont gérés manuellement.

433- Risques

- Les risques d'erreurs et de manipulations malveillantes sont élevés.
- Les utilisateurs se découragent et se désintéressent de leur système.

434- Recommandations

Il est impératif de prendre en compte les besoins exprimés par les utilisateurs. Ce sont :

- La correction des programmes de calcul des droits de départ et une formation adéquate des utilisateurs.
- La programmation des bulletins et les dates de fin de contrat pour la gestion des contractuels.
- L'automatisation des éditions des états de déclaration pour les impôts et la CNPS.

PARAGRAPHE 5 : APPLICATION COMPTABILITE 500 ET TIERS.

Ce progiciel est d'une acquisition récente en remplacement d'une version Saari Major V.8.01 qui n'arrivait plus à gérer un volume important d'informations. En plus, le fournisseur ne garantissait plus la maintenance que sous réserve d'un changement vers une nouvelle version .

51- points forts

- Ce progiciel acquis comporte les fonctionnalités suivantes.
  - Enregistrements comptables ;
  - Lettrage, rapprochements ;
  - Edition des états comptables (grand livre, balance, bilan…) ;
  - Suivi des tiers (gestion des clients, gestion des francs…)

Ces fonctionnalités sont demandées par la comptabilité.

- La formation des informaticiens et des utilisateurs à ce progiciel est assurée par le fournisseur.

52- Points faibles

- Les utilisateurs ne maîtrisent pas encore leur application malgré la formation reçue, ils en sont encore à une phase de découverte et d'apprentissage.
- L'installation et le paramétrage de cette application se poursuivent. Des erreurs sont à prévoir.
- La comptabilité prend beaucoup de retards.

53- Risques

- Il faut s'attendre à beaucoup d'erreurs dans l'utilisation de ce système en attendant sa maîtrise totale par les utilisateurs.

54- Recommandations

- Le processus d'installation du système doit s'accélérer.
- D'autres rencontres utilisateurs / formateurs sont nécessaires pour une plus grande, et rapide maîtrise du système.
- Le contrôle des comptes en comptabilité doit ratisser large (full – contrôle) pour garantir une opinion justifiée.

CONCLUSION PARTIELLE

Nous rappelons que notre évaluation du CI de la SICOGI porte sur

- la qualité des applications mises en exploitation
- l'adéquation des choix matériels
- L'organisation et les ressources humaines du SMIM
- les procédures de gestions et d'exploitations des systèmes informatiques.

1) **qualité des applications mises en exploitation**

Les applications de notre échantillon présentent beaucoup de faiblesses, notamment :

- au niveau de leur adéquation fonctionnelle avec les besoins opérationnels
- au niveau de la fiabilité des traitements effectués.

Ce qui justifie par ailleurs les nombreuses plaintes des utilisateurs.

2) **adéquation des choix matériels**

La SICOGI a fait des efforts en matière d'équipement en matériel informatique et de logiciel. Le problème est que tous ces investissements ne se font pas dans le respect du schéma directeur qu'elle a élaboré et qui se trouve par ailleurs dépassé aujourd'hui.

3) **organisation et ressources humaines du SMIM**

Du point de vue des ressources humaines, le SMIM dispose d'un personnel qualifié pour réaliser sa mission, au vu des fiches signalétiques du personnel dont nous avons retracé les grandes lignes dans le Tableau n° 4.

Du point de vue organisationnel, des efforts sont à faire(séparer des fonctions incompatibles, créer un profil de carrière compétitif, etc.)

4) **procédures de gestion et d'exploitation des systèmes**

Le système de sécurité informatique de la SICOGI nous paraît acceptable dans un environnement immédiat (en espace et temps). Mais il n'est pas indéfiniment inviolable . Avec l'avènement d'Internet et des réseaux inter urbains, de nouvelles portes s'ouvrent aux éventuels Hackers dont elle doit déjà se protéger.

PERSPECTIVES DE MISE EN ŒUVRE DES RECOMMANDATIONS

1- Création d'un comité informatique

Un Comité informatique doit être créé sur l'initiative du conseil d'administration avec une autorité suffisante. Il pourra y être représenté :

- la direction générale,
- le service informatique,
- et les utilisateurs.

Sa mission sera alors :

- la mise en place d'une véritable politique informatique en commençant par la révision du schéma directeur informatique,
- le suivi de sa mise en œuvre.
- L'élaboration et le contrôle des procédures de développement ou d'acquisition des applications et du matériel
- etc..

Il devra alors se réunir au moins deux fois par an.

Il est souhaitable que sa mise en place intervienne avant les nouveaux investissements en projet.

2- La création d'une responsabilité audit informatique

Au sein du service audit interne la création d'une telle responsabilité émane de la direction générale. Elle peut être confiée :

- soit à un auditeur formé à l'informatique.
- soit à un informaticien formé aux techniques de l'audit.

Une telle responsabilité sera placée sous l'autorité du chef du service audit interne.

La date de mise en œuvre dépendra du processus de spécialisation de l'agent choisi. Mais ce processus doit commencer dans les meilleurs délais.

3- Mise en place de procédures informatiques

Une procédure globale de la gestion informatique doit être mise en œuvre. Elaborée par le comité informatique ou par la direction générale à défaut, elle doit comprendre notamment :

- une procédure de développement et de maintenance des applications
- une procédure d'acquisition des applications sur le marché
- une procédure d'exploitation des applications
- une procédure utilisateur pour le traitement de l'information
- une procédure de sécurité.

