CESAG

Centre Africain d'études Supérieures en Gestion

Institut Supérieur de Comptabilité, de Banque et de Finance (ISCBF)

Diplôme d'Etudes Supérieures Spécialisées en Audit et Contrôle de Gestion

Promotion 18

(2006-2007)

Mémoire de fin d'études

THEME

AUDIT DE L'APPLICATION INFORMATIQUE DE GESTION DES STOCKS (ORACLE IC) DE LA SENELEC

Présenté par :

Mlle Ndieundé NDIAYE

Dirigé par :

Monsieur Mactar NDOYE

Chef du Département Audit Interne et Organisation de La SENELEC

re 2009

DEDICACE

Ce mémoire est spécialement dédié :

- A mes parents pour leur amour, leur affection, leur compréhension, leur confiance et leur soutien sans faille, tant matériel qu'émotionnel.
- A mes chers grands-parents Madické NDIAYE, Amy WADE, Mbaye THIAM et Rama GUEYE, qu'ils reposent en paix.
- A mes frères et sœurs.
- A mes cousins et cousines.
- A mes amis (es).

REMERCIEMENT

Je tiens particulièrement à remercier mon papa et ma maman adorés pour tout. Je ne pourrai pas assez vous remercier pour tout ce que vous avez fait pour vos enfants. Je prie juste le bon Dieu qu'il vous donne longue vie.

Mes remerciements vont aussi à l'endroit de :

- ✓ M. Mactar NDOYE, Chef du Département Audit Interne et Organisation de la SENELEC Vincent, pour son encadrement et ses conseils.
- ✓ M. Moussa YAZI, professeur de contrôle de gestion au CESAG.
- ✓ M. Mbacké DIOP, professeur d'analyse financière au CESAG.
- ✓ M. Karim FALL, Mmes Ndéye GUIRANE, Diéye Fatou NDIAYE, Yacine DIOP et Sama TOURE de l'Unité Stocks de la SENELEC.
- ✓ MM. Mor DIOP et Mar SAMBE de l'Audit Interne et Organisation de la SENELEC.
- ✓ M. Ousseynou MBAYE de la DFC de la SENELEC.
- ✓ MM. Nicolas Ismaila NIANG, El Hadji Malick Sy DIOP et Mmes Salimata SEMBENE et Nafissatou DIAGNE de la DSI de la SENELEC.
- ✓ MM. Djily FALL, Léonce SAMBOU et Mme Kébé de la DAJ de la SENELEC.
- ✓ M. Ndiagua SARR, Directeur associé de KPMG Sénégal.
- ✓ Mme Sylvie PEYROTTES de KPMG Sénégal.
- ✓ La Direction Générale et le corps professoral du CESAG pour la qualité de l'enseignement dispensé et leur constante disponibilité.
- ✓ Tous mes camarades de la 18 ème promotion de DESS Audit et Contrôle de Gestion du CESAG.

FIGURES ET TABLEAUX

LISTE DES FIGURES **PAGES**

LISTE DES TABLEAUX **PAGES**

LISTE DES ANNEXES **PAGES**

LISTE DES SIGLES ET ABBREVIATIONS

A.F.A.I. : Association Française de l'Audit et du conseil Informatique

A.S.I.: Audit des Systèmes d'information

CESAG : Centre Africain d'Etudes Supérieures en Gestion

CLUSIF : Club de la Sécurité des Systèmes d'Information Français

COBIT: Control Objectives for Business and related Technology

D.F.C.: Direction des Finances et de la Comptabilité

D.R.S. : Demande de Réapprovisionnement de Stock

D.S.I. : Direction des Systèmes d'Information

E.D.I. : Echange de données informatisées

I.F.A.C.I. : Institut Français de l'Audit et du Contrôle Interne

MARION : Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux

MEHARI : Méthode Harmonisée d'Analyse de Risques

ORACLE : Est un système de gestion de base de données relationnel (SGBDR) fourni par Oracle Corporation.

P.D.G. : Président Directeur Général

SENELEC : Société Nationale d'Electricité du Sénégal

S.I. : Sénégalaise d'Investissement

S.I. : Système d'information

SQL : Structured Query Language (ou langage structuré de requêtes)

SUXALI SENELEC : Convention signée par la SENELEC et ses employés pour le redressement du secteur

TABLE DES MATIERES

INTRODUCTION GENERALE

L'utilisation de l'informatique dans le cadre de l'audit n'est plus aujourd'hui un choix mais une nécessité. En effet, le volume et la complexité des données nécessaires à l'audit sont tels que les techniques manuelles s'avèrent inefficaces. Les auditeurs doivent également tenir compte de la nature évolutive des systèmes d'information. Des applications comme l'échange de données informatisées (EDI) pour la réalisation des tâches courantes telles que la saisie et le traitement de données et des approches telles que l'informatique départementale et individuelle les obligent à innover dans leur utilisation de l'informatique.

Par ailleurs, une gestion et une organisation efficaces de la fonction d'audit passent nécessairement par l'utilisation de l'informatique. Les responsables de l'audit doivent utiliser l'informatique afin que les ressources soient concentrées dans les domaines les plus préoccupants et que l'organisation recrute et forme un personnel adapté.

En outre, une entreprise crée de la valeur en traitant de l'information, en particulier dans le cas des sociétés de service. Ainsi, l'information possède une valeur d'autant plus grande qu'elle contribue à l'atteinte des objectifs de l'organisation.

En effet, nul n'ignore que l'informatique est devenue un outil incontournable pour un développement de l'entreprise.

L'expansion et les possibilités offertes par l'ordinateur font qu'il est nécessaire de disposer d'un système informatique d'un haut niveau de qualité pour assurer un excellent niveau de contrôle de l'entreprise, gage d'une information intègre et de pérennité de l'exploitation. Pour cette raison, l'informatique est un outil qui doit être disponible, performant, fonctionnel et sécurisé pour répondre efficacement aux attentes de l'entreprise et de ses clients.

En fait, les entreprises évoluent dans un environnement de plus en plus complexe et turbulent. Les décisions qui étaient par le passé plus ou moins faciles à prendre dans un environnement simple et stable, présentent actuellement plus de difficultés dans cet environnement risqué.

Toute décision, quelle soit interne ou externe, nécessite la prise en compte des différentes facettes de cet environnement. L'information prend ainsi une importance accrue pour une bonne prise de décision. Mais la qualité de cette décision dépend de la qualité de l'information sur laquelle on se base pour la prendre.

D'ailleurs le traitement de l'information, de la gestion se fait grâce à l'Informatique avec l'utilisation des applications informatiques d'où la nécessité de se doter d'un système d'information adéquat au sein de l'Entreprise.

Les auditeurs doivent régulièrement auditer les applications opérationnelles et notamment la comptabilité ainsi que l'ensemble des traitements qui sont situés en amont. Il est alors nécessaire d'avoir un certain nombre d'outils et de méthodes permettant de détecter rapidement des anomalies et des erreurs de façon à améliorer l'efficacité de ces missions.

Il est donc important de connaître les outils disponibles et de savoir dans quelles conditions les utiliser. C'est notamment le cas quand on est amené à s'interroger sur la qualité des données gérées par ces applications. Il est pour cela nécessaire de connaître les différents outils existants et la manière de les mettre en œuvre.

Aujourd'hui, il n'existe aucune division, en termes de main d'œuvre, entre les tâches gérées par des applications logicielles et celles gérées par un personnel humain. À l'inverse, les superviseurs humains et les systèmes de contrôle logiciels travaillent conjointement dans la gestion des processus métier et des serveurs Web, des bases de données et des intergiciels sur lesquels ils reposent. Toutefois, nombre de ces applications, tout particulièrement les applications Web, sont très vulnérables, que ce soit face à l'injection SQL ou au « cross-site scripting » (XSS). Même les plates-formes sur lesquelles ces applications sont exécutées sont bien plus vulnérables que leurs prédécesseurs, les dorsales et les lignes louées.

En conséquence, bien que ces applications facilitent l'exécution des processus métier, elles exposent en même temps l'organisation à de nombreux risques pour la sécurité, par rapport à leurs homonymes humains.

Garantir le bon fonctionnement de ces applications et, par extension, des processus métier qu'elles prennent en charge, est devenu crucial pour le succès d'une entreprise, et la gestion des faiblesses de ces applications a ainsi pris beaucoup d'importance. Le présent document permet de clarifier la problématique de la gestion des faiblesses des applications et propose des stratégies pour minimiser les dangers que ces faiblesses font courir aux processus métier.

Par contre, l'audit informatique apparu dans les années 70 est utilisé comme une mission d'évaluation de conformité par rapport à une politique de sécurité ou à défaut par rapport à un ensemble de règles et de sécurité. C'est un moyen efficace pour garantir la fiabilité du système informatique.

Ainsi **l'Audit de l'application informatique de gestion des stocks (Oracle IC) de la SENELEC**, objet du présent mémoire, nous permettra de montrer l'importance de la maîtrise de l'utilisation informatique et la nécessité pour les organisations de disposer d'applications fiables améliorant ainsi leur performance.

Dans les missions d'audit, les systèmes informatiques prennent de plus en plus d'importance. Les auditeurs se trouvent désormais régulièrement confrontés à des systèmes comptables ou financiers basés sur des systèmes informatiques dans l'exercice de leurs missions légales, contractuelles ou internes.

Or, ces systèmes informatiques subissent une évolution de plus en plus rapide. S'ils estiment, au départ, qu'il faut traiter l'informatique à part, les auditeurs sont convaincus, aujourd'hui, que l'informatique doit être intégrée dans leur démarche professionnelle et dans chacune de leurs préoccupations.

Ainsi, l'approche d'audit, usuellement adoptée dans les entreprises, doit répondre à ce nouveau contexte et aux risques nouveaux.

Une action de mise à niveau de l'approche d'audit s'impose alors aux organismes professionnels dans le monde et aux cabinets internationaux. C'est ainsi que ces organismes professionnels n'ont pas tardé à apporter et à mettre à jour les lignes directrices et le minimum de diligences pour un audit dans un milieu informatisé.

Les cabinets internationaux d'audit développent de plus en plus des méthodologies appropriées et font de gros investissements pour adapter les approches d'audit à un environnement devenu de plus en plus complexe et turbulent.

En plus de ces efforts, la législation, la jurisprudence et la doctrine à l'échelle internationale se sont enrichies de nouvelles règles destinées à réglementer et à contrôler certains aspects des systèmes informatisés.

Dans ce contexte de plus en plus complexe, l'auditeur se trouve face à de nouveaux problèmes auxquels il doit trouver des solutions. Il doit acquérir une connaissance suffisante en matière d'informatique pour pouvoir planifier, diriger, superviser et revoir ses travaux. En effet, tout au long de ses travaux, l'auditeur évalue le degré de la nécessité de compétences informatiques particulières pour la réalisation de l'audit. S'il se trouve dans cette situation, il est obligé de solliciter l'aide d'un professionnel ayant les compétences recherchées, il peut s'agir d'un collaborateur ou d'un spécialiste en matière d'audit des systèmes d'information externe à l'entité.

L'audit des systèmes d'information devient ainsi un pilier de contrôle nécessaire pour la bonne gestion d'une entreprise. En fait, le concept d'audit des systèmes d'information, apparu au cours des années 1970, a pour but d'évaluer la mise en conformité des processus et méthodes de l'entreprise avec un ensemble de règles en vigueur (fiscales, juridiques, technologiques...).

Cependant, l'apparition de la loi de sécurité financière dès le début des années 1990, ainsi que les nouvelles exigences réglementaires de type Sarbanes-Oxley, ont eu pour effet de généraliser et de systématiser la pratique de ces audits.

Lorsque l'entreprise décide - ou est contrainte - de réaliser un audit, elle est alors amenée à se poser des questions sur la façon de le mener à bien et d'appréhender avec le plus d'objectivité possible les résultats des investigations opérées. D'autant plus que l'Etat est impliqué dans la gestion de la SENELEC car l'électricité est considérée comme un domaine stratégique dans l'économie d'un pays.

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler. C'est alors que le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger.

Dans ce document, un processus métier est défini comme un ensemble d'actions facilitant les interactions de l'organisation avec des entités externes ou internes. Bien que l'utilisation de systèmes informatiques pour automatiser les processus métier soit une méthode beaucoup plus efficace et rentable que l'emploi de superviseurs humains, elle a des conséquences qui n'ont aujourd'hui pas encore été entièrement évaluées. Les organisations qui placent le temps d'accès au marché avant la sécurité choisissent souvent d'automatiser leurs processus métier à l'aide d'applications Web. Dans de nombreux cas, ces organisations n'établissent pas des fonctions de supervision et de contrôle de la sécurité suffisamment puissantes pour réduire les risques au maximum, ce qui peut avoir comme conséquence de graves pertes financières et une dévalorisation de leur réputation.

L'audit des systèmes d'information (A.S.I.) couvre des domaines aussi différents que ceux liés aux processus, à la sécurité du système d'information, à la gestion des droits d'accès ou aux applicatifs métiers (audit de codes...).

Disposer d'une information fiable, actualisée et sécurisée est primordial pour le pilotage des entreprises. Le système d'information et de communication est un facteur clé de succès pour les stratégies du dirigeant, le développement des entreprises et l'évolution des organisations. Il participe fortement à l'amélioration des performances administratives et commerciales de l'entreprise.

Ainsi se pose la question à savoir : « Quel est l'intérêt de faire l'Audit de l'application informatique de gestion des stocks (Oracle IC) de la SENELEC ? ».

L'Application Oracle IC au niveau de la SENELEC a pour but de fiabiliser la gestion et le suivi des Stocks de la SENELEC.

Le processus gestion et suivi des Stocks métier est un ensemble d'actions facilitant les interactions de l'organisation avec des entités externes ou internes pour les opérations de traitement des Stocks. L'utilisation du logiciel Oracle IC, quand bien même, assure une efficacité des traitements. Elle a des conséquences relatives à la sécurité, à l'optimisation des traitements, à des pertes financières.

Face à ces difficultés, on peut s'interroger sur les solutions possibles à travers la démarche suivante :

- prise de connaissance des supports organisationnels ;
- prise de connaissance de l'interface constituée par les procédures de gestion et de suivi des stocks ;
- diagnostic de l'application Oracle IC ;
- forces et faiblesses des supports organisationnels, des procédures de suivi et de gestion des stocks et de l'application Oracle IC ;
- synthèse des faiblesses ;
- recommandations.

La refonte des programmes et des applications ne peut pas s'inscrire dans le cadre du mémoire, compte tenu du délai dont nous disposons. Par ailleurs, l'élaboration d'un schéma directeur et d'un plan de développement informatique nécessitera un diagnostic des applications.

Ainsi certaines questions spécifiques retiennent notre attention :

- La SENELEC dispose-t-elle d'une organisation optimale pour la gestion des stocks ?
- Quelle est la fiabilité de l'utilisation d'Oracle IC au niveau de SENELEC ?
- L e logiciel Oracle IC est-il suffisamment sécurisé ?
- Le logiciel Oracle IC permet-il un traitement exhaustif des données de stocks ?

Pour répondre à ces questions, nous allons effectuer **l'audit de l'application informatique de gestion des stocks (Oracle IC) de la SENELEC** de Dakar.

Les objectifs poursuivis à travers cette étude se situent à plusieurs niveaux qui sont de manière spécifique :

- Décrire l'application Oracle IC ;
- Procéder à son évaluation ;
- Formuler des recommandations.

Ainsi, afin de pouvoir exécuter des audits informatiques, l'auditeur se devrait de s'informer sur le contexte technique ainsi que sur les méthodes d'analyse et d'approche utilisées pour la conception du système d'information de son entreprise. De ce fait, bien connaître les méthodes, le cycle de vie d'un système, l'analyse de l'existant ainsi que les diverses étapes de l'informatisation, constituent un background important pour les auditeurs en informatique. Surtout si l'intéressé est amené à auditer un projet dans un contexte de vérification de la politique informatique de son entreprise.

Ce mémoire permettra aux Responsables et Directeurs d'Entreprise, aux étudiants inscrits au cycle de formation d'audit, d'être sensibilisés et de se familiariser avec l'audit des applications informatiques.

D'où l'importance d'inciter les Responsables d'entreprises à mettre en place des structures de contrôle de deuxième niveau (Audit) pour garantir cette sécurité et disposer d'applications informatiques performantes a été notée.

Cette étude revêt des intérêts à plusieurs niveaux :

- Pour l'entreprise :

Ce projet a pour but de poser des méthodes génériques pour réaliser un audit du système d'information d'une entreprise. L'audit aura pour but de permettre à l'entreprise de maîtriser ses coûts et d'obtenir une valeur ajoutée sur son fonctionnement.

En effet, en préconisant des sauvegardes régulières par exemple (et donc en vous évitant la perte de données), l'auditeur vous fait faire potentiellement de grandes économies.
Notre étude permettra à la SENELEC de disposer donc d'une bonne maîtrise de l'application informatique Oracle IC.

- Pour le CESAG :

L'étude représente 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, le fruit de la formation dispensée. Il aura à apprécier notre capacité à résoudre les problèmes susceptibles d'être rencontrés dans l'exercice de notre métier qu'est l'auditeur interne et le contrôleur de gestion.

- Pour le lecteur :

Ce travail donnera à celui-ci une meilleure idée de la notion d'audit informatique et viendra enrichir la documentation déjà existante au Centre Africain d'Etudes Supérieures en Gestion (CESAG).

- Pour nous même :

Ce document va nous permettre de connaître les différents indicateurs que l'on pourra analyser durant l'audit. Il nous présentera aussi les différentes méthodes pour récupérer ceux-ci.

Nous présenterons aussi certains scripts qui pourraient être utiles pour la réalisation de l'audit. Nous finirons par une description de la présentation des résultats pour le rapport d'audit.

A travers ce thème, nous développerons aussi les outils pédagogiques acquis au cours de notre formation aussi bien sur le plan théorique que sur le plan pratique.

Ce mémoire sera, ainsi, structuré en deux parties :

- La première partie sera consacrée à la théorie sur l'audit des applications informatiques.
- La deuxième partie sera consacrée à l'étude du cas pratique d'Oracle IC au niveau de la SENELEC. Pour cela, nous ferons d'abord une prise de connaissance de l'entreprise, la présentation du logiciel Oracle IC, l'évaluation de la gestion des stocks et du logiciel Oracle IC et ferons des recommandations sur les faiblesses décelées.

PREMIERE PARTIE : THEORIE SUR L'AUDIT DES APPLICATIONS INFORMATIQUES

Une entreprise crée de la valeur en traitant de l'information, notamment dans le cas des sociétés de service. Ainsi, l'information possède une valeur d'autant plus grande qu'elle contribue à l'atteinte des objectifs de l'organisation.

Le système d'information coordonne grâce à l'information les activités de l'organisation et lui permet ainsi d'atteindre ses objectifs. Il est le véhicule de la communication dans l'organisation.

A la question de savoir ce qu'est l'audit, THORIN (1993) répond que « auditer c'est inventorier, analyser, tester et préconiser ». Reprise et détaillée par nous, cette définition retient notre attention en ce sens qu'elle présente l'audit comme étant le fait d'écouter, de décrire afin de déceler les faiblesses et les forces du système à améliorer.

L'audit a fait l'objet de nombreuses définitions tant de la part des professionnels du domaine que des divers groupes de travail (associations, instituts, etc.…). De cette multitude de définitions, nous en retiendrons une afin de cerner son contenu.

L'audit est selon THORIN (1993) :

- l'examen méthodologique des états financiers ou de tout autre domaine de l'entreprise, à ce titre, il permet de formuler une opinion sur les comptes et / ou d'apprécier les performances et l'efficacité à tous les niveaux du système ;
- fait par un professionnel : c'est une personne indépendante par rapport au domaine contrôlé et compétente au regard de sa formation multidimensionnelle qui donne un avis motivé sur une situation donnée ;
- exécuté dans les règles de l'art, c'est-à-dire avec des normes et des procédures qui permettent de se forger une opinion.

Comme dans toute branche de l'activité d'une entreprise, l'audit doit exister en informatique, et même davantage en fonction des vulnérabilités et des coûts qu'elle induit. En effet, un audit informatique n'a de sens que si sa finalité est définie : contrôle fiscal, juridique, expertise judiciaire, vérification de l'application des intentions de la direction, examen de l'efficacité ou de la sécurité d'un système, de la fiabilité d'une application.

Aussi, auditer rationnellement, c'est expliciter les finalités de l'audit, puis en déduire les moyens d'investigation jugés nécessaires et suffisants.

Un audit informatique encore appelé audit des systèmes d'information ne concerne pas nécessairement la sécurité. En effet, il peut aussi évaluer des aspects stratégiques ou de qualité des systèmes d'information. Par exemple, répondre à la question suivante : Est-ce que les systèmes d'information de l'entreprise répondent efficacement aux besoins des services métiers ? La démarche est très similaire, en choisissant et évaluant les processus informatiques proposés par le Cobit qui répondent le mieux à la demande du client.

Pour BENNAMI (2004 : 10/22) de l'école Mohammadia d'ingénieurs, les composantes d'un audit informatique sont :

- L'examen de l'organisation du service ;
- L'examen des procédures liées au développement ;
- L'examen des procédures liées à l'exploitation ;
- L'examen des fonctions techniques ;
- Le contrôle sur la protection et la confidentialité des données.

Cette première partie comprend :

- Les approches théoriques de l'audit des applications informatiques ;
- la revue de l'organisation générale de la sécurité informatique ;
- la méthodologie de l'étude de l'application Oracle IC.

CHAPITRE 1 : APPROCHES THEORIQUES DE L'AUDIT DES APPLICATIONS INFORMATIQUES :

L'utilisation de l'informatique dans le domaine de la gestion comptable et financière des organisations s'est considérablement développée ces dernières années. Ce développement et son accélération ont conduit les auditeurs à s'interroger sur la validité de l'approche et des outils traditionnels de l'audit, à adapter progressivement leur démarche et surtout à développer de nouveaux moyens d'investigation (Raffégeau & al. 1993 : 176).

Plusieurs points de vue sont développés depuis les années 70 avec la publication, par l'Institute of Internal Auditors (I.I.A.), du premier rapport sur l'audit et le contrôle des systèmes d'information.

Les innovations et l'évolution des nouvelles technologies, rendant caduques certaines démarches et outils d'audit, entraînent une mise à jour continuelle dans ce domaine.

Fort peu connu, l'audit informatique est un nouveau métier qui suscite beaucoup d'antipathies du fait de son caractère technique, de l'ignorance de plusieurs dirigeants d'entreprises et de cette tendance à croire à la neutralité de l'informatique. De nos jours, une évolution considérable de la perception de l'informatique dans l'organisation a été faite.

Ainsi, l'audit informatique peut être demandé par la direction générale pour l'assurance de la qualité de l'informatique, par le responsable informatique pour apprécier une opinion externe sur son organisation, par les contrôleurs internes pour l'assurance de la qualité de l'environnement informatique et par les utilisateurs pour la confirmation de leurs réclamations.

1.1. Définitions de l'audit informatique :

Comme préalable, il convient de noter que l'audit informatique est différent des autres audits formalisés et standards. Les définitions de l'audit informatique varient selon les auteurs et suivant le développement de l'informatique. Ainsi, selon COLLINS & al (1992 : 185), l'audit informatique se définit comme étant « un examen par lequel l'entreprise s'assure qu'elle a pris toute mesure raisonnable pour préserver la validité, la fiabilité et l'intégrité des traitements ainsi que la sauvegarde de tout fichier de base auquel le micro-ordinateur peut se lier ».

Et selon LY (2005 : 24), « L'audit informatique est une activité de contrôle du management informatique pour apprécier l'utilisation, l'exécution, l'efficacité et l'adéquation des éléments constitutifs du système informatique ou du système d'information avec l'objectif et l'orientation de l'entreprise.

Cependant, si le concept de l'audit informatique est aujourd'hui largement répandu, ce terme générique couvre en réalité des objectifs et des approches très variées.

L'audit informatique[1] (appelé aussi audit des systèmes d'information) est l'évaluation du niveau de contrôle des risques associés aux activités informatiques. L'objectif apparent est d'améliorer la maîtrise des systèmes d'information d'une entité. L'objectif réel est d'assurer le niveau de service adéquat aux activités d'une organisation, en particulier d'étudier la fiabilité et la pertinence de l'application Oracle IC de la SENELEC.

