CESAG

CENTRE AFRICAIN D'ÉTUDES SUPÉRIEURES EN GESTION

Institut Supérieur de Comptabilité

Mémoire de fin d'études

DESS Audit et Contrôle de Gestion

15ème Promotion

EVALUATION DU CONTROLE INTERNE INFORMATIQUE
CAS DE LA SENELEC

Présenté par : Almamy SAMASSI

Sous la Supervsion de : M. Mactar NDOYE
Auditeur Senior

FIGURES ET TABLEAUX

LISTE DES FIGURES **PAGES**

LISTE DES TABLEAUX **PAGES**

ANNEXES

LISTE DES SIGLES ET ABREVIATIONS

ATH	Association Technique pour l'Harmonisation des cabinets d'audit et conseil
ACI	Agent Commercial d'Intervention
APV	Agence Principale Vincens
BT	Basse Tension
CESAG	Centre Africain d'Etudes Supérieures en Gestion
CI	Contrôle interne
CII	Contrôle interne informatique
CNCC	Compagnie Nationale des Commissaires aux Comptes
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DAI	Department de l'Audit Interne
DAICG	Direction de l'Audit Interne et Contrôle Général
DCC	Direction Commerciale et Clientèle
DPS 7000	Marque de l'ordinateur central de la SENELEC
DRH	Direction des ressources
DSI	Délégué aux Systèmes d'information/ Délégation aux Systèmes d'Information
FOPES	Fonds de Promotion Economique et Sociale
GMAO	Gestion de la Maintenance Assistée par Ordinateur
IFAC	International Federation of Accountants
IFACI	Institut Français des Auditeurs Contrôleurs Internes

IP	Internet Protocol
IPM	Institut de Prévoyance Maladie
ISO	International Organization for Standardization
MI	Milieu Informatisé
SENELEC	Société Nationale d'Electricité
SI	Système d'Information
SIC	Système d'Information Clientèle
SIFC	Système d'Information Financière et Comptable
SIPRO	Système d'Information Production
SIRH	Système d'Information des Ressources Humaines
TSP	Terminal de Saisie Portable
UP	Usage Professionnel
VPN	Virtual Protocol Network

TABLE DES MATIERES

INTRODUCTION GENERALE

La gestion des ressources et des opérations est une tâche complexe. L'entreprise publique ou privée, pour qu'elle soit performante, doit constamment adapter ses méthodes de fonctionnement pour répondre aux besoins d'information rapides.

Devant une concurrence de plus en plus rude et efficace, de nouvelles méthodes diagnostiques comme la réingénierie des processus, la méthode ABC (Activity Based Costing) et le benchmarking ont fait leur apparition. Ce qui favorise le questionnement : comment faire plus, mieux et moins cher.

Dans cet environnement en constante évolution, la fonction informatique joue un rôle primordial dans la compétitivité de l'entreprise. Et cette dernière ne doit pas perdre de vue l'importance et la fiabilité de l'information financière pour l'aider dans sa prise de décisions. A cette fin, le contrôle interne informatique a un rôle essentiel à jouer : il contribue à améliorer l'efficacité et l'économie liées à certains processus décisionnels et permet de minimiser les risques de non contrôle et d'inexactitude sur les données financières, compilées et présentées par les applications afin de permettre le pilotage de l'entreprise.

Malgré sa situation quasi-monopolistique, la SENELEC a décidé d'améliorer considérablement sa gestion. C'est ainsi que l'entreprise étatique a placé sa fonction informatique au centre de son plan stratégique.

Problématique

L'environnement dans lequel évoluent nos organisations est, il faut le reconnaître, sous l'emprise totale de l'informatique. Les évolutions actuelles des systèmes d'information, présentées comme simplificatrices, économiques et génératrices de nouvelles opportunités, modifient profondément le fonctionnement de l'entreprise.

Les processus métiers sont dès lors fort dépendants de l'outil informatique et à ce titre, ils peuvent être considérablement impactés en cas de dysfonctionnement. Les risques encourus sont multiples et variés :

- sinistre qui détruit les fichiers commerciaux ou les banques de données,

- détournement des données par un « pirate » concurrent,
- panne paralysant tout le système informatique à un moment crucial.

Ces risques se sont accentués avec la complexification des systèmes d'information et leur mise en réseau, qui les rend de plus en plus vulnérables aux intrusions et aux dysfonctionnements.

Les conséquences économiques des sinistres informatiques selon le Club des Systèmes d'Information Français (CLUSIF) sont de plus en plus importantes depuis 1996. Il est bon de rappeler que la proportion d'entreprises ayant connu une fraude importante en 2002 est de près de 50% et celles reconnaissant que leurs systèmes d'information transportent des informations sensibles ou critiques sont plus de deux sur trois (Enquête réalisée par Ernst&Young France). Ces constats alarmants concernant la sécurité ou le contrôle interne justifient l'intervention du législateur dans la gestion des entreprises :

avec la loi sur la sécurité financière en France (LSF) : cette loi publiée au journal officiel depuis le 02 août 2003 fixe de nouvelles obligations et notamment dans son titre III – chapII relatif à la transparence des entreprises, des obligations relatives aux procédures de contrôle interne mises en place dans les sociétés.

Cette disposition a l'immense mérite de sous-entendre que les procédures de contrôle interne doivent être en place dans toute entreprise, qu'elle qu'en soit la taille. Elle conduira donc à faire disparaître l'assimilation entre grande entreprise et contrôle interne, voire la confusion entre audit interne et contrôle interne.

avec la loi Sabanes-Oxley (L S O) adoptée en juillet 2002 par le congrès américain : l'une des principales activités intégrée aux contrôles de la fourniture et du support, particulièrement adaptée à la conformité L S O, est l'activité baptisée : Ensure Systems Security dont l'objectif principal est de fournir des contrôles protégeant l'information contre toute utilisation, divulgation ou modification non autorisée et contre tout dommage ou perte à l'aide de contrôle logique assurant l'accès aux seuls utilisateurs autorisés

A l'instar des pays développés, l'outil informatique a investi tous nos secteurs d'activités économiques, devenant indispensable à nos organisations (et plus particulièrement les entreprises) à qui, il fait gagner en temps et en efficacité. Certes, la généralisation de

l'informatique dans les opérations comptables, financières et de gestion a des avantages indéniables, mais pose au plan du contrôle interne des problèmes liés Barry (2004 ; 240) :

- à l'adaptation des informations produites aux besoins des utilisateurs,
- à la périodicité de production des états nécessaires aux services opérationnels,
- à la fiabilité des applications développées ou à la maîtrise des progiciels acquis,
- à la conservation des données (sauvegarde contre les risques de manipulation frauduleuses ou de pertes).

Il faut en outre souligner d'autres risques, qui sont :

- au niveau de l'environnement informatique : l'absence de plan de secours,
- au niveau des applications : un mauvais paramétrage des règles de gestion,
- au niveau de la sécurisation des traitements et des données : un non respect du principe de séparation des tâches ou de la rupture de la piste d'audit permettant de remonter à l'origine d'une donnée,
- au niveau de la réglementation : le non respect de certaines contraintes locales (TVA, éditions réglementaires).

En dépit de son informatisation ancienne (depuis les années 80), la SENELEC ne dispose pas encore de procédures informatiques formalisées. A cela s'ajoutent les problèmes ci-dessous :

- absence Plan de secours (de back up) informatique,
- conservation des données importantes,
- la saturation du SIC,
- non maîtrise totale du progiciel ORACLE.

Alors, comment dans ces conditions, la société pourra t-elle maîtriser totalement son activité informatique ? La maîtrise des application et leur bonne gestion et administration sont, une partie intégrante du contrôle interne. C'est pourquoi, les procédures non formalisées de la fonction informatique de la SENELEC nécessitent une remise en cause pour l'adapter à l'évolution très rapide de l'informatique.

Par conséquent, notre question principale de recherche est : « **Comment peut-on évaluer le contrôle interne informatique afin qu'il soit plus efficace et suffisant ?** »

Plus explicitement :

- En quoi consiste le contrôle interne informatique ?
- Quelles les caractéristiques d'un environnement informatique ?
- Comment une fonction informatique peut-il satisfaire aux objectifs du contrôle interne ?
- Quels sont les risques inhérents à la fonction informatique ?
- Quelle est la démarche d'appréciation du contrôle interne informatique ?

Nous avons pour la recherche de réponses à ces interrogations opté pour le thème : « **L'évaluation du contrôle interne informatique : cas de la SENELEC** »

Objectif de l'étude

L'objectif principal de notre étude est de corriger les faiblesses du contrôle interne informatique (non formalisé) de la SENELEC afin qu'il puisse contribuer efficacement à la maîtrise des risques informatiques.

Notre travail comprendra alors les objectifs spécifiques suivants :

- décrire les composantes du contrôle interne de la fonction informatique ;
- évaluer le contrôle interne informatique existant ;
- faire des recommandations pertinentes

Intérêt de l'étude

Cette étude revêt des intérêts à plusieurs niveaux :

- d'abord, pour la direction générale de la SENELEC, ils y trouveront un dispositif de contrôle interne informatique adéquat, leur permettant de maîtriser les risques liés à l'activité informatique.
- ensuite, pour nous même, ce travail constitue un premier pas et une base pour de futures recherches en gestion. Il viendra enrichir sans aucun doute la formation théorique reçue.

- enfin, pour le Centre Africain d'Etudes Supérieures en Gestion (CESAG), qui est dans la sous région ouest africaine une grande école de gestion par essence et par excellence, ce travail viendra enrichir la documentation déjà existante.

Plan de l'étude

Notre mémoire sera subdivisé en deux (02) parties : la première sera consacrée à la revue de littérature sur le contrôle interne en général et sur le contrôle interne informatique en particulier. Dans la deuxième partie, nous parlerons de la SENELEC et de la DSI qui sera le cadre de notre étude. Nous procéderons par la suite au diagnostic des différents contrôles existants au niveau de la fonction informatique et ferons des recommandations.

PREMIERE PARTIE

Cadre théorique de l'évaluation du contrôle interne informatique

Pour atteindre ses objectifs, l'entreprise doit maîtriser ses activités. Dans toute grande entreprise informatisée, l'activité informatique occupe une place de première importance. C'est pourquoi, le contrôle interne de la fonction informatique doit être une priorité pour chaque entreprise, soucieuse de la maîtrise des risques informatiques, et partant, de la qualité de son système d'information. Ce dernier pourra ainsi produire des informations pertinentes et utilisables immédiatement.

Cette première partie tournera autour deux chapitres importants, qui permettront de mieux appréhender le cadre théorique de notre thème. Il s'agira non seulement du contrôle interne mais aussi de l'évaluation du contrôle interne informatique.

CHAPITRE I : LE CONTROLE INTERNE (CI)

Depuis que les scandales financiers (celui de ENRON surtout) ont défrayé la chronique, le CI est sous les feux des régulateurs. Cette pression pour une mise en œuvre de CI de qualité, ne doit pas occulter le fait que le CI est un dispositif de maîtrise des activités mis en place par l'entreprise, pour l'entreprise.

L'intervention du législateur est donc un catalyseur qui doit être perçu comme l'opportunité d'améliorer le fonctionnement de l'entreprise, et ce au travers d'une gouvernance claire et d'un CI adapté et efficace.

Par ailleurs, le CI dépendant de l'activité, il est impérieux d'accorder une attention soutenue à celui lié à l'activité informatique, car les SI sont désormais indissociables des processus de l'entreprise en général et du processus du reporting financier en particulier. Autant l'informatique améliore de façon substantielle la gestion des organisations, autant elle introduit des risques multiples et variés : d'où l'importance du contrôle interne informatique.

Dans ce chapitre, il sera question :

- d'abord de la définition et des objectifs du CI,
- ensuite des composantes du CI,
- enfin du contrôle interne informatique.

I Définition et objectifs

Pour bien cerner le terme « contrôle interne », nous allons donner une définition le concernant et préciser ses objectifs essentiels

I.1 Définitions

Selon le rapport du COSO (PRICEWATERHOUSECOOPERS, 2004 ; 18), « Le CI est un processus mis en œuvre par le conseil d'administration, les dirigeants et le personnel de l'entreprise, pour fournir une assurance raisonnable quant à la réalisation des trois (03) objectifs suivants :

- la réalisation et l'optimisation des opérations,

- la fiabilité des opérations financières,
- la conformité aux lois et règlements en vigueur ».

I.2 Les objectifs du contrôle interne

La définition du CI selon le COSO, évoquée plus haut, pose clairement les objectifs du CI.

L'utilisation des systèmes informatiques pour le traitement de l'information comptable ne change en rien la nécessité d'avoir un bon système de CI pour rencontrer les objectifs du CI.

Les objectifs du CII sont selon IFACI (1993 ; 33) :

- intégrité des informations ;
- sécurité
- conformité.

III.2-1 Intégrité des informations

Selon IFACI (1993 ; 34), « l'objectif du CI, est de garantir l'intégrité, la confidentialité et la disponibilité de l'information. Les données, élément principal d'un SI, sont traitées, triées, classées, résumées et manipulées afin de fournir les informations nécessaires au processus de décision. ». La direction se fie à l'intégrité des données et applications du système pour prendre des décisions importantes.

Dès lors, le maintien de systèmes de contrôle fiables devient une nécessité, car, pour que l'information financière soit utile à la prise de décisions, le système comptable doit produire des données et des états financiers fiables.

Tableau n°1 : Eléments d'intégrité des informations et des processus

Eléments	Définitions
Autorisé	Un élément d'information, d'une transaction à un système, est correctement saisi, développé, modifié ou utilisé avec l'autorité adéquate.
Exact	L'information et les processus s'y rattachant sont exacts et peuvent être utilisés comme prévus.
Complet	Aucune information demandée ne fait défaut. Aucune n'apparaît en double. Les transactions rejetées sont identifiées, vérifiées et réintroduites, le cas échéant.
Opportun	La tâche (ex : la transaction) est rapidement exécutée. (ex : les taux de service sont maintenus)
Saisi, traité et communiqué dans un laps de temps correct	Respect de la période et des autres jours de la date de séparation des exercices.
Sûr	L'information et les processus sont protégés contre tout accès, mise à jour, divulgation ou destruction non autorisés.

Source : IFACI (1993 ; 35)

III.2-2 Sécurité

Les activités de gestion de la sécurité consistent essentiellement à analyser la vulnérabilité du système informatique puis à définir des mesures adéquates. Pour REIX (2002 ; 416), « La Sécurité d'un SI est sa non vulnérabilité à des accidents ou à des attaques volontaires ». La sécurité inclut la protection des matériels, des logiciels et des données contre les tentatives d'accès et d'utilisation non autorisée. La sécurité relève de la responsabilité de chacun, et l'implication de la direction générale est un facteur essentiel de la réussite du programme de sécurité

III.2-3 Conformité

« Un défaut de conformité aux diverses procédures internes ou externes, aux lois et réglementations peut avoir des conséquences néfastes pour l'organisation » IFACI (1993 ; 38).

D'un point de vue public, cette conformité ou non-conformité a un impact sur l'image de marque professionnelle. Des contrôles sont nécessaires pour assurer la conformité :

- aux lois et réglementations au niveau international, national et local, aux règlements particuliers à un secteur d'activité économique,
- aux normes comptables, les informations financières devant respecter les principes acceptés, la réglementation fiscale, les règlements nationaux et les procédures internes de comptes rendues.
- aux normes d'audit concernant les conduites des audits, aussi bien les normes établies en interne que les normes internationales.

II Les composantes du contrôle interne

Le COSO structure l'analyse du CI selon les trois objectifs cités précédemment et pour chacun d'eux selon cinq (05) composantes PRICEWATERHOUSECOOPERS (2004 ; 19) :

- l'environnement de contrôle,
- l'évaluation des risques,
- les activités de contrôle,
- l'information et la communication,
- le pilotage (du contrôle interne).

II.1 L'environnement de contrôle

Dans un système de CI, l'élément dont on doit de prime abord tenir compte est l'environnement de contrôle (instauré par la direction générale) et qui influence directement le fonctionnement de tous les autres contrôles. Pour COOPERS et LYBRAND (2000 ; 35) : « L'environnement de contrôle constitue le fondement de tous les autres éléments du CI, en imposant discipline et organisation ». Il détermine le niveau de sensibilisation du personnel au besoin de contrôle.

II.2 L'évaluation des risques

L'entreprise doit être consciente des risques et les maîtriser. « Toute entreprise est confrontée à des risques externes et internes qui doivent être évalués » COOPERS et LYBRAND (2000 ; 49). La détermination des risques à l'instar des objectifs est une donnée dynamique. Par conséquent, tant à l'intérieur qu'à l'extérieur de l'entreprise, les modifications nécessitent une adaptation des objectifs qui doivent tenir compte de nouvelles menaces ou menaces en mutation.

II.3 Les activités de contrôle

Ces « activités de contrôle » sont les « dispositifs spécifiques » de chacun qui vont lui permettre de gérer ses activités dans le respect des objectifs généraux du CI (RENARD, 2004 ; 151). Ces actions permettent de s'assurer que les mesures nécessaires sont prises en vue de maîtriser les risques susceptibles d'affecter la réalisation des objectifs de l'entreprise. Concrètement, entrent dans cette composante, des actions aussi variées qu'approuver et autoriser, vérifier et rapprocher, apprécier les performances opérationnelles, la séparation des fonctions et la surveillance de l'intégralité, la réalité, etc.

II.4 Information et communication

« Si l'on ne dispose pas des bonnes informations, il est indispensable de diriger un processus d'entreprise. Les SI et de communication créent et diffusent de plus en plus d'informations » WILMOTS (2002 ; 83). Il va de soit que les CI portant sur les systèmes informatiques nécessitent une attention accrue et de la part de ceux qui doivent faire fonctionner le système, et de la part des auditeurs internes et externes. Les SI permettent au personnel de recueillir et échanger les informations nécessaires à la conduite, à la gestion et au contrôle des opérations (COOPERS et LYBRAND ; 2000 :28).

II.5 Le pilotage

Il faut comprendre par pilotage, le suivi et les modifications éventuelles de l'ensemble du processus de contrôle. Le pilotage regroupe les deux actions suivantes :

- le pilotage permanent s'inscrit dans le cadre des activités courantes et comprend les contrôles réguliers qui s'attachent aux visas, approbations, etc,

- les évaluations périodiques dont l'étendue et la fréquence dépendent essentiellement du niveau des risques et de l'efficacité de surveillance permanente (SARR ; 2004 : 11).

Le respect des mesures de CI doit être contrôlé en permanence et le système de CI doit être évalué et adapté.

III Contrôle interne informatique (CII)

Les CII généraux sont, au sens du COSO, « des principes et procédures qui contribuent à assurer un bon fonctionnement continu des SI » PROTIVITI (2004 ; 2). Lorsque ces contrôles généraux sont efficaces, ils apportent une garantie de pérennité du niveau de CI au sein des processus métiers ou fonctionnels.

III.1 L'environnement informatique

Selon les recommandations de la CNCC (2003 ; 155), « Un milieu est dit informatisé lorsqu'un ordinateur quels que soit sa taille ou son type, intervient dans le traitement de l'information qui présente une importance pour l'audit, que cet ordinateur soit exploité par l'entité ou par un tiers ». En d'autres termes, le système d'information dans un tel milieu est supporté en grande partie ou totalement par l'informatique. Ainsi, l'ordinateur remplace l'homme dans certaines tâches pour accélérer le traitement de l'information, effectue des opérations répétitives, des contrôles mécaniques et impose une nouvelle conception des procédures séparation des tâches.

III.2 Organisation générale d'une fonction informatique

L'organisation de la fonction informatique ne peut être efficace que si ses objectifs sont cohérents avec les objectifs globaux de l'entreprise. La fonction informatique doit avoir une mission, ainsi que ses différents services. Les principes de base de bonne organisation d'une fonction informatique tournent autour des éléments suivants (CNCC, 1995 ; 30) et DERRIEN (1992 ; 49) :

- les intervenants,
- les procédures de développement et de maintenance,
- les procédures d'exploitation,
- les procédures de traitement,

- la documentation,
- les procédures de sécurité
- Le comité informatique.

III.2-1 Les intervenants

Afin d'assurer la cohérence du plan informatique (adaptation du matériel aux besoins, mise en œuvre des protections nécessaires, etc.), il est souhaitable de :

- créer une véritable fonction informatique et de distinguer en son sein la fonction études de la fonction exploitation,
- organiser une réelle concertation avec les utilisateurs pour la conception et pour l'exploitation,
- mettre en place une démarche qualité pendant le développement et pour la maintenance (CNCC, 1995 ; 31).

Il faut organiser une liaison régulière entre les responsables de la conception et les exploitants afin d'assurer une maintenance régulière des applications.