Le suivi de ces procédures pourra alors être régulièrement évalué par le service d'audit interne.

CONCLUSION GENERALE

L'appréciation du C I des entreprises informatisées se fait à deux niveaux comme le préconisent (OBERT 1995 ; COOPERS & LYBRAND 2000 ; ATH 1991 ; JENKINS &PINKNEY 1984 ; CNCC 1995 etc.) et ce sont ;

- les contrôles généraux informatiques;
- les contrôles d'applications informatisée.

- **Pour les contrôles généraux informatiques** ;

L'O.E.C. (in OBERT ; 1995) recommande d'apprécier :

- l'organisation (séparation de fonctions étude, exploitation et utilisateurs; développement etc. ...)
- la sécurité, la sauvegarde et la reprise des travaux .
- les procédures d'exploitation, etc.
- les procédures de développement des applications, de mise en exploitation, la documentation etc.

- **Pour les contrôles d'applications informatisées**, il suggère d'apprécier :
  - les données d'entrée dans le système,
  - les traitements et les fichiers ,
  - les sorties et les résultats.

A la SICOGI, le dispositif de C.I mise en place présente beaucoup de faiblesses tant au niveau des contrôles généraux informatiques que des contrôles applicatifs.

- **Au niveau des contrôles généraux informatiques.**

Les systèmes de sécurité sont acceptables, la documentation existe ; le personnel informatique est qualifié, des tests informatiques sont effectués etc.

Cependant, des efforts restent à fournir au niveau , de la séparation des fonctions, du suivi d'une politique informatique

- **Au niveau des contrôles applicatifs**

Il existe beaucoup de faiblesses, tant de conception que de fonctionnement respectivement sur l'adéquation de leurs fonctionnalités aux besoins opérationnels que sur les renseignements des fichiers et la fiabilité des traitements .

La SICOGI dispose donc d'un personnel informatique qualifié pour une insuffisance de résultat. Nous sommes certainement en face d'un problème d'organisation. C'est pour cela que nous proposons la création d'un comité informatique mais aussi la création d'un poste d'auditeur informatique clairement responsabilisé et la mise en place de procédures de gestion de l'informatique.

BIBLIOGRGRAPHIE

I- OUVRAGES

1- ATH (1991), Audit Financier, Guide pour l'audit de l'information financière de l'entreprise, édition Clet
2- BARRY Mamadou (1994), audit et contrôle interne
3- CNCC (1992), appréciation du contrôle interne, CNCC édition
4- CNCC (1992), démarche et organisation de la mission générale Tome 2 CNCC édition
5- CNCC (1995), la démarche du commissaire au compte en milieu informatisé CNCC édition
6- COOPERS & LYBRAND (1998), (2000), la nouvelle pratique du contrôle interne
7- COLLINS Lionel & VALIN Gérard (1992), audit et contrôle interne, Dalloz
8- DERRIEN Yann (1992) techniques de l'audit informatique Edition Dunod Paris
9- FAIVRE Claude & LOREAU Yvon Michel (1993), l'audit de la micro-informatique, Publi-Union
10- IFACI (1995), la conduite d'une mission d'audit interne, Dunod
11- JENKINS Bryan ; & PINKNEY Anthony, (1984), audit des systèmes et des comptes gérés sur informatique Dunod Paris
12- KPMG (1996), le Kpmg audit servises (KAS),
13- KPMG (1996), l'environnement de contrôle des systèmes d'information I & II
14- LAMY Jean Paul (19996), Audit et certification des comptes en milieu informatisé, les éditions d'organisation
15- LAMY Jean Paul , (1997) l'audit en milieu EDI Edition CNCC
16- MIKOL Alain
17- OBERT Robert, (1995) révision et certification des comptes, Dunod Paris
18- THORIN Marc (2000), L'Audit informatique, hermès Sciences publication
19- RENARD Jacques (1998), théorie et pratique de l'audit interne, édition d'organisation

II- MEMOIRES ET MODULES DE COURS

1- ASSOUMANA Hassoumi (2000), l'audit face à l'informatique.
2- SARR Ababacar (2000), audit informatique

III- ARTICLES

1- ROUFF Jean Loup (février 2001) ; des concepts et des mots ; Audit n° 153
2- ROUFF Jean Loup (avril 2001), des moyens traditionnels toujours d'actualité Audit n° 154
3- BERGERET Florence (avril 2001), des outils informatiques en plein essor pour une utilisation accrue, Audit n° 154
4- VIDAUX François (avril 2001) ; l'informatique, un facteur d'innovation pour l'analyse des risques ; Audit n° 154
5- MORRISSEY Patrick (avril 2001) ; des milliers d'informations disponibles concourent à la réussite des missions ; Audit n° 154
6- BOUANICHE José (juin 2001) ; COBIT, référentiel de gouvernance de l'informatique; Audit n°155
7- D'ANDIGNE Charles Henri (janvier 2002), le MOCI n° 1529
8- GATES Bill (janvier 2002) ; Microsoft donne la priorité à la fiabilité des logiciels ; Décision Micro réseau n° 492
9- Le chroniqueur masqué " YELLOW " (janvier 2002) ; attention à la prise d'en-tête ! Décision micro- réseau n° 492
10- BEDIN François (janvier 2002) ; sept ultra portables ; décision micro- réseau n° 492
11- BIBARD Olivier (janvier 2002) ; Oracle consolide sa position décision micro

réseau n°492

12-REYNAUD Stéphane (janvier 2002) ; le 10 Gigabit Ethernet peut-il tuer A T M ? décision micro réseau n° 492