Dans le cas d'un système d'information comptable d'une entreprise par exemple, il sera nécessaire de vérifier que les Systèmes d'Information sont en mesure d'assurer l'intégrité des données comptables, la disponibilité optimale de l'application répondant à des besoins prédéfinis ou encore le correct interfaçage entre le système comptable et les autres systèmes de l'entreprise.

[1] http://fr.wikipedia.org/wiki/Audit_informatique

Le travail de l'auditeur sera de répondre à cette question en réalisant des investigations concernant le système tant du côté informatique que du côté des utilisateurs (le service comptabilité ou la direction financière). Afin d'adapter ses investigations au sujet de son audit, l'auditeur peut se baser sur les référentiels suivants:

- COBIT (décrivant le fonctionnement complet d'une direction des systèmes d'information) ;
- ITIL (un recueil de bonnes pratiques traitant des niveaux de service informatisé) ;
- Norme ISO.

L'audit informatique est l'examen d'un système d'informations pour porter un jugement, c'est-à-dire comparer ce qui est et ce qui devrait être ; autrement dit, l'appréciation dans un but précis et une situation concrète des systèmes d'information.

Se voulant alors plus concis, A.T.H. (1999) définissant l'audit informatique comme étant l'audit de la fonction informatique, précise qu'il ne faut pas confondre audit informatique et audit dans un cadre informatisé.

L'audit informatique découlant de l'optique de l'audit opérationnel, se présente alors comme étant l'audit du système d'information d'une organisation informatisée. Le champ d'application de l'audit informatique est considérablement plus large en ce sens qu'il inclut l'audit de la fonction informatique, l'audit de la sécurité informatique et de la qualité des systèmes d'information.

Pour Derrien (1992 : 17), l'audit informatique consiste à vérifier « la fiabilité de l'outil informatique et l'usage qui en est fait ». Cette définition réduit l'audit informatique à la vérification de l'outil informatique.

Ainsi, l'audit informatique apparaît donc comme un moyen permettant non seulement de se fier aux informations produites par la machine, mais également de s'assurer que toutes les dispositions ont été prises pour garantir la qualité de l'information tant du point de vue de la conformité que de la régularité.

Pour Thorin (2000), « l'audit informatique consiste à comparer l'observation d'un ou plusieurs objet (s), selon un ou plusieurs aspects, à ce qu'il (s) devrai (en) t être, pour porter un jugement et faire des recommandations ».

L'audit informatique (appelé aussi audit des systèmes d'information) est l'évaluation du niveau de contrôle des risques.

1.2. Typologie d'audit informatique :

L'audit informatique est composé de plusieurs types d'audit orientés dans des domaines différents et ayant non seulement des objectifs distincts mais également des méthodologies particulières. Les domaines les plus usuellement explorés sont notamment : la fonction informatique, le management du système d'information, l'exploitation du système d'information, le matériel informatique physique, le logiciel système ou application de base, les applications et logiciels d'exploitation, les bases de données, les réseaux et la sécurité physique et logique.

L'audit informatique est subdivisé en trois (3) grands groupes : l'audit de la planification du système d'information, l'audit de la fonction étude et développement et enfin l'audit des applications. Cette distinction présente quelques faiblesses en ce sens que l'audit de la planification du système d'information et l'audit de la fonction études et développement pourraient être inclus dans un même audit que couvrirait l'organisation du système informatique de l'entreprise.

Nous retenons alors la distinction faite par l'IFACI (1993), qui classe les différents types de l'audit informatique en trois (3) grands groupes, notamment l'audit de l'environnement informatique, l'audit de l'activité informatique et l'audit des applications informatiques.

L'audit informatique, l'audit des systèmes d'information[2] évalue les risques d'un environnement informatique ou d'une application, par exemple, les salaires ou la facturation. Ces missions se font en choisissant avec le client les processus métiers à évaluer, de même que les processus Cobit à évaluer parmi les 34 proposés.

L'audit d'un environnement informatique peut concerner l'évaluation des risques informatiques de la sécurité physique, de la sécurité logique, de la gestion des changements, du plan de secours, etc. Ou bien un ensemble de processus informatiques - ce qui est généralement le cas - pour répondre à une demande précise du client. Par exemple, apprécier la disponibilité des informations et des systèmes. Le CobiT permet justement de rechercher quels processus informatiques répondent le plus efficacement à une telle demande, par exemple la gestion des performances et des capacités et le plan de continuité dans le cas de la disponibilité.

La mission de l'audit d'une application informatique consiste à apprécier une application informatique en production, par exemple une application de gestion des salaires, une application financière, etc. Très souvent plusieurs domaines font partie d'un audit d'une application, en particulier:

- les données opérationnelles,
- les données de base,
- les paramètres,
- les interfaces entre l'application et d'autres applications,
- la gestion des droits d'accès à l'application.

Bien entendu, tout audit d'une application doit également apprécier la sécurité de l'infrastructure informatique nécessaire au fonctionnement de l'application.

Le livrable sera le rapport contenant les faiblesses relevées, leur niveau de risque et les mesures correctives proposées.

[2] http://www.aud-it.ch/audit%20informatique.html

Face à ces différents référentiels qui ne font point l'unanimité des différentes associations internationales des systèmes d'information, il convient d'étudier le management de l'informatique et les objectifs assignés à l'audit informatique.

1.3. Le management de l'informatique et les objectifs de l'audit informatique :

Nous étudierons d'abord la gestion de l'informatique, le dispositif de contrôle interne de la fonction informatique et nous analyserons les objectifs informatiques.

1.3.1. La gestion de l'informatique :

Le système d'information des entreprises informatisées est sujet à des risques qu'il importe de contrôler. L'organisation de la fonction informatique, les politiques et stratégies associées doivent être gouvernées de façon efficace afin d'assurer au système une performance par la maîtrise des risques encourus. Selon l'AFAI (2002), les principaux éléments matériels de la politique informatique qui assurent une meilleure gouvernance de technologies de l'information sont : le plan informatique, le plan de sécurité et le schéma directeur que nous définissons ci-après.

Le plan informatique est établi suivant un ordre, les buts retenus, classés par préférence et selon les délais d'obtention des moyens et actions. Il formalise les réflexions liées au développement de l'informatique dans l'entreprise, guide et permet le contrôle des actes non rédigés et les mutations dans le temps.

Le plan de sécurité quant à lui comprend tout le dispositif de contrôle, d'accès et de protection humaine, technique et naturelle.

Enfin, *le schéma directeur* est l'ensemble des buts de réalisation, de leur motivation et des conditions de réalisation. C'est un document de référence qui stipule les avantages escomptés, les contraintes (lois, règlements, normes, matériels, langages, logiciels, conditions de travail) et mentionne le degré de prudence.

C'est ainsi que pour l'IFACI (1993) :

- l'organisation de la fonction informatique doit permettre un contrôle étendu. Le contrôle doit d'abord être personnel puis hiérarchique. Cette situation est garante de la continuité de traitement et l'assurance de sa fiabilité.

- Les postes de responsabilité doivent être attribués par rapport au niveau de compétence et de disponibilité. Une bonne gestion des attributions des responsabilités du personnel signifie une séparation des tâches incompatibles. La gestion du centre de traitement, la maintenance du logiciel, l'exploitation, le contrôle des entrées et des sorties des données ainsi que leur protection sont les principales tâches incompatibles dans la fonction informatique. La politique des dirigeants doit être établie de sorte à rendre absolument impossible toute défaillance du système informatique. C'est en cela que le plan informatique général doit intégrer le plan de survie (avec back up) qui est le plan de relève qui assure la continuité de l'exploitation. Il doit être strictement établi de sorte à surpasser les risques d'accidents, de pannes, de fraudes et sabotages, de destruction et même les erreurs de conception et de réalisation.

- La politique informatique et le schéma directeur, définis par la direction, doivent être adaptés à la finalité de l'entreprise, être évolutifs, homogènes avec les objectifs et documentés. En matière de gestion du système informatique, tous les processus, activités et tâches doivent être inscrits dans une documentation qui servira de support à tous les employés. La documentation concerne également l'utilisation des logiciels d'exploitation, les modifications et maintenance de programmes. L'organisation doit par ailleurs disposer d'un programme d'acquisition de matériel et logiciel, du mode de financement (location, crédit-bail, achat) et doit établir un document comprenant les modalités possibles de contrats à signer éventuellement avec ses fournisseurs.

- L'organisation doit disposer d'une politique d'assurance de ses biens informatiques matériels et immatériels. Les procédures contractuelles des assurances et les différents types de polices d'assurances doivent être établies et évaluées.

Pour l'AFACI (1993 : 67), la gestion de l'informatique comprend aussi les politiques d'installations. En effet, les installations doivent être sécurisées contre les dégâts naturels, humains et techniques de sorte à bien protéger le patrimoine informatique. Il est recommandé à cet effet de disposer d'un site de secours parfaitement équipé et prêt à assurer la relève pour la continuité des activités de l'entreprise et ce, dans un délai suffisamment court, acceptable quelles que soient les circonstances. Ce site de sauvegarde, doit être entretenu et continuellement testé afin de s'assurer de son efficacité. On parle souvent de salle blanche ou de back up.

Le management doit définir les politiques de performances, de satisfaction et de sanctions des utilisateurs. La direction générale doit aussi préciser le niveau de services attendu, estimer quantitativement les performances, la disponibilité du système et prévoir les récompenses afin de motiver le personnel.

Toute modification doit être préalablement l'objet d'une autorisation dûment matérialisée. La direction de l'entreprise doit également établir les procédures et les responsabilités pour le diagnostic des incidents, le transfert de programme en production, la gestion des modifications du logiciel de base et les services d'assistance. Celle-ci doit réduire à néant les risques d'interruption de services, appréhender les changements de structure, de marché, de personnel et de logiciels et les changements d'ordre juridique au plan interne, nationale et internationale.

Selon l'AFAI (2002), la gestion de l'informatique implique nécessairement une politique de sécurité. La sécurité se présente comme le point le plus vulnérable aujourd'hui vis-à-vis de l'évolution technologique et du cyberespace qui reçoit chaque jour davantage d'internautes dont le nombre et les interventions ne sont toujours pas cernés. Il s'agira dans la gestion de la sécurité, de mettre en place des procédures et des dispositifs empêchant toute intrusion non autorisée et un contrôle permanent des transactions effectuées.

Il est souvent conseillé l'installation de logiciels de sécurité intégrés au système d'application de base et de logiciels antivirus. La sécurité physique quant à elle sera assurée par des vigiles aidés par des systèmes de sécurité électroniques existant tels que les caméras, les cartes d'accès, les badges, la prise d'emprunte…

Pour une gestion au quotidien de la sécurité informatique, il est indiqué que l'organisation doit disposer d'une *charte de la sécurité informatique* (AFAI, 1997) qui précise les identités et les responsabilités des propriétaires d'applications, les utilisateurs, les prestations de services. Cette charte porte sur trois (3) volets :

- La sécurité des micros ordinateurs autonomes ou en réseau local qui concerne la nature des besoins, les procédures de commandes de logiciels, d'installation de logiciels, de mise en service, les suivis de l'intégrité des logiciels, la sécurité des applications sensibles, les procédures de sauvegarde, la sécurité logique, la protection des outils de maintenance d'intégrité. Pour la protection de l'information, il est institué un système de gestion de mots de passe. Le système précise la nature des besoins sollicités, expose l'opportunité, l'efficacité, la confidentialité, et l'utilisation des mots de passe. Il protège contre l'utilisation frauduleuse des mots de passe et la circulation des mots de passe dans l'espace. Pour la protection de l'information dans le réseau, la charte englobe la sécurité du poste de travail, conserve l'authenticité de l'entité appelée, l'authenticité de l'entité appelante, l'habilitation de l'entité appelante. Elle gère également les connexions et les déconnexions de la liaison appelant / appelé, l'intégrité de la confidentialité des flux. Elle met en exergue en cas de besoin, la preuve des échanges, confirme les applications utilisées et la trace d'audit. Elle englobe aussi le service de sécurité de base.
- Le plan qualité doit inclure les buts, leur applicabilité, leur exigence, l'organisation, les méthodes, les procédures et contrôles, les règles, les normes, les standards, les conventions, les outils, les démarches de développement, les engagements ainsi qu'un glossaire (Thorin, 2000). Cependant, nous estimons que le plan qualité de l'informatique doit être fondé sur la performance du système informatique. Cette performance doit être évaluée par rapport au degré de réalisation des objectifs fixés, de leur mesure, de leur quantification, du coût, du temps,….
- Le contrôle de gestion de l'informatique qui est une innovation en ce sens qu'il fait du management des systèmes d'information un élément essentiel pour un suivi planifié avec l'instauration de tableau de bords informatique pour chaque service de contrôle et d'exécution.

1.3.2. Le dispositif de contrôle interne dans la fonction informatique :

Les dispositifs de contrôle interne doivent contribuer à la sauvegarde intégrale du patrimoine de l'entreprise et partant à sa survie. C'est ainsi que le contrôle interne est formulé selon huit (8) grands principes qui caractérisent des domaines bien précis notamment, l'organisation, l'autocontrôle, l'universalité du contrôle, l'harmonie du contrôle, l'indépendance, la bonne information, permanence et la compétence du personnel. Tout bon système de contrôle interne doit reposer sur l'application de ces principes source d'un bon niveau d'appréciation.

Selon le Guide Pratique d'audit des technologies de l'Information de l'IIA (2007) sur « l'audit des contrôles applicatifs », les contrôles sont classifiés de manière à comprendre les objectifs. Ainsi, on distingue :

- **les contrôles généraux ou contrôles d'infrastructure** qui s'appliquent à l'ensemble des composantes, processus et données d'un environnement système : politique de sécurité de l'information, l'administration, l'accès et l'authentification, la séparation des fonctions clés, la gestion des acquisitions et de la mise en place de systèmes, la gestion des changements des systèmes, la sauvegarde, la restauration de données et la continuité d'activité ;
- **les contrôles applicatifs** qui portent sur l'étendue des processus de l'entreprise ou ses applications : validation des données, séparation des tâches ;
- **les contrôles préventifs** qui permettent d'éviter la survenue d'erreurs, d'omissions ou d'incidents de sécurité ;
- **les contrôles de détection** qui visent à repérer les erreurs ou les incidents échappant aux contrôles de prévention ;
- **les contrôles correctifs** qui ont pour but de corriger les erreurs, omissions ou incidents une fois qu'ils sont détectés.

Ainsi, l'auditeur doit comprendre les procédures et le contrôle interne mis en place dans l'organisation avant le déroulement de sa mission. Toutefois, il est important de noter que la mise en place de ce dispositif de contrôle interne n'est pas du ressort de l'auditeur, d'ailleurs les organisations ne disposant pas de service d'audit interne, ont des procédures existantes formelles ou non qui leur permettent d'effectuer un certain niveau de contrôle sur leur activité.

La situation est plus délicate dans la fonction informatique. En effet, beaucoup ignorent que l'ensemble du matériel informatique est régi par une hiérarchie, une organisation similaire à l'organigramme du personnel des entreprises. Il parait plus facile à comprendre, l'hiérarchie d'une organisation et les contrôles internes mises en place que d'appréhender l'organisation du matériel informatique et du contrôle interne régissant le système informatique.

Le contrôle interne du système informatique a le même objet que le contrôle interne tel que le définit l'ordre des experts comptables français, comme étant « ...un ensemble de sécurité contribuant à la maîtrise de l'entreprise. Il a pour but, d'un coté, d'assurer la protection, la sauvegarde du patrimoine et la qualité de l'information, de l'autre, l'application des instructions de la direction et de favoriser l'amélioration des performances. Il se manifeste par l'organisation, les méthodes et procédures de chacune des activités de l'organisation pour maintenir la pérennité de celle-ci » (ATH, 1991 : 54). Le contrôle interne de la fonction informatique doit permettre à l'entreprise, de maintenir son intégrité et sa pérennité à travers les méthodes et procédures de chacune de ses activités informatiques.

L'auditeur informatique, face au contrôle interne du système informatique, doit fournir à l'entreprise une assurance sur le degré de maîtrise des risques informatiques et de tout l'ensemble de son système d'information. Les procédures de contrôle doivent être mises en œuvre à tous les niveaux de la structure informatique de sorte à doter chaque poste d'un moyen d'autocontrôle et d'un contrôle hiérarchique à un poste de niveau supérieur. Les micro-ordinateurs des utilisateurs finaux sont d'abord auto contrôlés par ces derniers, puis contrôlés par les micros ordinateurs de leurs supérieurs hiérarchiques et ceci jusqu'à l'ordinateur central.

Dans une mission d'audit informatique, qui est un audit opérationnel, l'évaluation du contrôle interne n'a pas la même portée qu'en audit financier. Ce n'est guère une présomption qui aurait une influence sur l'étendue des investigations, mais bien au contraire un simple atout pour une appréhension profonde. Car aujourd'hui l'environnement actuel impose à tout système informatique le minimum de contrôles de sécurité.

Selon SARDI (1993 : 78), « un apport en conseils pour les améliorations du contrôle interne de la fonction informatique est souvent sollicité ». Et cet apport est non des moindres mais d'une immense importance pour l'organisation en ce sens qu'il contribue absolument à créer de la valeur ajoutée, une valeur ajoutée fondée sur des objectifs informatiques fixés.

1.3.3. Objectifs de l'audit informatique :

Avant d'examiner les objectifs visés par l'audit informatique, il faut préalablement comprendre qu'un système d'information est un ensemble de collecte, de stockage, de traitement et de production d'informations, qui peut être plus ou moins automatisé (informatisé). Et, l'audit informatique se révèle comme étant l'examen du système d'information, en tout ou partie, pour porter un jugement sur celui-ci. Mais cette perception peut s'avérer confuse puisqu'en réalité tout le système n'est pas automatisé. C'est pourquoi, il ne faut négliger aucune des parties automatisées ou non. L'audit informatique d'un objet, peut donc porter sur un aspect automatisé comme sur un aspect non automatisé.

En réalité, l'audit informatique peut traiter d'un aspect fiscal, juridique ; peut porter sur les méthodes générales de gestion, sur le génie logiciel, sur l'utilisation et dans chaque cas, peut être correctif, détectif ou préventif des risques informatiques.

C'est en cela que THORIN (2000 : 138) a soutenu que « les finalités de l'audit informatique sont de porter un jugement sur les composants et les éléments temporels concernés du système informatique, à un moment et au lieu où ce jugement est utile pour l'ensemble d'individus qui peuvent être, ou non, le même que l'ensemble des destinataires d'informations produites par le système ».

L'objectif premier d'un audit informatique est toujours le même : vérifier la fiabilité de l'outil informatique et l'usage qui en est fait.

Malheureusement, cet objectif fondamental est difficile à atteindre. La complexité d'un environnement informatique et des chaînes de traitement qui y sont gérées est telle qu'il

est impossible à un auditeur, aussi compétent soit-il et même à l'issue d'une mission de longue durée, d'avoir la certitude de la fiabilité de cet environnement.

L'auditeur même s'il est un spécialiste de l'informatique, n'est pas toujours un spécialiste des domaines fonctionnels qu'il contrôle.

Bien que les trois dimensions susmentionnées concernant l'optique corrective, détective et préventive sont en parfaite adéquation avec tout objet d'audit opérationnel, il convient de marquer un point particulier par rapport à l'audit informatique.

Pour aller dans ce sens, ROVALEC (1991 : 99) soutient que : « l'audit informatique a pour objectif de vérifier et contrôler que toutes les causes de mauvais fonctionnements, de sources d'erreurs ou de risques de détériorations diverses et frauduleuses sont éliminées ou du moins, peuvent être détectées rapidement en cours d'exploitation ».

Remarquons que cette vision est restrictive puisque vérifier et contrôler n'inclut aucune finalité de correction. Il s'agit purement de l'aspect sécuritaire des systèmes d'information.

En fait, la sécurité des systèmes d'information suppose, la prévention et la protection du système vis-à-vis du risque. Or l'audit va bien au delà en apportant un aspect correctif. Cet aspect correctif est beaucoup plus perçu dans les procédures mises en place pour assurer le bon fonctionnement du système. Il est alors justifié d'orienter les objectifs de l'audit informatique par rapport à l'efficacité fonctionnelle du système d'information comme le soutient l'IFACI (1993).

- Le premier objectif de l'audit informatique selon l'IFACI (1993) est un objectif de management. Il revient à l'auditeur d'aider la direction dans le pilotage de son système d'information et de contribuer à la réalisation des objectifs informatiques fixés. Ces objectifs étant bien entendu souvent formalisés, il revient à une appréciation des documents internes, créés par l'organisation, relatifs à la fonction informatique (le plan informatique, le schéma directeur, le plan de sécurité, le manuel de procédures) et à une évaluation du contrôle interne de la fonction informatique.

- ❖ Les seconds objectifs de l'audit sont liés à des faits ponctuels, provenant des plaintes des utilisateurs, des programmeurs, de la direction, ou sont relatifs à des accidents ou des dommages internes comme externes ou le plus souvent relatifs à un souci de performance et de réadaptation. L'audit informatique dans ce cas aura donc des objectifs curatifs de recherches, d'investigations et de corrections.

Tout objectif de l'audit informatique est vraisemblablement lié aux risques encourus par le système d'information. Communément, trois (3) sources de risques sont distinguées[3] :

- Les risques d'origine naturelle (foudre, inondation, glissement de terrain,….) ;
- Les risques d'origine technique (incendie, feu, court circuit, dégât des eaux panne de machine, panne réseaux, obsolescence, mauvais entretien,….) ;
- Les risques d'origine humaine (événements accidentels, erreurs, grève, démission, actes délictueux, vols, sabotage, copies illicites,…).

A ces risques, il faut associer le premier objectif de l'audit informatique (objectif de soutien au management du système d'information). Une bonne gestion basée sur une efficacité des procédures, doublée d'un bon niveau de contrôle interne est une garantie suffisante d'une gouvernance assurée. L'audit informatique s'impose alors comme le moyen de la maîtrise de ces risques. Il prend en compte l'étude et l'évaluation de la dimension humaine, naturelle et technique. Il va même au delà en étendant ses investigations à l'ensemble des ressources utilisées par la fonction informatique et à ses politiques et stratégies. Parler de ressources utilisées par la fonction informatique, il ne faut pas seulement penser au matériel informatique uniquement. Ce matériel existe par rapport à une certaine dimension financière, il est exploité et décidé par le personnel et fonctionne sous le processeur d'un ensemble immatériel à en tenir compte.

Selon THORIN (2000), l'objectif de l'audit informatique pour ces années 2000, a dépassé l'aspect généraliste et s'intéresse à des points plus recentrés liés aux contrôles des questions de coûts d'opportunité, de qualité, de délais, de prix, d'exactitude, d'exhaustivité, de sécurité, de fiabilité et de performance du système d'information automatisée. Il est aussi plus technique avec l'audit des applications qui est de plus en

[3] Source : Nous-même

plus sollicité face à la multiplicité des applications due à la simplicité des programmations avec les langages de quatrième génération (SQL, C++ , Cobol, JAVA) effectuées même par les utilisateurs.

L'un des objectifs de l'audit des applications est de s'assurer que les actions effectuées par le personnel de la fonction informatique (directeur, chef de projet, programmeurs, analystes, maintenanciers, techniciens, utilisateurs) sont approuvées et autorisées. Les applications doivent être paramétrées de telle sorte à assurer que les fichiers et logiciels ne puissent pas être modifiés, mais plutôt sécurisés par la détection d'opérations anormales, accessibles si autorisés. La mise à jour des mots de passe, les contrôles des traitements, la pérennité, la continuité d'exploitation, le contrôle des sorties, de la piste d'audit sont également pris en compte dans l'audit des applications.

Enfin, l'audit informatique a pour finalité la contribution à la création de valeur ajoutée. « Tout auditeur informatique qui ne crée pas de la valeur ajoutée qualitative, mesurable et quantifiable doit s'interroger sur sa présence et son importance dans l'organisation », (SARDI, 1993 : 23). Cette importance de l'auditeur informatique est beaucoup plus avérée avec l'utilisation des nouvelles technologies.