III.2-2 Les procédures de développement et maintenance

Ces procédures sont celles qui doivent permettre d'assurer :

- une bonne coordination entre la fonction informatique et les utilisateurs pour la définition du cahier des charges relatif à chaque application,
- la fiabilité des applications avant leur mise en exploitation.

Les procédures doivent comporter notamment :

- une bonne définition des besoins (formats de saisie, traitements, contrôles, formats des éditions, etc.),
- la réalisation des tests garantissant la bonne programmation (jeux d'essais,…),
- l'adaptation, si nécessaire, des procédures « autour » de l'ordinateur (définition des rôles, exploitation et recyclage des listings d'anomalies, conservation des éditions…),
- une acceptation formelle de l'application avant sa mise en exploitation,

- une actualisation régulière en fonction de l'évolution des besoins des utilisateurs (CNCC, 1995 ; 31).

III.2-3 Les procédures d'exploitation

Elles sont destinées à empêcher ou détecter rapidement (CNCC, 1995 ; 32):

- l'utilisation de programmes par des personnes non autorisées,
- l'utilisation de programmes non autorisés (versions périmées, extraction de données protégées, …),
- les erreurs de chargement de fichiers,
- les modifications non autorisées de programmes ou de données,
- les défaillances techniques du matériel,
- etc.

III.2-4 Les procédures de traitement

Ces procédures sont étroitement liées aux procédures d'exploitation, mais elles doivent permettre de s'assurer du bon fonctionnement de chaque opération CNCC (1995 ; 33). Elles portent sur :

- la création des données par les services utilisateurs,
- leur saisie exhaustive,
- leur validité,
- leur traitement,
- leur centralisation dans les bons fichiers,
- le contrôle des sorties et des résultats obtenus,
- l'édition séquentielle des anomalies,
- le bon recyclage des anomalies.

III.2-5 La documentation

La documentation des systèmes et procédures informatiques est un élément essentiel de pérennité du système CNCC (1995 ; 33). C'est elle qui, en effet permet, quels que soient les changements de personnel, d'identifier les causes de dysfonctionnement éventuel, de procéder à des évolutions cohérentes. « La documentation doit être la base de contrôle de chaque

application » OBERT (2000 ; 149). C'est aussi un élément important pour la formation du personnel et par ailleurs c'est une exigence légale. Elle doit exposer clairement :

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

III.2-6 Les procédures de sécurité

L'ensemble de ces procédures perd de son efficacité s'il n'est pas accompagné de procédures de sécurité destinées à protéger l'intégrité physique de l'installation et des données.

III.2-7 Le comité informatique

C'est ce comité qui décide des orientations stratégiques de l'entreprise en matière informatique. Le comité informatique est en général composé selon DERRIEN (1992 ; 49) d'un ou plusieurs représentants de Direction Générale, des responsables de chaque Direction de l'entreprise ainsi que des principaux responsables de la Direction informatique. Ce comité suit régulièrement les principaux indicateurs de l'activité informatique et prend en compte les remarques et critiques des utilisateurs.

III.3 Les risques liés à la fonction informatique

L'organisation informatique peut engendrer des risques spécifiques qui résultent des différents facteurs décrits ci-dessous.

- la politique informatique,
- la séparation des fonctions,
- les procédures de développement,
- l'accès aux données et au matériel,
- la sécurité des traitements,
- la sécurité physique des installations et des données CNCC (1995 ; 26)

III.3-1 La politique informatique

Lorsque la politique informatique de l'entreprise, n'est pas suffisamment rigoureuse, il peut en résulter :

- un développement anarchique du matériel et des logiciels et des acquisitions inadaptées aux besoins,
- des coûts excessifs,
- une évolution non maîtrisée (CNCC, 1995 ; 26).

III.3-2 La séparation des fonctions

Le cumul des fonctions de développement, d'exploitation et de contrôle au sein de la fonction informatique génère des risques de modifications indues des programmes et des données (CNCC, 1995 ; 27).

III.3-3 Les procédures de développement

Des procédures de développement des applications insuffisamment maîtrisées peuvent aboutir à la mise en place de produits inadaptés, à des erreurs répétitives, à des surcoûts CNCC (1995 ; 27). La mise en service d'une application informatique doit par conséquent, au moins être précédée :

- d'un cahier des charges précis,
- d'une étude de faisabilité,
- d'une phase de test,
- d'une formation des utilisateurs.

III.3-4 L'accès aux données et au matériel

Une protection insuffisante des données et du matériel peut aboutir à la perte, la modification ou le détournement indus de données importantes pour l'entreprise (CNCC, 1995 ; 28).

III.3-5 La sécurité des traitements

Les procédures de l'entreprise doivent garantir, notamment :

- l'utilisation des bonnes versions de programmes,
- le bon enchaînement des différentes générations de fichier,
- l'exhaustivité des traitements,
- le contrôle des entrées et sorties (CNCC, 1995 ; 29).

III.3-6 La sécurité physique des installations et des données

La destruction de matériel ou de données pouvant entraîner des conséquences très graves pour l'entreprise, il est fondamental que l'entreprise respecte les règles en matière de :

- protection des installations électriques et informatiques contre les phénomènes naturels (l'orage, les baisses de tension, les coupures, etc.),
- protection contre les destructions, volontaires ou non, résultant d'incendies, etc.
- sauvegarde interne et externe des fichiers et programmes,
- assurance,
- système de secours en cas de panne prolongée (CNCC, 1995 ; 29).

III.4 Dispositif de contrôle interne informatique

Concernant les SI, les contrôles au niveau des processus comprennent :

- les contrôles globaux (contrôles généraux informatiques),
- les contrôles applicatifs (contrôles des applications informatisées).

III.4-1 Les contrôles généraux informatiques

Ce sont des CI au sein des processus de gestion et d'administration des SI, mis en œuvre par les informaticiens au niveau d'un site ou d'une plate forme technique ou par des utilisateurs, généralement responsables des applications.

Dépendant parfois de l'entité ou de la plate forme technologique considérée, les contrôles généraux informatiques regroupent notamment (PROTIVITI, 2004 ; 2) :

- l'organisation générale et la double séparation des fonctions entre informaticiens et non informaticiens d'une part, et entre études et exploitation informatiques, d'autre

part. Ces notions doivent être formalisées dans un organigramme de la Direction des Systèmes d'Information et une description des rôles et responsabilités de ses équipes,

- l'administration de la sécurité technique (réseau et systèmes d'exploitation),
- les procédures de développement / maintenance ou d'acquisition des logiciels et matériels,
- les procédures de mise en production des applications et de leurs évolutions,
- le suivi d'exploitation et la gestion des incidents,
- les sauvegardes et le plan de secours techniques,
- la gestion du parc informatique (cartographie, inventaires),
- les éventuels contrats d'infogérance,
- la méthodologie de gestion des projets informatiques (développements et infrastructures techniques).

Bien que la plupart des contrôles généraux soient réalisés au niveau de la Direction des Systèmes d'Information, certains sont sous la responsabilité des utilisateurs. « Ces CI sont complémentaires des CII précédents et leur combinaison est impérative pour constituer un environnement de contrôle fort » PROTIVITI (2004 ; 2). Dépendant généralement du domaine applicatif concerné, ils rassemblent notamment :

- les droits d'accès aux applications (séparation des fonctions au sein des utilisateurs),
- la validation des mises en production,
- les analyses d'impacts et les plans de secours,
- le suivi des transactions critiques et des modifications de paramétrages applicatifs,
- le suivi des obligations réglementaires (archivage fiscal, contrainte spécifiques au domaine d'activité de l'entreprise comme Bâle II pour les institutions financières).

III.4-2 Contrôles applicatifs

Ce sont des contrôles qui contribuent à assurer l'exhaustivité, la réalité et l'intégrité des données restituées par les applications informatiques. « Ces contrôles incluent les politiques, les procédures et les dispositifs de contrôle définis et mis en place dans les différentes entités par les propriétaires respectifs des applications et des données » PROTIVITI (2004 ; 3). Les contrôles applicatifs contribuent directement au CI des processus s'appuyant sur le SI, en

association avec les contrôles manuels. Dépendant uniquement du domaine applicatif concerné, ce sont notamment :

- les contrôles « programmés » : routine de contrôle de cohérence, de validation des données, etc.
- les états d'anomalies, les états de reporting et les processus de revue associés,
- les automatisations de calcul,
- les interfaces automatisées et les procédures de traitement des anomalies.

Conclusion

Le CI est toujours un sujet d'actualité. Son importance pour les organisations, a été démontrée tout au long de ce chapitre. L'enjeu du CI est la maîtrise des activités. Ainsi, il permet à l'entreprise de lutter efficacement contre la fraude et contribue à l'atteinte des objectifs.

Par ailleurs, le CII est indispensable pour la bonne marche des entreprises informatisées. En tant que rouage essentiel du CI, le CII nécessite une implication et une coopération importantes des directions informatiques et des directions utilisatrices.

CHAPITRE II : EVALUATION DU CONTROLE INTERNE INFORMATIQUE

La mise en place d'un dispositif de CI répond à l'exigence pour le management de faire face aux multiples risques internes et externes à l'entreprise. Il n'existe pas de système de CI éternellement efficace, surtout dans le domaine de l'informatique, où l'évolution est très rapide. « Le respect des mesures de contrôle interne doit être contrôlé en permanence et le système de contrôle interne doit être évalué et adapté » (WILMOTS, 2002 ; 84). D'où la nécessité d'apprécier et d'adapter constamment le CII afin de maîtriser effectivement et totalement l'activité informatique de l'entreprise.

Nous allons à travers ce chapitre présenter :

- dans un premier temps, les outils de l'évaluation du contrôle interne ;
- dans un deuxième temps, la méthodologie de l'évaluation du contrôle interne ;
- dans un troisième temps, le modèle d'analyse et approche pratique.

I Les outils de l'évaluation du CI

Les auditeurs utilisent une multitude d'outils pour l'évaluation du contrôle interne. Leur sélection est fonction de la nature du système d'information de l'entreprise auditée. Par conséquent, on peut les catégoriser en outils traditionnels et en outils informatiques.

I.1 Les outils traditionnels

Nous allons énumérer les plus couramment utilisés. Ils sont au nombre de en cinq. Ce sont les outils de collecte d'information, les outils de description, les outils de diagnostic, les outils de validation et les outils de formalisation.

I.1-1 Les outils de collecte de l'information

Ils sont au nombre de trois :

A Le questionnaire de prise de connaissance (QPC)

« En audit, lorsqu'on parle de questionnaire, il s'agit de questions que l'auditeur doit se poser et non de 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 » (ROUFF, 2001 : 14). Le QPC permet de conduire les interviews et les entretiens divers, et par la même occasion, se familiariser à la structure auditée et bien organiser sa mission.

B Les interviews

L'interview selon RENARD (2004 : 332) n'est ni un entretien, ni un interrogatoire« En audit interne, l'interview est coopératif ».

Sa réussite passe par le respect de certaines règles qui s'inspirent du nécessaire esprit de collaboration qui doit s'instaurer entre audité et auditeur. Ces règles selon RENARD (2004 ; 332) sont au nombre de (07) sept :

- il faut respecter la voie hiérarchique, c'est-à-dire informer le supérieur hiérarchique avant de procéder à une interview,
- rappeler clairement la mission et ses objectifs, l'interlocuteur de l'auditeur doit connaître le pourquoi et le comment de l'interview,
- évoquer avant toute autre chose, les difficultés, les points faibles et les anomalies rencontrées,
- les conclusions de l'interview, résumées avec l'interlocuteur, doivent recueillir son adhésion avant d'être communiquées sous quelques formes que ce soit à la hiérarchie,
- conserver l'approche système, c'est-à-dire se garder de toute question ayant un caractère subjectif et mettant en cause les personnes,
- savoir écouter, c'est-à-dire que l'auditeur doit éviter d'être celui qui parle le plus qu'il n'écoute,
- l'auditeur qui procède à l'interview doit considérer son interlocuteur comme un égal dans la conduite du dialogue.

C L'observation physique

Il consiste à aller observer ce qui se passe sur le terrain. La pratique de l'observation selon RENARD (2004 : 347) exige trois conditions :

- l'observation ne doit pas être clandestine, c'est-à-dire que l'auditeur prévient donc les responsables concernés pour les informer de sa visite et de ses intentions,
- l'observation ne doit pas être ponctuelle, c'est-à-dire elle dure un certain temps ou elle est répétée à plusieurs reprises,
- l'observation doit être toujours validée car elle est incertaine, sauf le cas où elle est elle-même une validation.

I.1-2 Les outils de description

Ils sont nombreux et variés.

A Le diagramme de circulation

Selon RENARD (2004 : 357), «Le diagramme de circulation, ou flow chart, permet de représenter la circulation des documents entre les différentes fonctions et centres de responsabilités, d'indiquer leur origine et leur destination et donc de donner une vision complète du cheminement des informations et de leurs supports».

Le flow chart facilite la compréhension des systèmes complexes et met en relief les points faibles.

B La piste d'audit (Chemin de révision)

La piste d'audit permet de remonter à l'origine d'une donnée. Selon ROUFF (2001 : 15), «Elle permet de retracer un document, une action en partant du point d'arrivée et en remontant à la source ».

A titre d'exemple : vérifier la logique d'un traitement informatique lorsque les données traversent des chaînes informatisées. La piste d'audit présente alors le caractère spécifique d'un audit informatique.

C L'organigramme fonctionnel

Contrairement à l'organigramme hiérarchique, l'organigramme fonctionnel est l'affaire de l'auditeur lui-même. Il le met en place quand il le trouve nécessaire. L'auditeur élabore le diagramme fonctionnel à partir d'informations recueillies par observations, interviews, narrations, …

«Il se caractérise par le fait que, dans les cases, sont inscrits des verbes désignant des fonctions et non des noms de personnes» (RENARD, 2004 : 352).

L'organigramme fonctionnel est très important pour l'auditeur car il permet d'enrichir ses connaissances sur l'organigramme hiérarchique associé aux analyses de postes.

I.1-3 Les outils du diagnostic

Ce sont :

A Le questionnaire de contrôle interne (QCI)

C'est un outil essentiel pour l'auditeur. «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 » (ROUFF, 2001 : 15).

Le QCI est un référentiel conçu dans le but d'évaluer le contrôle interne d'une fonction ou d'une entité. Pour être efficace, il doit être adapté aux spécificités de chaque organisation.

B Le tableau des forces et faiblesses

Selon ROUFF (2001 : 15), «Il donne une vue d'ensemble des forces et faiblesses apparentes ou réelles par rapport aux procédures et règles existantes et aux résultats attendus».

Cette technique permet l'indentification des risques spécifiques à chaque système de l'entreprise.

I.1-4 Les outils de validation

Ce sont :

A Le sondage statistique

«Le sondage statistique est une méthode qui permet à partir d'un échantillon, d'extrapoler à la population, les observations faites sur l'échantillon» (RENARD, 2004 : 349).

Plusieurs types de sondages sont applicables selon les objectifs recherchés. Ce sont:

- des sondages de dépistage : il est à considérer comme un test, une recherche permettant de déceler un dysfonctionnement,
- des sondages pour acceptation : ici le sondage a un rôle mixte ; dépistage possible si on ne connaît aucun élément de réponse, ou appréciation de l'ordre de grandeur si on a découvert un dysfonctionnement,
- des sondages pour estimation des attributs sont la plupart du temps purement informatifs.

B L'examen de l'évidence des contrôles

«Ils consistent 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 des personnes habilitées» (CNCC : 1992).

C La répétition des contrôles

Le travail effectué par le personnel de l'entreprise est refait par l'auditeur, par sondage. Exemple : le rapprochement des fichiers de données est refait par l'auditeur.

D Le test de conformité

Selon la CNCC (1992 : 48), «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».

E Le test de permanence

Il consiste à répéter le test de conformité pour un niveau de sondage acceptable. Le test de permanence permet de valider les points forts théoriques du contrôle interne. «Un point fort théorique n'en demeure réellement un que si la procédure décrite est celle qui est

effectivement appliquée. C'est l'objet des tests de permanence, de vérifier cette permanence de l'application de la procédure théorique» (DERRIEN, 1992 : 209).

I.1-5 Les outils de formalisation des travaux

Ce sont :

A La FRAP (Feuille de Révélation et d'Analyse des Problèmes)

La frappe est un outil d'analyse. L'auditeur l'utilise pour conduire son raisonnement à chaque fois qu'une observation révèle un problème, une difficulté.

Tableau n°2 : Modèle de FRAP

Modèle de FRAP **Feuille de révélation et d'analyse de problème** Référence papier de travail : FRAP N°
Problème :
Constat :
Causes :
Conséquences :
Recommandations :
Etabli par Approuvé par :

Source : RENARD (2004 ; 260)

A constat

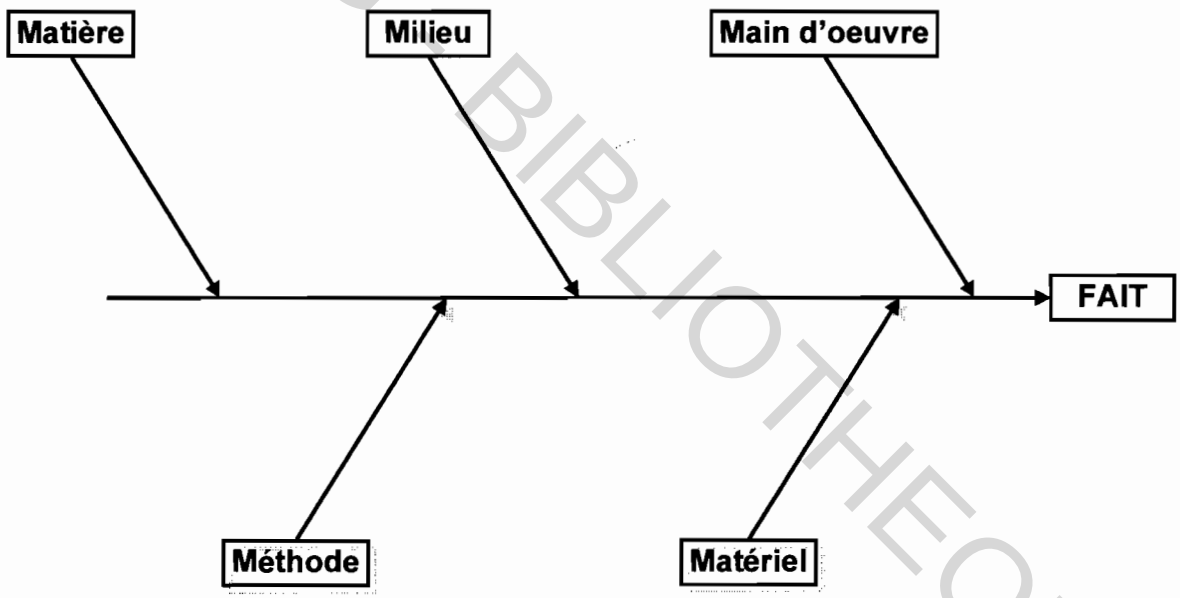
L'auditeur doit énoncer sous cette rubrique l'erreur, l'anomalie, le dysfonctionnement constaté

B causes

Les méthodes d'analyse causale sont nombreuses mais l'auditeur doit utiliser celle qui lui paraît la plus appropriée. L'IFACI (1995 : 97) recommande entre autres le diagramme d'Ishikawa ou d'arête de poisson ou la méthode des 5 M.

- Main d'œuvre,
- Milieu,
- Matière,
- Matériel,
- Méthode.

Figure n°1 Le diagramme d'Ishikawa



Source : RENARD (2000 ; 248)

C Conséquences

L'auditeur quantifie les conséquences du fait constaté dans la mesure du possible. «Les conséquences quantifiées ou appréciées sont également classées selon leur nature» (RENARD, 2004 : 268). On distingue ainsi, les conséquences financières, les conséquences juridiques, les conséquences économiques et les conséquences techniques.

D recommandations

« La recommandation est impérativement l'exacte contrepartie de la cause. (…). La recommandation est une simple remise en ordre » (RENARD, 2004 : 268)

E problèmes

Selon RENARD (2004 : 270), «Le rédacteur de la FRAP énonce le problème après avoir mis le point final à la recommandation».

I.2 Les outils informatiques

Ils sont multiples et variés. Les outils informatiques sont de plus en plus demandés par les auditeurs à cause de l'information intensive et incessante des entreprises de toute taille et tous secteurs. Les fonctionnalités recherchées sont nombreuses et répertoriés par VIDAUX (2001 : 19) comme suit :

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

Nous allons nous intéresser singulièrement à certains outils, qui, il faut le rappeler, ne sont pas les seuls à être utilisés pendant l'appréciation du CII.