13-MAURY Laurent (janvier 2002) ; des « pots de miel » pour attirer les hackers décision micro réseau n° 493

14-ROSE Philippe (octobre 2001) ; sécurité…demain j'investis ; Le Monde informatique n° 910

ANNEXE 1 PROPOSITION DE QUESTINNAIRE DE CONTROLE INTERNE (QCI)

II1 TRAITEMENTS AUTOMATISES DES CYCLES

Procédures

	Réponses		observations
	O	N	
1. Les règles d'administration de l'activité exploitation sont-elles consignées dans un manuel de procédures ?		x	
2. Ce manuel de procédures prévoit-il ,notamment : • Une séparation entre les activités développement et exploitation ? • Une séparation des tâches d'exploitation et de contrôle au sein de l'activité exploitation ? • Une interdiction absolue aux équipes d'exploitation de corriger les erreurs ? • Une interdiction absolue aux équipes d'exploitation de modifier des procédures, des programmes et le contenu des fichiers ? • Des consignes en cas d'incidents ? • Des consignes en cas de sinistres ? • Une rotation à l'intérieur des équipes d'exploitation ? • Un accès limité à la documentation d'exploitation ?			
3. Les instructions d'exploitation pour les applications comprennent-elles, notamment : • Un descriptif du flux d'application ?. • Les procédures de paramétrage ? • La liste des fichiers nécessaires ? • Les procédures de sauvegarde, de restauration et de reprise ?	X		
4. Une copie de ces documentations est-elle conservée à l'extérieur de l'entreprise ?			

Supervision de l'exécution			
5 Le journal console, ou un produit programme complémentaire, est-il utilisé à des fins de contrôle a posteriori sur: • Temps d'exécution ? • L'utilisation des programmes ? • L'utilisation des fichiers ? • Contrôle des traitements finissant anormalement ?		N/A	

FONCTION INFORMATIQUE

ANALYSE DES RISQUES

1 la fonction informatique obéit-elle aux règles suivantes : • Détermination des objectifs . - à long terme ? - à moyen terme ? - informel. ? • Plan directeur ? • comparaison des résultats aux objectifs ?	 X X 	 X	
La direction Informatique est-elle : • Hiérarchiquement rattachée à un niveau lui donnant l'autorité nécessaire à l'exécution de ses objectifs ?. • Intégrée en tant que service aux utilisateurs dans l'entreprise ?	 X X		
les Procédures de séparation de fonctions sont-elles sasatisfaisantes ?: • Les informaticiens ne sont pas habilités à exercer des fonctions en dehors du champ d'action de la fonction informatique?,. • Les chefs de projet, analystes et programmeurs ne sont pas habilités à exercer des fonctions dévolues à l'exploitation et vice-versa pour les équipes d'exploitation? • Les ingénieurs système ne sont pas habilités à développer des applications, ou à exercer des fonctions d'exploitation?	 	 X	

4 L'interdiction est faite au service informatique de négocier seul les opérations ou de contrôler des biens de l'entreprise est-elle respectée ?			
II3 MATERIELS Analyse des risques			
CAPACITE			
1 Les capacités disponibles sont-elles satisfaisantes compte tenu de l'historique comptable présent ?			Pas toujours
2 Les temps d'accès sont-ils satisfaisants pour les utilisateurs.		x	
3 La puissance du matériel est –elle suffisante ?			
Procédures de sauvegarde et de maintenance			
4 Existe-t-il des procédures formalisées de sauvegarde et de restauration ?			
5 Les procédures de sauvegarde couvrent-elles également l'environnement de tests ?			
6 La périodicité des sauvegardes est-elle adaptée aux besoins de l'entreprise ?.....	x		
7 Pour les applications considérées comme vitales, est-il procédé à une duplication des sauvegardes ?.			
8 Un historique suffisant des jeux de sauvegarde est-il conservé ?.			
9 L'exploitation a-t-elle des consignes suffisantes pour mettre en œuvre correctement les restaurations ?.			
10 Les procédures de sauvegarde et de restauration sont-elles périodiquement testées ?			
11 Le respect des procédures de sauvegarde et de restauration fait-il l'objet d'un contrôle périodique a posteriori par l'audit interne et / ou le gestionnaire de la sécurité ?.....	x		
Procédures de reprises			

12 Existe-t-il, selon les spécificités de l'entreprise, des procédures de reprise adaptées • Reprise à chaud ?. • Reprise à froid ?. • Reprise à chaud et à froid ?			
13 Les procédures de reprise sont-elles périodiquement testées ?.			
14 Existe-il des procédures de stockage des sauvegardes hors site ?.	x		
15 Le stockage des sauvegardes sur le site et hors site est-il réalisé dans des armoires ignifuges		x	
16 Le stockage hors site est-il en dehors des locaux de la fonction informatique ?.....	x		
17 Le choix du mode d'ordinateur de secours a-t-il été décidé sur la base d'une étude coût /efficacité ?			
Maintenance			
18 Le contrat de maintenance matériel souscrit par la société est-il : • Préventif ?. • Curatif ?			
19 Les obligations de l'utilisateur ont-elles été définies dans le contrat de maintenance …			
20 Quel est le délai d'intervention prévu à partir d'une demande ? • Moins de 24 heures ?. • Moins de 48 heures • Moins de 5 jours ? • Non défini au contrat ?			
21 Les interventions dans le cadre du contrat de maintenance sur le matériel font-elles l'objet d'un compte rendu écrit ?			
Organisation de la sécurité			