Ce premier chapitre nous a permis d'analyser un ensemble de théories développées autour du concept d'audit informatique.

En effet, une action de mise à niveau de l'approche d'audit s'impose aux organismes professionnels dans le monde et aux cabinets internationaux. C'est ainsi que ces organismes professionnels n'ont pas tardé à apporter et à mettre à jour les lignes directrices et le minimum de diligences pour un audit dans un milieu informatisé.

Les cabinets internationaux d'audit développent de plus en plus des méthodologies appropriées et font de gros investissements pour adapter les approches d'audit à un environnement devenu de plus en plus complexe et turbulent.

En plus de ces efforts, la législation, la jurisprudence et la doctrine à l'échelle internationale se sont enrichies de nouvelles règles destinées à réglementer et à contrôler certains aspects des systèmes informatisés.

Ainsi, les objectifs de l'audit informatique ont mis à jour la nécessité pour les gestionnaires de consacrer de l'importance au management rigoureux de l'informatique et au contrôle interne de la fonction informatique.

CHAPITRE 2 : LA REVUE DE L'ORGANISATION GENERALE DE LA SECURITE INFORMATIQUE :

La sécurité peut être définie comme l'ensemble des moyens mis en œuvre et dont le rôle est d'assurer une protection contre tout danger clairement défini. La sécurité d'un système d'information fait souvent l'objet de métaphores. En effet, on la compare régulièrement à une chaîne en expliquant que le niveau de sécurité d'un système est caractérisé par le niveau de sécurité du maillon le plus faible. Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue.

La sécurité des systèmes d'information (SSI)[4] est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir du système d'information. Assurer la sécurité du système d'information est une activité du management du système d'information.

Cela signifie que la sécurité doit être abordée dans un contexte global et notamment prendre en compte les aspects suivants :

1. La sensibilisation des utilisateurs aux problèmes de sécurité ;
2. La sécurité logique, c'est-à-dire la sécurité au niveau des données, notamment les données de l'entreprise, les applications ou encore les systèmes d'exploitation ;
3. La sécurité des télécommunications : typologie des réseaux, serveurs de l'entreprise, réseaux d'accès, etc.
4. La sécurité physique, soit la sécurité au niveau des infrastructures matérielles : salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, postes de travail des agents de l'entreprise, etc.

La sécurité des systèmes d'information[5] se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système, en mettant en place des mécanismes d'authentification et de contrôle. Ces mécanismes permettent d'assurer que les

[4] http://fr.wikipedia.org/wiki/Sécurité_du_système_d'information

[5] http://fr.wikipedia.org/wiki/Sécurité_du_système_d'information#Politique_de_s.C3.A9curit.C3.A9

utilisateurs des dites ressources possèdent uniquement les droits qui leurs ont été octroyés.

La sécurité informatique doit toutefois être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance. C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité, c'est-à-dire :

- élaborer des règles et des procédures, installer des outils techniques dans les différents services de l'organisation (autour de l'informatique) ;
- définir les actions à entreprendre et les personnes à contacter en cas de détection d'une intrusion ;
- sensibiliser les utilisateurs aux problèmes liés à la sécurité des systèmes d'informations ;
- préciser les rôles et responsabilités.

La politique de sécurité est donc l'ensemble des orientations suivies par une entité en termes de sécurité. À ce titre, elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système.

En fait, on appelle sécurité des systèmes d'information la structure de contrôle mise en place dans le but de protéger l'intégrité, la confidentialité, la disponibilité des ressources et des données de ces systèmes.

2.1. L'architecture de sécurité :

La sécurité est une des questions qui doit le plus attirer l'attention de l'auditeur. Selon ANGOT (2004 : 102), la sécurité doit être considérée d'abord au niveau de la sécurité générale et du maintien d'une information fiable et cohérente. Elle concerne principalement l'ensemble des procédures générales de « back-up » et de protection d'accès aux différentes parties du logiciel. On veillera à vérifier si la comptabilité (dans le cadre ou non de la sécurité générale), fait l'objet de prises de copies de sécurité (back-up) adéquates. Normalement, une copie journalière est suffisante avec maintien des copies de début de semaine, de la veille et de l'avant-veille.

Il est impératif de protéger les copies « back-up » de l'incendie, des dégâts des eaux et du vol. Pour ce motif, la conservation d'une copie périodique dans un lieu externe est hautement souhaitable.

En matière de protection d'accès, il y a lieu de vérifier :

- l'existence d'un système de mots de passe ;
- l'existence d'une procédure fiable obligeant à la modification des mots de passe ;
- l'existence de procédures de sécurité protégeant toute application d'un accès intempestif ou frauduleux et dénonçant les tentatives d'intrusion.

Il convient ensuite de contrôler la gestion de la sécurité spécifique en termes d'accès aux différentes fonctionnalités comptables telle qu'elle est organisée pour les utilisateurs de ces fonctions à l'intérieur des services comptables et financiers et à l'extérieur de ces services.

Dans ce domaine, l'existence d'une matrice de sécurité réglementant de manière souple et sélective les accès aux divers programmes de l'application, constitue une bonne solution. Certains logiciels permettent même d'organiser un contrôle d'accès sélectif par catégories d'utilisateurs au niveau de chaque type de données. Ainsi, la question de la sécurité se pose également en terme de « pérennité évolutive » du logiciel. En effet, le risque d'incident ou de blocage dans l'évolution du logiciel est d'autant plus grand, vu la « volatilité » des conceptions et fournisseurs de logiciel, que :

- l'auteur est petit et peu structuré ;
- la base clients est restreinte ;
- les programmes source du logiciel ne sont pas disponibles ;
- la documentation technique (organigramme général, dossiers d'analyse et de programmation, etc.) n'est pas disponible.

Avec le développement de l'utilisation d'Internet[6], de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs. Il est donc essentiel à l'entreprise représentée de connaître ses ressources qu'il faut protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur Internet.

Par ailleurs, avec le nomadisme, consistant à permettre aux personnels de se connecter au système d'information à partir de n'importe quel endroit, les personnels sont amenés à « transporter » une partie du système d'information hors de l'infrastructure sécurisé de l'entreprise. C'est pour répondre à ce besoin que s'inscrit cette partie sur la sécurité du système d'information. En effet, la sécurité est la situation dans laquelle un système informatique, connecté ou non à un réseau externe de télécommunication, est protégé des dangers internes ou externes.

Dés lors, la sécurité revêt une importance qui augmente avec le développement des réseaux IP. La complexité des technologies utilisées, la croissance exponentielle des terminaux à protéger ainsi que la prolifération de nouvelles menaces (virus, mais aussi outils de « hacking » facile d'accès) démontrent que la sécurité est, et sera toujours un enjeu stratégique majeur.

Les entreprises, de plus en plus multinationales, délocalisées, éclatées misent sur leur système d'information pour maintenir une cohésion efficace et fluidifier leurs échanges internes et externes. On voit ainsi apparaître des grands projets de réseau intranet, extranet au niveau mondial. Le « zéro papier » est de rigueur et toute la substance de

[6] http://www.commentcamarche.net/contents/secu/secuintro.php3

l'entreprise réside dans les hommes, et dans le système d'information qui constitue donc l'épine dorsale de cet ensemble.

De nombreuses grandes entreprises ont d'ores et déjà compris l'importance de ces enjeux et définissent une politique de sécurité qui est déterminé au niveau mondial pour ensuite être appliqué dans toutes les filiales. Ces règles ont souvent pour objet de réglementer non seulement la conception des systèmes d'information, mais surtout les comportements des utilisateurs.

La direction générale est chargée de gérer et de contrôler les opérations, ainsi que d'élaborer, de communiquer et de superviser les politiques et procédures de l'organisation. En matière de sécurité des systèmes d'information, la direction générale est responsable de l'évaluation des risques, de l'établissement de la politique de sécurité et de la mise en œuvre d'une structure organisationnelle.

Il est indispensable de définir une politique de sécurité à l'échelle de l'organisation, dans le but de canaliser le développement efficace des procédures et des pratiques de sécurité et de responsabiliser l'ensemble du personnel.

Les points suivants devront être étudiés :

- L'objet, le champ de la politique ainsi que les installations, les systèmes et le personnel concernés ;
- La stratégie de sécurité et son lien avec la stratégie globale de l'organisation ;
- Les objectifs de sécurité et les méthodes associées ;
- La responsabilité à tous les niveaux de l'organisation ;
- La définition des violations et des sanctions en cas de non-conformité.

Pour que l'ensemble du personnel perçoive bien l'importance de la sécurité, il est souhaitable que cette politique soit approuvée et émise par la direction de l'organisation. Par la suite, elle devra être actualisée et évaluée chaque année, et tous les employés devront prendre connaissance des modifications.

Devant la croissance rapide de la population et l'augmentation correspondante des besoins en courant électrique, on s'inquiète de plus en plus de la qualité de l'alimentation disponible pour les matériels informatiques. Donc pour être efficace, la sécurité des S.I. doit prendre en compte le matériel, les logiciels, les procédures et les plans stratégiques de l'organisation. Elle doit reposer sur des procédures de gestion très saines. Enfin, il est indispensable que l'ensemble du personnel de l'organisation soit conscient de l'importance de la sécurité. En fait, l'audit de la sécurité suppose une analyse approfondie de l'organisation et des procédures de sécurité.

2.2. Le contrôle de deuxième niveau (AUDIT) :

Plus aucune entreprise ne peut se passer de l'outil informatique, d'où la nécessité d'en assurer la sécurité, et de la protéger contre les risques liés à l'informatique. Or, comme on ne se protège efficacement que contre les risques qu'on connaît, il importe de mesurer ces risques, en fonction de la probabilité ou de la fréquence de leur apparition et de leurs effets possibles. Chaque organisation a intérêt à évaluer, même grossièrement, les risques qu'elle court et les protections raisonnables à mettre en œuvre. Les risques et les techniques de sécurisation seront évalués en fonction de leurs coûts respectifs. En fait, les risques étant inhérents à la vie de toute entreprise, il est nécessaire, pour pouvoir parer aux situations dangereuses, de les identifier, les quantifier, les hiérarchiser et les traiter.

Selon Hugues ANGOT (2004 : 265), les risques inhérents et les risques liés au contrôle dans un environnement informatique peuvent avoir un effet diffus et un effet spécifique à un type de comptes sur la probabilité d'anomalies significatives dans les circonstances suivantes :

- Les risques peuvent résulter de déficiences dans plusieurs des activités informatiques telles que : développement et maintenance des programmes, support logiciel, opérations, sécurité physique des équipements informatiques, contrôle d'accès à des utilisateurs privilégiés. Ces déficiences ont un effet diffus sur toutes les applications traitées par l'ordinateur.
- Les risques peuvent accroître le potentiel d'erreurs et de fraudes dans des applications spécifiques, des bases de données, des fichiers maîtres ou des

traitements spécifiques. Ainsi, les erreurs sont relativement fréquentes dans des systèmes exécutant des opérations logiques ou des calculs complexes, ou qui gèrent un nombre élevé d'exceptions. De même, les systèmes qui contrôlent les sorties de fonds ou d'autres liquidités peuvent faire l'objet de fraudes de la part des utilisateurs ou du personnel informatique.

Les clients recourent fréquemment aux nouvelles technologies pour développer des systèmes informatiques de plus en plus complexes qui peuvent comporter des liaisons micro-gros systèmes, des bases de données distribuées, des traitements utilisateur final et des systèmes de gestion qui transfèrent directement des informations dans les systèmes comptables. Ces systèmes augmentent le degré de sophistication global de l'environnement informatique et la complexité des applications concernées. En conséquence, ils peuvent accroître le risque et nécessiter une attention particulière.

Dans cette optique, l'audit par les risques est une technique de contrôle de l'information. En effet, elle est à la fois :

- un mode de représentation et de hiérarchisation des risques ;
- un résumé de la situation à un instant donné ;
- un instrument de communication et de management stratégique ;
- et une aide à la décision.

Le risque en termes de sécurité est généralement caractérisé par l'équation suivante[7] :

$$\text{Risque} = \frac{\text{Menace} * \text{Vulnérabilité}}{\text{Contre-mesure}}$$

La menace (en anglais « threat ») représente le type d'action susceptible de nuire dans l'absolu, tandis que la vulnérabilité (en anglais « vulnerability »), appelée parfois faille ou brèche représente le niveau d'exposition face à la menace dans un contexte particulier. Enfin la contre-mesure est l'ensemble des actions mises en œuvre en prévention de la menace.

[7] http://www.commentcamarche.net/contents/secu/secuintro.php3

Les contre-mesures à mettre en œuvre ne sont pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'intention des utilisateurs, ainsi qu'un ensemble de règles clairement définies.

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la manière d'agir de l'ennemi. Le but de ce dossier est ainsi de donner un aperçu des motivations éventuelles des pirates, de catégoriser ces derniers, et enfin de donner une idée de leur façon de procéder afin de mieux comprendre comment il est possible de limiter les risques d'intrusions. C'est pour atteindre ce niveau maximal de sécurité, (mais le risque zéro n'existant pas), que s'inscrit notre étude sur l'audit informatique. En effet, la sécurité de l'informatique pose un problème d'un ordre nouveau et que le simple ajout d'une serrure ne saurait résoudre.

La prolifération du nombre d'ordinateurs et de ses applications, compte tenu du volume, de la qualité et de l'importance des informations conservées dans les systèmes informatisés, a engendré une multitude de menaces intentionnelles ou non pouvant porter atteinte au caractère confidentiel, à l'authenticité et à l'accessibilité des données emmagasinées dans ces systèmes informatisés.

☞ L'accroissement du nombre de banques de données contenant différentes informations stratégiques pour l'entreprise a multiplié les risques de violation du caractère confidentiel. Il demeure de la responsabilité de l'entreprise de veiller à protéger adéquatement ses informations emmagasinées dans les ordinateurs.

☞ La perte d'un fichier ou d'une banque de données ou la non disponibilité des équipements informatiques en temps opportun, causée par une erreur de programmation, d'un sabotage ou d'un désastre naturel, peut parfois signifier pour une entreprise, la fin permanente des opérations.

☞ La prolifération des ordinateurs et des systèmes informatiques ainsi que leur interconnexion (à l'échelle de l'entreprise, de la nation, de la planète), a fait naître une forme de criminalité beaucoup plus sophistiquée, plus rentable que toutes les autres connues à ce jour, et dans laquelle on peut évoluer sans danger d'être pris. Les

conséquences de cette criminalité dite ''informatique'', peuvent être désastreuses pour les entreprises (exemple : SGBS PARIS).

2.3. La démarche Risk Management :

Le comité de Bâle définit le risque opérationnel comme : « le risque de pertes dues à l'inadéquation ou la défaillance de processus internes, au personnel ou aux systèmes ainsi que celles dues aux évènements externes. » En fait, cette définition inclut le risque légal mais elle exclut le risque stratégique et le risque de réputation.

Le S.I. consiste à établir des règles et avoir des actifs exécutés par des acteurs. L'approche par les contrôles consiste à vérifier la conformité _ on ne prend pas en charge les risques nouveaux_ tandis que l'approche par les risques consiste à recenser au préalable tous les risques de l'entreprise.

Dans une entreprise, on a un seul RSSI (Responsable Sécurité Système Informatique) qui est placé au niveau du DG et plusieurs RM (Risk Manager). Ainsi donc assurer la sécurité de son informatique est primordial pour toute entreprise. En fait, l'entreprise doit contrôler en permanence la qualité des mesures de sécurité mises en œuvre.
La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.

En Anglais, deux termes différents : **Security = "Safety"** sont utilisés pour parler de sécurité.

- La sécurité = « Security » pour qualifier la protection des systèmes informatiques contre des actions malveillantes intentionnelles.
- Domaine d'élection : les systèmes informatiques réalisant des traitements sensibles ou comprenant des données sensibles.
- La sécurité = « Safety »pour qualifier la protection des systèmes informatiques contre les accidents dus à l'environnement, les défauts du système.
- Domaine d'élection : les systèmes informatiques contrôlant des procédés temps réels et mettant en danger des vies humaines (transports, énergie).

L'objectif d'audit est donc de déterminer les risques encourus et les failles dans la sécurité du système d'information, les analyser et les classifier en fonction de leur degré de gravité, leur probabilité de survenance et leur implication sur le fonctionnement du système d'information.

L'Audit de la Sécurité couvre toutes les composantes du système d'information. Il doit aboutir, en cas d'insuffisances décelées, à la proposition des mesures à mettre en place pour renforcer la sécurité :

- Définition du modèle de sécurité ;
- Définition des procédures et choix des outils ;
- Ressources humaines nécessaires.

Notre objectif sera de procéder à l'évaluation de l'organisation générale mise en œuvre pour assurer la sécurité du système informatique.
Les travaux d'audit comportent des aspects à passer sous revue :

- Politique générale et plan de sécurité ;
- Management et pilotage de la sécurité ;
- Charte de sécurité ;
- Procédures de gestion opérationnelle de la sécurité ;
- Sensibilisation et formation du personnel à la sécurité informatique.

Une politique de sécurité est un ensemble de règles qui fixent les actions autorisées et interdites dans le domaine de la sécurité.

Quant aux *plans de sécurité*, ils comportent le schéma directeur sécurité et le plan opérationnel de sécurité.

=> Schéma directeur sécurité :

 Classification des ressources et leur niveau d'indisponibilité admise, qui est un préalable incontournable à l'appréciation de la gravité des risques.

 Classifications des risques et mesure de leurs impacts sur l'entreprise.

=> Plan opérationnel de sécurité :

Plan de mise en œuvre de la sécurité au niveau de chaque unité opérationnelle.

Une charte de sécurité (charte de management) qui est un contrat de confiance entre l'entreprise et les employés, fixant :

❖les droits, devoirs et responsabilités du personnel et de l'entreprise, quant à l'utilisation des systèmes informatiques ;

❖les sanctions en cas de non respect.

Cette charte peut être annexée au contrat de travail ou au règlement intérieur. En effet, l'un des grands problèmes des entreprises, telle que la SENELEC reste souvent lié :

- à la mauvaise gestion des systèmes informatiques ;
- à des risques accidentels (incendie, panne, catastrophe naturelle) ;
- à des erreurs d'utilisation ou dans la conception et la réalisation de logiciels, bug comme le problème actuel du mauvais fuel acheté ;
- à la malveillance liée au vol, au sabotage, au rebond, au virus ;
- et enfin aux détournements d'informations discrètes et confidentielles.

Ainsi il devient impératif pour les dirigeants d'entreprises d'avoir une meilleure maîtrise des risques informatiques afin d'éviter les conséquences assez souvent lourdes qui peuvent être classées en deux groupes :

D'abord, les conséquences directes :

- Destruction partielle ou totale des données ;
- Impossibilité temporaire ou définitive de reprise d'activité ;
- Frais d'expertise liés aux sinistres ;
- Frais de réparation de remplacement des matériels ;
- Immobilisation du personnel.

Ensuite, les conséquences indirectes :

- Perte de l'exploitation ;
- Perte de fonds et de biens ;
- Engagement de la responsabilité de l'entreprise.

2.4. La méthode d'analyse des risques informatiques :

Nous parlerons de la méthode MARION, de la méthode MEHARI et du COBIT.

2.4.1. La méthode MARION :

La méthode MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux) est issue du CLUSIF[8] (Club de la Sécurité des Systèmes d'Information Français) et la dernière mise à jour date de 1998.

Il s'agit d'une méthodologie d'audit, qui, comme son nom l'indique, permet d'évaluer le niveau de sécurité d'une entreprise (les risques) au travers de questionnaires pondérés donnant des indicateurs sous la forme de notes dans différents thèmes concourant à la sécurité à savoir :

- ✓ La sécurité organisationnelle ;
- ✓ La sécurité physique ;
- ✓ La continuité ;
- ✓ L'organisation informatique ;
- ✓ La sécurité logique et exploitation ;
- ✓ La sécurité des applications.

L'objectif de la méthode :

L'objectif est d'obtenir une vision de l'entreprise auditée à la fois par rapport à un niveau jugé " correct ", et d'autre part par rapport aux entreprises ayant déjà répondu au même questionnaire.

[8] http://www.clusif.asso.fr

Le niveau de sécurité est évalué suivant 27 indicateurs répartis en 6 grands thèmes, chacun d'eux se voyant attribuer une note de 0 à 4, le niveau 3 étant le niveau à atteindre pour assurer une sécurité jugée correcte.

À l'issue de cette analyse, une analyse de risque plus détaillée est réalisée afin d'identifier les risques (menaces et vulnérabilités) qui pèsent sur l'entreprise.

Le fonctionnement de la méthode :

La méthode est basée sur des questionnaires portant sur des domaines précis. Les questionnaires doivent permettre d'évaluer les vulnérabilités propres à l'entreprise dans tous les domaines de la sécurité.

L'ensemble des indicateurs est évalué par le biais de plusieurs centaines de questions dont les réponses sont pondérées (ces pondérations évoluent suivant les mises à jour de la méthode).

Le déroulement de la méthode :

La méthode se déroule en 4 phases distinctes :

Phase 0 : Préparation

Durant cette phase, les objectifs de sécurité sont définis, ainsi que le champ d'action et le découpage fonctionnel permettant de mieux dérouler la méthode par la suite.

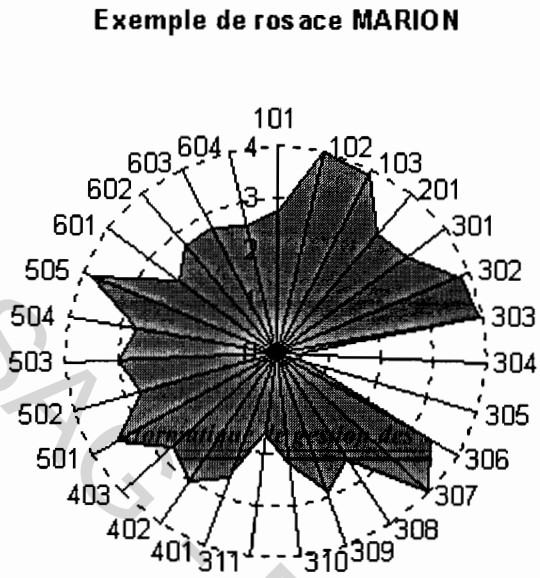
Phase 1 : Audit des vulnérabilités

Cette phase voit le déroulement des questionnaires ainsi que le recensement des contraintes propres à l'organisme.

Le résultat des questionnaires permet d'obtenir la " rosace " propre à l'entreprise.

Cette rosace, l'aspect le plus connu de la méthode, présente les 27 indicateurs sur un cercle, avec le niveau atteint. Cela permet de juger facilement et rapidement des domaines vulnérables de l'entreprise, la cohérence et l'homogénéité des niveaux de sécurité des différents indicateurs, et donc d'identifier également les points à améliorer.