I.2-1 Les outils d'analyse des risques

L'analyse des risques selon VIDAUX (2001 : 20), doit se faire de la manière suivante :

- 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 pour en déduire des fiches d'évaluation par entité opérationnelle.

Il propose SPHYNX ou HORUS, des logiciels capables de faire une analyse complète et une cartographie des risques, notamment :

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

A Les jeux d'essais

Cette technique est d'une grande utilité pour les auditeurs en milieu informatisé. Selon OBERT (2004 : 159), « Cette technique consiste à faire traiter par une chaîne informatique des données préparées par le commissaire aux comptes pour comparer les résultats obtenus avec les résultats attendus : ces données comportent généralement des éléments « anormaux » destinés à tester le fonctionnement des contrôles intégrés dans le programme ».

B Utilisation de contrôles programmés

Lorsque les contrôles programmés correspondent aux besoins de contrôle de l'auditeur et si ce dernier a pu s'assurer de son bon fonctionnement, il pourra alors faciliter son contrôle des comptes par l'exploitation des listings d'anomalies générés par l'ordinateur et la vérification de leur apurement à la date de clôture. « S'il n'existe pas de contrôle programmés et que l'environnement de sécurité informatique n'est pas fiable, l'auditeur doit développer ses propres contrôles pour s'assurer que toutes informations ont bien été enregistrées » OBERT (2004 ; 159).

C Utilisation de fichiers de l'entreprise et de programmes spécifiques

Ce type de contrôle peut porter sur la vérification des calculs et additions. « Ces logiciels sont en effet capable de refaire les calculs sur des fichiers importants en un temps limité » OBERT (2004 ; 159).

D Les progiciels d'aide à la révision

Ce sont des programmes informatiques d'application générale destinés exécuter certaines fonctions de traitement des données parmi lesquelles (OBERT, 2004 ; 160) :

- lecture de fichiers,
- sélection d'informations,
- comparaison d'informations,
- exécution de calculs,
- questionnaires,
- impressions d'états sous la forme spécifiée par l'ordinateur.

Ces travaux peuvent être réalisés simultanément sur un ou plusieurs fichiers. Ce sont des logiciels souples et adaptables à un client donné.

I.2-2 Les outils micro-informatiques

Le micro-ordinateur est souvent utilisé pour les travaux sur les grands sites au cours des missions d'audit. « Cette technique permet de rapatrier sur le disque du micro-ordinateur les fichiers désirés sur l'ordinateur central, (…). Les fichiers ainsi exportés pourront ensuite être traités de manière autonome par le micro-ordinateur, (…), avec les outils informatiques sur le micro-ordinateur » (LAMY, 1996 : 70).

I.2-3 Les outils d'aide à la mission

En dehors des logiciels utilitaires, il existe selon MORRISSEY (2001: 25) des logiciels spécifiques d'aide à la mission, qui sont :

A Des logiciels de planification et de suivi des missions

Ce sont des logiciels de marché, régulièrement utilisés et qui permettent la réalisation, le suivi des missions et des recommandations.

Exemple : HORUS

B 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 contrôle.

Certains sont obligatoires (plan comptable) ou sont un recueil de normes d'audit (ISO) ou 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 plus, les résultats de ces investigations sont sauvegardés afin de pouvoir les comparer à d'autres missions

C Les logiciels de présentation

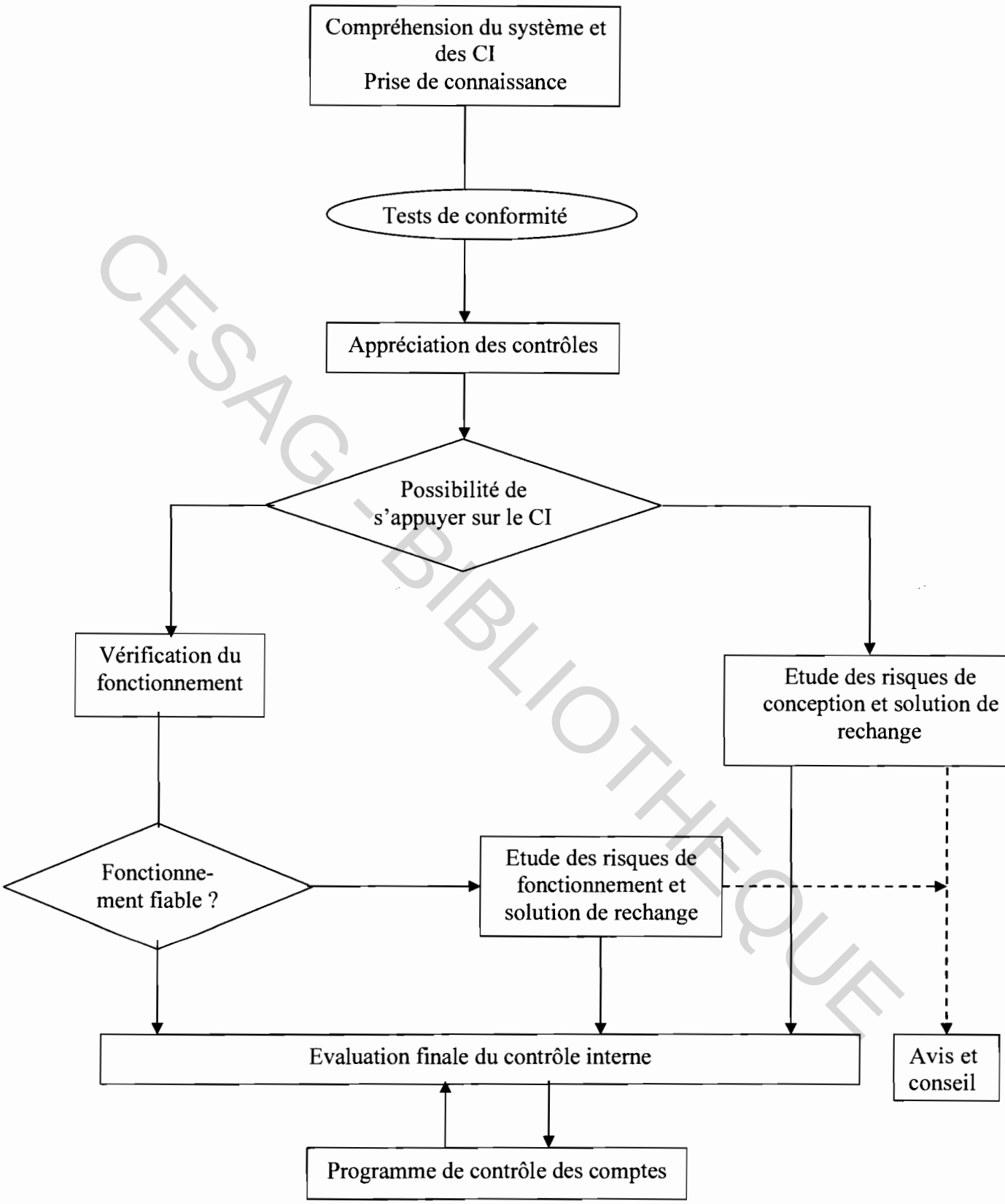
Une chose est d'effectuer un bon travail durant la mission d'audit, une autre en est de capter l'attention des dirigeants de l'entreprise auditée lors de la présentation des résultats. Une présentation ne peut produire l'effet désiré que lorsqu'elle est concise et précise. Les logiciels de dessin sont à cet effet d'une grande utilité. Ils sont utiles dans l'illustration des rapports et pour la réalisation des diagrammes de circulation. « Et POWER POINT excelle dans ce domaine, en concurrence avec FREELAND » (MORRISSEY, 2001).

II La méthodologie de l'évaluation du contrôle interne

Notre méthodologie d'évaluation du CI de la fonction informatique sera décrite ci-dessous et doit permettre :

- de déterminer et d'apprécier la fiabilité des CII
- d'identifier les anomalies de conception ou de fonctionnement du CII

Figure n°2 : Les étapes de l'évaluation du CI



Source : CNCC (1995 : 19)

II.1 Compréhension des systèmes de contrôle interne

Cette étape est essentielle dans le déroulement de la mission d'audit, car elle permet à l'auditeur de s'imprégner des réalités de la fonction informatique. L'existence d'une fonction informatique influe sur toutes les phases de l'audit.

La prise de connaissance consiste en une collecte d'informations ayant trait au système à étudier et à ses particularités. Dans le cas d'espèce, il s'agira d'apprécier la qualité de l'organisation d'ensemble de la fonction informatique. L'objectif de cette prise de connaissance est de comprendre tous les facteurs pouvant avoir un impact sur les comptes. La prise de connaissance selon la CNCC (1995 ; 43), doit porter sur les éléments suivants :

- structure de la fonction informatique et séparation des fonctions en son sein,
- matériel utilisé,
- procédures préalables à la mise en service des systèmes,
- procédures d'exploitation,
- procédures de traitement des données,
- procédures de sécurité,
- listes des applications et sortie des données.

II.1-1 La structure de la fonction informatique

Lors de la prise de connaissance de l'organisation de la fonction informatique, l'auditeur s'attache :

- au rattachement de la responsabilité informatique dans l'organigramme,
- à l'existence d'un véritable plan informatique garantissant la cohérence des systèmes et leur évolution,
- à l'effectif du personnel chargé de mettre en œuvre les décisions informatiques,
- aux dépenses d'investissement et de fonctionnement de l'informatique,
- à la répartition des fonctions entre la fonction informatique et les autres fonctions,
- à la séparation des fonctions au sein de l'informatique (conception, programmation et exploitation),
- à la compétence du personnel et les procédures de recrutement et licenciement (1995 ; 44).

II.1-2 Le matériel utilisé

Pour pouvoir évaluer les risques liés au matériel, l'auditeur doit obtenir une description :

- du type de matériel utilisé,
- de son implémentation géographique,
- des connections existant entre les différents matériels,
- de la capacité de chaque matériel et son ancienneté,
- des évolutions en cours ou prévues CNCC (1995 ; 45).

De même pour les logiciels en service, l'auditeur doit avoir :

- leur inventaire,
- leur origine interne ou externe),
- leur utilisation (fréquence, volumes traités, etc.)
- les évolutions prévues,
- les liens qui existent entre eux CNCC (1995 ; 45).

II.1-3 Les procédures préalables

L'objectif ici, est d'évaluer les risques pouvant résulter de l'utilisation d'applications inadaptées et insuffisamment testées. L'auditeur doit obtenir les informations concernant :

- le processus de décision avant l'acquisition, le développement ou modification de matériel ou d'applications,
- les procédures d'élaboration des cahiers de charges ou de recensement des besoins,
- le critère de choix des sous traitants (pérennité, clauses de contrat, accès aux programmes sources),
- l'implication des utilisateurs dans la définition des besoins et le processus de test des nouvelles applications,
- la formation des utilisateurs CNCC (1995 ; 46).

Pour ce qui est des « applications maisons », l'auditeur doit examiner :

- la qualité des normes de programmation imposée aux informaticiens,
- le respect de toutes les phases d'autorisation et de validation du projet,

- la nature et le volume des tests réalisés,
- les procédures de constitution des fichiers et traitements initiaux,
- les procédures d'autorisation à toute modification ultérieure.

II.1-4 Les procédures d'exploitation

L'auditeur examine les procédures mises en place pour assurer le bon déroulement de l'exploitation :

- manuel,
- auto contrôle de fonctionnement par l'ordinateur,
- supervision des comptes rendus d'exploitation,
- contrôle de bibliothèque de fichiers amovibles,
- vérification des versions de fichiers utilisés,
- procédures de test ou d'auto contrôle du matériel,
- dispositif de contrôle intégrés en matière d'exhaustivité et d'exactitude des traitements CNCC (1995 ; 47).

II.1-5 La sécurité

Les risques liés à la sécurité sont très élevés en matière d'informatique. L'auditeur s'attachera à examiner par conséquent les procédures mises en place sur les points ci-dessous :

A Sécurité physique

- accès aux locaux,
- protection du matériel contre la destruction,
- protection de l'installation électrique,
- assurance.

B Sécurité logique

- Protection de l'accès aux fichiers,
- Gestion des mots de passe,
- Enchaînement de génération de fichiers.

C Plan de secours

- existence,
- test périodique.

D Sauvegarde

- fréquence,
- nombre de générations,
- stockage externe de tous fichiers vitaux,
- stockage interne,
- consigne au personnel en matière de mini et micro,
- vérification régulière du respect des procédures de sécurité.

E **Documentation** qui doit respecter les règles fondamentales de sécurité CNCC (1995 ; 49).

II.1-6 La liste des applications et des sorties informatiques

L'auditeur doit demander :

- la liste des applications utilisées par l'entreprise,
- la liste des fichiers existants,
- l'inventaire des états produits par chaque application et leurs destinataires,
- les liens existant les différentes applications,
- les volumes et la fréquence des traitements par application.

II.2 Le test de conformité

L'objectif de ce test n'est pas de permettre à l'auditeur de conclure que la procédure est régulièrement appliquée ; mais de confirmer que son descriptif représente bien la procédure telle qu'elle est prévue par le service informatique. « Cette confirmation de la compréhension du système, ou de la vérification de son existence, est réalisée par un test de conformité (ou d'existence) » (CNCC, 1992 : 48).

II.3 Appréciation des contrôles

Une fois les objectifs de la mission clairement définis et la collecte des informations de base effectuée, l'appréciation des contrôles peut alors commencer. Cela implique l'élaboration d'un plan de contrôle dépendant à la fois des objectifs recherchés et des spécificités du système. Ce plan de contrôle peut s'inspirer d'un questionnaire de CI, qui devra le plus souvent être aménagé de façon à rester pleinement pertinent dans le cas particulier étudié.

Il s'agit de s'assurer que le processus satisfait aux objectifs de CI selon un référentiel préalablement conçu.

Cette évaluation portera sur l'organisation de la fonction informatique. En effet, il faut prendre en compte surtout la séparation des fonctions et la définition des responsabilités. La séparation doit être nette entre le service informatique et les autres services de l'entreprise. « S'il est fréquent que le système informatique participe à l'autorisation et à l'enregistrement de certaines opérations, il doit le faire sous le contrôle des services utilisateurs » OBERT (2000 ; 147). La séparation doit être également observée à l'intérieur de la fonction informatique pour qu'aucune personne ne dispose sans contrôle de la maîtrise totale du système. Quant à la définition des responsabilités, elle est du ressort du directeur général. « Il est important, pour le bon fonctionnement du CI, que la direction générale de l'entreprise définisse, de préférence par écrit, les responsabilités et les pouvoirs respectifs des informaticiens et des utilisateurs » OBERT (2000 ; 148).

Les faiblesses relevées, doivent être portées à la connaissance des dirigeants. Par ailleurs l'auditeur doit également procéder à l'examen des procédures alternatives éventuellement mises en place afin de pallier les insuffisances apparentes du système.

Tableau n°3 : Insuffisance de contrôle et risques potentiels

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

Source : DAI de la SENELEC (2004)

II.4 Vérification du fonctionnement des systèmes

Ce sont des tests de fonctionnement, visant à s'assurer de l'existence effective des points forts dégagés au cours des travaux. En effet, les informations collectées au stade de la prise de connaissance du système méritent d'être vérifiées, car il est fréquent que :

- le fonctionnement réel du système diffère de la perception qu'en a un individu isolé ;
- la documentation ne reflète qu'imparfaitement l'état du système en raison notamment de la difficulté de la tenir à jour.

Les tests ont pour objectif 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. Ce sont l'examen de l'évidence des contrôles ; la répétition des contrôles, l'observation physique.

Auxquels, il faut ajouter les jeux d'essais, des logiciels d'audit, la réalisation de « chiffriers » de contrôle de traitement.

Pour JENKINS et PINKNEY (1984 : 238), les tests de fonctionnement dans un environnement informatique, se situent à quatre niveaux :

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

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

- **des contrôles de matérialité des contrôles**; 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 car l'auditeur ne dispose pas toujours du savoir-faire et de l'expérience du personnel pour répéter ces contrôles à sa place.

II.5 Etude des risques de conception, de fonctionnement et solution de rechange

La vérification du fonctionnement devrait révéler des zones à risques non couverts par des points forts. Ces zones représentent alors les points faibles du fonctionnement, et elles constituent avec les points faibles de conception, l'ensemble des faiblesses du CI. 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 les résultats, sur les comptes et états financiers.

La FRAP est d'une grande utilité lors de cette étape. Elle permettra à l'auditeur de relever chaque fois que cela est possible un dysfonctionnement, une erreur, une malversation, une insuffisance, etc.

La FRAP selon RENARD (2004 : 259), est un moyen d'analyse simple et claire, d'une efficacité redoutable et conduit le raisonnement de l'auditeur à seule fin de l'amener à formuler une recommandation.

II.6 Recommandations

La recommandation formulée par l'auditeur doit être judicieuse car la qualité de son travail en dépend. Il y aura autant de recommandation que de FRAP utilisée. « Chaque constat donne lieu à une recommandation de l'auditeur » (RENARD, 2004 : 299).

Concernant les faiblesses, A.T.H (1991 : 151) écrit : « En cas d'incidences significatives 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 ».

L'auditeur à travers les recommandations, propose des améliorations d'un coût raisonnable et ayant pour objectif d'éliminer toute source de risques dont l'entreprise ou la fonction auditée peut éviter.

III Modèle d'analyse et approche pratique de l'évaluation

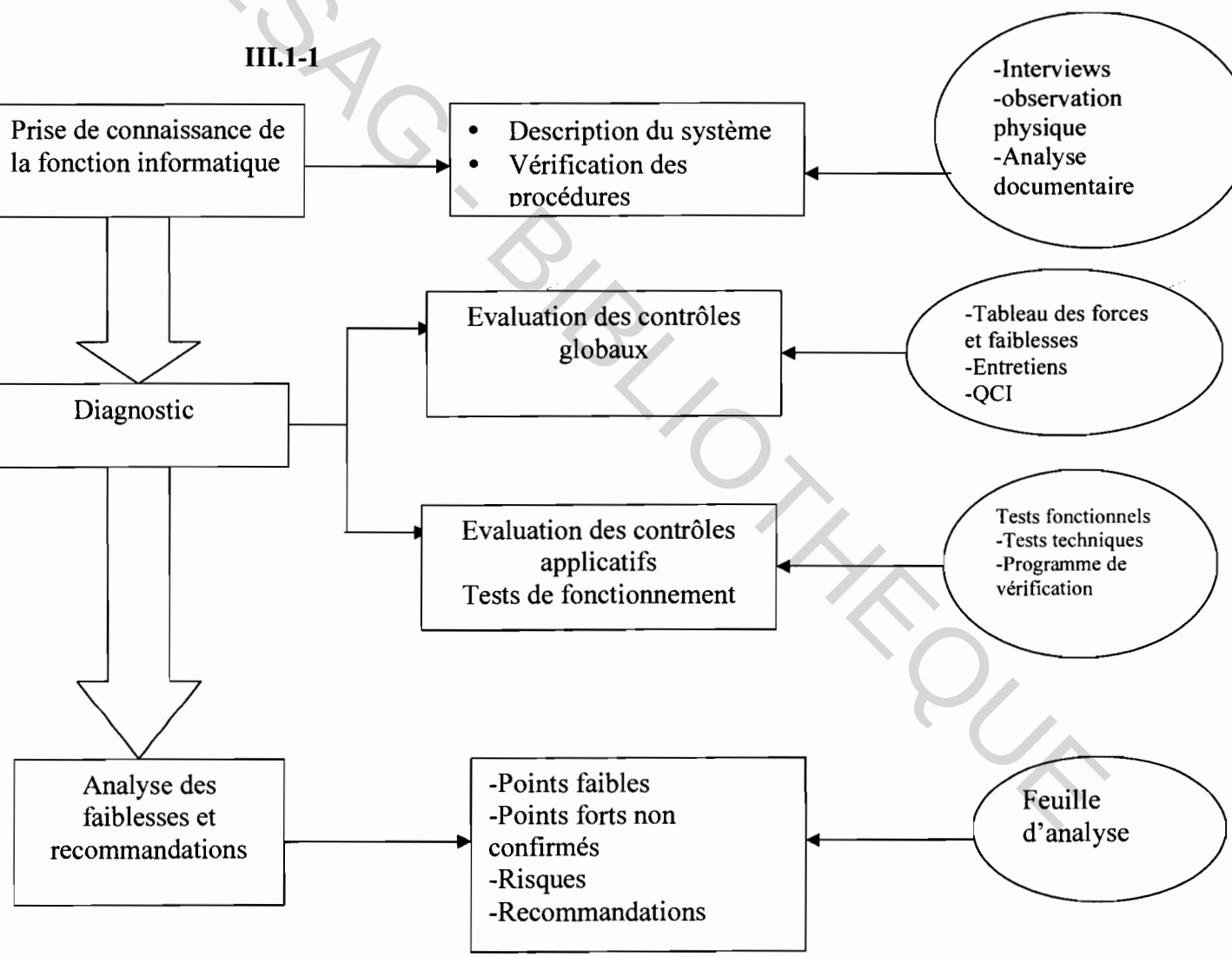
Dans le cadre de mener à bien notre étude sur l'évaluation du CI attaché à la DSI de la SENELEC, nous avons axé notre démarche sur la méthodologie de l'audit mais en occultant le programme de contrôle des comptes.