22 Existe-t-il une stratégie de la sécurité portant sur la protection : • Des accès physiques ? • Des procédures de sauvegarde, restauration et reprise? • Un plan de sauvegarde en cas de destruction du patrimoine informatique physique ?.			
23 Cette stratégie a-t-elle été développée par des professionnels compétents en ce qui concerne la sécurité dite physique ?			
24 La sécurité physique est-elle coordonnée et supervisée par le responsable de la sécurité générale de l'entreprise, en liaison avec le gestionnaire de la sécurité ?.			
25 Cette stratégie est-elle périodiquement révisée pour tenir compte de l'évolution de la configuration et/ou de la structure du système d'information ?			
Accès physique			
26 Existe-t-il des procédures limitant l'accès physique aux actifs informatique : • Les utilisateurs ne sont pas admis dans les locaux de l'informatique? • Le personnel d'exploitation a, seul, accès à la salle machine? • Le personnel d'exploitation n'a pas accès à la bandothèque? • Les tiers accédant aux locaux informatiques font l'objet d'une autorisation préalable? • Les documentations ne sont accessible qu'aux personnes autorisées?	x X x		
27 Les procédures d'accès physique sont-elles renforcées par des systèmes de badge, de carte magnétique ou de code ?.	x		
28 La gestion du système retenu est-elle satisfaisante pour traiter les problèmes suivants : • Vol ? • Démission, licenciement ?. Changement périodique des codes ?.			

29 Le système de protection des accès physiques assure-t-il une protection 24 heures/24 par des procédés d'alarme ou de gardiennage ?	x		
30 Les ressources physiques de la fonction informatique sont-elles installées dans les locaux difficiles d'accès ?	x		
31 En cas de crise (mouvements sociaux, par exemple), les accès aux locaux informatiques peuvent-ils être fermés rapidement ?			
Incendie			
32 L'entreprise a-t-elle mis en place un système de détection : • Détecteur de fumée ?. • Détecteur de chaleur ?	 X x		
33 Existe-t-il des instructions incendies suffisamment connues du personnel informatique : • Interdiction de fumer ? • Volume de papier maximal acceptable à la salle machine ? • Nettoyage périodique, y compris dans les faux planchers ? • Actions à suivre en cas d'incendie ? • Etc. ?.	 X X		 Existe mais jamais tester
34 Les instructions incendies font-elles l'objet d'une formation adéquate et d'exercices périodiques ?.		x	
Dégâts des eaux			
35 Existe-t-il des procédures suffisantes permettant de prévenir ou de limiter les dégâts des eaux :? • Implantation adéquate ? • Détecteur du niveau d'eau dans les faux planchers ? • Faux planchers en pente ? • Etc.. ?			

Alimentation électrique			
36 l'installation comprend-elle un transformateur d'isolement et un régulateur de tension pour se prémunir des variations du courant électrique ?			
37 L'installation permet-elle la continuité de l'exploitation en cas de coupure électrique : • Volant d'inertie ? • Onduleur + batteries ?. • Onduleur + batterie + groupe électrogène ?. • Dispositions prises pour protéger les enregistrements contre la destruction accidentelles et assurer une exploitation continue ?			
38 Des méthodes générales visant à prévenir ou à déceler les erreurs accidentelles causées par un dérangement des appareils sont-elles mises en place ?.			
II4 LOGICIELS Analyse des risques			
Organisation et structure			
Structure			
1 Les structures permettent-elles un contrôle efficace sur la fonction informatique ?			
2. le service informatique est-il séparé des services exerçant des fonctions non compatibles • Négociation ou autorisation des opérations? • Enregistrement initial des opérations? • Garde des biens de l'entreprise (ex. moyens de paiement sur support papier ou magnétique) ?	X X X		

3. La division des tâches est-elle assurée dans le service informatique ? • Conception, programmation et exploitation de l'ordinateur? • Contrôle des données entrées et sorties? • Accès aux fichiers réglementé et limité au strict besoin de l'exploitation?		x	
4. La division des tâches a-t-elle été conservée dans les services utilisateurs ?.....			
Phase de développement interne			
5 L'étude fonctionnelle est-elle approuvée par les utilisateurs?			
6 Lors de recettes provisoires, les utilisateurs participent-ils réellement à la mise au point des jeux d'essais ?			
7 la recette provisoire des utilisateurs n'est-elle donnée que lorsque les résultats sur jeux d'essais sont satisfaisants			
8 En cas de développement de système sous SGBD, les phases de développement sont-elles coordonnées et supervisées par un gestionnaire de données, ou un technicien ayant une formation suffisante. Ce gestionnaire de données, ou ce technicien, s'assure-t-il de l'efficacité du développement en matière de :. • Définition des données de base et conception de la structure de la base de données ?... • Maintien des procédures nécessaires pour s'assurer de l'intégrité, de la sécurité, de l'exhaustivité et de l'exactitude des données ? • Exploitation de la base de données ?. • Amélioration des performances? • Définition des règles d'accès ? • Définition des procédures de sauvegarde, de restauration et de reprise ?			