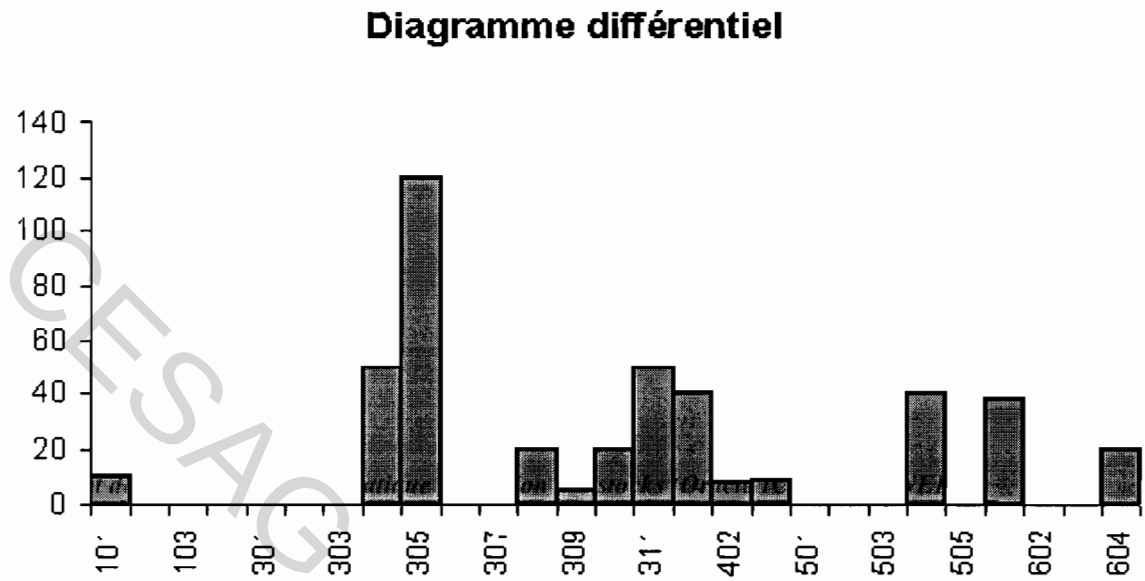
Figure N°1 : La rosace Marion



Source : Clusif (2003)

D'autres possibilités de diagrammes existent. Parmi lesquels le diagramme différentiel qui permet de mieux comprendre l'importance des différents facteurs (d'après la méthode) et donc également de mettre les vulnérabilités de l'entreprise en perspective. Dans ce diagramme, chaque barre est proportionnelle à la différence entre la cotation 3 et la cotation réelle de l'existant, multipliée par le poids du facteur (le différentiel est nul si le facteur est déjà supérieur à 3).

Figure N°2 : Le diagramme différentiel



Source : Clusif (2003)

Phase 2 : Analyse des risques

Cette phase voit l'exploitation des résultats précédents et permet d'effectuer une ségrégation des risques en Risques Majeurs (RM) et Risques Simples (RS).

Le Système d'Information est alors découpé en fonctions qui seront approfondies en groupes fonctionnels spécifiques, et hiérarchisés selon l'impact et la potentialité des risques les concernant.

Phase 3 : Plan d'action

Durant cette ultime phase de la méthode, une analyse des moyens à mettre en œuvre est réalisée afin d'atteindre la note " 3 ", objectif de sécurité de la méthode, suite aux questionnaires. Les tâches sont ordonnancées, on indique le degré d'amélioration à apporter et l'on effectue un chiffrage du coût de la mise en conformité[9].

[9] http://www.securite.teamlog.fr/publication/4/5/164/

2.4.2. La méthode MEHARI :

La Méthode Harmonisée d'Analyse de Risques (MEHARI) a été élaborée par la Commission Méthodes du CLUSIF (Club de la Sécurité des Systèmes d'Information Français).

Le but de la méthode MEHARI est de mettre à disposition des règles, modes de présentation et schémas de décision. L'objectif de la méthode est de proposer, au niveau d'une activité comme d'une entreprise, un plan de sécurité qui se traduit par un ensemble de sécurité répondant aux exigences des objectifs fixés.

Le modèle de risque MEHARI se base sur six facteurs de risque indépendants et six types de mesures de sécurité.

Les phases de MEHARI sont les suivantes :

- Phase 1 : établissement d'un plan stratégique de sécurité globale ;
- Phase 2 : établissement de plans opérationnels de sécurité réalisés par les différentes unités de l'entreprise ;
- Phase 3 : consolidation des plans opérationnels[10].

2.4.3. Le COBIT :

La nécessité d'avoir un cadre de référence en matière de sécurité et de contrôle des technologies de l'information a poussé l'ISACA (Information system Audit and Control Association) à créer la méthode COBIT en 1996.

Le COBIT[11] (Control Objectives for Information and related Technology – Objectifs de contrôle de l'Information et des Technologies Associées) est un outil fédérateur qui

[10] http://www.securite.teamlog.fr/publication/4/5/165/

permet d'instaurer un langage commun pour parler de la gouvernance des systèmes d'information tout en tentant d'intégrer d'autres référentiels tels que ISO 9 000, ITIL…

Cette méthode est diffusée en France par sa branche française, l'AFAI (Association Française de l'Audit et du Conseil Informatique). L'objectif était de faire le lien entre les risques métiers, les besoins de contrôle et les questions techniques, en se basant sur les meilleures pratiques en audit informatique et SI.

En fait, le COBIT est une approche orientée processus, qui regroupe en 4 domaines (planification, construction, exécution et métrologie, par analogie avec la roue de Deming) 34 processus distincts qui comprennent en tout 215 activités et un nombre plus important encore de "pratiques de contrôle".

Le cadre de référence se décline en check lists méthodiques couvrant quatre domaines, 34 objectifs de contrôle généraux (très synthétiques) et 302 objectifs de contrôle détaillés. Chacun de ces objectifs répond à 3 familles d'impératifs : économiques et fiduciaires, sécuritaire et qualité.

Les outils de la mise en œuvre contiennent une présentation de « success story » d'entreprises qui ont mis en place rapidement et avec succès la méthode COBIT. Cette partie intègre deux outils d'analyse de sensibilisation du management et de diagnostic de contrôle informatique.

Le COBIT est donc étroitement lié aux objectifs de l'entreprise tout en s'intéressant plus particulièrement à l'informatique. Il permet de rassurer le management, d'uniformiser les méthodes de travail et de garantir la sécurité et les contrôles de leurs services informatiques.

[11] http://fr.wikipedia.org/wiki/CobiT

CHAPITRE 3 : LA METHODOLOGIE DE L'ETUDE :

C'est l'approche utilisée pour conduire l'étude. Elle décrit les données à collecter, les outils de collecte.

3.1. Le modèle d'analyse :

Le modèle d'analyse s'appuie sur la description du modèle.

Concernant cette description du modèle, la démarche que nous avons retenue pour traiter notre sujet est la suivante :

- une phase de prise de connaissance générale de l'entreprise ;
- une phase d'appréciation du contrôle interne informatique et de la gestion des stocks (Oracle IC) c'est-à-dire le diagnostic ;
- une phase de recommandation.

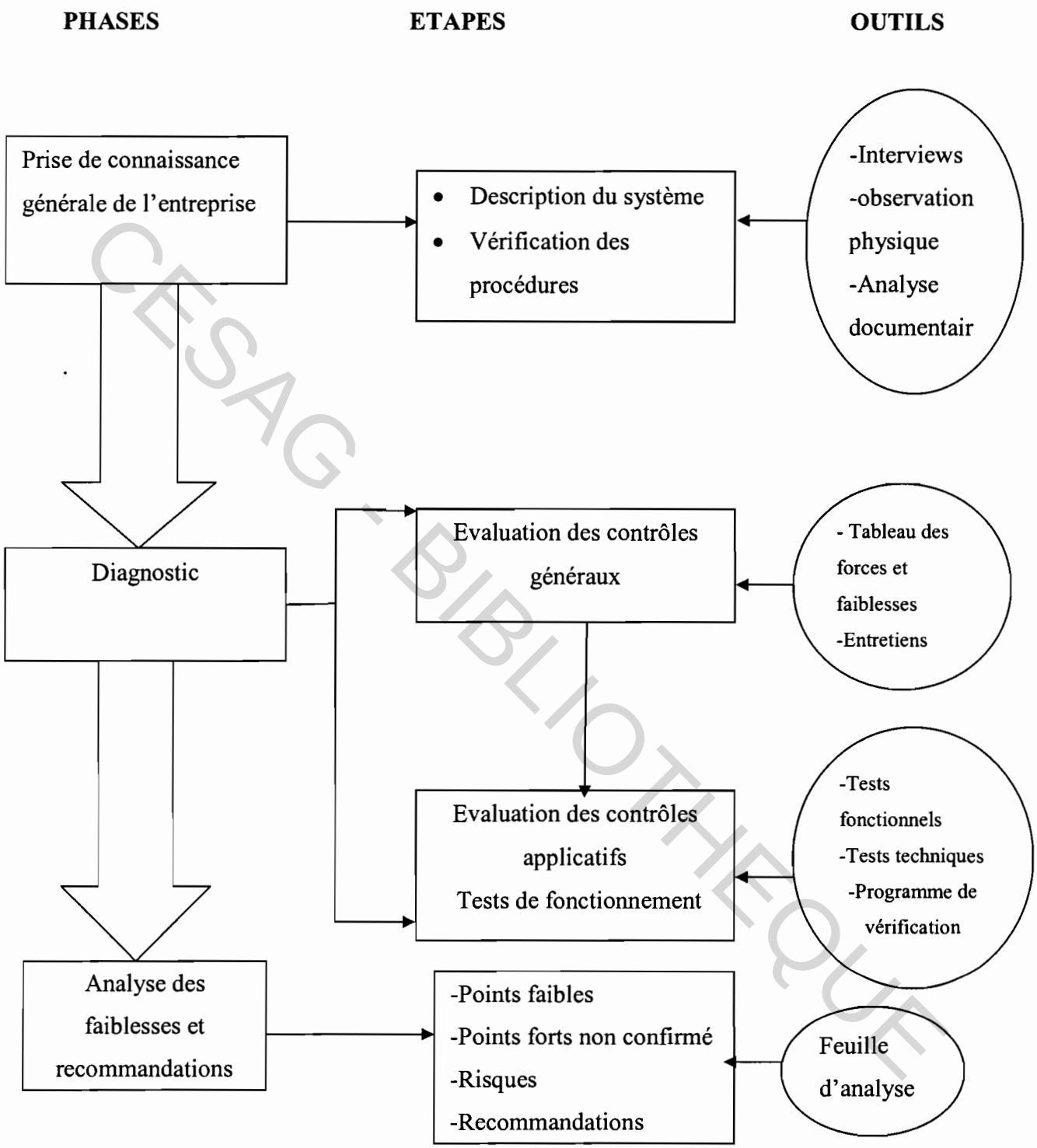
De façon schématique, ce modèle peut se présenter comme suit (voir Figure N°3):

a) La prise de connaissance générale de l'entreprise :

Cette phase nous a permis de comprendre le contexte général de l'entreprise, son organisation interne, sa structure et sa culture. Elle nous a également permis de nous imprégner des spécificités de la gestion des stocks de l'entreprise.

Ainsi les informations de la société, dont nous avons eu connaissance sont : l'historique, la forme, l'objet social, le capital, le chiffre d'affaire, la nature de l'activité, les lieux de production, la note de direction portant changement du nouveau organigramme de Mai 2009, l'état des stocks dans les différents magasins de Bel-Air et de Hann.

Figure N°3 : Modèle d'analyse



Source : Nous-même

b) L'appréciation du dispositif de contrôle interne informatique et de la gestion des stocks :

Cette phase nous a permis :

- d'appréhender l'environnement général de l'entreprise ;
- d'apprécier les procédures de traitement de la gestion des stocks ;
- d'apprécier le logiciel IC de gestion des stocks.

Cette phase a débouché sur l'identification des forces et faiblesses du système du module Oracle IC.

c) La phase des recommandations :

Elle nous a permis de faire des recommandations sur les faiblesses relevées. Pour les modalités d'application pratique, nous avons eu des entretiens avec les responsables de l' Audit Interne, de l'Informatique, de la Comptabilité des Stocks et de la Gestion des Stocks.

3.2. Méthode de collecte des données :

Différentes méthodes ont été utilisées pour la collecte des données.

A. Procédure d'échantillonnage :

Dans le cadre de notre étude, nous avons interviewé en plus du personnel du département informatique, les personnes pouvant être impliquées dans le processus de gestion des stocks et des inventaires de fin d'année :

- le chef du département comptable ;
- le directeur de l'unité Stock ;
- le chef du département de la Gestion des stocks ;
- le directeur du département audit interne ;
- l'agent chargé de la gérance des magasins de Bel-Air.

B. Les outils de collecte des informations :

Pour la collecte des informations, certains outils ont été utilisés parmi lesquels on peut citer le guide d'entretien, l'observation physique, l'analyse documentaire et le questionnaire de contrôle interne.

a) Le guide d'entretien :

Il a servi aux entretiens que nous avons eus avec le personnel et les responsables des différentes structures. Les interviews ont porté en général sur :

- la description des composantes du contrôle interne de la fonction informatique,
- les questions spécifiques aux contrôles de la gestion des stocks,
- les procédures d'inventaire des stocks de fin d'année et
- les sécurités mises en place.

Pour la réalisation des entretiens, nous avons séjourné au niveau des structures concernées ; notre séjour au niveau des unités « Comptabilité des Stocks » et « Gestion des Stocks » nous a permis de nous familiariser avec l'utilisation du logiciel Oracle IC.

b) L'observation physique :

Elle nous a permis de prendre connaissance avec les structures dédiées à l'utilisation de Oracle IC et à la gestion des Stocks :

- effectif,
- méthodes de travail,
- outils de travail,
- sécurité dans les traitements,
- systèmes de sauvegarde des données.

L'observation s'est faite en faisant l'inventaire physique des stocks au niveau des magasins de Hann et Bel-Air.

c) L'analyse documentaire :

Elle nous a permis de prendre connaissance :

- du manuel de procédures de gestion des Stocks,
- du manuel de procédures des acquisitions des biens et services,
- du guide d'application du logiciel Oracle IC,
- des rapports d'audit informatique, d'audit financier sur les stocks et des rapports sur l'inventaire physique des stocks,
- des rapports des Commissaires aux Comptes.

d) Le questionnaire de contrôle interne

Il a été utilisé afin d'approfondir les informations obtenues précédemment. Il a également permis d'évaluer le système de contrôle interne de la SENELEC. Pour cela nous avons recueilli les réponses des responsables des structures concernées par la gestion des STOCKS sous Oracle IC.

Il a été administré en des documents photocopiés du fichier sur le questionnaire d'évaluation du contrôle interne (voir annexe 1).

L'informatique est un domaine encore mal appréhendé en matière d'audit. Par ailleurs, l'informatisation fait courir de nouveaux risques à l'entreprise tout en améliorant son efficacité.

Toutes les parties impliquées dans la sécurité de l'information s'accordent pour reconnaître que les risques de délits informatiques sont aujourd'hui plus sérieux que jamais. Cette situation est due à la convergence d'un certain nombre de tendances. Et dans la mesure où celles-ci devraient se poursuivre dans un avenir prévisible, les entreprises s'en trouveront encore plus menacées.

De la réduction des vulnérabilités au management des risques, la sécurité des systèmes d'information a longtemps consisté à mettre en œuvre des solutions génériques sur des systèmes et des réseaux maîtrisés par l'entreprise.

DEUXIEME PARTIE : AUDIT DE L'APPLICATION INFORMATIQUE DE GESTION DES STOCKS (ORACLE IC) DE LA SENELEC

Les entreprises évoluent dans un environnement de plus en plus complexe et turbulent. Les décisions qui étaient par le passé plus ou moins faciles à prendre dans un environnement simple et stable, présentent actuellement plus de difficultés dans cet environnement risqué. Toute décision, quelle soit interne ou externe, nécessite la prise en compte des différentes facettes de cet environnement. L'information prend ainsi une importance accrue pour une bonne prise de décision. Mais la qualité de cette décision dépend de la qualité de l'information sur laquelle on se base pour la prendre.

Parmi ces informations nécessaires aux personnes externes à l'entreprise (investisseurs, organismes financiers, etc.), les informations comptables et financières occupent une place prépondérante. La garantie de la qualité de ces informations dépend de l'opinion d'un professionnel indépendant, notamment le commissaire aux comptes. Il constitue la meilleure indication du degré de confiance que l'on peut accorder à ces informations.

L'opinion de l'auditeur doit s'appuyer sur un examen très complet des documents financiers et des pièces justificatives correspondantes, et il a pour but d'indiquer si ces documents reflètent la situation financière réelle de l'entreprise.

L'auditeur doit donner aussi son opinion sur le système de contrôle interne de l'entreprise dans le souci d'apporter une aide au client et pour permettre une réduction de l'étendue des travaux traditionnels d'audit.

Ainsi nous étudierons la présentation d'ensemble de la SENELEC puis l'application informatique de gestion des stocks (Oracle IC) de la SENELEC. Cette étude est rendue possible grâce au stage de formation que nous avons eu au niveau de la SENELEC et plus spécifiquement au niveau de ses structures ci-dessous:

- Département Audit Interne et Organisation,
- Département Informatique,
- Unité Comptabilité Stocks et
- Unité Gestion des Stocks.

CHAPITRE 4 : PRESENTATION D'ENSEMBLE DE LA SENELEC :

La Société Nationale d'Electricité (SENELEC), située au 28, rue Vincens à Dakar, en tant qu'acteur principal dans la fourniture d'électricité au Sénégal, et suite à la nouvelle politique de l'État en matière énergétique, a connu une grande réforme en vue de faire face aux défis auxquels elle est confrontée notamment le changement du rôle de l'État et l'implication du privé dans la nouvelle politique énergétique.

Dans le cadre de cette réforme, la SENELEC s'est engagée dans une politique d'investissements et de renforcement de ses installations existantes. Cette redynamisation s'est traduite par une augmentation des stocks et l'amélioration de la qualité du service. Cela a conduit à l'acquisition d'énormes immobilisations lesquelles, si elles ne sont pas bien gérées, ne contribueront pas à l'atteinte des objectifs de la société. En effet, face à cette forte demande, la SENELEC a investie au cour de ces dernières années dans la construction de nouvelles centrales et de circuits de distribution. Ceci a entraîné une augmentation des achats, multipliant ainsi les risques liés à la gestion des stocks.

Avec un capital social de 125 676 650 000 F CFA, la SENELEC est l'une des grandes entreprises industrielles du Sénégal.

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

4.1. Organisation et Fonctionnement de la SENELEC :

La SENELEC est une société anonyme qui a une mission de service publique prioritaire : Fournir du courant électrique au maximum de foyers, d'artisans et d'entreprisses pour participer au développement économique du Sénégal.

L'Etat assure la régulation et le contrôle du secteur pour la recherche de l'efficacité du système économique eu égard à la position stratégique de l'industrie électrique dans l'économie nationale. L'Etat assure ces fonctions à travers le Ministère de l'Energie et des Mines qui assure la tutelle administrative et technique du secteur de l'énergie par

l'intermédiaire de la Direction de l'Energie et de la Commission de Régulation du Secteur de l'Energie.

Depuis sa création en 1984, Senelec a été l'un des moteurs les plus dynamiques du développement économique et social du Sénégal. De 604 GWh en 1983, ses ventes sont passées à 1540 GWh en 2005. Dans le même temps, sa pointe de 99 MW à 343 MW et sa puissance installée de 184 MW à 582,60 MW dont 150 MW de production privée.

Aujourd'hui, le principal défi que la société doit relever est celui du financement de son développement dans un contexte caractérisé par la globalisation de l'économie mondiale. Pour garantir le succès de cette entreprise, le Gouvernement du Sénégal a adopté un certain nombre de textes qui prévoit la libéralisation du secteur autour des axes suivants :

- Ouverture du segment de la production au secteur privé pour la réalisation et la gestion de centrales électriques
- Maintien à Senelec, du monopole du transport de l'électricité sur l'ensemble du territoire ainsi que de l'exclusivité de la distribution sur son périmètre.

La mise en place d'une nouvelle organisation à la SENELEC s'avère nécessaire afin de corriger les dysfonctionnements présentement constatés et augmenter l'efficacité de la gestion par une meilleure coordination des unités, un fonctionnement harmonieux des unités opérationnelles et fonctionnelles, une délégation de pouvoir appropriée pour raccourcir les étapes de décisions.

La note de direction n° 013/2009 réglemente l'organigramme général et le fonctionnement de la SENELEC (voir Annexe N°2). Cette présente note de Direction n° 013/09 du 25 Mai 2009 publie les structures des différents Directions en s'appuyant sur les nouveaux principes de gestion dont les plus importants sont :

- ✓ La réduction des centres de décision,
- ✓ La limitation des niveaux hiérarchiques de management, à trois :
  - o Directeur,
  - o Chef de département,
  - o Chef de service.

En application des principes de gestion, la nouvelle organisation de la SENELEC se présente comme suit :

- La Direction Générale (DG) qui coordonne les activités de la SENELEC,

- La Direction Générale Adjoint (DGA) et les directions qui lui sont rattachées par la délégation du Directeur Général :

Dépendant directement du Directeur Général (DG), il supervise les structures de support :

- ✓ La Direction du Contrôle Général ;
- ✓ La Direction de l'Administration, du Patrimoine et des Approvisionnements ;
- ✓ La Direction des Affaires Juridiques ;
- ✓ La Direction des Systèmes d'information ;
- ✓ La Direction de la Qualité, de la Sécurité et de l'Environnement ;
- ✓ Le Projet de Gestion du Rendement Global ;
- ✓ Le Projet de Maîtrise de la Demande et Economies d'Energie ;
- ✓ Le Projet Courant Porteur Ligne et Innovation Technologique.

Il supervise la rédaction des rapports aux organes délibérants, veille à l'application stricte des procédures et règles de la société et assiste le Directeur Général dans l'exercice de ses fonctions.

Il est chargé de suivre et d'évaluer la réalisation des objectifs assignés aux cellules de projets énumérées, ci-dessus. Il assure l'intérim du Directeur Général en cas d'absence de celui-ci.

- La Direction de l'Audit Interne et du Contrôle de Gestion (DAICG) :

Elle conçoit les procédures pour assurer la transparence des opérations et l'exactitude des transactions. Elle est chargée de l'audit technique, financier, comptable et social des procédés et règles de gestion des unités.

Elle est chargée de contrôler, mesurer et analyser l'activité de l'entreprise. Elle apporte au Directeur Général, à travers un système d'information fiable, les éléments essentiels pour

le management de l'entreprise. Elle fait un contrôle de vérification mais surtout de pilotage, détermine des indicateurs de gestion technique, commerciale, comptable et financière pertinents, les suit, les mesure, en relève les écarts de réalisation par rapport aux objectifs fixés pour informer et conseiller les directions opérationnelles et alerter le Directeur Général à travers un tableau de bord. Elle est chargée du reporting, de l'analyse des résultats de l'entreprise pour le Directeur Général, de l'élaboration du budget général de l'entreprise et du suivi de son exécution.

Elle suit les tendances et l'évolution des résultats par rapport aux prévisions du Modèle Financier de SENELEC. Elle est chargée de la transmission à temps et dans les formes convenues des informations aux Comités d'Investissement et Financier créés au sein du Conseil d'Administration.

- La Direction du Contrôle Général (DCOG) :

Elle a pour mission la protection des biens de l'entreprise en exerçant un contrôle ciblé sur le respect des procédures administratives, comptables, financières, commerciales, d'achat et de gestion de stocks. Elle contrôle le respect des normes techniques de réalisation des ouvrages d'exploitation et de maintenance.

- La Direction des Ressources Humaines (DRH) :

Elle est chargée de la gestion prévisionnelle et de la gestion administrative centralisée des ressources humaines. Elle est responsable de l'élaboration de la stratégie de formation, élabore puis exécute les plans de formation.

- La Direction de la Production (DP) :

Elle assure la maintenance et l'exploitation des installations de production de la société et le suivi des contrats O&M (Operations & Maintenance). Elle gère les stocks de combustibles et lubrifiants mis à sa disposition.

- La Direction du Transport (DT) :

Elle assure la maintenance et l'exploitation des réseaux de transport et de télécommunications. Elle est également responsable du placement optimal des moyens de production du Réseau Interconnecté, des achats, exportations et importations d'énergie.

- La Direction de la Distribution (DD) :

Elle a pour mission l'élaboration des politiques et la fixation des objectifs globaux dans le domaine de la distribution ; elle assure la maintenance et l'exploitation du réseau Moyenne Tension et Basse Tension de Dakar et banlieue, y compris le dépannage.

- La Direction Commerciale et de la clientèle (DCC) :

Elle a pour mission l'élaboration des politiques et la fixation des objectifs globaux dans le domaine de la gestion commerciale et du processus clientèle qu'elle gère au mieux des intérêts de l'entreprise et pour la satisfaction du client.

- La Direction des Etudes Générales (DEG) :

Elle est chargée des études économiques générales, de la tarification, des études tarifaires, de la planification stratégique, des études de planification technique, économique et financière.

- La Direction de l'Equipement (DEQ) :

Elle assure le processus de réalisation des projets d'investissement retenus, est responsable de l'ingénierie et des travaux de tous les projets de renforcement et d'extension des installations de production et des réseaux de transport et de distribution, y compris les projets de génie civil et des réseaux de télécommunications.