III.1 Elaboration du modèle d'analyse

Contrairement à notre revue de littérature qui a mis en exergue les cinq composantes du CI, notre modèle s'articule autour des points suivants :

- prise de connaissance de la fonction informatique ;
- diagnostic ;
- analyse des faiblesses et recommandations.

Figure n°3 : Modèle d'analyse



Source : nous même

Prise de connaissance de la fonction informatique

Cette phase est essentielle. Comme au niveau général de l'entreprise, nous avons procédé à une prise de connaissance spécifiquement informatique.

III.1-2 Diagnostic

Cette phase est composée de deux étapes que nous avons suivies au cours de notre étude. Il s'agit de l'évaluation des contrôles globaux et celle relative aux contrôles programmés.

III.1-3 Recommandations

Cette phase nous a permis, après avoir relevé puis analysé les points faibles théoriques et les points forts non confirmés, de faire des recommandations.

Tableau n°4: Décomposition des variables d'évaluation

VARIABLES	DIMENSIONS	INDICATEURS	MESURES
L'organisation de la fonction informatique	➢ Organisation interne	▪ Organigramme ▪ Définition des postes ▪ Séparation des fonctions	-Existence -Manuel de procédure -effectivité
	➢ Contrôles hiérarchiques	▪ Procédures de supervision des tâches	-Existence et application
	➢ Mise en place des systèmes	▪ Plan informatique	-existence et application
	➢ Sécurité physique	▪ Procédures de prévention ▪ Procédures de back up	-Existence et application -Existence et test de simulation (6 mois au moins)
	➢ Sécurité logique	▪ Historique des tentatives d'accès illicites ▪ Mots de passe ▪ Sauvegarde des programmes et fichiers	-Journalisation et analyse -Existence -Effectivité
Les applications en service	➢ Fiabilité	▪ Traitements erronés ▪ Contrôles programmés	-Non existence -Existence et efficacité

Source : nous même

III.2 La collecte des données

La collecte des données s'est faite selon les étapes suivantes.

III.2-1 Procédure d'échantillonnage

A Les interviewés

Pour notre interview, nous avons eu comme interlocuteurs les personnes suivantes :

- le directeur du contrôle de gestion (DCG) ;
- le chef du service BUDGET et ANALYSE ;
- le délégué aux systèmes d'information ;
- le chef du service d'études ;
- le chef du service d'exploitation ;
- le directeur de l'audit interne (DAI) ;
- le directeur commercial (DC) ;
- le chef du service de distribution.

Notre interview a couvert aussi bien les personnes intervenant dans les services utilisateurs que celles assurant les activités informatiques.

B Les applications en service

Les applications utilisées présentement par la SENELEC sont le progiciel ORACLE et une application développée en interne appelée : le SIC.

III.2-2 Méthode de collecte des données

Les outils ci-dessous nous ont permis de faire la collecte des données. Ce sont :

- **les interviews** avec des personnes pouvant nous fournir des informations utiles pour notre étude. Elles ont été menées à l'aide d'un guide d'entretien (voir annexe 5) dont l'objectif est de faire la description du contrôle interne attaché à la fonction informatique :

- **analyse documentaire** : elle nous a permis de nous rendre compte de l'existence effective des procédures de développement et de maintenance, de l'inexistence des procédures informatiques. Nous avons passé en revue la documentation et nous nous sommes assurés de l'existence d'un plan informatique ;
- **l'observation physique** ; nous avons avec l'aide du chef de service Infrastructures et réseau pu constater que les procédures de sécurité concernant les systèmes informatiques existent et fonctionnent.
- **le questionnaire de contrôle interne** ; nous l'avons construit à partir de nos interviews avec les fonctionnels et les opérationnels. Nous nous sommes appuyés sur le questionnaire standard d'audit informatique qui nous a servi de référentiel. Le questionnaire a été administré au DSI et aux trois (03) chefs de service de la DSI. Il a également été administré aux responsables des services utilisateurs et leurs collaborateurs. Notre questionnaire a été élaboré dans le but de satisfaire les objectifs du CI de fonction informatique (voir annexe n°1).
  - **Tests fonctionnels ;** ils ont consisté à faire des contrôles croisés entre d'une part les informaticiens et d'autre part les utilisateurs de sorte à mettre en relief les forces et faiblesses du système informatique.
- **Tests techniques** ; appelés aussi jeux d'essais, ils ont consisté en des traitements réels par des applications de notre échantillon.

Conclusion partielle

L'évaluation CI est une nécessité pour toute entreprise. Le CI ne fournissant qu'une assurance raisonnable, c'est son évaluation qui permet de l'adapter au changement, c'est-à-dire faire face aux menaces nouvelles ou menace en mutation. Par conséquent, pour être optimum, le CII doit être constamment évalué pour l'adapter à l'évolution rapide de l'informatique. Les outils d'évaluation sont nombreux mais ceux qui intéressent notre étude sont les outils informatiques.

DEUXIEMME PARTIE

Evaluation du contrôle interne informatique de la SENELEC

Après notre revue de littérature sur le CI et singulièrement sur le CI informatique, cette deuxième partie est pour nous l'occasion de nous faire une idée sur le CI attaché à la fonction informatique de la SENELEC.

Notre appréciation dans ce cadre portera d'une part sur des contrôles globaux et d'autre part sur des contrôles applicatifs

Cette deuxième partie sera composée de deux chapitres à savoir :

- la présentation d'ensemble de la SENELEC
- diagnostic et les recommandations

CHAPITRE I : PRESENTATION D'ENSEMBLE DE LA SENELEC

La société nationale d'électricité (SENELEC) est située au 28, rue Vincens à Dakar.

Avec un capital de plus de 119 milliards de francs CFA, la SENELEC est l'une des grandes entreprises industrielles du Sénégal.

I Présentation de la SENELEC

Il sera question ici de l'historique, de l'organisation, des activités de la SENELEC et du contexte des travaux.

I.1 Historique

La fusion de la société de patrimoine Electricité Du Sénégal et de la société chargée de l'exploitation des ouvrages, Société Sénégalaise de Distribution d'Energie Electrique donne naissance en 1983 à une société unique, créée par la loi n°83/72 du 05 juillet 1983 : la Société Nationale d'Electricité (SENELEC).

La première décennie (1985-1995), qui a suivi la création de la société a permis la mise en œuvre du premier projet du secteur électrique destiné à l'accroissement des infrastructures de la nouvelle société. C'est ainsi que le renforcement du parc de production, des réseaux de transport et de distribution s'est effectué progressivement avec pour conséquence, l'augmentation du volume de ventes d'énergie.

Dans le cadre de la reforme du secteur de l'énergie, le gouvernement avait décidé en janvier 1998, d'une ouverture de capitale au public, pour pouvoir régler le problème de délestage. La société a ainsi été transformée en société anonyme et le 31 mars 1999 le capital est ouvert à un partenaire stratégique : HYDRO QUBEC et ELYO.

Face à la persistance des difficultés dans la distribution de l'électricité, le gouvernement sénégalais décide de rompre avec ses partenaires stratégiques. Après une concertation entre l'Etat et ces derniers, la rupture est consommée le 21 septembre 2000 et l'Etat sénégalais redevient l'unique actionnaire de la SENELEC.

I.2 Organisation de la SENELEC

La SENELEC pour pouvoir mettre en application son projet d'entreprise « SUXALI SENELEC » a adopté une nouvelle organisation, qui se présente comme l'indique son organigramme (voir l'annexe 6).

I.2-1 Au niveau stratégique

Une **Direction Générale** coordonne les activités de la SENELEC. Elle est épaulée par un **Secrétariat Général** dont les missions se présentent comme suit :

- assister le Directeur général dans ses fonctions et assurer son intérim en cas d'absence ;
- coordonner la préparation des réunions des organes délibérants ;
- veiller à l'application et au respect des décisions de la direction générale ;

I.2-2 Au niveau hiérarchique

Nous trouvons à la SENELEC des collaborateurs directs du directeur général et ceux du secrétaire général.

- Sept (07) Directions et deux (02) Délégations sont sous la responsabilité directe du directeur général à savoir :
  - la **Direction de la Production** qui a en charge l'exploitation et la maintenance des unités de production du réseau interconnecté, des centrales régionales et secondaires ;
  - la **Direction des réseaux** : elle a pour mission l'exploitation et la maintenance de l'ensemble des réseaux basse, moyenne et haute tension ;
  - la **Direction Commerciale** qui est chargée de la définition et du suivi de l'exécution des politiques devant assurer une meilleure qualité de service à l'ensemble de la clientèle (clients spéciaux, clients d'affaires, clients administrations, clients réguliers) ;
  - la **Direction de la Planification et de l'Equipement** : elle a pour mission d'effectuer des études de la planification technique et économique en vue de

définir les plans d'investissement à moyen et long termes relatifs à la production, au transport et à la distribution ;

- la **Direction des Etudes et Relations avec les Institutions** : elle est chargée des études économiques, tarifaires et des statistiques générales de l'entreprise. Elle est aussi chargée des relations avec les autorités de tutelle (Commission de Régulation du Secteur de l'Electricité et l'Agence Sénégalaise d' Electrification Rurale), de la négociation et du suivi des accords avec l'Etat (contrat de concession, cahier des charges) ;
- la **Direction des ressources humaines** qui est chargée de l'administration et du développement prospectif des ressources humaines de l'entreprise ;
- la **Direction des Finances et du Contrôle de gestion** : elle est responsable de la recherche et de la mobilisation des ressources financières et chargée du contrôle de gestion ;
- La **Délégation à la Communication** qui s'occupe de la définition et de la mise en œuvre de la stratégie de communication interne et externe en vue d'améliorer l'image de marque de l'entreprise. Elle gère les relations publiques de la SENELEC ;
- La **Délégation aux Mouvements d'Energie et Télécommunication** : elle est responsable du placement optimal des moyens de production du réseau interconnecté, des achats auprès des producteurs indépendants et des importations d'énergie électrique dans le cadre des accords internationaux ;

o Trois (03) directions et deux (02) Délégations sont la responsabilité directe du secrétaire général :

- la **Direction de l'Audit Interne et Contrôle Général** qui veille au respect des normes techniques de réalisation, d'exploitation et de maintenance des ouvrages. Elle veille également à l'application de critères objectifs pour le choix d'entreprises prestataires de service ainsi qu'au respect par toutes les parties des dispositions contractuelles ;
- la **Direction de la Comptabilité** : elle est chargée de l'enregistrement exhaustif de toutes transactions commerciales et financières de la société, de la production dans les délais imposés des états financiers de fin d'exercice ;

- la **Direction Achats et Logistique** : elle est chargée de l'ensemble des services généraux de l'entreprise et des fonction relatives à l'approvisionnement en matériels, fournitures d'exploitation et d'entretien ;
- la **Délégation des Systèmes d'Information** qui est responsable du système d'information informatique de la l'entreprise
- la **Délégation aux Affaires juridiques** : elle pour mission de conseiller la Direction Générale sur les questions d'ordre juridique. Elle donne des avis sur les questions soumises par les différentes unités et participe à l'élaboration des différents contrats. Elle est aussi chargée du suivi des contentieux.

I.3 Les activités de la SENELEC

La SENELEC assure la production, le transport et la distribution de l'électricité sur toute l'étendue du territoire sénégalais.

I.3-1 La production

La SENELEC dispose de plusieurs zones de production :

- **le réseau interconnecté** : il est situé dans la partie occidentale du pays. Il sert à alimenter toutes les villes qui lui sont connectées; c'est-à-dire Dakar, Diourbel, Kaolack et Saint-louis. Les installations de production de ce réseau se situent à Bel Air et au Cap des Biches (pour Dakar) ; Saint-Louis et Kaolack (Fatick).
- **le réseau non interconnecté**
  - les centrales régionales : elles sont au nombre de deux et sont constituées par la centrale de Boutoute (Ziguinchor) et celle de Tambacounda.
  - les centrales secondaires : dix-huit (18) centrales secondaires sont exploitées par la SENELEC. Elles permettent de satisfaire les localités centrales régionales non interconnectées.

I.3-2 Le transport

Les moyens de transport sont constitués de lignes haute tension de 225 kV exploitées en 90 kV et de lignes moyenne tension de 30kv. Les principales lignes sont :

- ligne 225kv : Cap des Biches-Tobène-Sakal
- ligne 90kv : C3 Hann ; C3 Bel Air ; C4 Cap des Biches.

I.3-3 La distribution

Les lignes de distribution sont constituées de ligne moyenne tension 30 kV et 6,6 kV et des réseaux de distribution Basse tension

I.4 Contexte des travaux

L'évaluation du CI est intervenue dans un contexte d'amélioration sensible de la gestion de la SENELEC. En effet, la nouvelle direction souhaiterait évaluer en termes humains, matériels et financiers, la conformité et l'efficacité de ses SI pour mieux apprécier l'adéquation de ces derniers par rapport aux besoins réels, présents et futurs de l'organisation.

La volonté d'ouvrir une ère nouvelle dans la gestion de la SENELEC s'articule autour de trois objectifs majeurs :

- l'amélioration de la qualité des services,
- l'assainissement et la modernisation de la gestion,
- l'optimisation de l'usage des ressources.

L'atteinte de ces objectifs passe entre autres par la mise en place d'un SI informatique robuste, fiable et conviviale. Ainsi la mission a été organisée autour des objectifs spécifiques suivants :

- évaluation de la fonction informatique,
- évaluation des applications existantes.

II La fonction informatique de la SENELEC

La présentation de cette fonction essentielle se fera à travers les éléments suivants :

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

II.1 Organisation et gestion la DSI

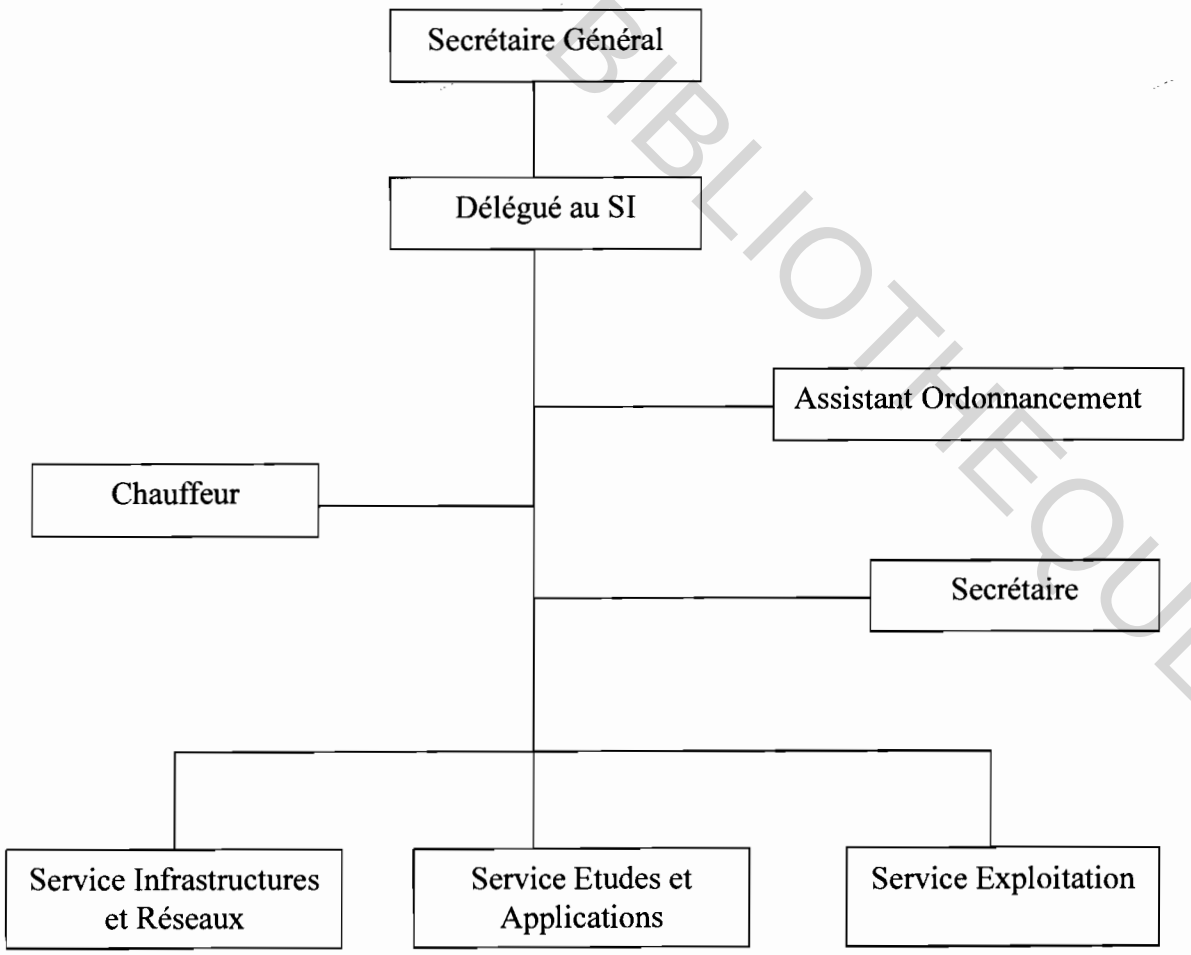
La DSI, garante de la cohérence du SI de la SENELEC est ainsi organisée.

II.1-1 Présentation de la DSI

La fonction informatique de la SENELEC est désignée par Délégation aux systèmes d'Information. Les SI sont placés sous la responsabilité de la DSI, qui joue un rôle de support pour l'organisation SENELEC et doit contribuer à la bonne marche des unités opérationnelles et de gestion. Pour cela, des missions lui ont été assignées et la DSI, est aujourd'hui structurée en trois (03) services :

- le service Infrastructures et Réseaux,
- le service Etudes et Applications,
- le service Exploitation.

Figure N°4 L'organigramme de la DSI



Source : DSI (2005)

1.1-1 Missions

La Délégation aux SI est chargée de :

- la gestion sécurisée des infrastructures informatiques et des télécommunications de données,
- la réalisation, l'acquisition et/ou la maintenance des applications logicielles,
- la gestion sécurisée des données,
- la veille technologique,
- la politique d'acquisition du parc de matériels informatiques.

1.1-2 Le service Infrastructures et Réseaux

Ce service est chargé de la gestion des systèmes et des réseaux de télécommunications des données de la SENELEC. Il assure l'acquisition, le suivi et la maintenance de l'ensemble du parc de matériels informatiques. Il assure aussi la formation et le support technique aux utilisateurs.

1.1-3 le service Etudes et Applications

Il est chargé des développements, de la maintenance, de la documentation des applications, de l'intranet/Internet, du paramétrage, de l'acquisition des progiciels et de la prise en compte des requêtes ou restitutions des utilisateurs, dès la phase de conception des produits.

1.1-4 le service Exploitation

Ce service est chargé de la gestion et de la sécurité des données :

- disponibilité des données en temps réel, via un accès sécurisé ;
- sauvegarde régulière des informations de manière localisée et délocalisée ;
- gestion de l'archivage des documents suivant un procédé respectant les valeurs caractéristiques des différentes fonctions de la SENELEC en relation étroite avec la Documentation.

II.1-2 Architecture des systèmes d'information

Elle est bâtie sur un ensemble de deux types de plateforme :

- une plateforme propriétaire type mainframe Bull DPS7000,

- une plateforme Windows utilisant un réseau privé virtuel IP basé sur le réseau SENTRANET de la SONATEL.

1.2-1 Système propriétaire sur DPS7000

Ce système est constitué de deux mainframe DPS7000 couplés partageant toutes les ressources (Disques de stockage et dérouleur de bandes).

Une double liaison Ethernet à 2MB permet de raccorder les DPS7000 au VPN de la SENELEC comme un serveur.

Les trois passerelles ATLANTIS (SRV1 SRV2 EXPL) gèrent l'utilisation des micro-ordinateurs en émulation « terminal » et les échanges de données avec les autres systèmes.