9 En cas de conversion existe -t-il un contrôle sur la « montée en charge » des fichiers ou l'installation de la base de données ? si la réponse est oui, le contrôle donne –t –il une assurance suffisante que les données sur les nouveaux fichiers ou la base de données sont: • Exhaustives ? • Toutes enregistrées ?. • .Toutes enregistrées dans la bonne période ? • Exacte : validation suffisante sur l'exactitude des données ?.			
Modifications			
10 Les modifications de programmes et d'applications sont-elles soumises aux mêmes contrôles que les programmes nouveaux et applications nouvelles, à savoir : • interdiction faite aux opérateurs de modifier les programmes ? • contrôle des test effectués et de l'approbation finale des modifications ? • acceptation des changements par la section exploitation, uniquement si approuvés ?			
11 Un contrôle efficace dans la section exploitation empêche –t- il les modifications non approuvées ?			
12 Existe –t –il une séparation entre les activités de test et de production ?			
13 Toute modification n'est – elle testée qu'avec des jeux d'essai de l'environnement de test ?			
14 Toute modification fait – elle l'objet d'une demande écrite des utilisateurs ?			
15 Toute modification est – elle effectuée sur des copies de programmes ?			
16 La mise en production du programme modifié est – elle précédée de l'accord du responsable hiérarchique du programmeur et de l'utilisateur ?			
MAINTENANCE			
17 le contrat de maintenance application est-il : • Préventif ? • Curatif ?			
18 Les obligations de l'utilisateur sont-elles définies dans le contrat de maintenance ?....			
19 La périodicité des visites de maintenance est-elle suffisante pour une prévention efficace ?			

20 L'assistance lors de l'exploitation des applications est-elle fréquente ?	x		
21 L'assistance se fait-elle par : • Téléphone ?. • Envoi d'une disquette ou dépannage à distance ?. • Déplacement sur le site ?	 X X		
22 les mises à jour sont-elles : • Imposées par le concepteur? • Sur demande de la société ?			
23 les mises à niveau sont-elles : • Fréquentes ? • Inexistantes ?.			
24 les délai d'intervention sont-ils satisfaisants pour : • L'assistance ?. • Les mises à jours ?			
25 Toutes les interventions sur les logiciels dans le cadre du contrat de maintenance font-elles l'objet d'un compte rendu écrit ?.			
26 Les logiciels sont-ils : • La propriété de l'utilisateur ?. • Exploités avec une licence d'exploitation ? • Loués par l'utilisateur ?.			La SICOGI développe certaines applications
27 Toute la documentation concernant la mise en œuvre des logiciels est-elle en possession de l'utilisateur : • Disquette de base? • Mode opératoire? • Procédure écrite?	 X X		
FORMATION			

28 Y a-t-il eu une formation initiale des utilisateurs lors de la mise en place du système : • Formation externe ?. • Formation interne ?			Oui pour certaines applications mais pas toutes
29 Le niveau de formation des utilisateurs est-il cohérent avec les foncions occupées?			
30 La formation sur les logiciels systèmes et leur utilisation est-elle : • faite par stage ?. • Autodidacte ?.			
Documentation et procédures			
1 La documentation du système comprend-elle des informations suffisantes sur les domaines suivants : • Contrôles sur les tests avant réception finale du système par les utilisateurs ? • Examen des jeux d'essais et des productions en période de croisière ? • Sondage des fichiers ? • Essai de détection de toute manipulation de fichier par procédure « pirate »			
SECURITE			
Minimisation des risques internes à la fonction informatique			
32 Existe-t-il des procédures assurant l'intégrité des systèmes mis en production ?.....			

33 Ces procédures permettent-elles un contrôle suffisant dans les domaines suivants : • Protection contre les accès non autorisés ? • Journalisation des modifications ?. • Correspondance entre programmes d'exploitation sources et objets ?.			
34 Ces procédures font-elles l'objet d'un contrôle périodique à postériori par une personne indépendante, comme le gestionnaire de la sécurité ou de l'audit interne informatique ?.			
35 Le service informatique est-il séparé des services émetteurs et des services utilisateurs ?			
36 Les procédures suivantes sont-elles mises en place : • Séparation entre les fonctions de programmation et d'exploitation ? • Connaissance limitée des programmes par les opérateurs ? • Supervision de l'exploitation de l'ordinateur ? • Accès aux salles d'ordinateur limité au personnel d'exploitation ?.	 X x	 X	
37 Des méthodes générales visant à prévenir ou déceler les erreurs accidentelles causées par la faute de l'opérateur, par un dérangement des appareils ou par une lacune du programme sont-elles mises en place ?.			
38 Des méthodes permettant de reconstituer les fichiers à la suite d'erreurs mineures de traitement ou de destruction mineure d'enregistrements sont-elles mises en place. • Détection rapide des erreurs ? • Instructions précises concernant les conditions de correction d'erreurs et d'arrêt à la disposition des opérateurs ?. • Conservation de fichiers de secours ?.			
39 Les ressources logiques, y compris les commandes et les programmes utilitaires, auxquelles peuvent accéder les professionnels de l'informatique par terminaux ou consoles, sont-elles affectées en accord avec les règles de séparation des fonctions nécessaires à un bon contrôle interne ?			