Elle peut en accord avec les exploitations déléguer la réalisation de certains projets, notamment dans le cadre du renforcement des installations.

- La Direction des Finances et de la Comptabilité (DFC) :

Elle est responsable de l'enregistrement exact, exhaustif et traçable de toutes les transactions comptables et financières de Senelec, de l'établissement et de la présentation à bonne date et selon les règles de l'art des états financiers de synthèse approuvés par les auditeurs externes.

- La Direction de la Communication (DCOM) :

Elle élabore la stratégie de communication et doit utiliser des outils efficaces pour donner une perception positive de l'image de l'entreprise. Elle est responsable de la communication externe et interne de l'entreprise, et gère les relations publiques.

- La Direction des Systèmes d'Information (DSI) :

Elle élabore le plan directeur informatique optimal, est responsable de la sécurité informatique et assure la gestion du parc de matériel informatique, la maintenance et l'exploitation du matériel et des logiciels de gestion.

Elle assiste les directions techniques dans la mise en place d'applications et d'outils spécialisés. Elle assure l'implantation de nouveaux progiciels et la formation des utilisateurs.

- La Direction de l'Administration, du Patrimoine et des Approvisionnements (DAPA) :

Elle gère les services administratifs et généraux ainsi que les baux immobiliers ; elle est responsable de la gestion du patrimoine, de l'élaboration, de la mise à jour et de la mise en place des procédures administratives et des notes d'organisation.

- La Direction des Affaires Juridiques (DAJ) :

Elle gère les assurances. Elle est responsable du traitement des dossiers contentieux entre Senelec et ses clients et entre Senelec et les tiers avec l'appui des conseils. Elle joue le rôle de risk manager de l'entreprise.

Il faut noter que le sous secteur de l'électricité du Sénégal est confronté à des problèmes liés à l'obsolescence des installations électriques, à un manque de financement, à une demande en électricité en constante progression et supérieure à la production entre autres.

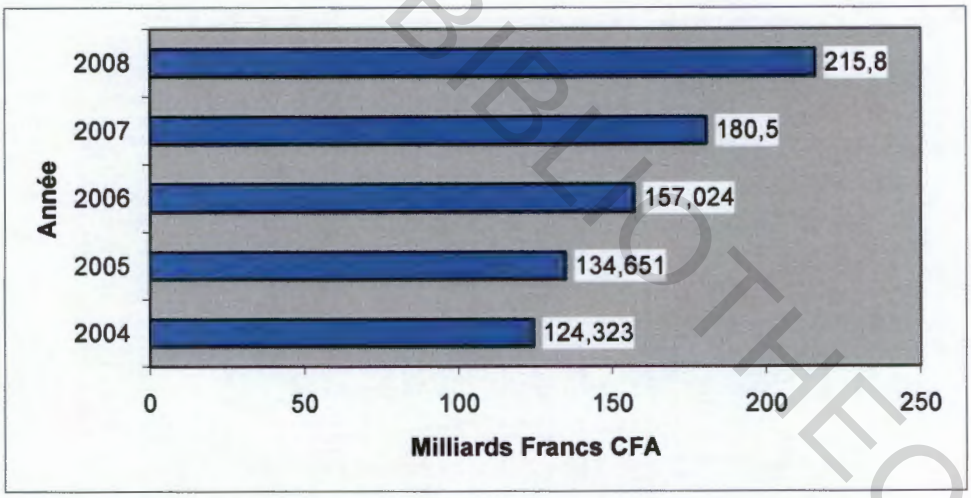
Le chiffre d'affaire de la Senelec en 2008 s'élève à 215.800.000.000 Francs CFA. (Voir Tableau N°1).

Tableau N°1 : Chiffres d'Affaires

Année	CA Milliards
2004	124,323
2005	134,651
2006	157,024
2007	180,5
2008	215,8

Source : MBAYE (2008)

Figure N°4 : Accroissement du chiffre d'affaires



Source : MBAYE (2008)

4.2. 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.

a) 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 centrales 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.

b) 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 30 kV. Les principales lignes sont :

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

c) 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.

4.3. Le Statut Juridique et Fiscal :

Pour trouver un moyen légal de contourner les points faibles de la législation, la SENELEC doit :

- ✓ Conduire les démarches idoines auprès de l'Etat pour faire de ses agents assermentés des auxiliaires de justice dont les procès verbaux font foi jusqu'à preuve du contraire.

- ✓ Mener les démarches auprès des Autorités pour que la fraude d'électricité soit expressément définie et pénalisée par la législation Sénégalaise comme cela se fait en France.

- ✓ Mettre à la disposition des avocats une expertise à même de leur faciliter la compréhension de certaines questions techniques.

- ✓ Apporter une assistance opérationnelle aux agents intervenants dans la lutte contre la fraude sur le système de montage et la démarche à tenir en cas de refus de transaction de client.

- ✓ Informer l'ensemble du personnel sur l'importance et les conséquences de la fraude.

- ✓ Sensibiliser l'Etat sur l'impact négatif de la fraude sur l'économie nationale, ses conséquences sur le prix de l'électricité et sur la trésorerie de l'entreprise.

- ✓ Informer la clientèle sur les méfaits de la fraude, ses effets sur la qualité du Service et le prix de l'électricité ainsi que les risques encourus par les fraudeurs.

- ✓ Sensibiliser le pouvoir judiciaire sur les effets et les conséquences de la fraude.

En définitive, nous considérons que l'aspect le plus important de ce programme de lutte contre la fraude d'électricité, demeure la **sensibilisation** et la **conscientisation** du personnel de l'entreprise sur le danger que représente ce phénomène quant à la sauvegarde de l'outil de travail.

Le dur contexte dans lequel évolue SENELEC, doit amener toutes les composantes de l'entreprise à réfléchir sur les moyens de relever le niveau de rendement, mais également à se mobiliser pour faire face à tout ce qui entrave son développement, surtout quant cela provient de l'extérieur.

Ainsi, un appel est lancé à tout le personnel de l'entreprise, pour une mobilisation, une vigilance et une fermeté, en particulier les intervenants de la chaîne commerciale pour parvenir à l'éradication en urgence de ce fléau …

4.4. Le contexte des travaux :

L'audit d'une application est intervenu 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 système d'information robuste, fiable et conviviale. Ainsi la mission a été organisée autour des objectifs spécifiques suivants :

- ✓ évaluation de la fonction informatique,
- ✓ étude de l'application informatique Oracle IC.

CHAPITRE 5 : LA DESCRIPTION DE L'EXISTANT INFORMATIQUE :

La présentation de cette fonction essentielle qu'est l'existant informatique de la SENELEC se fera à travers les éléments suivants :

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

5.1. Organisation et gestion de la DSI :

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

5.1.1. Présentation de la DSI :

La fonction informatique de la SENELEC est désignée par Direction des 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.

a) Missions :

La DSI 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.

b) 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.

c) 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, dés la phase de conception des produits.

d) 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.

5.1.2. 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.

a) 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.

b) Synoptique général du réseau privé IP :

La SENELEC a opté pour la solution SENTRANET VPN Haute Disponibilité. Le SENTRANET est le réseau de transport sécurisé de la SONATEL, pour les accès permanents utilisant le protocole TCP/IP à très haut débit.

La SENELEC dispose de deux types de liaisons :

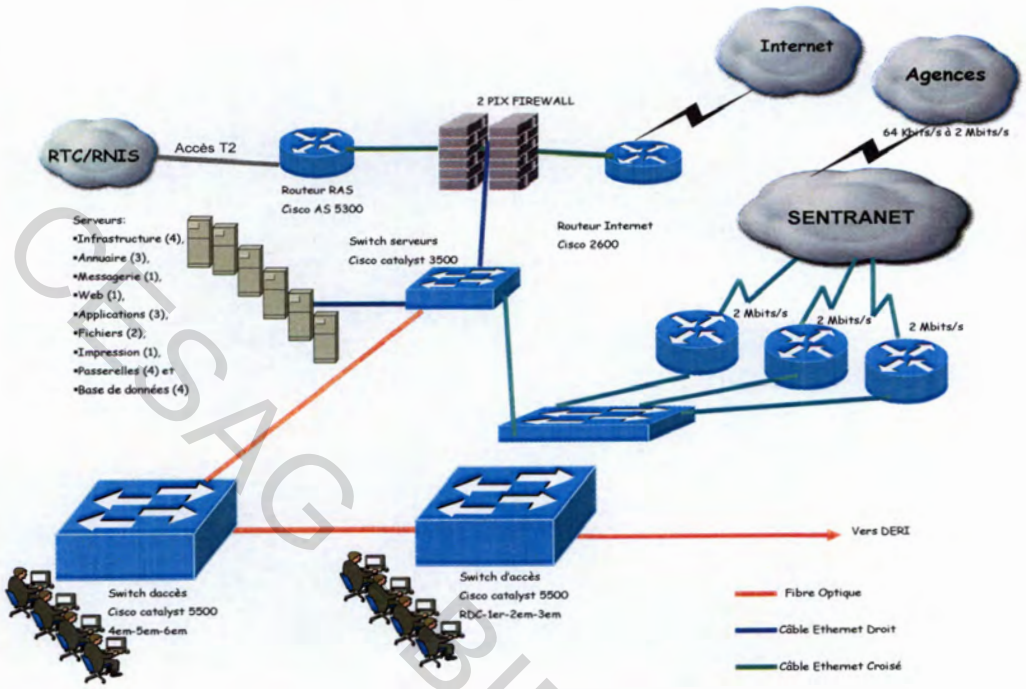
- Liaisons SENTRANET pouvant aller de 64Kbit/s à 2 Mbit/s au niveau des agences et complexes industriels et de 6 Mbits/s au niveau du siège
- D'un réseau FH (Faisceau Hertzien) avec des liens allant de 8Mbits an niveau des agences de Dakar à 155Mbits au niveau de Hann, Cap des biches et Vincens

Une ligne de secours est assurée par RNIS pour l'ensemble des sites (SENTRANET ET FH).

La SENELEC dispose en plus d'une liaison Internet de 4MB/s.

Le réseau de la SENELEC est ouvert au monde extérieur grâce au réseau IP. Pour empêcher les intrusions pirates, la SENELEC a installé le système de protection réseau PIX Firewall Cisco (Voir Figure N°5).

Figure N°5 : Réseau PIX Firewall Cisco.



Source : NTAP & KANDE (2008 : 20)

Le VPN de la SENELEC s'adosse ainsi 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.

5.2. Le système informatique de la SENELEC :

C'est un système dense et varié.

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.

5.2.1. Description du patrimoine informatique :

Le patrimoine informatique de la SENELEC est bien fourni et, est composé de matériel et de logiciels.

Pour le matériel, le parc informatique de la société comprend :

- 100 serveurs (BDD, infrastructures, applications, messagerie, Web, impression, etc.) ;
- 96 routeurs ;
- 380 switch ;
- 52 imprimantes réseau ;
- 920 postes de travail ;
- 600 imprimantes individuelles ;
- 01 Mainframe Bull DIANE ;
- 60 onduleurs ;
- 02 ASA Firewall (pare-feu) ;
- 01 serveur ISA ;
- 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 ;
- liaisons FH entre les sites Vincens, Hann, Mbao et Cap des biches.

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

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 ;
- ORACLE 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.

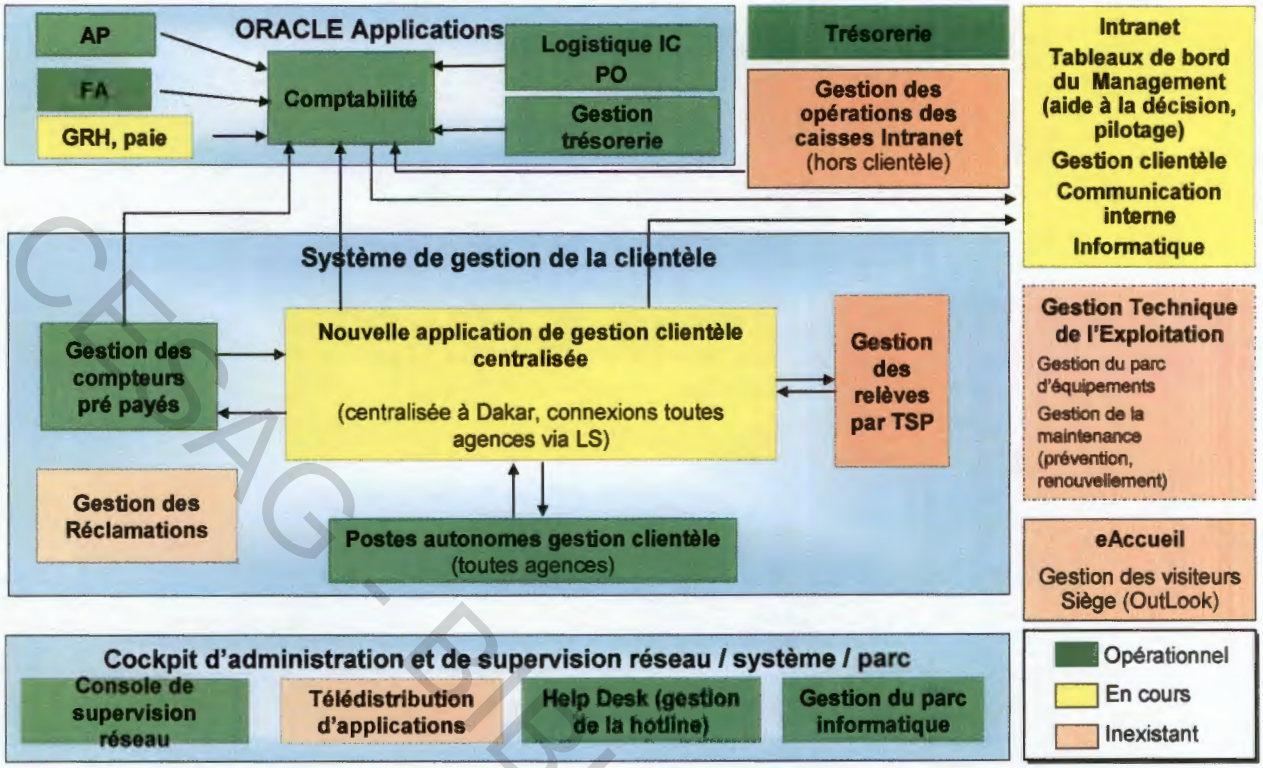
L'entreprise a développé un seul logiciel spécifique appelé « logiciels maison ». C'est l'application SIC permettant de suivre les revenus clients à partir de différents modules.

En effet, le Système d'Information applicatif tourne autour des principales applications suivantes :

- L'ERP ORACLE : l'outil comprend les modules de Gestion des Stocks (IC), de Gestion des achats (PO), de Gestion des Immobilisations (FA), de Gestion des Fournisseurs (AP), de Gestion de la Paie (Payroll), de Gestion des Ressources Humaines (RH) et de Gestion de la Comptabilité (GL).
- Le Système d'Information Clientèle (SIC).

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

Figure N°6 : Cartographie Applicative du Système d'Information de la SENELEC



Source : KANDE (2008 : 13)

5.2.2. Description de l'application Oracle :

C'est un progiciel applicatif de gestion, composé de plusieurs modules intégrés pour la gestion des données comptables et budgétaires.

Il regroupe un ensemble de modules périphériques, qui déversent d'une manière automatique ou par interface leurs données vers un module principal « oracle G L » qui constitue le référentiel central des informations comptables.

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 Figure N°7).

- ***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.

- ***Oracle AP (Account Payables) : 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.

- ***Oracle PO (Purchasing Order) : 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.

- ***Oracle FA (Fixed Assets) : Gestion des immobilisations***

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

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

Cette application a deux 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.

- ***Oracle IC (Inventory control) : 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.

Le logiciel **ORACLE IC** est dédié à la gestion des stocks et alimenté par :

- ✓ Des opérations provenant du module Oracle P.O « gestion des achats ».
- ✓ Des opérations manuelles saisies par les magasiniers.

Les écritures correspondantes se déversent dans le module Oracle G L « Comptabilité Générale ».

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.

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.

❖ ***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, des insertions et mises à jour. Les règles de sécurité sont les suivantes :

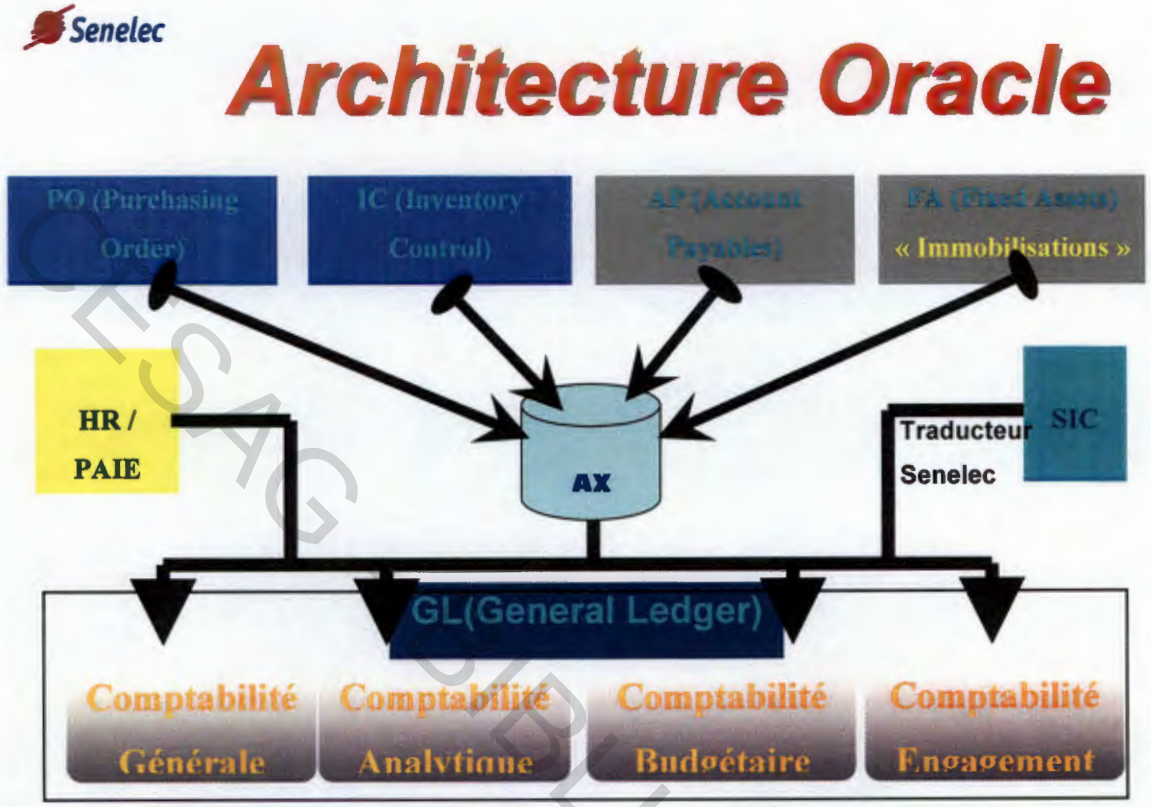
- o limitation à certaines responsabilités ;
- o l'accès à une société : accès exclusif à FOPES, accès limité à SENELEC.

❖ ***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.

Figure N°7 : Différents modules de l'application Oracle



Source : MBAYE (2009)

Ainsi donc nous avons fait une présentation exhaustive de la SENELEC et de sa fonction informatique. En effet, cette dernière est de taille moyenne. Elle est subdivisée en services importants que sont les services « Infrastructures et Réseaux », « Etudes et Applications » et « Exploitation ». La direction des systèmes d'information est composée de personnel qualifié et le patrimoine informatique est important et varié.

CHAPITRE 6 : AUDIT DE L'APPLICATION ORACLE IC :

Les stocks de la SENELEC sont placés sous la responsabilité de:

- l'Unité Stock du service Comptabilité « Fournisseurs et Stocks » de la Direction des Finances et de la Comptabilité (DFC),
- l'Unité Gestion des Stocks du Service Achats de la Direction de l'Administration, du Patrimoine et des Approvisionnements,
- les services « Infrastructures et Réseaux », « Etudes et Applications « Exploitation » de la Direction des Systèmes d'Information,
- l'Audit interne (suivi inventaire).

La Senelec, pour la gestion de ses Stocks dispose de 70 magasins éparpillés à travers le territoire national.

Les principaux types de Stocks sont :

- Carburant
- Imprimés et Fournitures de Bureau
- Lubrifiants
- Matières Premières
- Matériel Réseau Distribution
- Matériel Réseau Transport
- Pièces Centrales
- Pièces Services Généraux

Le nombre des articles de stocks avoisine 36 000 unités.

6.1. Description de l'interface de la gestion des stocks :

- **Produits pétroliers :**

Le chef de l'exploitation ou le chef contrôle essai appelle le pétrolier retenu et lui demande de livrer la quantité sur le bon de commande indiqué par l'agent technique chargé de suivre le combustible.

L'agent de garde enregistre le camion à l'entrée, le conduit à l'aire de stationnement et informe les agents de car de l'arrivée du camion.

L'agent statistique jauge chaque année à 8 heures les bacs pour avoir la hauteur des bacs. Le chef de la division contrôle et essai vérifie les données consignées dans la fiche (nouveau stock des bacs) et établit une lettre de demande d'ouverture des vannes qu'il signe et faxe à la société gestionnaire du réseau PIPE LINE pour leur demander d'ouvrir les vannes. La société gestionnaire du réseau PIPE LINE envoie un de ces agents à la centrale qui a formulé la demande.

L'agent de car, en présence de l'envoyé de la société gestionnaire du réseau PIPE LINE, jauge les bacs devant recevoir le fuel pour avoir la hauteur avant dépotage en prenant la température et il consigne les données relevées dans une fiche de relevé.

L'envoyé de la société gestionnaire du réseau PIPE LINE demande à sa société d'ouvrir les vannes pour le remplissage.

A partir de là, la procédure est similaire à celle relative à la réception par camion à l'exception de l'intervention du chimiste qui détermine la densité du produit.

- **Articles de stocks :**

A chaque fois que le stock d'un article du magasin atteint un minima, le responsable du magasin général demande au fichiste d'établir une demande de réapprovisionnement de stock (DRS).

Les minima des articles de stock sont appréciés en rapport avec l'expérience acquise par le responsable du magasin général des niveaux de consommation.

La DRS est transmise au contrôleur de stock puis au chef d'unité pour la vérification de conformité des libellés des articles et du respect de leurs nomenclatures.

Lorsque la DRS est acceptée par la Direction Générale, le service Achats établit un bon de commande (BC) ou lettre de commande (LC).

Au moment de la livraison des articles commandés, le responsable du magasin général et un contrôleur des stocks procèdent aux vérifications d'usage : conformité des éléments entre le bon de commande et le bordereau de livraison.

Pour le matériel technique, il est fait appel aux exploitants pour des suppléments d'information, notamment la correspondance des caractéristiques technique de l'article livré avec celui qui a été commandé.

S'il y a une conformité de l'article reçu avec celui qui a été commandé, l'adjoint du magasinier général établit un bon d'entrée réelle en deux volets, 1 blanc et 1 vert sur la base du bon de commande.

Le bon de commande est conservé dans le chrono des bons de commande.
Le volet vert du bon d'entrée est transmis à la comptabilité fournisseur avec décharge.
L'un des magasiniers renseigne la fiche casier sur la base du bon d'entrée réelle.
Le fichiste remplit la fiche kardex sur la base du bon d'entrée réelle et du DRS.
Les fiches casier et les fiches kardex sont ensuite rangées dans des bacs.
Les articles reçus sont rangés dans des casiers.
Sur chaque casier figure une étiquette qui comporte :

- l'emplacement A, B, …
- l'étalage A1, A2, ….

Le rangement n'obéit pas à des critères relatifs aux nomenclatures ou à la famille des articles : les articles les plus sensibles au vol sont placés au dessus de l'étalage.

Sur la base de la fiche kardex, le fichiste procède à la saisie au micro des entrées dans le système Oracle IC (gestion de stocks) en quantité.

La saisie des éléments de stock n'est pas effectuée de manière automatique au niveau du magasin général.