1.2-2 Synoptique général du réseau privé IP

Le VPN de la SENELEC s'adosse sur le SENTRANET de la SONATEL et est structuré comme suit :

- une interconnexion de tous les sites avec le siège,
- un accès distant via RTC/RNIS géré par un routeur RAS type CISCO AS5300,
- un accès INTERNET via CISCO 2600 géré par un serveur Internet,
- plusieurs serveurs.

II.2 Le système informatique de la SENELEC

C'est un système dense et varié.

II.2-1 Historique et évolution

L'informatisation de la SENELEC est loin d'être récente et les perspectives concernant l'informatique sont bonnes.

2.1-1 Historique

Le service informatique de la SENELEC a connu une véritable instabilité depuis une vingtaine d'années. De service mécanographique, elle est passée service informatique en

1986. Depuis lors, elle est passée de Département en Direction et de Direction en Délégation. Ces différents changements se perçoivent à travers le tableau ci-dessous

Tableau n°5: Historique de l'informatique

Années	Dénomination	Rattachement
1986	Département Informatique	Direction du Contrôle de gestion (DCG)
1992	Département Informatique	Direction Administration Comptabilité et Informatique (DACI)
1994	Département Informatique	Direction Innovation Planification et Equipement (DIPE&DIIPE)
1999	Direction des systèmes d'information	Direction Générale
2002	Département Informatique	Direction de la logistique
2003	Délégation à l'informatique	Direction Générale
2004	Délégation aux SI	Secrétariat Général

Source : DSI (2005)

Il existe un plan directeur élaboré par un cabinet. Ce schéma directeur prend en compte les besoins exprimés par le projet d'entreprise « SUXALI SENELEC » et qui à moyen terme, doit permettre à la SENELEC d'être très performante.

2.1-2 Extrait du Schéma directeur informatique et sa mise en œuvre

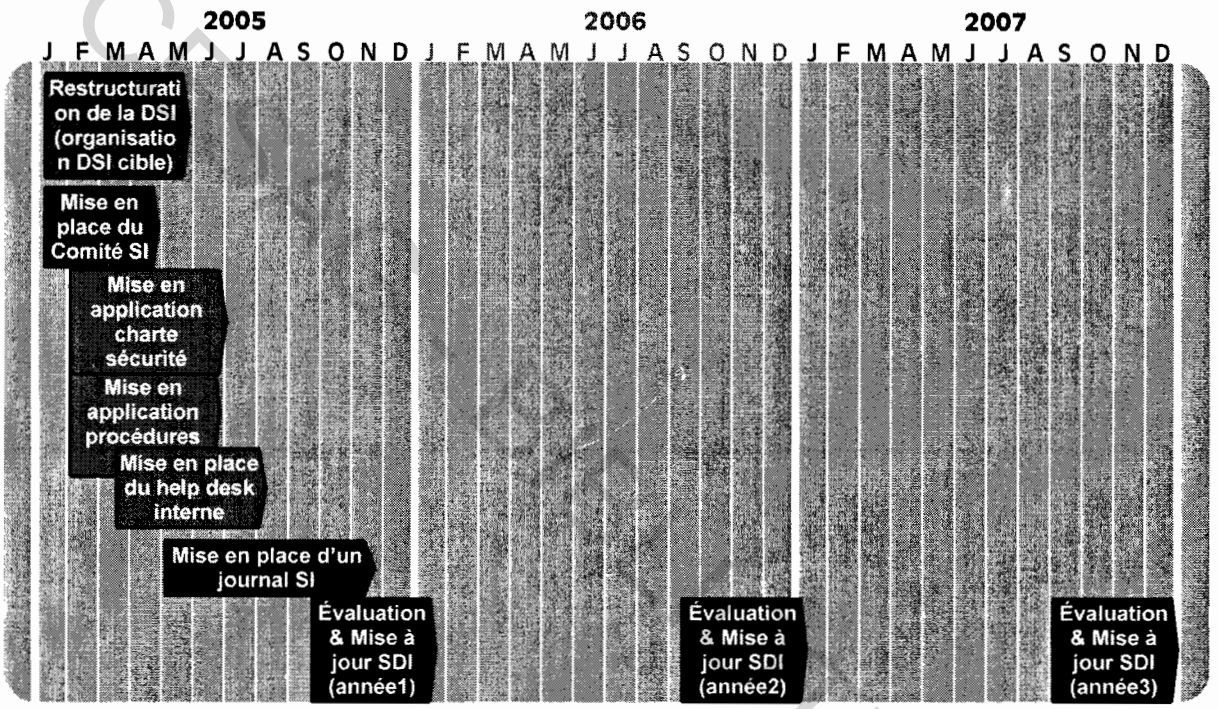
a) Le schéma directeur

Le plan directeur informatique de la SENELEC est étalé sur trois ans, de 2005 à 2007 et est axé sur les points suivants : Organisation, Infrastructure et Applications.

- **Organisation**

Il s'agit de la restructuration de la DSI, de la mise en place d'un comité directeur, d'un help desk interne et d'un journal du SI ; de la mise en application de la charte sécurité et des procédures.

FIGURE n°5 : Extrait du schéma directeur (Organisation)



Source : DSI (2005)

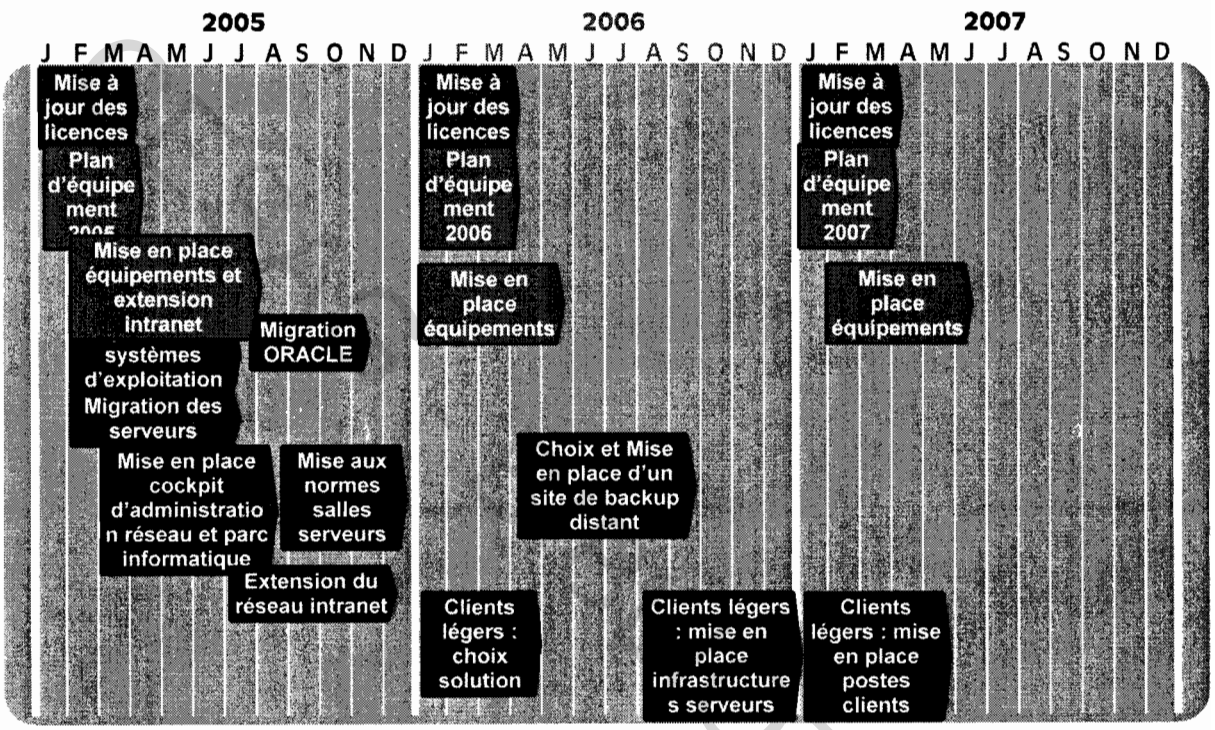
- **Infrastructures**

Le schéma directeur concernant les infrastructures, présente les éléments ci-dessous :

- mise à jour des licences ;
- plan d'équipements 2005 ;
- mise en place des équipements et extension de l'intranet, du système d'exploitation, migration des serveurs et ORACLE ;
- mise en place d'un cockpit d'administration réseaux et parc informatique ;
- mise aux normes salles serveurs ;
- extension du réseau intranet

- choix et mise en place d'un site de back up ;
- client légers : choix et solution ;
- clients légers : mise en place infrastructures serveurs ;
- mise en place des postes clients.

FIGURE n°6 Extrait du schéma directeur (infrastructures)



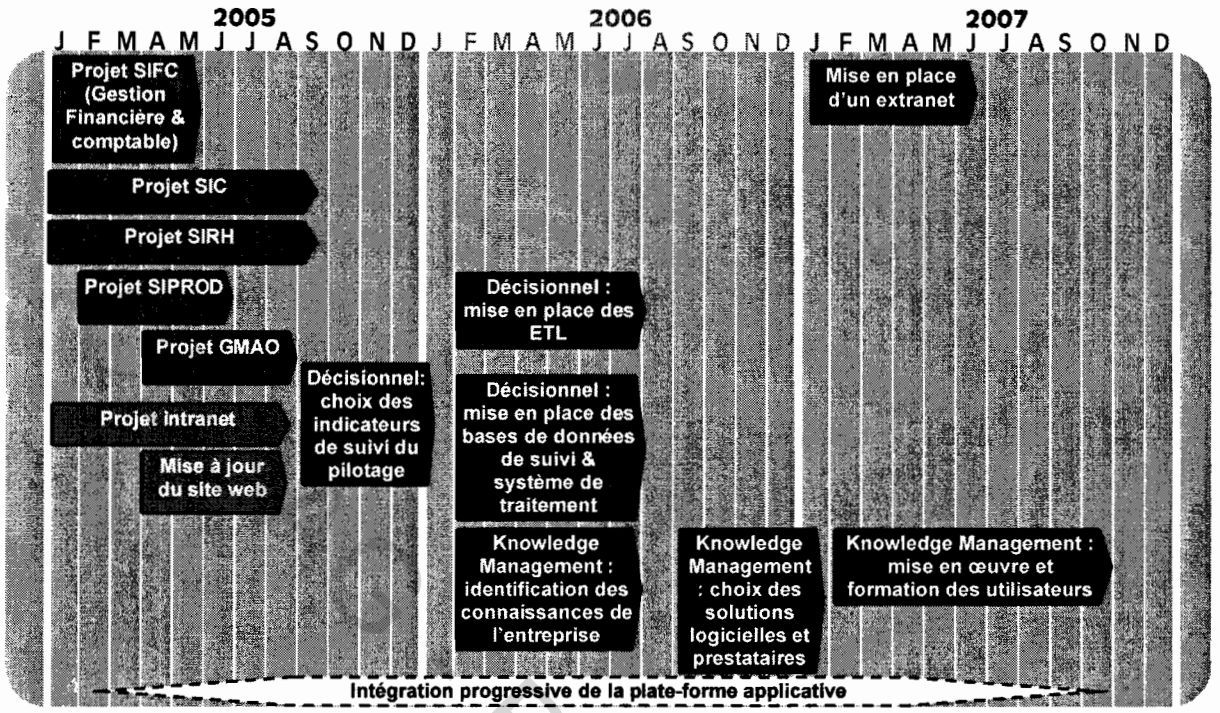
Source : DSI (2005)

- **Applications**

Le plan directeur des applications tourne autour des points suivants :

- projet SIFC ;
- projet SIC ;
- projet SIRH ;
- projet SIPROD ;
- projet GMAO ;
- projet Intranet ;
- mise à jour du site Web ;
- etc.

FIGURE n°7 Extrait du schéma directeur (applications)



Source : DSI (2005)

b) La mise en place du plan directeur

Le plan directeur informatique de la SENELEC fixe des objectifs claires et précis, qui doivent être atteints sur trois (03) années, découpées en trois phases (2005 ; 2006 ; 2007).

Cet important projet informatique, qui doit soutenir le développement de l'activité de l'entreprise, risque de connaître de sérieuses difficultés. En effet, le schéma directeur devrait normalement connaître un début d'application depuis janvier 2005. Mais l'absence de budget pour le service informatique depuis 2004 pourrait entraver la réalisation effective de cet important projet.

Nous avons découvert à la suite de notre analyse documentaire que les budgets antérieurs du service informatique étaient dérisoires. En outre, le responsable de la Délégation nous a affirmé que ça fait deux (02) ans qu'ils n'ont pas bénéficié de budget. Cette situation, si elle n'est pas corrigée risque d'avoir un impact négatif partiellement ou totalement sur la mise en place d'un SI cohérent devant permettre la réalisation du plan stratégique.

II.2-2 Description du patrimoine informatique

Le patrimoine informatique de la SENELEC est bien fourni et, est composé de :

- matériel ;
- logiciels.

2.2-1 Matériel

Le parc informatique de la société comprend :

- 376 unités centrales ;
- 391 écrans ;
- 203 imprimantes ;
- 58 onduleurs
- 04 serveurs d'infrastructures ;
- 03 serveurs Annuaire ;
- 04 serveurs de base ;
- 01 serveur de messagerie ECHANGE ;
- 01 serveur WEB ;
- 03 serveurs d'applications ;
- 02 serveurs de fichiers ;
- 04 passerelles ATLANTIS ;
- 01 serveurs d'impression ;
- 01 PIX Firewall (pare-feu) ;
- 01 serveur ISA ;
- 01 SWITCH (Catalyst 3524) avec des ports GIGABIT pour le BACKBORN ;
- 02 LS de 2MB et 1MB reliant à la SONATEL ;
- Double lien fibre Optique entre le bâtiment DRH et le siège ;
- Double lien fibre Optique entre le bâtiment DCC et le siège.

2.2-2 Les logiciels

La SENELEC utilise pour sa gestion différents types de logiciels, regroupant les logiciels systèmes, les progiciels acquis et les logiciels développés en interne.

a) Le progiciel acquis

Depuis 1998, la SENELEC s'est dotée d'un logiciel standard puissant : « ORACLE APPLICATIONS ». Ce progiciel est totalement intégré et comprend les modules suivants :

- ORACLE IC : gestion des stocks ;
- ORACLE PO : gestion des achats ;
- ORACE FA : gestion des immobilisations ;
- ORACLE AP : gestion des fournisseurs ;
- ORACLE RH : pour le calcul de la paie.

Le module ORACLE GL en interaction avec les autres modules permet de gérer :

- la comptabilité générale ;
- la comptabilité analytique ;
- la comptabilité budgétaire ;
- la comptabilité engagement.

b) Le logiciel développé en interne

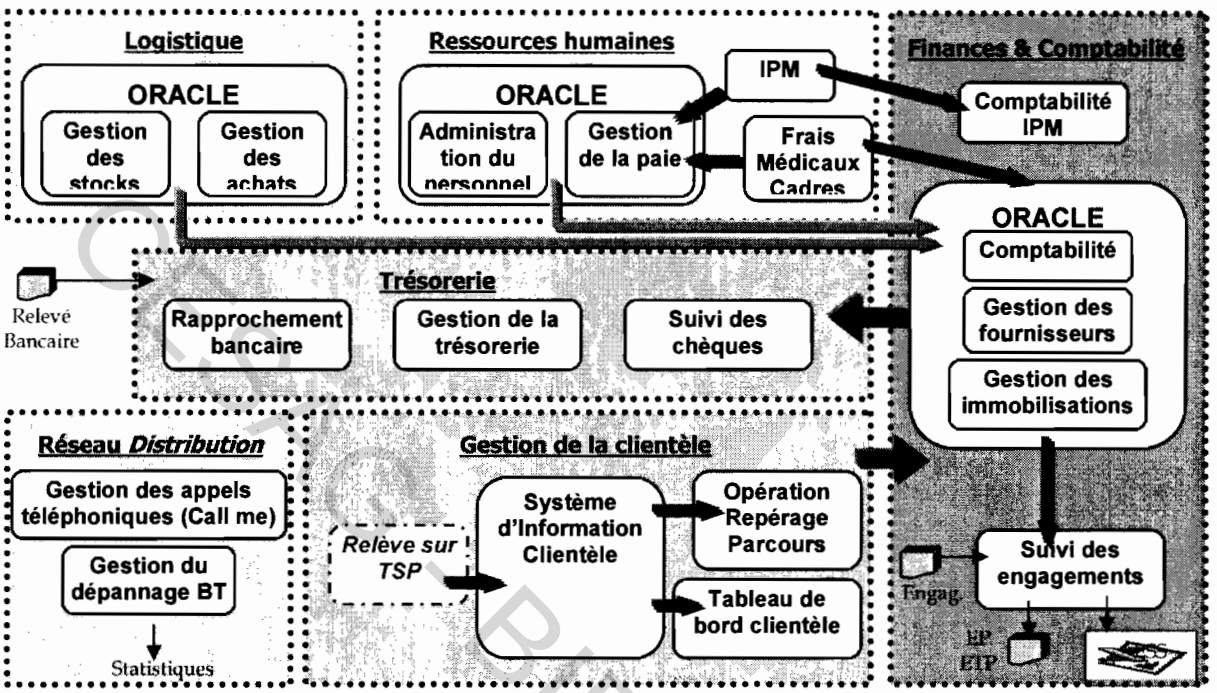
L'entreprise a développé un seul logiciel spécifique appelé « logiciels maison ». C'est l'application SIC permettant de suivre les revenus clients à partir de différents modules.

c) La cartographie des applications

Cette cartographie montre les différentes interactions existant entre les applications (développées en interne et acquises sur le marché) utilisées par la SENELEC.

FIGURE n°8

La cartographie actuelle de la plate-forme applicative



Source : DSI (2005)

II.2-3 Description des applications

Après l'interview qu'a bien voulu nous accorder le personnel informatique et particulièrement le chef du service Etudes et Applications, nous avons noté que le SIC est un produit entièrement maison regroupant plusieurs modules. Contrairement au SIC, l'application Oracle est un progiciel acquis sur le marché, composé aussi de plusieurs modules intégrés pour la gestion comptable et budgétaire.

2.3-1 L'application SIC

Elle gère différents modules.

A Les différents modules du SIC

Le SIC comprend plusieurs modules.

a) La gestion des abonnés

Ce module permet de gérer un client pendant toute la durée de son contrat avec la SENELEC. IL permet de visualiser toutes les informations concernant un client et de les modifier éventuellement. On peut accéder à un client par plusieurs critères.

b) La programmation des visites

Ce module permet d'élaborer le calendrier journalier des visites à effectuer chez le client suite à une demande d'abonnement, d'avenant, de changement de compteur ou de résiliation.

c) La nouvelle demande d'abonnement

Ce module a pour objet le traitement et le suivi d'une nouvelle demande. La demande est suivie étape par étape depuis l'enregistrement au guichet, jusqu'à la première facturation.

d) L'avenant au contrat

Ce module a pour objet le suivi et le traitement des demandes d'avenant. La demande est suivie étape par étape depuis l'enregistrement au guichet jusqu'au traitement final.

e) La résiliation

Ce module a pour objet la résiliation du contrat d'un client. Les demandes sont suivies étape par étape.

f) Le changement de compteur

Ce module a pour objet de prendre en compte les demandes de changement de compteur suite à une défectuosité constatée. La demande est suivie étape par étape depuis son enregistrement jusqu'au traitement final ; c'est-à-dire le remplacement du compteur défectueux, la facturation et la prise en compte du nouveau compteur dans le fichier des abonnés.

g) La relève facturation cyclique

Ce module permet de gérer l'activité de la relève des compteurs de la clientèle d'une agence. Chaque agence a la latitude de la programmation de sa relève, de l'édition des coupons de

relève, de la saisie des index relevés, de l'estimation des clients non relevés et du déclenchement de la facturation.