37 Les ressources logiques, y compris les commandes et les programmes utilitaires, auxquelles peuvent accéder les utilisateurs de leurs terminaux , sont-elles affectées en accord avec les règles de séparation des fonctions nécessaires à un bon contrôle interne ?			
39 Les micro-ordinateurs ayant accès à l'unité centrale, sont-ils soumis à des règles de sécurité suffisantes, lorsqu'ils peuvent lire ou mettre à jour les ressources logiques ?.....			
Minimisation des risques externes à la fonction informatique			
38 Existe-t-il une stratégie de la sécurité des accès logique dans l'entreprise ?.....			
41 Cette stratégie a-t-elle été développée par une équipe pluridisciplinaire se composant d'informaticiens et d'utilisateurs ?.			
45 Cette stratégie est-elle mise en œuvre et supervisée par un gestionnaire de la sécurité suffisamment indépendant de la fonction informatique ?.			
46 Cette stratégie a-t-elle été développée selon un processus cohérent : • Etude de faisabilité, ?. • Etude fonctionnelle ?. • Programme et tests ? • Mise à l'essais auprès des utilisateurs en mode non bloquant ?. • Mise en place définitive ?.			
41 Cette stratégie est-elle périodiquement révisée au fur et à mesure de l'évolution de la configuration et / ou de la structure du système d'information ?			

48 Si l'entreprise utilise des mots de passe, les règles suivante sont-elles suivies par l'entreprise ?			
• Gestion des mots de passe par une personne suffisamment indépendante, de préférence le gestionnaire de la sécurité ?.		X	
• Le responsable des mots de passe, procède-t-il régulièrement aux tâches suivantes :			
- Maintenance avec les utilisateurs des profils d'accès selon l'évolution de l'entreprise ?			
- Contrôle sur le respect des procédures ?	x		
- Contrôle de la diffusion des mots de passe aux utilisateurs ?			
- Enquête sur les forçages ?			
• Les procédures relatives aux mots de passe assurent-elles une protection suffisante :			
- Quatre caractères alphanumériques minimum ?	x		
- Pas d'affichage à l'écran ?	x		
- Difficilement reconstituable ?			
- Changement au moins tous les mois ?			
- Création selon un programme générant des caractères au hasard ?			
- Protection de l'entrée directe aux tables d'accès ?	x		Tous les deux mois
- Procédure de diffusion des mots de passe garantissant un secret suffisant ?	x		
- Déconnexion automatique des terminaux après forçage ou après les heures normales de travail ?	x		
49 existe –t –il des procédés de journalisation des accès adaptés aux besoins de l'entreprise, selon le degré de sensibilisation à l'erreur, à la fraude ou à la malveillance du système d'information ?			
50 Cette journalisation permet-elle d'analyser les éléments suivant :			
• Autorisation des sollicitations (fichier, programme, transaction) ?.			
• Localisation et fréquence des forçages ?			
• Changement des profits d'accès ?			

Si l'entreprise utilise des techniques (**encodage/ décodage?**), existe-t-il des procédures satisfaisantes de gestion des clefs ?			
Existe-t-il des procédures permettant de contrôler a postériori l'intégrité du système d'information ?.			
V. DISPOSITIONS LEGALES ET REGLEMENTAIRES			
Plan comptable général			
1 Les traitements automatisés de la comptabilité générale et tous les systèmes automatisés concourant, directement ou indirectement, à l'établissement des états financiers, satisfont-ils aux dispositions générales du Plan Comptable relatives à l'utilisation de traitements automatisés ?			
2 Le système comptable permet-il un contrôle a posteriori par des organes de contrôle (vérificateur fiscal, commissaires aux comptes, expert judiciaire) ?			
Les entrées dans le système comptable font-elles l'objet de l'édition d'un journal archivé sur papier ou sur microfilm ?			
4 Les entrées en provenance de systèmes en interface font-elles l'objet également d'une édition de journal dans les mêmes formes ?			
5 Chaque donnée imputée fait-elle l'objet d'un justificatif constitué par un document écrit ?			
6 Le système permet-il un chemin de révision du grand-livre à la pièce de base, et vice-versa : Est-il possible, à tout moment, de reconstituer à partir des pièces justificatives appuyant les données entrées, les éléments des comptes, états de renseignements, soumis à la vérification, ou, à partir de ces comptes, états et renseignements, de retrouver ces données et les pièces justificatives ?			
7 Les règles de sécurité appliquées par l'entreprise sont-elles de nature à garantir un traitement complet, exact et autorisé des données comptables ?.			
8 Les données de la comptabilité générale et des comptabilité auxiliaires, à la date de clôture, sont-elles archivées sur support magnétique pour les périodes sujettes à contrôle fiscal ?.			

9 Les traitements informatisés de la paie des personnels : • Ne portent-ils que sur des données objectives aisément contrôlables par les intéressés ?. • Ne servent-ils qu'au paiement des rémunérations et accessoires, aux déclarations fiscales et sociales et aux versements des cotisations ?			
Continuité de l'activité			
1 Les systèmes informatiques critiques pour l'activité (financière et comptable) de l'entreprise ont-ils été identifiés ?.			
2 Les procédures de reprise tiennent compte : • Des activités ?. • Des contraintes informatiques ?.			
3 Pendant combien de temps l'entreprise peut-elle fonctionner sans les systèmes critiques : • Quelques heures ? • Plusieurs jours ?			
4 Existe-t-il un plan de secours adapté, documenté et mis à jour : • Concernant les procédures utilisateurs ?. • Approuvé par la direction ?. • Couvrant les principales activités financières et comptables ?			
5 les utilisateurs ont-ils spécifiés leurs besoins pour la reprise d'activité notamment pour : • La durée d'indisponibilité acceptable ?. • La reprise des autres applications ? • La reprise des applications critiques ?			
6 Les utilisateurs ont-ils développé des modes opératoires particuliers si le traitement normal est interrompu ?.			