La comptabilité matière donne l'ordre au magasin du démarrage de la saisie.

Cet état de fait est lié au système de traitement qui autorise la saisie pour des périodes de 1 mois. Après chaque période de saisie, l'Informatique procède au traitement des éléments saisis en arrêtant l'utilisation de Oracle IC par les opérateurs.

Les consommations de fuel sont déterminées journalièrement de la manière suivante : (Volume à J – Volume à J-1) * densité corrigée.

Ces consommations ne font pas l'objet d'une demande formulée par une unité de la centrale mais dépendent du fonctionnement des groupes.

Elles sont répertoriées mensuellement dans la structure des combustibles et lubrifiants qui est envoyée à la comptabilité matière pour la saisie.

Pour les sorties d'articles du magasin général :

- les services demandeurs établissent des bons de sortie visés par les supérieurs hiérarchiques et soumis aux magasiniers ;
- le magasinier vérifie la correspondance des signatures et des nomenclatures.

Le magasinier gère le stock suivant leur niveau et les possibilités offertes à chaque service.

En général, tout ce qui est demandé par les services n'est pas servi par le magasinier. Toutefois le suivi du niveau des stocks n'est pas formalisé et le système Oracle ne permet pas d'obtenir les seuils de commande (stock mini).

- **Procédures d'inventaire des stocks :**

Les étapes de la procédure sont les suivantes :

➢ **Arrêter les fiches Kardex** en déterminant la quantité inventoriée et la date de l'inventaire

➢ **Procéder au rapprochement inventaire physique / fiche Kardex**

Ce rapprochement n'est effectué que pour déceler les anomalies des fiches Kardex. Ce sont les quantités déterminées à l'issue des comptages physiques qui doivent être retenues.

- **Déterminer les écarts physique / Kardex** qui, sauf erreur ou omission, devraient correspondre aux écarts physique / comptable ; leur analyse en amont permettant d'identifier les anomalies susceptibles de générer des écarts physique / comptable.

Les quantités physiques déterminées étant rapprochées aux quantités indiquées sur les fiches Kardex, les écarts relevés sont soumis au magasinier et, au besoin, à ses supérieurs suivant l'importance de l'écart. A charge pour eux de le justifier et de corriger l'écart. Au cas contraire, un écart non justifié et non corrigé est entériné et renseigné dans la colonne « écart physique / Kardex » de l'état d'inventaire.

- **Saisir les quantités inventoriées et les dates d'inventaire** ; ces saisies se feront sur Excel. Les états fournis par l'Informatique, devront servir de support pour la réalisation des saisies ; ils ne doivent présenter aucune rature ou surcharge.
  Il faudra veiller à insérer les nouveaux articles non pris en compte sur les états.

- **Validation et contrôle des inventaires** par le Département Audit Interne et organisation.
  Un planning est élaboré par l'Audit et l'Unité Matières dans la période comprise entre le vendredi 2 janvier 2009 et le mercredi 14 janvier 2009 pour la validation des inventaires.

  Le contrôle est effectué systématiquement après saisie des états d'inventaire du lundi 5 au lundi 19 janvier 2009.

- **Analyse de la précision de l'inventaire** par l'identification des anomalies à l'origine des différences d'inventaire par l'Audit Interne en collaboration avec l'Unité Matières, la Gestion des Stocks et les magasins concernés.

L'Audit procède à l'analyse et au traitement des documents à l'aide de ORACLE.

- **Correction des anomalies** constatées par l'Unité Matières ou le Service Gestion des Stocks ou l'unité concernée.

- **Approbation** des saisies d'inventaire par la hiérarchie (un responsable de l'Audit n'ayant pas participé à l'inventaire).

- **Ajustement** des inventaires par la Comptabilité Matières ; ce qui permet d'avoir, par magasin, organisation, article, etc., la situation des écarts d'inventaire.

- Publication des **résultats** des inventaires par le Département de l'Audit Interne et organisation.

- L'Audit chargé de faire demande de **Justification** des écarts d'inventaire pour chaque magasin concerné.

- Rédaction du **rapport** annuel sur les stocks par l'Audit Interne.

6.2. Présentation de Oracle IC :

Une responsabilité autorise les droits d'accès à un module, à des fonctionnalités et groupe d'états.

Pour chaque utilisateur, l'application n'affiche que les responsabilités auxquelles il est rattaché.

Les responsabilités retenues pour le module IC sont :

- **SN – Opérateur Stock**
- **SN – Auditeur Stock**
- **SN – Auditeur Comptable Stock**

Les modules sont :

a) Réceptions
b) Retours au fournisseur
c) Mouvements de réception.
d) Transfert entre organisations.

e) Transfert entre magasins.
f) Mouvements divers.
g) Mouvements matières.
h) Recherche de quantités en stock
i) Recherche de quantités en multi organisations
j) Recherche d'article de l'organisation
k) Processus d'inventaire de Stock Sur Oracle IC

1. Réceptions :

Responsabilités : ***SN - Opérateur Stocks***

Mouvements ➔ Réception ➔ Réceptions

- Choisir l'organisation de réception de la commande ou du transfert.

Cette organisation correspond à l'organisation de livraison spécifiée dans la commande ou dans le transfert inter organisation.

- Validation du choix
- Recherche de la commande à réceptionner suivant un certain nombre de critères :
  - ✓ Type d'Origine,
  - ✓ Commande,
  - ✓ Numéro d'expédition, etc.
- Saisie du numéro de la commande dans le champ « Commande », ou saisie du numéro d'expédition dans le champ « Livraison » :
  - o Si c'est une première réception sur la commande alors Cliquer sur « nouvelle réception ».
  - o Si c'est une n-iéme réception sur la commande (n varie entre 2 et 99) alors Clic « ajouter à la réception ».
- Fermeture de la fenêtre en cours.

- Affichage de la commande recherchée en ramenant les lignes avec leur quantité à réceptionner.

2. Retours au fournisseur :

Responsabilités : ***SN - Opérateur Stocks***

Mouvements ➔ Réception ➔ Réceptions

- Choix de l'organisation de réception de la commande qui est l'organisation de livraison spécifiée dans la commande.
- Validation du choix.
- recherche la commande réceptionnée à retourner suivant un certain nombre de critères :
  - ✓ Type d'Origine : Fournisseur
  - ✓ Commande : choisir la commande réceptionnée à retourner
  - ✓ Réception : choisir le numéro de la réception à retourner
- Affichage du champ « Quantité Parent » qui correspond à la quantité déjà réceptionnée :
  - ✓ cliquer sur le champ « Quantité »
  - ✓ Saisir la quantité à retourner
  - ✓ Puis cocher la case
  - ✓ Cliquer sur le champ « Retourner à » pour l'article au fournisseur ou à réceptionner
- Fermeture de la fenêtre.

3. Mouvements de réception :

Responsabilités : ***SN - Opérateur Stocks***

Mouvements → Réception → Mouvements de réception

- Choix de l'organisation de réception de la commande qui correspond à l'organisation de livraison spécifiée dans la commande.
- validation du choix.
- Recherche de la commande à réceptionner suivant un certain nombre de critères :
  - ✓ Type d'Origine,
  - ✓ Commande,
  - ✓ Fournisseur, etc.
- Saisie du numéro de la commande dans le champ « Commande »,
- Saisie des quantités à réceptionner et clic sur la case à crochet.
- Sauvegarde en cliquant sur l'icône de la barre d'outils.
- Fermeture de la fenêtre.

4. Transfert entre organisations :

Responsabilités : ***SN - Opérateur Stocks***

Mouvements → Transfert entre organisations

- Choix de l'organisation d'expédition.
- Validation du choix.
- Saisie de la date du mouvement (la date du jour s'affiche par défaut).
- Choix de l'organisation de destination dans la liste de valeur du champ « Vers l'organisation ».

- Affichage automatiquement « **Transfert inter organisation** ».
- Saisie du numéro de la Demande d'Approvisionnement (facultatif) dans le champ « Origine ».
- Saisie du numéro du bordereau d'expédition dans le champ « Numéro ».
- Saisie de la date de réception prévue.
- Clic sur le bouton « **Lignes du mouvement** »
- Saisie des informations obligatoires suivantes :
  - ✓ le code article dans le champ « Article »,
  - ✓ le code du magasin d'origine dans le champ « Magasin »,
  - ✓ le code du magasin destinataire dans le champ « Vers le magasin »,
  - ✓ la quantité du mouvement dans le champ « Quantité ».
- Sélection motif du mouvement dans la liste de valeur du champ « Motif ».
- Le champ « Référence » est facultatif.
- Saisie à la suite, si le bordereau d'expédition présente plusieurs lignes.
- Clic sur la croix pour fermer la fenêtre en cours

5. Transfert entre magasins

Responsabilités : ***SN - Opérateur Stocks***

Mouvements → Transfert entre magasins

- Choix de l'organisation concernée.
- Validation du choix.
- Saisie de la date du mouvement (la date du jour s'affiche par défaut).
- Clic dans la liste de valeur « Type », affiche automatiquement « **Transfert entre Magasins** ».

- Saisie du numéro du Bordereau d'Expédition dans le champ « Origine ».
- Clic sur le bouton « **Lignes du mouvement** ».
- Saisie des informations obligatoires suivantes :
  - ✓ le code article dans le champ « Article »,
  - ✓ le code du magasin d'origine dans le champ « Magasin »,
  - ✓ le code du magasin destinataire dans le champ « Vers le magasin »,
  - ✓ la quantité du mouvement dans le champ « Quantité ».
- Sélection du motif du mouvement dans la liste de valeur du champ « Motif ».
- Saisir le numéro de la Demande d'Approvisionnement dans le champ « Référence ».
- Si le bordereau d'expédition présente plusieurs lignes, les saisir à la suite.
- Ensuite cliquer sur la croix pour fermer la fenêtre en cours.

6. Mouvements divers : SN - Opérateur Stocks

Responsabilités : ***SN - Opérateur Stocks***
Mouvements → Mouvements divers

- Choix de l'organisation concernée.
- Validation du choix.
- Saisie de la date du mouvement (la date du jour s'affiche par défaut).
- Choix du type de mouvement dans la liste de valeur du champ « Type » :
  - ✓ Réception fournisseur (Entrées en stock des commandes sans PO),
  - ✓ Retour / Reversement (Retour en stock),
  - ✓ Sorties diverses (Demande de sortie marchandises).
- Saisie du numéro du Bon dans le champ « N° Bon ».

- Imputation (Clé Comptable Flexible) **dans le Champ « Compte »** :
  - ✓ Si toutes les lignes de mouvement ont la même imputation, la saisir à ce niveau,
  - ✓ Sinon saisir l'imputation dans le champ « wwwww » au niveau des lignes de mouvement.
- Clic sur la liste de valeur du champ « Alias compt. » et Choix de l'alias correspondant au mouvement :
  - ✓ « Réception fournisseur » alias « IC Réception sans PO »,
  - ✓ « Retour / Reversement » : choisir le retour correspondant,
  - ✓ « Sorties diverses » : choisir la sortie correspondante.
- Validation du choix.
- Complément des champs de la Clé Comptable Flexible.

7. Mouvements matières :

Responsabilités : ***SN - Opérateur Stocks, SN – Auditeur Stock, SN - Auditeur Comptable Stock***

Mouvements → Mouvements matières

- Choisir l'organisation concernée.
- Cliquer sur le bouton « OK » pour valider votre choix.
- Saisir les critères de la recherche :
  - ✓ Périodes : date début / date fin,
  - ✓ Article : code article,
  - ✓ Magasin : magasin de l'organisation,
  - ✓ Type d'origine et n° du bon,

- ✓ Type de mouvement,
- ✓ Quantités mouvementées.

- Rechercher les différentes informations.
- Fermeture de la fenêtre en cours.

8. Recherche de quantités en stock :

Responsabilités : ***SN - Opérateur Stock, SN – Auditeur Stock, SN-Auditeur Comptable Stock***
En stock, disponibilité → Quantité en stock

- Choix de l'organisation concernée.
- Validation du choix.
- Saisie des critères de recherche :
  - ✓ « Magasin » : choisir le code d'un magasin dans la liste de valeur, sinon le système affiche la quantité totale de tous les magasins de l'organisation en cours.
  - ✓ « Quantités» : saisir une plage de quantités si nécessaire.
  - ✓ « Voir par » : Choisir **Lieu** et crochet sur « Détaillé » pour avoir les quantités par magasin.
  - ✓ « Article/Version » : Saisir le code d'un article pour afficher la quantité de cet article uniquement.
- Recherche pour visualiser les quantités.
- Fermeture de la fenêtre en cours.

9. Recherche de quantités en multi organisations :

Responsabilités : ***SN - Opérateur Stock, SN – Auditeur Stock***
En stock, disponibilité → Quantité multi organisation

- Choix de l'organisation de la 1ère organisation.
- Validation du choix.
- Choix d'un article unique ou une intervalle d'article dans le champ « Articles ».
- Choix des codes des organisations dans le champ « Code », le champ « Num » s'affiche automatiquement.
- Lancement.
- Fermeture de la fenêtre en cours.
- Affichage du menu principal.
- Clic sur « Voir » et choix « Traitements ».
- Clic sur « Rechercher ».
- Clic sur le bouton « **Rafraîchir les données** » pour avoir le résultat « **Terminé - Normal** ».
- Clic sur le bouton « **Voir la sortie** ».
- Clic sur le menu « Outils » et ensuite clic sur « Copier fichier ».
- Attente du chargement de la page web.
- Enregistrement de l'état.

Le fichier est visualisé et imprimé à partir de « Microsoft Word » avec une mise en page adéquate :

- ✓ Réduction des marges gauche et droite à 2cm,
- ✓ Taille des caractères à 8,
- ✓ Format paysage.

10. Recherche d'article de l'organisation :

Responsabilités : ***SN - Opérateur Stock, SN – Auditeur Stock, SN – Auditeur Comptable Stock***

Articles ➔ Rechercher un article

- Choix de l'organisation concernée.
- Clic sur le bouton « OK » pour valider votre choix.
- Saisie des critères de recherche :
  - ✓ « Masque art. » : code de l'article recherché,
  - ✓ « Description » : description de l'article,
  - ✓ « Afficher quantité » permet d'afficher la quantité en stock de l'article recherché.

  NB : si les deux champs « Masque art. » et « Description » sont vides, le système affiche l'ensemble des articles de l'organisation.
- Clic sur le bouton « Rechercher », les informations s'affichent.

11. Processus d'inventaire de Stock Sur Oracle IC :

Responsabilité : **SN – Auditeur inventoriste Stock**

- Ouvrir.
- Choisir l'organisation.
- Clic sur liste de valeur.
- Choisir l'état dans la liste de valeur.
- Choisir l'inventaire dans la liste de valeur.

- Lancer traitement.
- Aide – consulter traitements.
- Rechercher.
- Rafraîchir les données.
- Termine normal ➔ voir la sortie.
- Spécial --- copier fichier.
- Fichier ---- enregistrer sous.
- Choisir un emplacement : ex Mes documents.
- Nom fichier : ex sur écran.
- Type fichier : fichier texte (*.Txt).
- Enregistrer.

OUVRIR WORD

- Fichier.
- Ouvrir.
- Chercher Le Fichier Enregistré.
- Ouvrir.
- Sélection du Document : Edition – Sélectionner Tout (Ctrl - A).
- Taille police = 9.
- Enlever la sélection par un clic.
- Fichier – Mise en page.
- Marge gauche et droite = 1,5cm.
- Paysage par un clic.
- Ok.
- Enregistrer le document : Fichier – Enregistrer.
- Type de Fichier : Document Word.

6.3. Feuilles de révélation et d'analyse de problème (FRAP)

Le questionnaire de contrôle en annexe a permis d'aboutir aux FRAP.

FRAP 1
Problème : Identification des articles à leur entrée en stock
Constat : Les inventaires tournants ont révélé 6000 articles qui n'ont pas de nomenclatures mais des codes provisoires.
Causes : - Insuffisances d'information sur leur référence technique - Défaillance des opérations de réception.
Conséquences : - Difficulté du suivi de leurs mouvements et de leur dénombrement ; - Réception d'articles ne correspondant pas aux besoins exprimés par les unités ; - Risque de commande d'articles existants mais dont les quantités en stocks sont inconnues.
Recommandations : - S'assurer de la correspondance entre les articles commandés et ceux effectivement réceptionnés ; - Mettre en place un plan spécial pour identifier les articles concernés (nature, services utilisateurs) en vue de leur créer des nomenclatures pour une gestion optimale des stocks.
Etabli par : **Approuvé par :** Ndieundé NDIAYE Chef Unité Gestion Stocks

FRAP 2

Problème : Procédures informatiques des habilitations et des accès

Constat :

Inexistence de procédures pour les habilitations des utilisateurs et d'accès au réseau

Causes :

Tâches d'élaboration des procédures écrites non satisfaites par l'informatique

Conséquences :

- Déficience dans le respect des habilitations et des accès au réseau ;
- Défaut de mise à jour des habilitations et des accès ;
- Tâches incompatibles réalisées pour défaut du respect des habilitations et des accès ;
- Mots de passe demeurant inchangées pendant de longues périodes.

Recommandations :

- Rédiger les procédures de définition des habilitations et des codes d'accès ;
- Prévoir les périodes de modifications des mots de passe.

Etabli par : Ndieundé NDIAYE

Approuvé par : Responsable informatique

FRAP 3
Problème : Procédure de gestion des incidents
Constat : Aucune indication sur la gestion des incidents.
Causes : Procédures déficientes
Conséquences : - Difficultés pour la mise en œuvre des reprises en cas d'incidents ; - Pertes d'information.
Recommandations : Elaborer les procédures de gestion des incidents et un plan de informatiques.
Etabli par : **Approuvé par** : Ndieundé NDIAYE Responsable informatique

Ainsi ces FRAP montrent les différents problèmes rencontrés au cours de notre étude avec leurs causes et leurs conséquences. En fait, la FRAP est le papier de travail synthétique par lequel l'auditeur documente chaque dysfonctionnement, conclut chaque phase du travail terrain et communique avec l'audité concerné. Vu l'importance de notre questionnaire de contrôle, d'autres FRAP ont été élaboré (voir annexe n°3).

6.4. Synthèse des forces et des faiblesses relevées :

L'examen du questionnaire de contrôle interne nous a permis de relever les forces et les faiblesses de l'application Oracle IC par rapport à son support et les conditions de son utilisation par la SENELEC.

6.4.1. Forces relevées dans l'utilisation du logiciel Oracle IC :

- **Système d'Information (Oracle IC) :**
  - Couverture de tous les sites de stockage par le module Oracle IC ;
  - Existence des procédures de contrôles des accès, des entrées, des rejets et des traitements ;
  - Existence de procédures informatiques et des mises à jour ;
  - Existence de vérification de la fiabilité de l'application Oracle IC ;
  - Existence de traçabilité des données ;
  - Existence de plan de renouvellement des équipements informatiques.

- **Suivi des stocks :**
  - Création systématique d'un bon de réception pré numéroté pour toute réception ;
  - Rapprochement périodique avec des données internes et externes pour garantir leur cohérence ;
  - Procédures d'inventaire satisfaisantes ;
  - Inventaire physique périodique (tournant sur l'année et de fin d'année) de toutes les catégories de stock ;
  - Instructions écrites émises avant les inventaires ;
  - Arrêt des mouvements et relèvement des références des dernières réceptions et livraisons ;
  - Rangement rationnel des stocks pour faciliter les comptages avant l'inventaire ;
  - Utilisation d'étiquettes pré numérotées ;
  - Responsabilité des comptages confiée à des personnes indépendantes de celles chargées de la surveillance des stocks ;
  - Utilisation d'un système de double comptage ;

- Description des stades d'avancement des travaux en cours suivie par des personnes compétentes, en l'occurrence les techniciens de la Direction de l'Equipement ;
- Protection des stocks contre les risques d'une détérioration physique ;
- Des fiches de stock en quantité et en valeur sont-elles tenues en comptabilité ;
- Ajustements préalables des fiches approuvées par un responsable ;
- Contrôle de la valorisation satisfaisant : coût moyen pondéré déterminé par Oracle IC ;
- Contrôle systématique de l'exactitude arithmétique de l'inventaire physique valorisé par Oracle IC ;
- Obtention par Oracle IC des durées de rotation des articles pour la constitution des provisions pour dépréciation.

6.4.2. Faiblesses relevées dans l'utilisation du logiciel Oracle IC :

➢ **Identification des articles à leur entrée en stock :**

Les inventaires tournants ont révélé 6000 articles qui n'ont pas de nomenclatures mais des codes provisoires à cause des insuffisances d'information sur leur référence technique et des défaillances des opérations de réception. Il s'ensuit :

- Difficulté du suivi de leurs mouvements et de leur dénombrement,
- Réception d'articles ne correspondant pas aux besoins exprimés par les unités,
- Risque de commande d'articles existants mais dont les quantités en stocks sont inconnues.

➢ **Procédures informatiques des habilitations et des accès :**

Il n'existe pas de procédures pour les habilitations des utilisateurs et d'accès au réseau par défaut de procédures écrites. Les conséquences sont :

- déficience dans le respect des habilitations et des accès au réseau ;
- défaut de mise à jour des habilitations et des accès.

Les conséquences de cette faiblesse peuvent être :

- tâches incompatibles réalisées pour défaut du respect des habilitations et des accès ;
- mots de passe demeurant inchangés pendant de longues périodes.

➢ **Procédure de gestion des incidents :**

Aucune indication n'est relevée sur la gestion des incidents. Cette situation peut faire naître :

- des difficultés pour la mise en œuvre des reprises en cas d'incidents,
- des pertes d'information.

➢ **Optimisation et efficience de la gestion : définition des lieux de stockage et des responsabilités des gestionnaires de stocks :**

Certains sites de stockage ne sont pas appropriés : dispersion des articles, accès difficile pour retrouver les articles : magasins de la Centrale C4. Mieux, le Parc de Hann reçoit indistinctement en pleine air les transformateurs neufs, les transformateurs en réparation et les transformateurs réparés. La raison de cet état de fait est l'absence d'une politique de sécurisation des stocks. Les conséquences sont :

- défauts de maîtrise des stocks ;
- incidence négative sur la politique d'approvisionnement ;
- défaut de sécurisation des stocks.

➢ **Maîtrise des mouvements de stocks :**

A cause d'un défaut de responsabilisation d'une entité unique pour le suivi des stocks, les commandes relatives à des projets ne passent pas par les magasins ; elles ne sont pas prises en compte dans Oracle IC. Les conséquences sont :

- défaut d'une responsabilisation du suivi des stocks par une entité unique ;
- non identification par les gestionnaires des stocks de certains articles ;
- non immatriculation de certains articles qui sont le réseau ;
- propriété de la Société sur certains articles difficilement prouvables.

➢ **Émission d'un bon de sortie pré numéroté :**

Au niveau des magasins de certaines Centrales, face au besoin pressant de réparation de groupe en panne, des bons provisoires sont établis et parfois non régularisés. Par conséquent le suivi des mouvements (sorties) de stocks au niveau des magasins des centrales est défaillant.

➢ **Enregistrement en comptabilité à la même période des mouvements :**

L'enregistrement en comptabilité est fait à partir de Oracle IC. Il n'y a pas toujours coïncidence entre la comptabilisation des opérations et les dates de mouvements de stocks. Des rattrapages de saisie des mouvements de stocks dans Oracle IC sont effectués en fin d'année. Cet état de fait est lié à :

- l'insuffisance de formation au logiciel Oracle de certains magasiniers ;
- l'inexistence de période d'arrêté mensuel au niveau de Oracle IC (ouverture et clôture du module).

Les risques sont :

- retard des arrêtés comptables,
- écarts entre données comptables et inventaire.

➢ **Surveillance des stocks :**

Les stocks sont en plein air ou éparpillés dans certaines localités à cause de l'inexistence de magasins.

Les risques peuvent être :

- non maîtrise des stocks,
- déperdition des stocks.

➢ **Stocks mini- stock max :**

Le sous module Oracle IC de suivi du niveau des stocks et des seuils de déclenchement des commandes n'est pas activé dans à cause d'un problème de paramétrage du logiciel Oracle IC. Ceci entraîne de facto une déficience de la politique d'approvisionnement.