Avant chaque facturation, le système offre à l'utilisateur la possibilité de contrôler et de recycler les anomalies de consommation en temps réel.

h) La facturation acyclique

Ce module a pour objet la facturation exceptionnelle du client (en dehors du cycle normal). Il offre d'énormes possibilités.

i) La gestion des coupures, délais et moratoires

Ce module a pour objet la gestion des coupures (sélection et édition des bons de coupures), des délais, des moratoires et le suivi de l'après coupure ; c'est-à-dire saisie du compte rendu de la coupure, l'édition des bons de remise après paiement, la sélection et l'édition des bons de vérification pour les abonnés sous coupures.

j) La fonction caisse

Ce module gère des sessions d'encaissement.

k) Les mouvements auxiliaires hors caisse

Ce module est un complément de celui de la fonction caisse. Il permet de gérer les avis de débit, les avis de crédit, les régularisations extracomptables, l'extourne C.A.R, le redressement du compte client et l'édition du journal hors caisse.

l) Le reclassement

Ce module permet de modifier la référence commerciale d'un client suite à une réorganisation de la tournée de relève, à un rééquilibrage des bordereaux ou groupe, à un transfert de client d'une agence à une autre.

m) La fraude

Ce module a pour objet le traitement et le suivi de la fraude depuis sa déclaration jusqu'à la facturation du client.

n) Le programme de recensement

C'est un complément au module de la fraude. Ce module permet d'une part de détecter les présomptions de fraude et d'autre part de mettre en conformité le fichier « Abonnés » suite aux informations recueillies sur le terrain.

p) Les branchements provisoires

C'est un contrat de fourniture d'énergie à durée déterminée où les consommations d'électricités sont évaluées au forfait et réglées à l'avance. La procédure peut être ainsi résumée :

- saisie de la demande d'un branchement provisoire ;
- prise en compte des informations technico-commerciales ;
- pose du branchement, saisie de la pose et programmation de la dépose ;
- dépose du branchement et régularisation des factures.

q) La segmentation du compte client

Ce module permet le transfert et le suivi des clients résiliés dont la facture finale est échue, du portefeuille normal vers le précontentieux et le contentieux jusqu'à sa passation en pertes diverses.

Quant aux clients « normaux », ils seront différenciés par la notion de « qualité payeur » dont les valeurs permettent de discriminer les clients lors de l'analyse du compte client pour coupure.

r) Les tableaux de bord encaissement

Ce module permet le suivi régulier des encaissements au niveau des différents établissements de la SENELEC. Il permet de visualiser les encaissements physiques globaux validés, les encaissements non validés, les encaissements d'une agence ou d'un secteur donnée.

s) Les tableaux de bord du SIC

Ce module permet de comparer les résultats des différents centres de responsabilités aux objectifs préalablement fixés ou à des ratios. Les informations sont extraites du système opérationnel, triées et agrégées par centre de responsabilité.

B Sécurité du système et confidentialité de l'information

Une sécurité entoure le SIC. L'application comporte trois (03) niveaux de sécurité à savoir :

a) Au niveau utilisateur

L'utilisateur potentiel de l'application est pré-identifié dans le système, avec consignation de matricule, du mot de passe secret et crypté, de l'établissement d'appartenance et des droits liés à sa fonction.

Ces paramètres permettent les filtres suivants :

- autorisation de création du mot de passe,
- autorisation à travailler sur le SIC,
- autorisation à accéder à un module,
- autorisation à accéder à un sous module.

b) Au niveau établissement d'appartenance

Les données sont décentralisées car chaque agence (établissement) est responsable d'un lot de clients. Pour modifier un client géré par un établissement donné, il faut que l'utilisateur en soit membre.

c) Au niveau information

Certaines informations très importantes font l'objet de surveillance particulière. En cas de modification de l'une de ces informations, l'événement est journalisé, c'est-à-dire que l'on consigne dans un fichier, le matricule de l'intervenant, la date, l'heure, le numéro du terminal, l'ancienne et la nouvelle valeur. Ce journal est édité pour la hiérarchie pour contrôle.

2.3-2 L'application Oracle

Cette application gère plusieurs modules périphériques, qui sont intégrés et partagent certaines règles et informations de gestion :

- gestion commune de fichier fournisseurs
  - adresse ;
  - informations fiscales ;
  - conditions de règlement ;
  - facturation.
- fichier des ressources humanes
  - les habilitations ;
  - traitement des salaires.
- rapprochement des données
  - commandes /réceptions ;
  - réception/facturation ;
  - facturation/règlement.
- fichier des immobilisations
  - calcul des amortissements
- entités comptables
  - clé comptable flexible ;
  - calendrier comptable ;
  - devise.

A Les différents modules de l'application Oracle

L'application Oracle est une famille de produits intégrés où plusieurs modules se partagent des données ou des valeurs suivant un schéma bien défini (voir annexe n°4)

a) Oracle GL : (General Ledger): Comptabilité générale

Oracle GL occupe une position centrale dans l'application Oracle en tant que « synthétiseurs » des événements gérés dans les autres modules.

b) Oracle AP : Gestion des fournisseurs

Oracle AP gère les événements cycliques porteurs d'informations comptables. Il gère et boucle le cycle fournisseur qui commence de la réception d'une facture jusqu'à son règlement.

c) Oracle PO : Gestion des achats ou des commandes

Cette application gère l'ensemble des achats de la SENELEC. L'application contient sept (07) familles de produit, disposant chacune d'un compte ouvert pour les opérations la concernant.

d) Oracle FA (Fixed Assets) : Gestion des immobilisations

L'application gère les immobilisations en calculant leur amortissement pour l'exercice venant de prendre fin.

e) Oracle HRMS (Human Ressources Management System) : Gestion des ressources humaines

Cette application a deux (02) sous modules :

- Oracle Paie qui gère l'administration du personnel (états civils, niveau de rémunération, les éléments de salaire et les congés),
- Oracle RH gère les ressources humaines comprenant la formation, la gestion des carrières, la gestion des compétences et le système d'évaluation.

f) Oracle IC : Gestion des stocks

Cette application permet la comptabilisation des matières et gère le stock à partir du magasin central vers les autres magasins disséminés dans tout le pays.

B Sécurité du système

Il y a autour de l'application Oracle divers types de sécurités. Il y a les règles de sécurité et les règles de validation croisées.

a) les règles de sécurité

Elles sont effectuées à chaque niveau de responsabilité pour restreindre l'accès à certaines valeurs de segment lors des interrogations, de l'utilisation de la liste de valeurs, desinsertions et mises à jour. Les règles de sécurité sont les suivantes :

- limitation à certaines responsabilités ;
- l'accès à une société ;
  - accès exclusif à FOPES ;
  - accès limité à SENELEC.

b) Les règles de validation croisée

Ce sont des règles de validation inter segment, qui permettent de contrôler les combinaisons de clé comptable flexible utilisées et qui sont incorrectes. Elles rendent ainsi plus fiable le traitement des informations de gestion.

Les combinaisons invalides seront accompagnées d'un message d'erreur à la saisie, précisant le motif d'invalidation.

Conclusion

La fonction informatique de la SENELEC est de taille moyenne. Elle est subdivisée en services importants que sont les services « Infrastructures et Réseaux », « Etudes et Applications » et « exploitation ». La Délégation aux systèmes d'information est composée de personnel qualifié et le patrimoine informatique est important et varié.

Le système d'information et de gestion de la clientèle (SIC) est une application importante pour la société, qui a en outre acquis sur le marché un progiciel puissant « ORACLE APPLICATIONS » dans le but d'améliorer considérablement son SI.

CHAPITRE II : DIAGNOSTIC ET RECOMMANDATIONS

Notre analyse de terrain concernant le CI de la fonction informatique, nous a conduit à examiner deux contrôles principaux de la fonction informatique de la SENELEC. Il s'agit d'une part des contrôles globaux (contrôles généraux informatiques) et d'autre part des contrôles applicatifs (contrôles d'applications informatisées).

I LES CONTROLES GLOBAUX

Nos interviews avec le délégué aux SI et les différents chefs de service de la DSI, les tests fonctionnels et les analyses documentaires, nous ont permis d'apprécier ces contrôles qui sont indispensables à une fonction informatique.

Notre examen a porté sur l'organisation générale de la fonction informatique scindée en :

- contrôles organisationnels ;
- contrôles de la sécurité informatique.

I.1 Contrôles organisationnels

Nous avons subdivisé ces contrôles en :

- organisation et positionnement du service informatique ;
- contrôles hiérarchiques ;
- contrôles de mise e place des systèmes.

I.1-1 Evaluation de l'organisation et du positionnement du service informatique

La grille d'analyse des tâches nous a permis d'analyser les différentes tâches des agents de la DSI.

Tableau n°6 : Grille d'analyse des tâches du personnel informatique

N°	Nature des opérations	TACHES / INTERVENANTS	DSI	IR	EA	EXP	IR	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				
4	De	Etude			X			
5	De	Recherche de solution logiciel (analyse)			X			
6	De	Gestion des projets informatiques			X			
7	De	Rédaction des dossiers techniques			X			
8	Co	Organisation et mise en place des procédures				X		
9	De	Installation et mise en place des cartes réseaux					X	
10	De	Ecriture (développement)			X			
11	Ex	Assistance aux utilisateurs					X	
12	Co	Suivi et encadrement des stagiaires					X	
13	Ex	Tests des programmes			X			
14	Ex	Rédaction de guide utilisateurs						
15	Ex	Formation des utilisateurs						
16	Ex	Exploitation				X		X

Source adapté : nous même **Légende :**

Co : tâches destinés au contrôle
De : tâches destinées à l'étude et au développement
Ex : tâches destinées à l'exploitation
M. **N'diaye** : Le délégué aux systèmes d'information (**DSI**)
M. **Kandé** : Chef du service Infrastructures&Réseaux (**IR**)
M. **Huchard** : Chef du service Etudes et Applications (**EA**)
M **Mbodje** : Chef du service Exploitation (**EXP**)
M. **Touré** : Agent du service Infrastructures&Réseaux (**IR**)

Ce tableau montre qu'il y'a cumul de tâches incompatibles à la DSI.

1.1-1 Points forts

- Un organigramme existe et définit clairement les postes.
- Cette organisation de la DSI fait apparaître une séparation des fonctions entre informaticiens et les utilisateurs chargés de l'exploitation.

1.1-2 Points faibles

- L'organigramme n'est pas régulièrement mis à jour. Pour preuve, le nouvel organigramme de la DSI qui devrait être mis en place depuis l'année dernière, n'est pas encore devenu effectif.
- A regarder de près la grille d'analyse, nous nous rendons compte de la non séparation de certaines tâches incompatibles :
    - le chef du service Etudes et Applications intervient dans les tâches d'exploitation ;
    - un agent du service Infrastructures&Réseaux intervient dans les charges d'administrations et d'exploitation.
- Il n'existe pas d'autonomie budgétaire à la DSI. Ceci induit, du fait des hiérarchies à respecter, une lourdeur dans le circuit administratif de décision et d'autorisation. Ce qui est contraire au principe de réactivité qui doit caractériser le fonctionnement des services de la DSI dont l'objectif essentiel est de satisfaire les clients internes à travers une disponibilité maximale des ressources informatiques.
- Il n'y a aucune valorisation des prestations de services internes entre la DSI et les autres directions.
- La DSI est rattachée au secrétariat général. Ce qui la met dans une position de subordination qui ne favorise pas une souplesse de fonctionnement, une autonomie et une réactivité indispensable au regard de ses attributions et responsabilités au sein de l'organisation.
- Le statut de Délégation attribué à la fonction informatique ne rend pas compte de l'aspect stratégique de son activité et de son importance dans l'organisation SENELEC.

- Il n'existe pas de plans de carrière au sein de la fonction informatique. Ce qui ne permet pas au personnel de faire une projection de leur évolution professionnelle à moyen terme.
- Il n'y a pas de politique de formation. Les formations sont effectuées au coup par coup afin de faire face à un besoin immédiat, et ne sont pas structurées de manière à inscrire l'évolution des compétences de chaque agent dans la durée. En outre, la répartition de formations est hétérogène au sein de la DSI. Cette situation engendre notamment une concentration des compétences sur quelques agents ainsi qu'une mauvaise répartition des charges de travail.
- Il y a absence d'un comité informatique au sein de la SENELEC.

1.1-3 Risques

- La non satisfaction des besoins des utilisateurs, faute de moyens conséquents.
- Le service fourni par la DSI n'étant pas évalué, il y a risque d'existence de la non qualité.
- Le DSI risque de se laisser accaparer par les aspects opérationnels des projets informatiques au détriment de ses fonctions managériales et l'activité informatique.
- Il y a risque de démotivation et de perte des compétences.
- Le personnel risque d'être à la traîne de la technologie.
- Les choix de matériels effectués par la DSI risque de l'être plutôt en fonction de l'intérêt technique qu'en fonction de leurs qualités intrinsèques. De même, les priorités en matière de développement de logiciel pourraient être influencées par la qualité des relations de la DSI avec les différentes Directions de la SENELEC, ou encore par le caractère plus ou moins innovant de l'application à concevoir, autant que par l'importance que représente celle-ci pour l'entreprise.

1.1-4 Recommandations

- Il faut régulièrement mettre à jour l'organigramme de la DSI.
- Une réorganisation des attributs des services et personnes pour améliorer la séparation et la répartition des tâches, ainsi que la productivité.
- Il faut repositionner la DSI vis à vis de la Direction Générale et des autres Directions, c'est-à-dire la rattacher directement à la Direction Générale et lui conférer un statut de

Direction dans le nouvel organigramme. Cela permettra d'intégrer l'informatique dans la réflexion stratégique (plan stratégique).

- La mise en place de plan de carrière et de programme de formation doit être effective pour tous les agents de la DSI de sorte qu'ils aient une visibilité claire de leur évolution professionnelle et que la DSI puisse assurer la veille technologique.
- Profiter de la création des nouveaux postes de contrôleur de gestion délégué prévue par la SENELEC, pour en installer un à la DSI. Ce contrôleur de gestion délégué pourrait aider à la valorisation des prestations de service interne et faire un rapport au contrôleur de gestion de la SENELEC. Ce qui incitera la DSI à améliorer considérablement ses offres de service.
- Il faut mettre en place un comité informatique, qui sera composé d'un représentant du Directeur Général, le DSI et les responsables des autres Directions et Délégations.
- Il faut permettre à la DSI d'élaborer son propre budget comme toutes les autres Directions et Délégations. La DSI pourrait être aidée dans cette tâche par le contrôleur de gestion délégué.

I.1-2 Evaluation du contrôle hiérarchique

1.2-1 Points forts

- L'utilisateur potentiel du SIC est pré-identifié dans le système, avec consignation du matricule, du mot de passe secret et crypté, de l'établissement d'appartenance et des droits liés à sa fonction. De même, dans Oracle GL, la gestion des responsabilités s'articule autour des notions « d'utilisateurs » et « responsabilités ». Chaque utilisateur de Oracle GL est identifié par un mot de passe, pour accéder à une ou plusieurs responsabilités dans Oracle Application. Une responsabilité correspond à un niveau d'autorisation qui limite les possibilités d'un utilisateur aux seules fonctions et données, en rapport avec les activités qui lui incombent à la SENELEC. Chaque responsabilité détermine :
  - la ou les applications auxquelles l'utilisateur a accès ;
  - l'entité comptable qu'il peut utiliser ;
  - la liste des fonctions qu'il peut utiliser ;
  - les états que l'utilisateur peut exécuter.

Cela contribue à la séparation de fonctions et à la protection des données et des informations.

- Certaines informations au niveau du SIC font l'objet d'une surveillance particulière. Et en cas de modification d'une de ces informations, l'événement est journalisé. Quant à Oracle GL, la liste des responsabilités est la suivante :
  - administrateur système (réservé à l'informatique) ;
  - gestionnaire comptable ;
  - opérateur comptable ;
  - manager budget.

De manière générale dans l'application Oracle, les transferts de valeurs entre modules sont contrôlés par les responsables désignés, habiletés à exécuter certaines actions. Les contrôles de supervision sont donc de ce fait prévus et assurés.

- Il existe à la SENELEC une Direction d'Audit Interne dynamique qui pourrait exercer un contrôle de second degré.

1.2-2 Points faibles

- Toutes les attributions de la DSI ne sont pas couvertes par le staff en fonction.
- Il n'existe aucune compétence en audit informatique au sein de la DAICG. Ce qui limite considérablement son champ d'intervention. La DAICG ne peut par exemple organiser une mission d'audit de la DSI.
- Le DSI ne dispose pas d'outils dédiés lui permettant de couvrir de façon optimale l'ensemble des critères généralement utilisés en matière de pilotage de l'activité informatique : critères économiques, de performances opérationnelles, de satisfaction des directions opérationnelles, de gestion des compétences des collaborateurs et de suivi des risques.

1.2-3 Risques

- La DSI pourrait être exclue des missions de la DAICG.
- La non atteinte des objectifs de la DSI

1.2-4 Recommandations

- Il faut renforcer les compétences de la DAICG par le recrutement d'un spécialiste en Audit informatique.

- Il faut mettre en place un tableau de bord informatique pouvant servir d'outils de pilotage au DSI.

I.1-3 Contrôle de mise en place des systèmes

1.3-1 Points forts

- La DSI dispose d'un plan directeur formalisé et approuvé par la Direction Générale. Ce schéma directeur élaboré par un cabinet, permettra à la SENELEC de contrôler le devenir de son système informatique.
- Des tests sont effectués sur les applications développées avant leur mise en service.
- L'étude fonctionnelle de ces applications a été approuvée par les utilisateurs.

1.3-2 Points faibles

- Il n'existe pas de procédures formalisées de fonctionnement au sein de la DSI, à l'image de la SENELEC toute entière. Cela dénote de l'absence d'une démarche structurée d'intervention.
- Il n'existe pas de règles liées à la documentation des modifications (objet du besoin de modification, l'identité du demandeur, l'auteur du script, les conditions, la date, l'explication de la situation présente, le problème qui se pose et l'objectif à atteindre après la modification, la procédure ou le script lui-même, le tests en base de tests).
- La formation des utilisateurs présente parfois des insuffisances, qui engendrent une charge supplémentaire de support pour la DSI.
- La DAICG n'a pas été associée à la mise en place du projet Oracle dès le départ.
- Aucun document écrit ne décrit les dispositions prises par la DSI pour faire évoluer le SI selon des critères de qualité définis conjointement avec les directions opérationnelles.
- Absence d'une démarche adéquate d'acquisition du progiciel : le choix du projet Oracle ne s'est pas fait sur la base d'une étude approfondie. Ce qui a eu pour conséquence :
    - une concertation insuffisante des acteurs ;
    - une analyse des besoins incomplets ou insuffisants ;
    - une absence d'analyse détaillée de l'ensemble des fonctionnalités des applications avec les besoins réels des utilisateurs ;

- une mauvaise estimation de l'ampleur et de la complexité du projet, qui s'est caractérisée par une sous-évaluation des charges de travail, une implication insuffisante des utilisateurs et une appréciation des délais non estimée avec réalisme.

- Certains aspects relatifs à la conduite de changement n'ont pas été suffisamment pris en compte dans la gestion du projet Oracle :
  - en effet, le niveau de maîtrise des outils logiciels par les utilisateurs reste hétérogène ;
  - la mise en place du projet Oracle ne s'est pas accompagnée d'une démarche de conduite de changement, qui serait matérialisée par une appropriation par les utilisateurs de leurs outils ;
  - De plus, une partie du retard constaté dans le projet s'explique aussi par une résistance au changement des utilisateurs qui n'ont pas une culture informatique développée.

1.3-3 Risques

- Dans la mesure où aucune procédure de fonctionnement, ni méthodologie d'intervention n'est définie en amont, il ne peut exister un système de contrôle performant.
- Il y a risque de modification anarchique.
- La non implémentation des procédures de gestion dans les applications.

1.3-4 Recommandations

- La mise en place d'un manuel de procédures au sein de la DSI est plus que nécessaire et contribuera à n'en point douter à l'amélioration de l'activité informatique. Le manuel « des systèmes et procédures informatiques », qui fixe les normes de travail informatique, est un bon outil de contrôle interne de la fonction informatique.
- Il faut mettre en place une documentation concernant la maintenance et la documentation des applications.
- Il faut renforcer la formation des utilisateurs de sorte à les rendre plus autonomes dans l'utilisation des applications en service.
- La SENELEC devra revoir et le plutôt sera le mieux, sa méthode de qualification des applications, afin de :

- associer plus étroitement les utilisateurs à la définition des jeux de tests ;
- réaliser formellement une validation des produits livrés ;
- se conformer aux meilleures pratiques en la matière.

I.2 Contrôle des sécurités informatiques

Les sécurités informatiques sont une priorité pour toute organisation. La DSI en est bien consciente mais…

I.2-1 Tests d'évaluation

2.1-1 Sécurité physique

Nous avons échangé avec le chef du service Infrastructures et Réseaux sur les problèmes sécurité physique. Il ressort de notre entretien que les mesures prises pour protéger les ressources informatiques de la SENELEC laissent à désirer. Autrement dit, les protections mises en œuvre en ce qui concerne ce patrimoine important sont insuffisantes.

2.1-2 Sécurité logique

La gestion des habilitations est une composante essentielle du dispositif de sécurité logique du SI de la SENELEC. Pour cela des procédures des habilitations ont été mises en œuvre au siège et dans les agences.

Nous avons à partir de l'agence de Médina essayer de modifier un client géré par l'agence principale, mais notre tentative s'est avérée infructueuse. De même nous avons demandé à l'utilisateur du « traitement de la demande » d'accéder au module « relève facturation ». La tentative a échoué.