7 Ces modes opératoires prévoient-ils : • Des procédures manuelles dégradées ?. • La durée possible de fonctionnement en mode dégradé ?			
8 Le système d'information a-t-il été conçu à minimiser les indisponibilités par : • La protection contre le piratage ?. • La prévision d'un réseau de secours ? • L'assistance des fournisseurs pour le matériel et les composants informatiques ?. • La maintenance préventive ?.			
9 Les sauvegardes suivantes sont-elles correctement réalisées ? • Des traitement ou des modifications critiques ? • Des cycles des principaux traitements ?. • Des fichiers de données ? • Des programmes ?. • Des logiciels systèmes ? • Des procédures d'exploitation ? • Des procédures utilisateurs ? • ETC..			
10 Ces sauvegardes sont-elles réalisées et conservées de façon régulière : • Localement ? • Hors site ?. • Dans des armoires ignifuges ?. • ETC…			

Contrôle utilisateurs			
1 Les utilisateurs sont-ils satisfaits des applications informatiques du point de vu : • De l'exhaustivité des traitements ? • De l'exactitude des traitements ? • Du temps de réponse ?. • De l'adéquation des résultats ? • De la convivialité ?.			
2 Les utilisateurs sont-ils satisfaits de : • La qualité du reporting ?. • L'aide en ligne ?			
3 les utilisateurs sont-ils satisfaits des services rendus par le département informatique du point de vue de : • L'assistance ? • La maintenance des programmes ? • Des travaux à la demande ? • Des délais de réponse aux demandes utilisateurs ?			

SICOGI
Service des moyens informatiques et de la méthode

ANNEXE 2

Gestion des Courriers

Fonctionnalités de l'application :

- Gestion du courrier arrivé
- Gestion du courrier départ
- Consultation
- Statistiques
- Editions

Nature des développements : Développement spécifique interne (SICOGI)

Langage de programmation utilisé : Clipper 5

Date de mise en service de l'application : janvier 1998

Matériel supportant l'application : Digital Venturis 4100 486 DX2 33 Mhz

Nombre d'utilisateurs :

- Secrétariat administratif
- Services généraux

Volumes estimés : 6000 à 7000 courriers par an

Environnement :

- MS-DOS
- Mono poste

Immobilisations Saari V2.04

Fonctionnalités de l'application :

- Gestion des immobilisations, des dotations aux amortissements
- Gestion des cessions, des familles, des lois

Nature des développements : Progiciel

SICOGI
Service des moyens informatiques et de la méthode

Date de mise en service de l'application : Fin 1996

Matériel supportant l'application : Compaq Deskpro

Nombre d'utilisateurs : 1

Volumes estimés : environ 50 000 immobilisations

Environnement réseau : Application monoposte sous MS-DOS

Suivi tableau d'amortissement

Fonctionnalités de l'application : Saisie et Edition du tableau d'amortissement des VPL

Nature des développements : Développements spécifique interne (SICOGI)

Langage de programmation utilisé : Dbase 4

Date de mise en service de l'application : 1998

Matériel supportant l'application : Micro-ordinateur 386

Nombre d'utilisateurs : 1

Environnement réseau : Application monoposte sous MS-DOS

Calcul du remboursement d'un prêt

Fonctionnalités de l'application

- Calcul de la mensualité de remboursement d'un prêt (début de période, fin de période)
- Détermination du taux d'intérêt d'un prêt
- Calcul de la valeur résiduel d'un prêt

Nature des développements : Développements spécifique interne (SIGOGI)

Langage de programmation utilisé : Clipper 5

Date de mise en service de l'application : Janvier 1997

Nombre d'utilisateurs : Services Commercial et Exploitation

Environnement réseau : Utilitaire de calcul sous MS-DOS

Gestion des Prospects

Fonctionnalités de l'application :

- Prise en compte des prospects (saisie, modification, supression)
- Gestion des tables (banques, nationalités, utilisateurs, opérations)
- Consultation du fichier
- Editions

Nature des développements : développement spécifique interne (SICOGI)

Langage de programmation utilisé : Clipper 5

Date de mise en service de l'application : Février 1996

Matériel supportant l'application : Serveur Compaq proliant 3000 R (DCE)

Nombre d'utilisateurs : 5

Volumes estimés : 15 000 Prospects

Environnements :

- Novell Netware 4.10
- MS-DOS

ANNEXE 3

Comptabilité Major Saari V.8.01

Fonctionnalités de l'application :

- Enregistrements des écritures comptables
- Lettrage, rapprochement
- Editions : balance, grand livre, états financiers, brouillard, journaux
- Suivi des tiers

Nature des développements : Progiciel

Date de mise en service de l'application : Février 1995, formation en août 1995

Matériel supportant l'application : Serveur Unisys SVI 5907 (DAF) remplacé

Nombre estimés : 1300 comptes, 800 à 1000 écritures par jour

Environnement

- MS-DOS
- Novell Netware 3.12

Gestion des Réclamations

Fonctionnalités de l'application

- Mise à jour des réclamations
- Mise à jour des réponses aus réclamations
- Consultation des réclamations
- Statistiques sur les réclamations
- Editions périodiques
- Tables des services et desnatures de réclamations

Nature des développements : développement spécifique interne (SICOGI)

Langage de programmation utilisé : Clipper 5

Date de mise en service de l'application : L'application n'est pas encore mise en exploitation.