Les faiblesses ci-dessus, relevées, ont suscité de notre part des recommandations.

6.4.3. Synthèse des recommandations liées aux faiblesses constatées sur l'utilisation du logiciel Oracle IC au niveau de SENELEC :

Dans le but d'améliorer et de corriger les failles et vulnérabilités observées au niveau de l'applications informatique de gestion des stocks Oracle IC de la SENELEC, nous soumettons cet ensemble de recommandations aux différents responsables du domaine, afin d'y accorder une attention particulière et de trouver des solutions adéquates.

Nos recommandations se résument en quelques points :

- Elaborer un manuel de procédures renfermant toutes les procédures au niveau du département informatique ;
- Favoriser la formation et le stage du personnel, en particulier les magasiniers, sur le logiciel Oracle afin de les rendre encore plus performants ;
- S'assurer de la correspondance entre les articles commandés et ceux effectivement réceptionnés ;
- Mettre en place un plan spécial pour identifier les articles concernés (nature, services utilisateurs) en vue de leur créer des nomenclatures pour une gestion optimale des stocks ;
- Rédiger les procédures de définition des habilitations et des codes d'accès ;
- Prévoir les périodes de modifications des mots de passe ;
- Elaborer les procédures de gestion des incidents et un plan informatique ;
- Sécuriser les stocks en mettant en place des sites appropriés les préservant des vols, des intempéries ;
- Les articles utilisés au sein de l'entreprise doivent clairement être identifiés en leur affectant des références internes ou des nomenclatures. Pour cela le Service de Gestion doit :
  - enregistrer toutes les entrées en stocks,
  - leur créer des nomenclatures ou des références (immobilisations stockées) ;
- Régulariser systématiquement les bons provisoires ayant entraîné des sorties de stocks dans Oracle IC le jour de leur survenance pour éviter le suivi des mouvements de stocks ;
- Définir des périodes d'arrêté mensuel au niveau de Oracle IC et s'assurer de l'exhaustivité de la saisie de l'ensemble des mouvements intervenus au cours d'une période pour fiabiliser le suivi des stocks dans Oracle IC ;
- Créer des magasins dans toutes les localités qui reçoivent des articles pour éviter les déperditions d'articles ;
- Activer les sous modules Minima et Maxima de suivi du niveau individuel des articles en stock pour optimiser la politique d'approvisionnement.

CONCLUSION GENERALE

L'informatique a poursuivi ces dernières années une évolution qui atteint la plupart des fonctions classiques de l'entreprise, la vie quotidienne et les systèmes industriels.

L'audit informatique qui a pour but de prévenir, éviter ou limiter les difficultés nées de l'informatique ou liées à l'informatique, se traduit en terme de conformité aux réglementations et à la politique générale de l'entreprise, de sécurité pour la protection de l'actif informatique, d'efficacité de l'outil informatique mis à la disposition de l'entreprise pour améliorer les performances de gestion et en réduire les coûts.

Une informatisation qui n'est pas réussie sur le plan technique, ou qui est adoptée ou mal vécue, perturbe le fonctionnement de l'entreprise et peut avoir des conséquences financières graves.

Le développement, sans cesse croissant, des nouvelles technologies de l'information est l'un des facteurs ayant permis aux entreprises d'accroître leur productivité et d'améliorer les prestations offertes à leurs clients.

L'audit de l'application informatique (Orale IC) exploitée dans le cadre de la gestion des stocks de la SENELEC nous a permis de faire :

- d'une part, une description du système et une évaluation exhaustive de la fonction informatique. Cependant nous avons noté certaines faiblesses même si le système a bénéficié d'importants investissements et repose sur un personnel compétent et expérimenté.
- D'autre part, une évaluation de l'application ORACLE IC qui a montré la capacité de gérer les stocks en temps réel.

Ainsi nous pouvons dire que le Service de Gestion des Stocks (Oracle IC), à l'image de tout autre type de système de management, est perfectible. Malgré les efforts consentis au niveau du développement des ressources humaines, l'idéal serait d'améliorer l'environnement de travail du personnel. Ceci, dans l'optique d'augmenter leur motivation pour la réussite de la mission du Service, voire de la SENELEC.

Il existe une certaine corrélation entre la gestion des stocks et les faiblesses de contrôle interne constatées dans le logiciel Oracle IC.

Le fichier du magasin Transport appelle quelques observations :

- un stock comptable nul pour tous les articles, aucun inventaire n'étant pris en compte ;
- certains articles n'ont pas de prix unitaire (liste transmise au Département transport pour retrouver les commandes correspondantes)

A l'issue de tout cela, une prompte réaction serait souhaitable pour sa prise en compte dans Oracle IC pour l'exercice 2009.

L'idéal est de faire en sorte qu'il n'y ait aucunes faiblesses dans l'utilisation de l'application informatique de gestion des stocks (ORACLE IC).

Tout cela aiderait enfin à améliorer aussi bien la qualité des services offerts aux clients surtout externes, que l'image de marque de la SENELEC. Et, grâce à la garantie que pourrait apporter une bonne gestion de l'application informatique Oracle IC, ceci pourra rentabiliser l'entreprise en sécurisant ses investissements financiers dans l'optique de gagner la confiance des actionnaires et des bailleurs de fonds.

En définitive, nous pouvons prétendre que l'audit des applications informatiques est l'audit du progrès, de la communication et de la promotion de la culture de contrôle interne qui constitue un des éléments fondamentaux pour garantir le déroulement adéquat des procédures informatiques.

Pour un lendemain meilleur, la SENELEC doit adapter son organisation au nouveau contexte juridique et réglementaire en respectant ses objectifs et ses principes d'organisation.

ANNEXES

ANNEXE 1 :	**QUESTIONNAIRE D'EVALUATION DU CONTROLE INTERNE**
ANNEXE 2 :	**ORGANIGRAMME DE LA SENELEC**
ANNEXE 3 :	**FEUILLES DE REVELATION ET D'ANALYSE DE PROBLEME (FRAP)**
ANNEXE 4 :	**MAGASINS DISTRIBUTION ET PRODUCTION**
ANNEXE 5 :	**MENU PRINCIPAL ORACLE IC**
ANNEXE 6 :	**ORGANISATION DANS ORACLE IC**
ANNEXE 7 :	**CONSULTATION ARTICLE DANS ORACLE IC**
ANNEXE 8 :	**MENU INVENTAIRES DANS ORACLE IC**
ANNEXE 9 :	**ANALYSE D'INVENTAIRE DANS ORCLE IC**
ANNEXE 10 :	**ANALYSE DE PRECISION INVENTAIRE DANS ORACLE IC**

Annexe N°1: QUESTIONNAIRE D'EVALUATION DU CONTROLE INTERNE

Rubriques	Oui	Non	N/A	Commentaire
Organisation des sites de stockage				
Le management de la société a t- il mis en place un mode de gestion optimale et efficiente des stocks : définition des lieux de stockage, des responsabilités des responsables des magasins ?		x		- Certains sites de stockage ne sont pas appropriés : dispersion des articles, accès difficile pour retrouver les articles : magasins de la Centrale C4 - Parc de Hann pour recevoir en pleine air les transformateurs neufs, les transformateurs en réparation et les transformateurs réparés
Système d'Information (Oracle IC)				
1. Le module Oracle IC couvre t-il tous les sites de stockage ?	x			
2. Existe –il des procédures des contrôles des accès, des entrées, des rejets et des traitements ?	x			
3. Existe-t-il des procédures informatiques et les mises à jour ?	x			- existence de guide d'application pour Oracle IC
4. Est-ce que ces procédures sont respectées par les utilisateurs ?			x	

5. Existe –t-il une vérification de la fiabilité de l'application Oracle IC ?	x			
6. Existe-t-il des procédures pour les habilitations des utilisateurs et d'accès au réseau ?		x		les procédures ne sont pas consignées dans un manuel de procédures.
7. Existe-t-il une traçabilité des données ?	x			
8. Existe-t-il une procédure de gestion des incidents ?		x		les procédures ne sont pas consignées dans un manuel de procédures.
9. Y'a-t-il un plan de renouvellement des équipements informatiques ?	x			
Suivi des stocks				
1. les articles sont ils correctement identifiés lors de leur entrée en stocks ?			x	Des nomenclatures sont créées pour tous les articles. Cependant certains articles ont des codes provisoires à cause d'informations manquantes sur leurs références techniques

2. Les mouvements de stock sont –ils bien appréhendés ?		x		Les commandes relatives à des projets échappent au suivi des gestionnaires des Stocks. Elles ne sont pas prises en compte dans Oracle IC
3. Les magasins sont –ils séparés des services de réception et d'expédition ?		x		
4. Toute réception donne-t-elle lieu à l'émission d'un bon de réception pré numéroté ?	x			
5. Toute expédition est-elle accompagnée de l'émission d'un bon de sortie pré numéroté ?		x		Au niveau des magasins de certaines Centrales, face au besoin pressent de réparation de groupe en panne, des bons provisoires sont établis et parfois non régularisés
6. Les soldes sont-ils rapprochés périodiquement avec des données internes et externes pour garantir leur cohérence ?	x			Cette opération n'est effectuée qu'au moment des inventaires
7. Quelles mesures permettent de suivre les mouvements ?			x	le module Mouvement de Oracle IC

8. À quelles conditions, les stocks obsolètes peuvent-ils être mis au rebut ou cédés ?			x	Si l'immobilisation principale à laquelle ils sont rattachés est réformée
9. Quelles procédures sont mises en place pour s'assurer que tous les mouvements physiques de stocks sont enregistrés en comptabilité à la même période que ces mouvements ?		x		l'enregistrement en comptabilité est fait à partir de Oracle IC. Il n'y a pas toujours coïncidence entre la comptabilisation des opérations et les dates de mouvements de stocks
10. Les procédures d'inventaire sont-elles satisfaisantes ?	x			
11. Toutes les catégories de stock font-elles l'objet d'un inventaire physique périodique ? Quelle est cette périodicité ?	x			inventaires tournants : juin et septembre inventaire de fin d'exercice
12. Des instructions écrites sont-elles émises avant les inventaires ?	x			

13. Les mouvements sont-ils arrêtés et les références des dernières réceptions et livraisons relevées ?	x			
14. L'inventaire est-il précédé d'un rangement rationnel des stocks pour faciliter les comptages?	x			
15. Des étiquettes pré numérotées sont-elles utilisées ?	x			
16. Si non, quelles mesures sont prises pour s'assurer que tout est compté et relevé ?	x			suivi des Stocks à partir du listing Oracle
17. La responsabilité des comptages est-elle confiée à des personnes indépendantes de celles chargées de la surveillance des stocks concernés ?	x			
18. Procède-t-on à un double comptage ?	x			

19. La description des stades d'avancement des travaux en cours est-elle effectuée par des personnes compétentes ?	x			les agents (ingénieurs, techniciens supérieurs) de la Direction de l'Equipement sont chargés du suivi des projets
20. Les stocks sont-ils convenablement surveillés ?		x		existence de localités sans magasin : stocks en plein air, éparpillés
21. L'accès aux magasins est-il limité aux seules personnes autorisées ?		x		
22. Les stocks sont-ils protégés contre les risques d'une détérioration physique ?	x			
23. Des fiches de stock en quantité et en valeur sont-elles tenues en comptabilité ? Pour tous les stocks ?	x			
24. Ces fiches indiquent-elles les quantités minimum et maximum à respecter ?		x		le sous module stocks mimi-stock max n'est pas activé dans Oracle IC

25. Ces fiches sont-elles ajustées après chaque inventaire physique ?	x			
26. Les ajustements des fiches sont-ils préalablement soumis à l'approbation d'un responsable ?	x			
27. La protection des accès logiques aux systèmes informatiques est-elle assurée ?	x			
28. Le contrôle de la valorisation est-il satisfaisant ?	x			
29. Procède-t-on à un contrôle systématique de l'exactitude arithmétique de l'inventaire physique valorisé ?	x			Grâce au sous - module Inventaire de Oracle IC
30. Les magasiniers doivent-ils signaler périodiquement les stocks inutilisables ou à rotation lente ?		x		

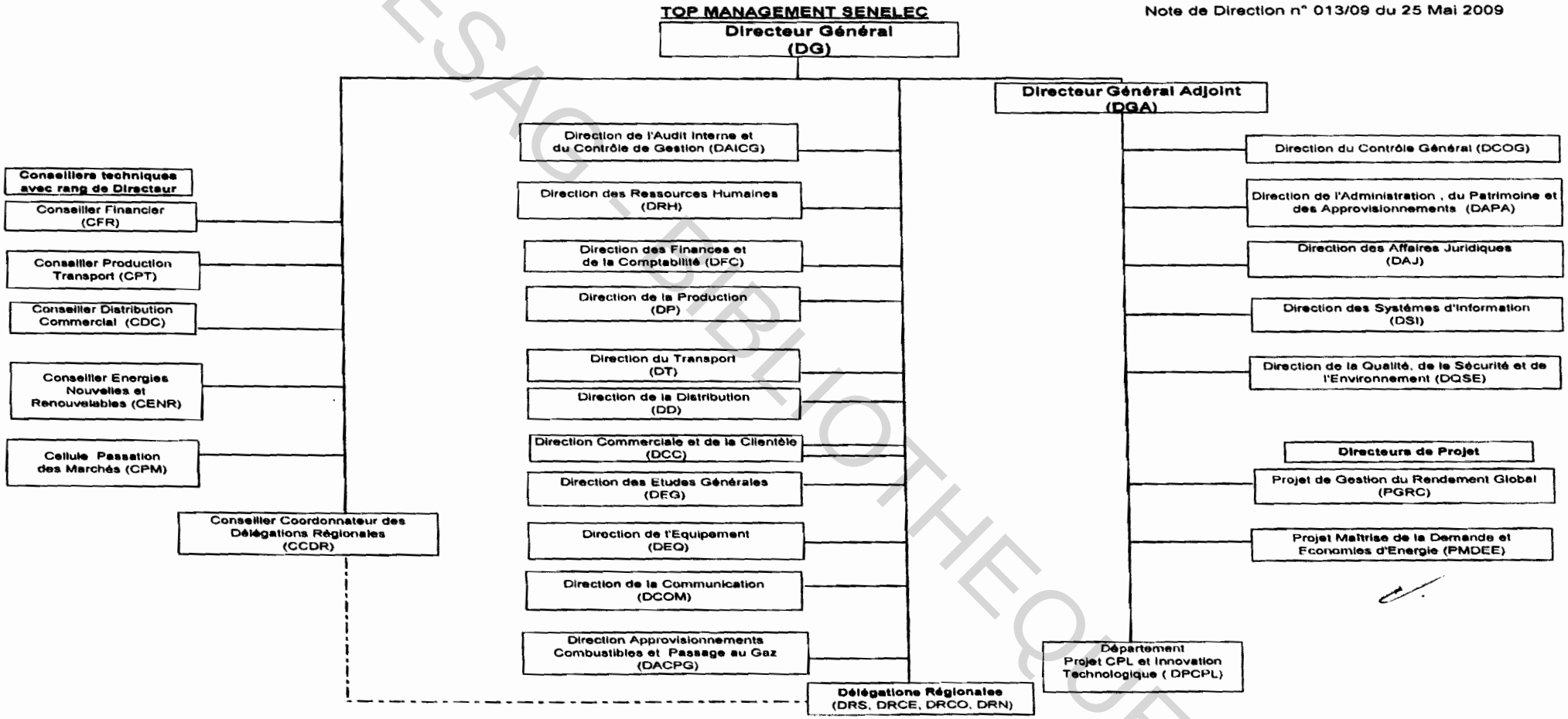
31. Procède-t-on à un examen périodique des fiches de stocks pour relever les articles à rotation lente ?	x			
32. Quels critères servent à la détermination de la provision pour dépréciation ?	x			taux de rotation et l'ancienneté
33. La séparation des fonctions est-elle adéquate ?	x			

Fait à DAKAR, le 31 Août 2009

Par Ndieundé NDIAYE, Stagiaire au DAIO de la SENELEC.

Annexe N°2: ORGANIGRAMME DE LA SENELEC

La note de direction n° 013/2009 a diffusé l'organigramme général de la SENELEC comme suite.



Annexe N°3: FEUILLES DE REVELATION ET D'ANALYSE DE PROBLEME (FRAP)

Le questionnaire d'évaluation du contrôle interne ci-dessus a permis d'aboutir à d'autres FRAP qui vont aussi contribuer à la bonne compréhension de notre étude.

FRAP 4
Problème : Optimisation et efficience de la gestion : définition des lieux de stockage et des responsabilités des gestionnaires de stocks
Constat : Certains sites de stockage ne sont pas appropriés : dispersion des articles, accès difficile pour retrouver les articles : magasins de la Centrale C4, Parc de Hann pour recevoir en plein air les transformateurs neufs, les transformateurs en réparation et les transformateurs réparés.
Causes: Absence d'une politique de sécurisation des stocks
Conséquences : - Défauts de maîtrise des stocks ; - Incidence négative sur la politique d'approvisionnement ; - Défaut de sécurisation des stocks.
Recommandations : Sécuriser les stocks en mettant en place des sites appropriés, les préservant des vols, des intempéries.
Etabli par : Ndieundé NDIAYE — **Approuvé par :** Chef Unité Gestion Stocks

FRAP 5

Problème : **Maîtrise des mouvements de stocks**

Constat :

Les commandes relatives à des projets échappent au suivi des gestionnaires des Stocks. Elles ne sont pas prises en compte dans Oracle IC

Causes:

- Défaut d'une responsabilisation du suivi des Stocks par une entité unique.

Conséquences :

- Non identification par les gestionnaires des stocks de certains articles ;
- Non immatriculation de certains articles qui sont le réseau ;
- Propriété de la Société sur certains articles difficilement prouvables.

Recommandations :

Les articles utilisés au sein de l'entreprise doivent clairement être identifiés en leur affectant des références internes ou des nomenclatures. Pour cela, le Service de Gestion doit :

- enregistrer toutes les entrées en stocks,
- leur créer des nomenclatures ou des références (immobilisations stockées).

Etabli par :
Ndieundé NDIAYE

Approuvé par :
Chef Unité Gestion Stocks

FRAP 6
Problème : **Emission d'un bon de sortie pré numéroté**
Constat : Au niveau des magasins de certaines Centrales, face au besoin pressant de réparation de groupe en panne, des bons provisoires sont établis et parfois non régularisés.
Causes: Urgence pour les interventions au niveau des groupes en panne.
Conséquences: Suivi des mouvements (sorties) de stocks défaillants.
Recommandations : Régulariser systématiquement les bons provisoires le jour de leur survenance.
Etabli par : Ndieundé NDIAYE **Approuvé par** : Chef Unité Gestion Stocks

FRAP 7
Problème : **Enregistrement en comptabilité à la même période des mouvements**
Constat : L'enregistrement en comptabilité est fait à partir de Oracle IC. Il n'y a pas toujours coïncidence entre la comptabilisation des opérations et les dates de mouvements de stocks. Des rattrapages de saisie des mouvements de stocks dans Oracle IC sont effectués en fin d'année.
Causes : - Insuffisance de formation au logiciel Oracle de certains magasiniers ; - Inexistence de période d'arrêté mensuel au niveau de Oracle IC (ouverture et clôture du module).
Conséquences : - Retard des arrêtés comptables ; - Ecarts entre données comptables et inventaire.
Recommandations : - Définir des périodes d'arrêté mensuel au niveau de Oracle IC ; - S'assurer de l'exhaustivité de la saisie de l'ensemble des mouvements intervenus au cours d'une période.
Etabli par : Ndieundé NDIAYE **Approuvé par** : Chef Unité Gestion Stocks

FRAP 8

Problème : **Surveillance des stocks**

Constat :

Existence de localités sans magasin : stocks en plein air, éparpillés.

Causes :

- Négligence de la gestion des stocks ;
- Non implication des responsables hiérarchiques dans le suivi des stocks.

Conséquences :

- Non maîtrise des stocks ;
- Déperdition des stocks.

Recommandations :

Créer des magasins dans toutes les localités qui reçoivent des articles.

Etabli par :

Ndieundé NDIAYE

Approuvé par :

Chef Unité Gestion Stocks

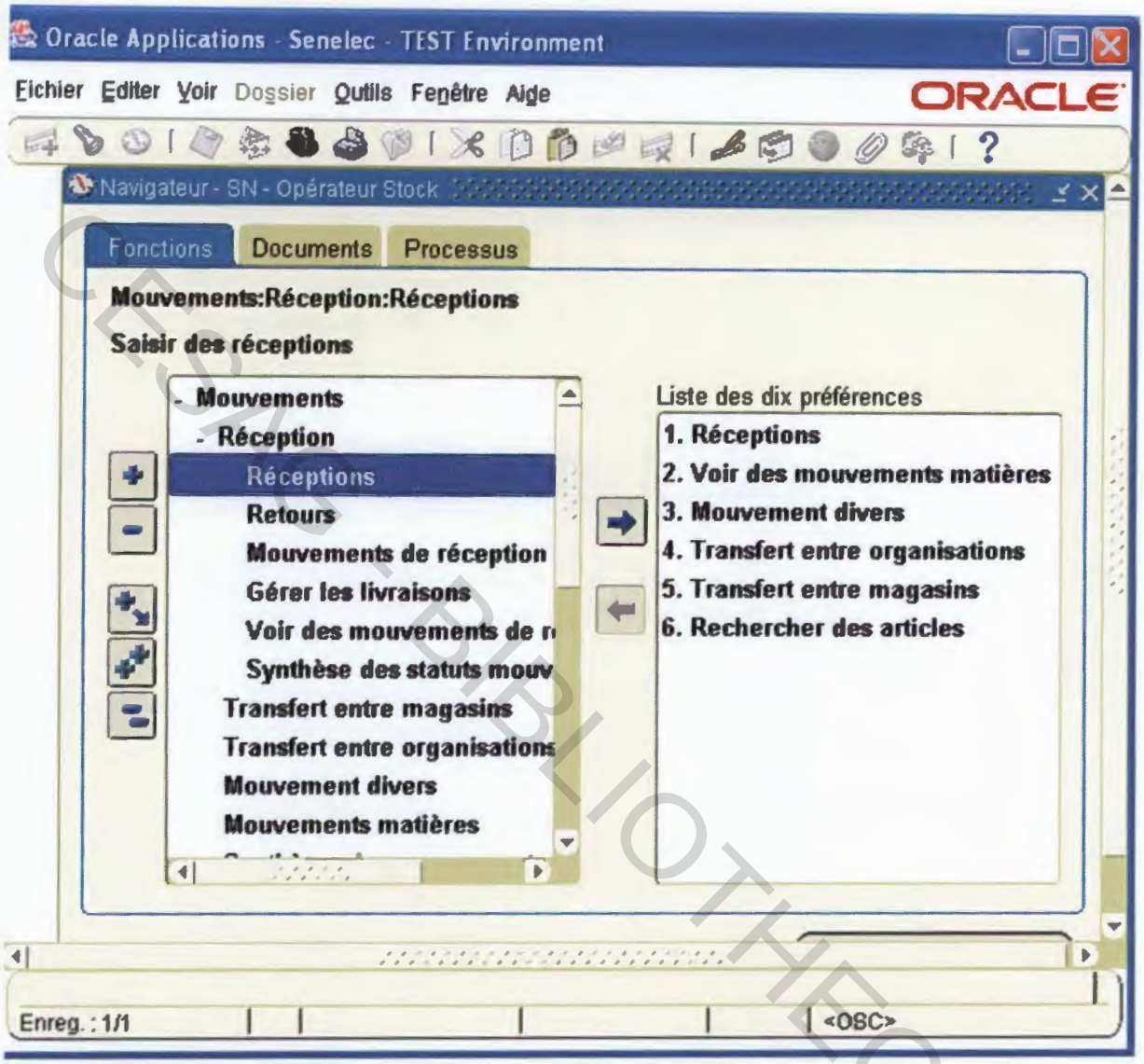
FRAP 9
Problème : **Suivi et respect des quantités minimum et maximum**
Constat : Le sous module stocks mimi- stock max n'est pas activé dans Oracle IC.
Causes : Problème de paramétrage du logiciel Oracle IC.
Conséquences : Politique d'approvisionnement déficient.
Recommandations: Activer les sous modules Minima et Maxima de suivi du niveau individuel des articles en stock.
Etabli par : Ndieundé NDIAYE **Approuvé par** : Chef Unité Gestion Stocks