Au niveau de l'application Oracle, cette sécurité est plus élaborée et fonctionnent normalement et au niveau des modules auxiliaires et au niveau du module principal.

I.2-2 Evaluation de la sécurité physique

2.2-1 Points forts

- Il existe un contrat de maintenance souscrit par la SENELEC.
- Les serveurs sont bien protégés.

- Le personnel d'exploitation n'a pas accès à la bandothèque.
- Il existe un système de détection de fumée et chaleur.
- Un transformateur d'isolement et un régulateur de tension existent pour assurer la protection contre les variations du courant électrique.
- Les conditions de température des salles machines sont impeccables.
- Une copie des sauvegardes des données de production est conservée dans une banque de la place.

2.2-2 Points faibles

- Il n'existe pas à ce jour de plan de continuité des activités.
- Des instructions incendies sont méconnues des agents ainsi des comportements à observer en cas d'incendie.
- Les sauvegardes de données ne font pas l'objet de tests afin de s'assurer de leur intégrité et de leur fiabilité.
- La continuité de fonctionnement n'est pas assurée sur chaque segment du réseau (salle machine, routeurs de connexion à Internet).
- Certains onduleurs sont dans un état de délabrement avancé.
- Le taux de panne des machines est élevé.
- Absence de cartographie du réseau et de risque.
- Absence de plan de back up formalisé.

2.2-3 Risques

- L'absence de procédures de plan de continuité formalisées entraînerait une perte de temps considérable en cas d'un sinistre grave et la SENELEC risque de ne pas pouvoir assurer la continuité de son activité dans un temps relativement court.
- En cas d'incendie criminel ou non, le risque de panique général est probable et cela pourrait entraîner des dégâts matériels énormes et des pertes en vies humaines.
- La non localisation rapide des problèmes sur le système informatique.

2.2-4 Recommandations

- Il faut mettre en place un plan de continuité incluant :

- un plan de secours focalisé sur le traitement des incidents (restauration des sauvegardes, système de back up, procédures d'escalade en cas de dysfonctionnement majeur).
- des procédures dégradées manuelles, définissant un mode de fonctionnement dégradé de la SENELEC et ses agences en cas e cas d'indisponibilité de ses systèmes.
- un plan de reprise d'activité, couvrant les SI (restauration des fichiers) mais également la reprise des sauvegardes d'informations non stockées sur support magnétique.

Le plan de continuité doit être tenu à jour selon l'évolution des procédures de gestion et des systèmes de l'entreprise. Il doit être testé périodiquement (au moins une fois chaque 06 mois) pour détecter des faiblesses et apporter des améliorations nécessaires.

- Il faut mettre en place une procédure de sécurité incendie.
- La disposition des appareils en salles machines au siège et dans les agences pourrait être améliorée. Il conviendrait en effet de:
  - reprendre le courant stabilisé et le câblage du siège ;
  - les locaux sont à revoir pour la sécurisation du système informatique ;
  - organiser les racks et la disposition des serveurs dans les salles machines différentes afin de se prémunir en cas de sinistre localisé dans une salle des serveurs ;
  - s'assurer que la totalité des serveurs sont branchés sur des prises munies d'onduleurs en bon état ;
  - remplacer les 400 machines NEC achetées sur appel d'offre par la SENELEC.
  - signer des contrats de maintenance pour les serveurs et les micro-ordinateurs. Ceci d'autant plus que les serveurs contiennent des applications centralisées et donc sensibles pour l'ensemble des sites utilisateurs de la société.
  - mettre en place une cartographie du réseau avec les Directions et Services utilisateurs de sorte qu'on puisse :
    - identifier rapidement l'équipement en cause de dysfonctionnement ;
    - catégoriser les risques et leur degré de criticité en cas de panne par rapport aux activités de chaque direction opérationnelle.

- formaliser sous forme de procédure les règles de back up en cas de sinistre. Ces règles devraient être spécifiées tant pour le siège que pour les agences :
  - la localisation des établissements du back up ;
  - l'ordonnancement des tâches en cas de sinistre ;
  - une affectation claire des responsabilités de chacun en de reprise des activités.

I.2-3 Evaluation de la sécurité logique

2.3-1 Points forts

- L'accès aux différents modules du SIC se fait par mots de passe et identifiants personnels. Les paramètres (consignation du matricule, droits liés à sa fonction, etc.) filtrent les entrées et permettent l'utilisation des différents modules par les vrais utilisateurs.
- Chaque utilisateur de Oracle GL est identifié par un mot de passe, pour accéder à une ou plusieurs responsabilités dans l'application Oracle.
- Un dispositif (Firewall) a été installé afin de sécuriser l'accès au SI
- Il existe un logiciel de sécurité qui protège contre des virus.

2.3-2 Points faibles

- Les procédures de gestion des habilitations ne sont pas standardisées et homogénéisées.
- Les journaux d'audit et de sécurité ne sont pas exploités de façon systématique afin de contrôler les transactions effectuées par les utilisateurs et les administrateurs de sécurité.
- Les procédures d'utilisation de l'Internet ne sont pas toujours respectées et le contrôle de ces règles n'est pas réalisé.
- L'absence d'une politique centralisée et homogène de mise à jour des licences des logiciels anti-virus.

2.3-3 Risques

Les mesures de protection en matière de gestion des habilitations étant insuffisantes, les risques de malveillance internes et externes (fraudes, destructions de données, usurpation d'identité, intrusions, etc.) sont probables.

2.3-4 Recommandations

Les règles concernant les mots de passe doivent être uniformisées.

- Un renouvellement des mots de passe doit être mis en place, tous les 60 jours.
- Les mots de passe doivent avoir une longueur minimum pour toutes les applications, supérieure ou égale à 06 caractères.
- Tout mot de passe doit être alphanumérique.
- La réutilisation des mots de passe doit être interdite avant 05 générations

Une charte d'utilisation d'Internet et du mail doit être diffusée et signée par tous les utilisateurs.

Les journaux des firewall logiciels et matériel doivent être revus par l'administrateur réseau de façon systématique et régulière afin de vérifier :

- les tentatives d'intrusion ;
- les cas de non respect de la charte de l'Internet.

La prévention d'intrusions (y compris les chevaux de trois) comprend également les piratages internes, et sous-entend la mise en place d'une cartographie des ports par serveurs et postes du réseau.

Des logiciels de traçabilité des intrusions doivent être mis en place de sorte que les agents de la SENELEC soient en mesure :

- d'identifier le parcours d'un intrus (et localiser éventuellement les dégâts logiques causés).
- de pouvoir stopper un intrus une fois qu'il a pénétré le réseau.

II CONTROLES APPLICATIFS

L'informatisation de la SENELEC est avancée et c'est pourquoi nous avons accordé une attention toute particulière aux différentes applications (en service), qui jouent un rôle de premier plan dans la gestion de la société.

Nos analyses ont été effectuées à partir :

- d'un questionnaire de contrôle interne d'audit informatique (voir annexe 1) ;
- des tests techniques effectués dans les zones de test avec l'aide des informaticiens et des utilisateurs dans le but de porter un jugement sur les contrôles programmés.

Pour nous, les éléments ci-dessous, jouent un rôle primordial dans le fonctionnement et la fiabilité des contrôles programmés au niveau d'une application.

Ces éléments sont entre autres :

- autorisation et validation des opérations dans le système ;
- saisie correcte ;
- enregistrement correct des données dans les fichiers adéquats ;
- rejet des anomalies pour correction ou recyclage ;
- traitement correct par le système ;
- pas d'addition, de duplication ou de modification irrégulière ;
- mise en évidence des anomalies ;
- exactitude et exhaustivité des sorties d'informations.

II.1 Tests d'évaluation

Tout au long de notre étude sur les applications informatisées, nos avons été animés du souci de fonctionnement normal et correcte des contrôles programmés. C'est pourquoi, nous avons activement participé aux vérifications des différents contrôles aussi bien à la DSI qu'au niveau des services opérationnels.

Nous avons nos résultats sous forme de fiabilité des applications utilisées.

Nous avons pour cela, suivi non seulement les traitements effectués par l'application SIC mais aussi celles réalisées par l'application Oracle.

Au niveau du module Oracle FA, nous avons extrait une immobilisation (un ordinateur IBM ayant pour numéro d'inventaire 35317/031) des 34000 que possède la SENELEC pour vérifier le calcul des amortissements. Avec l'aide de l'utilisateur attitré de ce module, nous avons effectué cette opération dans la zone de test prévue. Mais avant, nous avons pris le soin de calculer manuellement l'amortissement mensualisé en tenant compte de la durée de vie, de la valeur d'origine et de la date d'acquisition de cette immobilisation.

Nous avons appelé le résultat manuel A1 et le résultat de notre test informatique A2 (voir annexe 3).

Nous avons remarqué que A1=A2.

De même pour le module Oracle HR, nous avons dans la zone de test, bien sûr avec l'aide d'un agent qui s'occupe du projet Oracle, calculé le traitement salarial de deux agents extraits du fichier paie mais avec des situations différentes.

- un agent qui est en congé ;
- les agents à matricule 10000 ;

Lorsqu'un agent est en congé par exemple en avril et que cet agent effectue des heures pendant ce même mois. L'agent d'ordonnancement de sa Direction les pointe par inadvertance et les transmet à l'unité traitement et salaire où on les saisit sans s'en rendre compte. Oracle HR va signaler ces éléments lors du test de la paie dans état appelé « Erreur éléments non pris en compte ». Ceci pour rappeler au chef de l'unité traitement et salaire que ces heures ne sont pas à prendre pour ce mois de congé mais pour le mois suivant.

Pour tout agent à matricule 10000, lorsqu'une retenue lui est faite pour la cotisation de l'IPM ; Oracle HR va mentionner cela dans un état appelé « Erreur sans éléments standard » pour signifier au chef de l'unité traitement et salaire que cet agent est exempté de la cotisation pour l'IPM.

II.2 Fiabilité des applications

II.2-1 L'application SIC

Le SIC est l'une des applications les plus importantes et utilisées de la SENELEC. Elle est composée de plusieurs modules qui couvrent l'essentiel des fonctions du cycle ventes/clients.

A Traitement de la nouvelle demande d'abonnement

a Points forts

Le module gère les codes tri suivants:

- 10 In formations commerciales ;
- 20 Caractéristiques techniques ;
- 30 Informations financières ;
- 40 Mise en service ;
- 50 Mutation ;
- 60 Validation ;
- 70 Fiche navette ;
- 80 Listes de demandes ;
- 90 Consultation d'une demande.

Il a pour objet le traitement et le suivi d'une demande, étape par étape depuis l'enregistrement jusqu'à la nouvelle facturation.

L'identification des abonnés, le rapport entre l'abonné et le local occupé pour les abonnements à usage domestique sont bien traités par ce module.

b Points faibles

- Pour les abonnés à usage professionnel, sur 70 dossiers, 12 renseignent sur la police du client précédent et 13 sur l'ancienne adresse de l'abonné. Soit des taux respectifs de 17% et 19% révélant ainsi des faiblesses à ce niveau.
- Les contrôles effectués sur l'historique de recouvrement du client révèlent que sur 119 dossiers usages domestiques sélectionnés, 32 renseignent sur la police du client précédent, 27 mentionnent l'ancienne de l'abonné. Soit respectivement des taux de contrôle de 27% et 23% qui sont faibles.
- L'examen des opérations de contrôle d'identification nous a permis de constater que si un certains nombre d'informations utiles telles que l'adresse, les noms et prénoms, le

numéro de la carte nationale d'identité sont enregistrées ; elles ne sont pas organisées en fichier actifs permettant d'effectuer des contrôles sur le passé de l'abonné.

c Recommandations

Il faut créer un fichier des abonnés permettant d'avoir des relations interactives entre :

- la police de l'abonné ;
- les noms et prénoms ;
- la carte nationale d'identité ;
- le conjoint de l'abonné ;
- l'adresse de l'abonné ;
- le numéro du compteur.

De sorte que l'enregistrement d'une de ces données permet de fournir des renseignements sur tous les autres abonnés.

B Analyse des délais de traitement de la nouvelle demande

a Points forts

Ce module gère les codes tri suivants :

- 10 Saisie demande ;
- 15 Edition fiche de contrôle ;
- 20 Retour visite ;
- 25 Retour bon de travaux ;
- 30 Acceptation travaux ;
- 35 Saisie fiche de contrôle ;
- 40 Acceptation dossiers ;
- 45 Edition du contrat ;
- 50 Edition fiche PI ;
- 60 Saisie fiche PI ;
- 70 Mutation ;
- 80 Fiche navette ;
- 85 Liste des demandes ;

- 90 Retour dossiers ;
- 95 Saisie directe ;
- 96 Modification abonnés prédécesseurs ;
- 97 Liste des abonnés mutés et non transférés ;
- 98 Liste des abonnés en instance de première facturation.

Ce module traite des délais de la nouvelle demande qui selon la Direction Commerciale :

- durée de visite 07 jours ;
- durée de réalisation 03 jours.

Soit environ une durée de traitement globale de dossier de 10 jours.

b Points faibles

- Sur 80 clients sélectionnés, nous avons observé que la durée moyenne de traitement global du dossier est de 60 jours.
- En poussant l'analyse par une segmentation de la durée globale par intervalle :
  - Durée comprise entre 1 et 10 jours : 02 dossiers sur 80 ; soit 2,5% ;
  - Durée comprise entre 11 et 20 jours : 03 dossiers sur 80 ; soit 3,75%.
- Pour ce qui concerne la durée de réalisation, l'échantillon de 80 dossiers donne une durée moyenne de 11 jours, soit près de 4 fois les 03 jours visés comme objectif.
- Les renseignements permettant de calculer les de traitement du dossier de la nouvelle demande ne peuvent être obtenus que de façon manuelle.
- Le nombre de dossiers à traiter et la méthode de consultation d'un client au niveau GA10 et NA80 ne permettent pas une analyse efficiente des statistiques de performance de traitement en terme de gains de temps et de sécurité (risques d'erreurs, confusion des dates).

c Recommandations

Le module doit être amélioré de sorte qu'il puisse fournir les renseignements sur :

- les données statistiques pertinentes concernant les durées de traitement globales du dossier.
- les durées moyennes de visite.

- les durées d'intervention des ACI.

C Rélève-Facturation

a Points forts

Ce module gère les codes tri suivants :

- 10 Programme de la relève ;
- 20 Edition fiche de relève ;
- 30 Saisie des index ;
- 40 Estimation des index ;
- 50 Correction de la saisie ;
- 60 Listes (relevés, non relevés, estimés) ;
- 70 Demande état de contrôle des consommations ;
- 75 Consultation des anomalies de consommation ;
- 80 Demande facturation ;
- 95 Suivi relève facturation.

Il permet de gérer l'activité de relève des compteurs de la clientèle d'une agence. Avant chaque facturation, le système offre la possibilité à l'utilisateur de contrôler et de recycler les anomalies de consommation en temps réel.

b Points faibles

- Le module ne renseigne que par client et par facture redressée.
- Possibilité de manipulation des index de consommation ;
- Impossibilité d'obtenir la reconstitution ou la traçabilité de l'ensemble des opérations à partir du système.
- Les renseignements ne peuvent être obtenus que manuellement à partir de l'exploitation des dossiers de redressement.
- Le manque de contrôle à posteriori entraîne le risque de manipulation des index de consommation.

c Recommandations

- Le système doit permettre d'avoir une vue d'ensemble des motifs de non relève avec des renseignements statistiques par police, par motif, avec le taux de récurrence de ces motifs et l'identification des ACI ayant visité ces clients.
- Le traitement des redressements doit être suivi à partir d'un module permettant de distinguer les différentes séquences des opérations, les causes, les autorisations, l'identification des agents.
- L'édition d'un journal des redressements devrait être à la portée des exploitants par l'accès à un module banalisé aux fins de contrôle à tout moment.

D Recouvrement APV

La gestion des activités de recouvrement est principalement suivie à travers le SIC au niveau des modules suivants : la gestion des abonnés « GA », la gestion des coupures, délais et moratoires « GC

a Points forts

Le module GA gère les codes tri suivants :

- 10 Consultation des abonnés ;
- 15 Modification référence ;
- 20 Modification informations administratives et appareils en place ;
- 25 Modification code tarif et usage et numéro compteur ;
- 40 Affectation abonnés au précontentieux central
- 45 Affectation abonnés au précontentieux subdivision ;
- 50 Affectation abonnés au contentieux ;
- 80 Saisie directe ASC ;
- 85 Transfert ASC ;
- 90 Transfert abonnés.

Pour ce qui est du module GC, il regroupe les codes tri ci-dessous :

- 10 Saisie des délais ;
- 15 Liste des délais ;
- 20 Saisie des factures en vérifications ;

- 25 Liste facture en vérification ;
- 30 Saisie des moratoires ;
- 40 Analyse des comptes pour coupure ;
- 43 Sélection et édition de bons de coupures ;
- 45 Abonnés proposés à la coupure ;
- 50 Saisie des abonnés coupés ;
- 55 Liste des abonnés sous coupures ;
- 60 Edition des bons de remises ;
- 65 Liste des remises en cours ;
- 70 Saisie des remises ;
- 75 Liste des abonnés remis ;
- 80 Edition des bons de vérification ;
- 85 Liste des abonnés sous vérification ;
- 90 Saisie des abonnés vérifiés ;
- 95 Liste des abonnés vérifiés
- 97 Saisie des coupures ;
- 98 Consultation d'un abonné coupé ;
- 99 Modification d'un abonné coupé.

b Points faibles

- Absence de procédure organisant le recouvrement dans son fonctionnement, ses moyens, ses objectifs et activités.
- Le non respect de la procédure de gestion des coupures, délais et moratoires.

Le risque est que des clients théoriquement sous coupure restent alimentés, car la procédure telle qu'appliquée actuellement ne permet pas de s'assurer de l'effectivité des coupures.

c Recommandation

Il faut améliorer le fonctionnement des différents modules de sorte qu'ils puissent prendre compte la procédure de recouvrement.

E La gestion des encaissements

a points forts

Ce module couvre les codes tri suivants :

- 10 Saisie des mouvements caisses ;
- 20 Validation journée caisse ;
- 30 Confirmation chèque certifié ;
- 40 Annulation de mouvement caisse ;
- 50 Relevé de compte ;
- 55 Edition de journal de caisse ;
- 60 Gestion des caisses ;
- 75 Edition bordereau remise chèque ;
- 77 Edition récapitulation des timbres ;
- 80 Récapitulation de l'encaissements/portefeuille.

Il permet la gestion des sessions d'encaissement

b Points faibles

Il n'existe pas de code tri permettant d'obtenir à partir du système le cumul des encaissements :

- Par nature :
  - espèces ;
  - chèques ;
  - monétiques
  - virement bancaire ;
  - prélèvement automatique.
- Par période :
  - semaine ;
  - mois ;
  - année.
- Le système ne permet pas la prise en compte des clients spéciaux, notamment l'encaissement de l'ASC.

- Le système ne permet pas de contrôler et d'éditer les journées d'encaissement non validées.

Ce qui entraîne l'absence de moyen de contrôle d'exactitude.

c Recommandations

- Il faut améliorer le fonctionnement de ce module par la mise en place d'un code tri qui permettra d'effectuer un contrôle d'exactitude du cumul des encaissements.
- Il faut également améliorer le fonctionnement du module afin qu'il puisse prendre en compte l'encaissement des clients spéciaux, le contrôle et l'édition des encaissements non validés.

F Mouvements hors caisse (HC)

a Points forts

Ce module contient les codes tri suivants :

- 10 Avis de débit ;
- 20 Avis de crédit ;
- 40 Avis de crédit CAR ;
- 50 Régularisation intra auxiliaire ;
- 60 Extourne CAR ;
- 65 Liste des CAR ;
- 70 Extourne ASC ;
- 90 Redressement client ;
- 95 Edition journal hors caisse.

Ce module est un complément de la fonction caisse. Il permet de faire des régularisations au débit et au crédit du compte client.

b Points faibles

- La limite essentielle de ce module est que l'utilisateur qui effectue les opérations est le seul informé de ce qui se passe tant qu'un tirage banalisé n'est pas fait par la DSI.
- Le système ne permet pas d'obtenir des soldes globaux par type d'opérations de mouvements débit et crédit hors caisse.

c Recommandations

- Il faut créer un module banalisé d'édition des mouvements hors caisse permettant aux responsables de chaque site ou unité de tirer de façon quotidienne tous les mouvements hors caisse réalisés.