Matériel supportant l'application : Serveur Compaq proliant 3000 R (DCE)

Nombre d'utilisateurs : Service Assistance clientèle

Volumes estimés : par jour 100 à 200 réclamations en période de pointe.

Environnement :

- MS-DOS
- Netware

Rapprochement bancaire major

Fonctionnalités de l'application :

- Rapprochement de la comptabilité Major avec celles de la banque
- Format des écritures AFB

Nature des développements : Progiciel

Date de mise en service de l'application : Août 1995, Formation effectuée en août 1996.

Nombre d'utilisateurs : service comptabilité

Environnement réseau : MS-DOS

Paie Major

Fonctionnalités de l'application :

- Calcul de la paie
- Gestion du personnel
- Mise à jour des informations sur le personnel

Nature des développements : progiciel

Date de mise en service de l'application : Fin 1996, formation effectuée en août 1996.

Matériel supportant l'application : Serveur Unisys SV15907 (DAF) remplacé

Nombre d'utilisateurs : 2

Volumes estimés : 210 employés

Environnement réseau : MS-DOS en monoposte

Paie 500Sage Sybel

Fonctionnalités de l'application :

- Calcul de la paie, billetage, Edition des bulletins de paie
- Gestion du personnel, Gestion des prêts
- Mise à jour des informations sur le personnel

Nature des développements : Progiciel

Date de mise en service de l'application : Novembre 1997, formation effectuée le 27 janvier 1998

Matériel supportant l'application : Serveur Compaq proliant 3000 R (DAF)

Nombre d'utilisateurs : 2

Volumes estimés : 210 employés

Environnement réseau :

- MS-DOS
- Windows NT Server 4.0
- Windows 95

Immobilisations Maestria

Fonctionnalités de l'application :

- Mise à jour des immobilisations
- Gestion des dotations
- Gestion des cessions

SICOGI
Service des moyens informatiques et de la méthode

Nature des développements : Progiciel

Date de mise en service de l'application : Novembre 1996

Matériel supportant l'application : Serveur Compaq proliant 3000 R (DAF)

Nombre d'utilisateurs : 2

Volumes estimés : 50 000 immobilisations

Environnement réseau :

- Windows NT
- Windows

Budget de Trésorerie Major

Fonctionnalités de l'application :

- Analyse de trésorerie
- Budget de trésorerie

Nature des développements : Progiciel

Date de mise en service de l'application : Micro ordinateur fonctionnant sous DOS

- Service comptabilité
- Section finances et fiscalité

Environnement réseau :

- Mono poste
- MS-DOS

Trésorerie 500 et budget

Fonctionnalités de l'application :

- Analyse de trésorerie

- Budget de trésorerie
- Etats financiers de trésorerie

Nature des développements : Progiciel

Date de mise en service de l'application : Novembre 1997

Matériel supportant l'application : Serveur Compaq proliant 3000 R (DAF)

Nombre d'utilisateurs

- Service comptabilité
- Section finances et fiscalité

Environnement réseau :

- Windows NT Server 4.0
- Windows 95

Rapprochement bancaire 500

Fonctionnalités de l'application

- Rapprochement des écritures de banques avec celles de la comptabilité
- Etat de rapprochement automatique
- Interfaces avec les banques

Nature des développements : Progiciel

Date de mise en service de l'application : Novembre 1997

Matériel supportant l'application : Serveur Compaq proliant 3000 R (DAF)

Nombre d'utilisateurs :

- Service comptabilité
- Section Finances et fiscalité

Environnement réseau :

- Windows NT Server 4.0
- Windows

Etat financier 500

Fonctionnalités de l'application :

- Conception d'états financiers personnalisés différents de ceux de SAARI
- Conception d'état financiers personnalisés pour la gestion courante de l'entreprise à partie des fichiers SAGE

Nature des développements : Progiciel

Date de mise en service de l'application : Novembre 1997

Matériel supportant l'application : serveur Compaq proliant 3000 R (DAF)

Nombre d'utilisateurs :

- Service Comptabilité
- Section Finances et fiscalité

Environnement réseau

- Windows NT Server 4.0
- Windows 95

Annexe 4 : GUIDE D'ENTRETIEN AVEC LE S M I M

Ce guide nous a permis de conduire l'entretien avec le chef du SMIM et son adjoint.

Organisation du service

1- Quelles sont les responsabilités du service et comment sont-elles gérées ?

2- Quelle est la position du SMIM dans l'organisation générale de la SICOGI ?

3- Quelles sont les différentes activités et quelle en est la répartition entre les agents ?

Gestion du patrimoine informatique de la SICOGI

4- Existe-t-il un schéma directeur pour conduire la politique informatique, et quelles en sont ses caractéristiques ?

5- Quels sont les moyens informatiques (équipement matériel et logiciel) de la SICOGI dont vous avez la charge ?

6- Existe-t-il des procédures formalisées pour l'acquisition du matériel et des logiciels ? quelles en sont les différentes étapes ?

7- Pour les développements spécifiques en interne, quelle est la procédure ?

8- Quelle est la procédure suivie pour la maintenance ?

9- Quels sont les dispositifs pour sécuriser le patrimoine informatique ?

Les applications informatiques

10- Quelles sont les applications qui gèrent la comptabilité, les services financiers, les ventes et les achats ?

11- Quelles sont leurs spécifications fonctionnelles mise en service ?

12- Qui s'occupe de leur mise en exploitation ?

13- Quelles dispositions sont prises pour sécuriser les fichiers de données et le programmes.

Etc..