G Résiliation

a Points forts

Il contient les codes tri suivants :

- 10 Saisie demande de résiliation ;
- 20 Edition des bons d'intervention ;
- 30 Saisie des bons d'interventions ;
- 40 Estimation ;
- 50 Liquidation (facturation) ;
- 60 Suivi des compteurs non coupés et non déposés ;
- 70 Fiche navette résiliation ;
- 80 Liste de demandes
- 90 Retour dossiers ;
- 99 Recherche numéro de police.

Il a pour objet la résiliation du contrat d'un client.

b Points faibles

- L'examen des résiliations permet de constater qu'il n'existe pas de fichiers séparés de suivi des clients résiliés : clients résiliés débiteurs et clients résiliés créditeurs sont dans le même fichier client.
- Le module ne permet pas d'obtenir des résiliations effectuées pour une période donnée.
- Le module ne permet pas également de retracer l'ensemble des résiliations faites pour cause de défaut de paiement, pour absence de consommation, ou par suite de demande du client.

c Recommandations

Le module doit permettre d'obtenir en ligne l'ensemble des clients résiliés. Un système de partage de fichiers permettra de mettre fin à la transmission manuelle des dossiers.

H Fraude

a Points forts

Ce module regroupe les codes tri suivants :

- 10 Saisie de la déclaration fraude ;
- 20 Edition des bons d'intervention
- 30 Saisie retour visite ;
- 40 Retour travaux ;
- 50 Edition fiche PI
- 60 Saisie fiche PI
- 65 Facture de régularisation ;
- 70 Facture rappel fraude
- 75 Facture rappel compteur défectueux ;
- 80 Fiche navette ;
- 85 Retour dossiers
- 90 Retour dossier liste globale des déclarations

Ce module permet de procéder à la régularisation des anomalies techniques et des manques à gagner qui en résultent.

b Points faibles

- Nous avons remarqué que pour l'essentiel de ce module, le principal indice de présomption de la fraude repose sur la durée anormale qu'une instance peut avoir. La faiblesse relevée est qu'il ne permet pas de détecter les cas de fraude et de malversation.

c Recommandations

- Il faut améliorer le fonctionnement du module afin qu'il puisse détecter les cas de fraude.

II.2-2 L'application Oracle

Nous avons analysé la fiabilité de l'application Oracle à travers celle de ses modules périphériques et du module central.

A Le module AP : Gestion des fournisseurs

Les modules sont intégrés et transférables. Ce qui permet à l'utilisateur de Oracle AP de disposer à tout moment des informations sur le site d'un fournisseur et des modalités des commandes.

La création d'un fournisseur se fait par habilitation partagée entre les responsables Oracle PO et de Oracle AP.

Les factures saisies dans AP ne sont pas automatiquement transformées en écritures comptables. La centralisation est faite par l'interface (AX-AP) qui après contrôle les transforme en pièces comptables.

A partir du pupitre des factures, un certain nombre de contrôle peut être exercé sur une ou deux factures. Ce sont :

- l'approbation : elle consiste à valider une facture pour qu'elle soit imputable ou payable ;
- le blocage : il consiste à empêcher le paiement d'une facture.

Ces différentes actions assurent les contrôles en entrée et au cours des traitements.

B Le module PO : Gestion des achats

Ce module périphérique joue un rôle important dans les commandes lancées par la SENELEC, de la demande d'achat jusqu'à la création du bon de commande.

Lorsqu'une demande d'achat est créée, le module valide cette opération ; c'est-à-dire, vérifie si la personne demandeur a la responsabilité nécessaire pour effectuer cette opération. Si oui, le système génère un bon de pré-engagement et laisse le processus suivre son cours. Après consultation des fournisseurs, le système contre passe le bon de pré-engagement et crée un bon de commande.

Le module dispose d'un autre contrôle dit « bloquant » pour éviter les dépassements de budget.

C Oracle FA : Gestion des immobilisations

Cette application contient un programme qui calcule la dotation aux amortissements et les ajustements, et met à jour l'amortissement cumulé.

Le programme lance trois traitements séparés pour :

- calculer les plus ou moins values des immobilisations cédées, et rattraper l'amortissement des immobilisations cédées et reconstituées ;
- calculer la dotation aux amortissements et ajustement de la période, et ferme la période en cours ;
- lance le journal d'écriture de l'amortissement.

En plus, si l'amortissement de certaines immobilisations se solde par un échec, celles-ci sont listées dans un fichier de journalisation.

Le calcul de l'amortissement au cours de notre test informatique a confirmé le fonctionnement normal et fiable des contrôles programmés.

D Oracle HR : Gestion des ressources humaines/calcul de paie

Ce module calcule la paie de tous les agents, en additionnant les éléments fixes déjà enregistrés dans la base aux éléments variables qui peuvent être :

- rappel ;
- absence ;
- heures supplémentaires consolidées ;
- heures supplémentaires récupérées ;
- permanence ;
- astreinte ;
- déplacement ;
- caisse ;
- panier ;

- sujétion ;
- fraude ;
- quart ;
- heures statutaires.

Différents éléments de contrôle interviennent pour empêcher que des erreurs ne se glissent dans le traitement de la masse salariale de la société. Ces éléments de contrôle avant la paie sont :

- erreurs Absence ;
- erreurs Congé ;
- erreurs Eléments non pris en compte ;
- erreurs IR ;
- erreurs NR ;
- erreurs Sans éléments standard ;
- erreurs Supplantation ;
- erreurs Sans mode de paiement.

Il y a également des contrôles a posteriori pour s'assurer que le traitement s'est bien déroulé. Ces éléments sont :

- net à payer négatif ;
- indemnité de déplacement en nombre ;
- indemnité de déplacement en valeur ;
- acompte de déplacement ;
- heures supplémentaires ;
- reversement quinzaine.

F Oracle IC : Gestion des stocks

Les contrôles programmés au niveau de ce module permettent de vérifier l'ensemble des mouvements de stocks d'une période ou d'un article. Ils permettent également de retrouver les valorisations des divers mouvements ainsi que les différentes commandes et réceptions fournisseurs.

G Oracle GL : Gestion de la comptabilité et du budget

Ce module est le référentiel central des informations comptables. Il réalise les tâches suivantes :

- enregistrement et révision des informations comptables : importation de données à partir des modules auxiliaires ou les saisies directes par opérations diverses pour la mise à jour des mouvements réels budgétaires.
- manipulation des informations comptables :
  - préparation rapide de simulations et d'états ;
  - préparation du processus budgétaire.

L'alimentation de la base s'effectue de trois manières :

- manuellement : par saisie directe et importation de pièces comptables.
- automatiquement par définition de pièces répétitives ou de formules de répartition.
- par importation via l'interface (AX).

Les pièces manuelles sont saisies directement ou groupées en lots afin de faciliter les recherches ultérieures et de contrôler les montants saisis.

Oracle GL vérifie en fin de saisie si les totaux débiteurs et créditeurs sont conformes aux montants de contrôle (en cas d'utilisation de lots) et s'ils sont équilibrés.

L'interface AX exerce également un contrôle sur les opérations réalisées à partir des modules périphériques.

Nous avons par exemple tenté de saisir une opération sur un compte d'un centre de responsabilité désactivé. L'interface AX a bloqué la saisie et a donné l'explication de l'erreur.

Nous avons changé de méthode en prenant cette fois un compte d'un centre de responsabilité activé dans lequel nous avons volontairement introduit une erreur, c'est-à-dire au lieu de prendre Filiale = 03, nous avons pris Filiale = 04.

L'interface a réagi en bloquant la saisie (voir l'annexe 2).

Les contrôles réalisés par l'interface AX et les contrôles programmés de Oracle GL assurent les validations et les contrôles de traitement des états express générés par ce module.

II.2-3 Synthèse et analyse des résultats

Nous allons récapituler ici les résultats de notre évaluation sur le terrain, concernant les contrôles généraux et les contrôles spécifiques.

A Synthèse des résultats

Le Tableau ci-après résume les résultats de nos différents tests sur les trois (03) types de contrôle : contrôles globaux, contrôle de l'application ORACLE et contrôle de l'application SIC.

Tableau n°7 : Synthèse des résultats de l'évaluation

Type de contrôle	**1**	**2**
Contrôles globaux	FORTS	FORTS
Contrôle de l'application ORACLE	FORT	
Contrôle de l'application SIC		FAIBLE

B Analyse des résultats

1 : les deux (02) types de CI étant satisfaisants (contrôles globaux forts et contrôle de l'application ORACLE fort), le risque lié aux contrôles informatiques est d'un niveau bas dans ce cas.

2 : l'un des deux (02) types de CI n'étant pas satisfaisant (contrôle de l'application SIC FAIBLE), nous estimons que le risque lié au contrôle est important. Dans ce cas, les contrôles par recoupement des données sorties du système, doivent être privilégiés.

Conclusion partielle

Cette deuxième partie de notre étude nous a permis d'apprécier concrètement la fonction informatique de la SENELEC. Notre évaluation a porté sur les points suivants :

- organisation et repositionnement de la DSI,
- adéquation effectif informatique,
- politique de sécurité et amélioration des procédures d'exploitation ;
- appréciation de l'application SIC,
- appréciation de l'application Oracle.

Organisation et positionnement de la DSI

Les procédures organisationnelles mises en œuvre par la DSI couvrent un certain nombre de domaines clés, notamment la mise en place d'un schéma directeur. Néanmoins, l'insuffisance ou l'absence de budget, le manque de comité informatique pourraient porter un coup dur aux objectifs de la DSI.

Politique de sécurité et amélioration des procédures d'exploitation

Le système de sécurité physique présente de nombreuses failles qu'il faudra rapidement corriger afin qu'elles ne portent atteinte aux ressources informatiques de la société.

L'amélioration des procédures d'exploitation se fera par la prise en compte des domaines clés de l'exploitation, les tâches d'exploitation applicatives ou spécifiques et l'élaboration d'une cartographie du réseau physique et logique.

L'application SIC

Elle regroupe plusieurs modules, qui disposent de nombreuses fonctionnalités. Mais des améliorations sont à faire pour améliorer le fonctionnement du SIC et ses traitements. Il s'agit de l'amélioration de son environnement et ses fonctionnalités.

Cette amélioration de l'environnement de fonctionnement du SIC se fera par la prise en compte par la DSI des carences et dysfonctionnements constatés au niveau de l'application et de son environnement technique et organisationnel. Ce sont :

- mise en service des nouveaux terminaux de saisie portable ;

- amélioration de la disponibilité des liaisons de télécommunication ;
- revue des traitements exécutés en temps différé

Quand à l'amélioration fonctionnelle, elle se fera par la prise en compte par la DSI des fonctionnalités suivantes :

- révision de la grille des habilitations d'accès,
- recherche multi agence d'un client,
- saisie d'autres pièces que la carte d'identité nationale,
- édition délocalisée des factures et états de facturation.
-

L'application Oracle

Cette application a apporté un plus à la gestion des activités de la SENELEC en terme de gain de temps et de rapidité. C'est un progiciel puissant dont les contrôles programmés fonctionnent correctement pour assurer la fiabilité des traitements effectués.

Chaque module est accompagné d'une documentation utilisateur bien fournie.

Néanmoins, il faut améliorer les fonctionnalités en prenant compte des aspirations nouvelles des utilisateurs.

III Perspectives de mise en place des recommandations

III.1 Mise en place d'un comité informatique

La politique informatique est de prime abord l'affaire de la Direction Générale. Elle doit par conséquent découler des choix stratégiques effectués par l'entreprise. La Direction Générale ne peut pas ne pas assumer de cette responsabilité. Pour que la politique informatique tienne compte de l'intérêt de l'entreprise, la Direction Générale doit mettre en place un comité informatique qui décidera des orientations stratégiques de la société en matière informatique.

Il sera composé de :

- un ou plusieurs représentant de la Direction Générale,

- les principaux responsables du service informatique,
- les responsables des Directions,
- des utilisateurs.

Ce comité aura pour rôle :

- élaboration de la stratégie informatique à moyen terme,
- élaboration du budget ou plan annuel,
- actualisation du plan à court terme,
- suivi régulier des principaux indicateurs du plan,
- la prise en compte des remarques et critiques des utilisateurs.

La mise en place de ce comité doit se faire le plus rapidement possible afin qu'il puisse s'approprier le schéma directeur (déjà élaboré par un cabinet) dont l'exécution devrait normalement commencer en janvier 2005.

Cela lui permettrait de juger de l'opportunité d'un tel investissement, de l'approuver ou faire des propositions d'amélioration.

III.2 Création d'une responsabilité audit informatique

La dynamique équipe de l'audit interne doit être renforcée par le recrutement d'un spécialiste en audit informatique.

Ce recrutement d'une personne expérimentée et titulaire d'un diplôme en audit informatique s'impose et doit se faire dans les plus brefs délais. Cela permettra à la Direction de l'audit interne d'exercer normalement sur la DSI un contrôle de second degré suffisant, en l'incluant dans son programme annuel ou pluriannuel d'audit.

III.3 Création d'un poste de responsable de sécurité du système d'information

La création d'un tel poste devrait être envisagée sous de meilleurs délais. Le responsable de sécurité du système d'information doit être en mesure d'appréhender correctement l'ensemble des risques attachés à l'exercice des métiers de la sécurité et aux spécificités de ses activités.

Ayant pour vocation à intervenir en qualité de maître d'ouvrage pour les questions de sécurité ; le responsable de la sécurité devrait hiérarchiquement être rattaché à la DAICG de sorte qu'il dispose d'une totale indépendance vis-à-vis de la DSI.

Il pourra à ce titre intervenir en tant que coordonnateur des moyens et conseiller privilégié du comité informatique lors de la discussion des projets informatiques.

III.4 Mise en place des procédures informatiques

Comme toutes les autres fonctions, la DSI a besoin de procédures de gestion informatiques pour mieux maîtriser ses activités. Ce projet deviendra bientôt réalité avec les appels d'offres lancés par la SENELEC.

Ces procédures, qui seront élaborées par des professionnels de haut niveau, pourront être évaluées par la DAICG.

CONCLUSION GENERALE

L'évaluation du CII est une étape, qu'il ne faut pas négliger au cours d'une mission en milieu informatisé, pour pouvoir maîtriser le risque d'audit.

Cette évaluation des systèmes informatiques, pour qu'elle soit efficace, doit porter les deux types de contrôle ci-après :

- les contrôles globaux (contrôles généraux),
- les contrôles applicatifs (contrôles des applications informatisées).

LES CONTROLES GLOBAUX

Ces contrôles jouent un rôle essentiel dans l'efficacité du CII. Leur analyse permet de s'assurer de la permanence des contrôles applicatifs dans le temps. Les contrôles globaux tournent généralement autour des points suivants :

- les contrôles sur les opérations du centre de traitement,
- les contrôles sur les logiciels d'exploitation,
- les contrôles d'accès,
- les contrôles sur le développement et la maintenance des applications.

LES CONTROLES APPLICATIFS

Les contrôles applicatifs contribuent directement au CI des processus, en association avec les CI manuels. Par conséquent, il existe deux (02) types de contrôles applicatifs :

Les contrôles manuels : contrôles effectués par l'utilisateur pour compléter les contrôles programmés.

Les contrôles programmés : contrôles effectués automatiquement par une application. Ils comprennent :

- les contrôles d'accès à l application,
- les contrôles à la saisie des données,
- les contrôles des traitements,
- les contrôles des sorties

Pour que le CII d'une entreprise soit optimum, c'est-à-dire, maintenir son niveau de CII satisfaisant, les contrôles globaux et les contrôles applicatifs doivent être forts

Le contrôle interne lié à la fonction informatique de la SENELEC présente des insuffisances.

Au niveau des contrôles globaux

La DSI dispose d'un organigramme, d'un schéma directeur dont l'exécution a commencé.

Mais des efforts énormes restent à faire. Il s'agit par exemple de la mise en place du manuel de procédures informatiques, qui permettra aux activités informatiques de se dérouler normalement et correctement. Il faut en outre mettre régulièrement à jour l'organigramme de la DSI, pour l'adapter aux réalités nouvelles de la fonction informatique.

Au niveau des contrôles applicatifs

Pour ce qui concerne les applications informatisées, il existe beaucoup de faiblesses au niveau de l'application maison. Cette application est un peu dépassée et présente des insuffisances niveau de la fiabilité des traitements.

La SENELEC est une entreprise ambitieuse avec son projet d'entreprise « SUXALI SENELEC ». Le système d'information jouera à n'en point douter un rôle crucial dans l'atteinte de des objectifs. C'est la raison pour laquelle, nous proposons la mise en place d'un comité informatique. Il faut en outre penser au renforcement des compétences de la DAICG par le recrutement d'un spécialiste de l'audit informatique.

BIBLIOGRAPHIE

I OUVRAGES

1 ANGOT Hugues, FISHER Christian, THEUNISSEN Baudoin (1994), Audit comptable, audit informatique, édition Entreprise De Boeck Université.

2 ATH (1991), Audit financier, Guide pour l'audit de l'information financière de l'entreprise, édition clef.

3 BARRY Mamadou (2004), Audit et contrôle interne, édition les presses de la sénégalaise de l'imprimerie.

4 CNCC (1992), Appréciation du contrôle interne, CNCC édition.

5 CNCC (1992), Démarche et organisation de la mission générale Tome 2, CNCC édition.

6 CNCC (1995), La démarche du commissaire aux comptes en milieu informatisé, CNCC édition.

7 CNCC (2003), Référentiel normatif et déontologique, CNCC édition.

8 COOPERS & LYBRAND (2000), La nouvelle pratique du contrôle interne, les éditions d'organisation.

9 COLINS Lionel ; VALIN Gérard (1992), Audit et contrôle interne : Aspects financiers, opérationnels et statégiques édition Dalloz Paris.

10 DERRIEN Yann (1991), Les techniques de l'organisation informatique, édition Paris Dunod.

11 DERRIEN Yann (1992), Les techniques de l'audit informatique, édition Dunod Paris.

12 DELSOL Xavier (1999), Guide d'audit des associations : le diagnostic juridique, social, fiscal, comptable financier et informatique ; édition Paris Juris-service.

13 FAIVRE Claude et LOREAU Yvon Michel (1993), L'audit de la micro-informatique, édition Publi-Union.

14 IFACI (1993), Audit et contrôle des systèmes d'information. Module 1 : management de l'audit et du contrôle interne, réalisation : PR DONNELEY France.

15 JENKINS Bryan & PINKNEY Anthony (1984), Audit des systèmes et des comptes gérés sur informatique, édition Dunod Paris.

16 LAMY Jean Paul (1996), Audit et certification des comptes en milieu informatisé, les éditions d'organisation.

17 LAMY Jean Paul (1997), L'audit en milieu EDI, CNCC édition.

18 MIKOL Alain (2000), Encyclopédie de la Comptabilité, Contrôle de Gestion et Audit, édition Economica.

19 OBERT Robert (2000), Révision et certification des comptes, édition Dunod Paris.

20 OBERT Robert (2004), Audit et commissariat aux comptes, Aspects internationaux ; édition Dunod Paris.

21 PRICEWATERHOUSECOOPERS (2004), Contrôle interne : Au-delà des concepts, 40 questions aux praticiens, « Pocket Guide ».

22 THORIN Marc (2000), L'audit informatique, hermès Sciences Publication.

23 REIX Robert (2002), Systèmes d'information et management des organisations, édition VUIBERT PARIS.

24 RENARD Jacques (2000), Théorie et pratique de l'audit interne, édition d'organisation.

25 RENARD Jacques (2004), Théorie et pratique de l'audit interne, édition d'organisation.

26 WILMOTS Hans (2002), Aspects pratiques de l'organisation administrative et du contrôle interne : contrôlez-vous suffisamment les différentes procédures et activités de votre organisation pour assurer la gestion efficace de votre entreprise, édition Standaard.

II MEMOIRES ET SUPPORTS DE COURS

1 ASSOUMANA Hassoumi (2000), L'auditeur face à l'informatique.

2 KONAN Konan Thomas (2002), Evaluation du CI au cours d'un audit légal en MI

3 OUOLEGUEM Boubacar (2004), Evaluation du CI : cas de la mutuelle de Cambérène.

4 SARR Ababacar (2004), Audit informatique.

III ARTICLES

1 BOUANICHE José (juin 2001), COBIT, référentiel de gouvernance de l'informatique, revue Audit n° 155.

2 http://www.protiviti.fr/downloads/PRO/pro-fr/lebulletin03.pdf.

3 MORRISSEY Patrick (avril 2001), Des milliers d'informations disponibles concourent à la réussite des missions, revue Audit n°154.

4 ROUFF Jean Loup (février 2001), Des concepts et des mots, revue Audit n°153.

5 ROUFF Jean Loup (avril 2001), Des moyens traditionnels toujours d'actualité, revue Audit n°154.

6 VIDAUX François (avril 2001), L'informatique, un facteur d'innovation pour l'analyse des risques, revue Audit n° 154.