Annexe N°4: MAGASINS DISTRIBUTION ET PRODUCTION

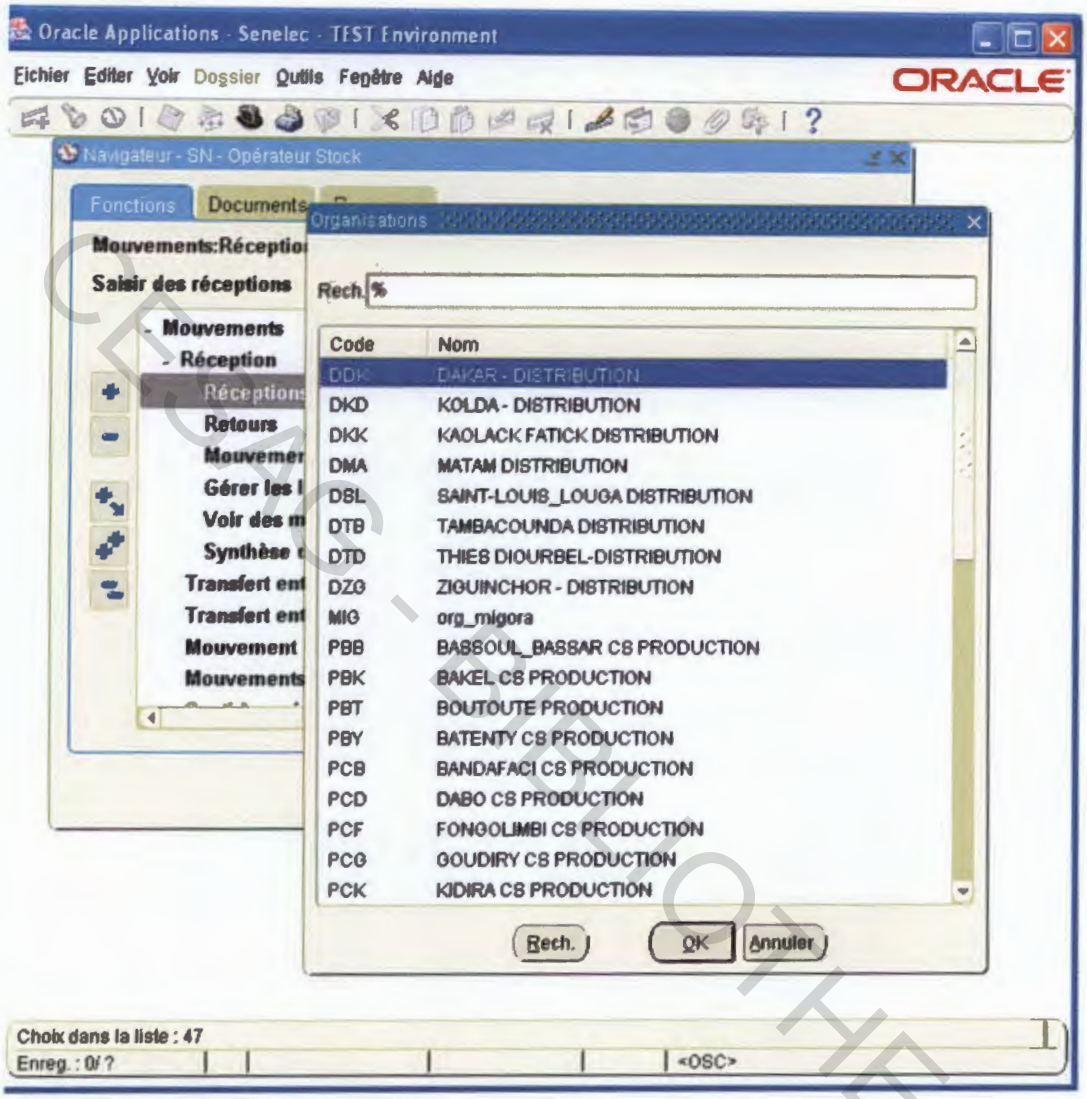
ANNEXE 2 : MAGASINS DISTRIBUTION ET PRODUCTION			
Organisation		**Indice**	**Magasin**
1	DDK	1011	Magasin Général
2	DDK	1012	Parc de Hann
3	DDK	1013	Labo de Compteurs
4	DDK	1014	Pièces détachées
5	DDK	1015	Pompe Carburant
6	DDK	1016	Consommab. Informat.
7	DDK	1017	Imprimés et F.de Bureau
8	DDK	1110	Rufisque
9	DDK	1140	Guédiawaye
10	DDK	1990	Réforme
11	DDK	1999	Prêt
12	DDK	1019	Transfos
Distribution DAKAR			
13	PDK	1011	Centrale C1
14	PDK	1012	Centrale C2
15	PDK	1111	Centrale C3
16	PDK	1112	Centrale C4
17	PDK	1211	Centrale Kounoune
18	DPC	1310	Dêpot Passage Combust
19	DPC	1311	" " "
20	DPC	1312	" " "
21	DPC	1313	" " "
22	DPC	1314	" " "
Production DAKAR			
23	DDKD	5100	Kolda
24	DKK	4000	Kaolack
25	DKK	4100	Fatick
26	AMA	3200	Matam
27	ASL	3000	Saint-Louis
28	DTB	4200	Tamba
29	DTD	2100	Mbour
30	DTD	2000	Thiès
31	ASL	3400	Louga
32	DTD	2200	Diourbel
33	DTD	2215	Touba
34	DTD	2300	Tivaouane
35	DZG	5000	Ziguinchor
Magasins Distribution Régions			
36	PBT	5001	Boutoute
37	PRK	4121	Kahone
38	PRD	5100	Kolda
39	PRT	4299	Tamba

40	PSL	3099	Saint-Louis
41	PRK	4122	Kahone 2
Magasins Régions	**Production**		
42	PBB	4130	Bassoul Bassar
43	PBK	4207	Bakel
44	PBY	4020	Beinttenti
45	PBY	4120	"
46	PCB	4213	Bandafaci
47	PCD	5018	Dabo
48	PCF	4211	Fomgolimbi
49	PCB	4201	Goudiry
50	PCK	4208	Kidira
51	PCN	4017	Ndanda
52	PCP	5017	Pakour
53	PCS	4212	Saraya
54	PCT	5009	Thionck-Essyl
55	PVC	5107	Vélingara
56	PDJ	4135	Djenda
57	PDL	5013	Djouloulou
58	PDN	4125	Dionewar niodior
59	PKE	4206	Kédougou
60	PKG	4015	Koungheul
61	PKP	4202	Koumpentoum
62	PMA	5101	Marsassoum
63	PMG	5105	Médina Gounass
64	PMS	4016	Médina Sabakh
65	PMY	5019	Médina Yoro Foula
66	PND	5102	Ndiama Couta
67	POR	3202	Ourossogui
68	PSA	4210	Salémata
69	PSE	5106	Sédhiou
70	PSI	5008	Sindia

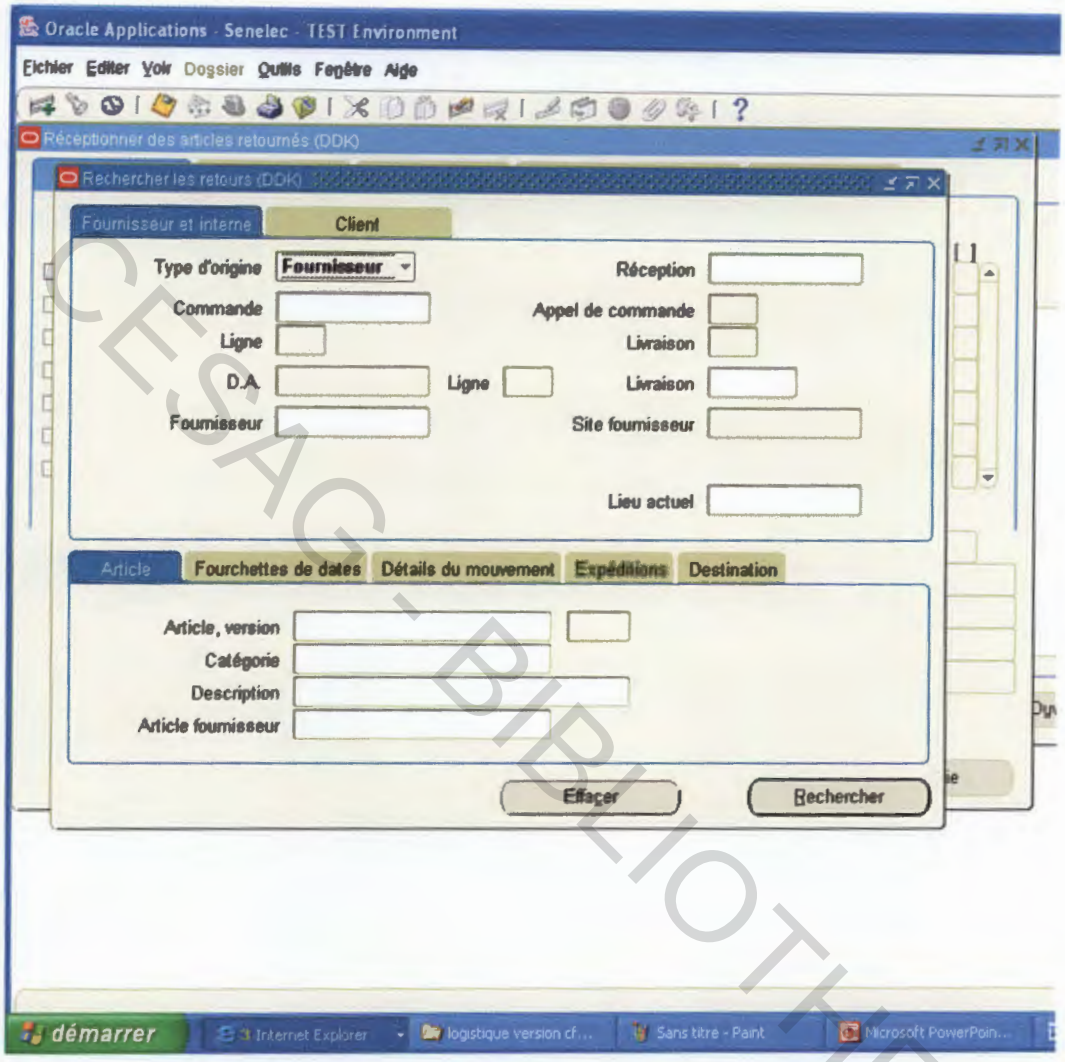
Annexe N°5: MENU PRINCIPAL ORACLE IC



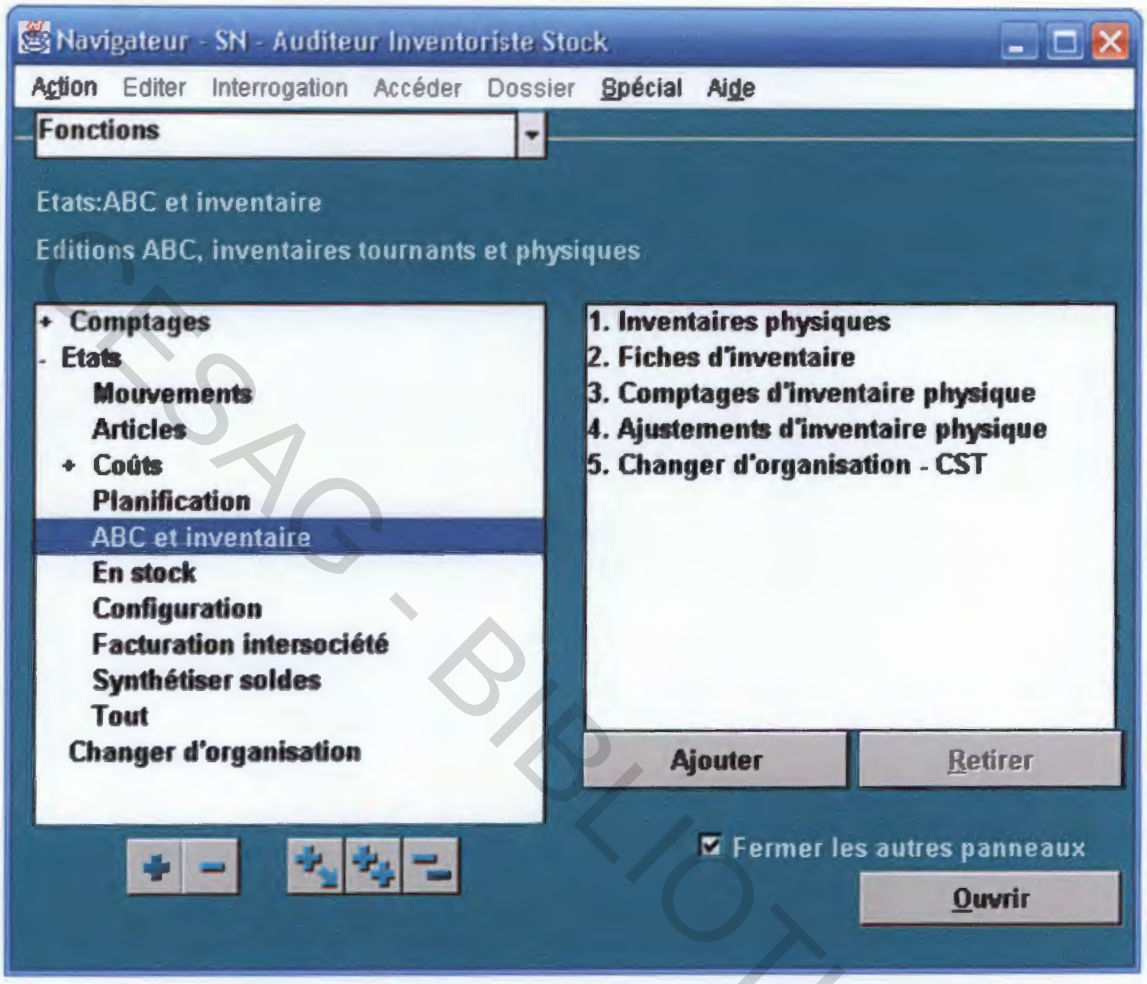
Annexe N°6: ORGANISATION DANS ORACLE IC



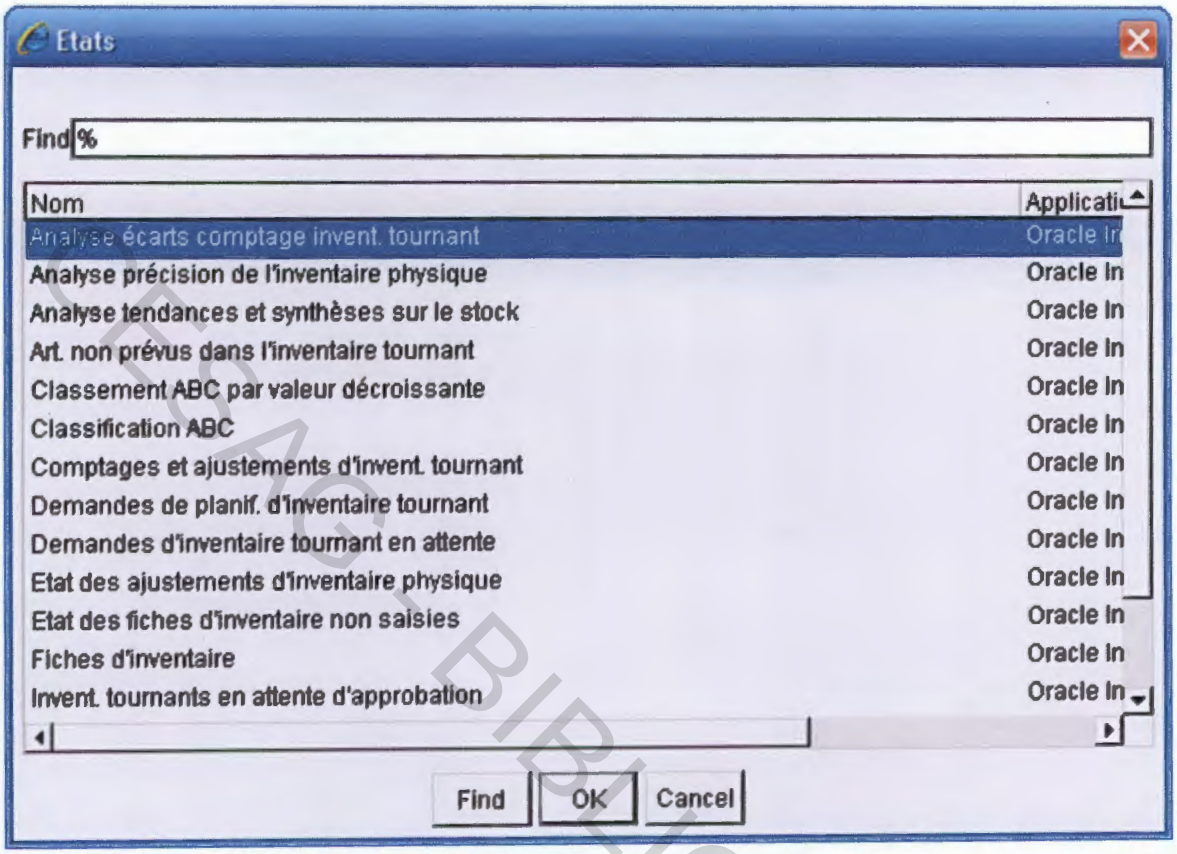
Annexe N°7: CONSULTATION ARTICLE DANS ORACLE IC



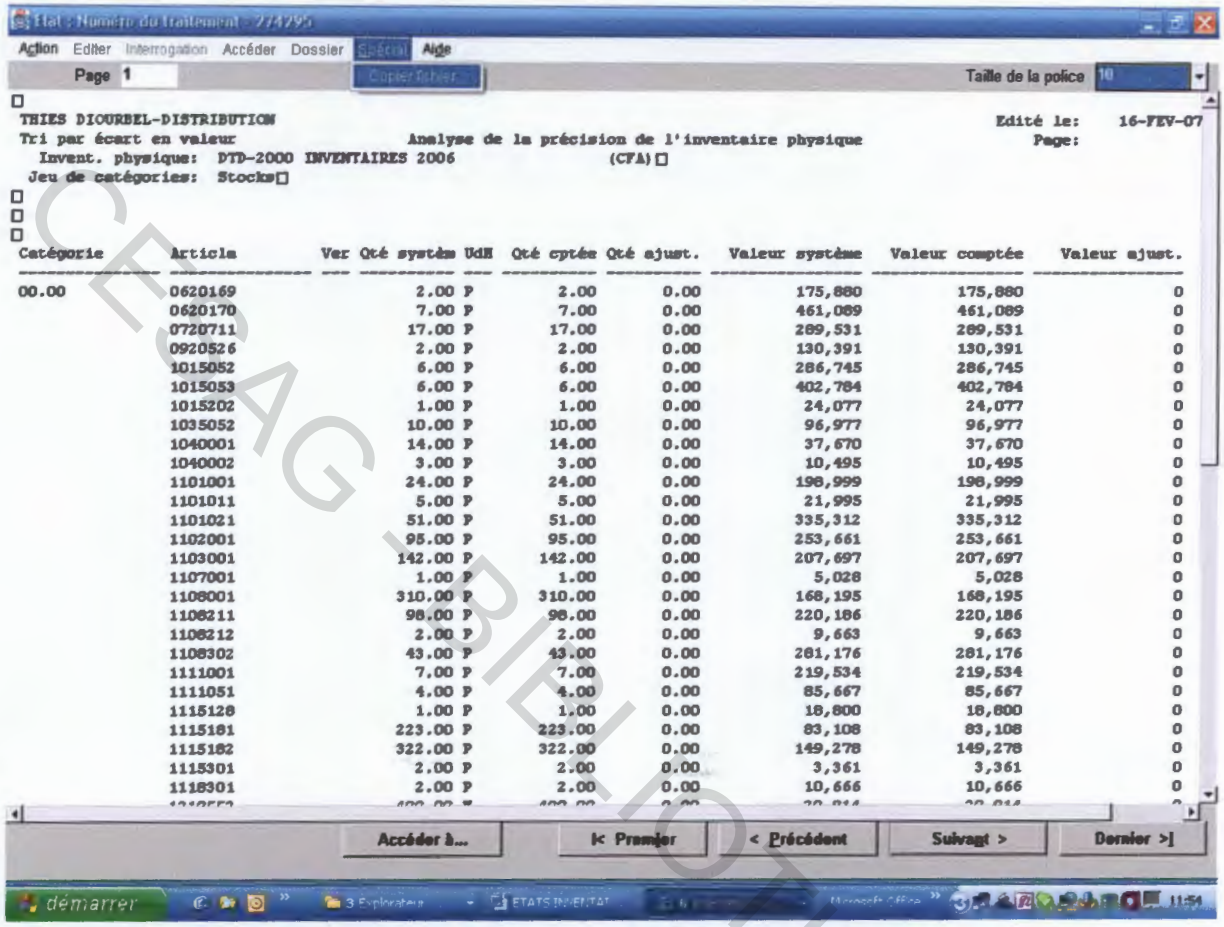
Annexe N°8: MENU INVENTAIRES DANS ORACLE IC



Annexe N°9: ANALYSE D'INVENTAIRE DANS ORACLE IC



Annexe N°10: ANALYSE DE PRECISION INVENTAIRE DANS ORACLE IC



Etat : Numéro de traitement : 274295

Action Editer Interrogation Accéder Dossier Spécial Aide

Page 1 Copier fichier Taille de la police 10

THIES DIOURBEL-DISTRIBUTION — Edité le: 16-FEV-07

Tri par écart en valeur — Analyse de la précision de l'inventaire physique — Page:

Invent. physique: DTD-2000 INVENTAIRES 2006 (CFA)

Jeu de catégories: Stocks

Catégorie	Article	Ver	Qté système	UdM	Qté cptée	Qté ajust.	Valeur système	Valeur comptée	Valeur ajust.
00.00	0620169		2.00	P	2.00	0.00	175,880	175,880	0
	0620170		7.00	P	7.00	0.00	461,089	461,089	0
	0720711		17.00	P	17.00	0.00	289,531	289,531	0
	0920526		2.00	P	2.00	0.00	130,391	130,391	0
	1015052		6.00	P	6.00	0.00	286,745	286,745	0
	1015053		6.00	P	6.00	0.00	402,784	402,784	0
	1015202		1.00	P	1.00	0.00	24,077	24,077	0
	1035052		10.00	P	10.00	0.00	96,977	96,977	0
	1040001		14.00	P	14.00	0.00	37,670	37,670	0
	1040002		3.00	P	3.00	0.00	10,495	10,495	0
	1101001		24.00	P	24.00	0.00	198,999	198,999	0
	1101011		5.00	P	5.00	0.00	21,995	21,995	0
	1101021		51.00	P	51.00	0.00	335,312	335,312	0
	1102001		95.00	P	95.00	0.00	253,661	253,661	0
	1103001		142.00	P	142.00	0.00	207,697	207,697	0
	1107001		1.00	P	1.00	0.00	5,028	5,028	0
	1108001		310.00	P	310.00	0.00	168,195	168,195	0
	1108211		98.00	P	98.00	0.00	220,186	220,186	0
	1108212		2.00	P	2.00	0.00	9,663	9,663	0
	1108302		43.00	P	43.00	0.00	281,176	281,176	0
	1111001		7.00	P	7.00	0.00	219,534	219,534	0
	1111051		4.00	P	4.00	0.00	85,667	85,667	0
	1115128		1.00	P	1.00	0.00	18,800	18,800	0
	1115181		223.00	P	223.00	0.00	83,108	83,108	0
	1115182		322.00	P	322.00	0.00	149,278	149,278	0
	1115301		2.00	P	2.00	0.00	3,361	3,361	0
	1118301		2.00	P	2.00	0.00	10,666	10,666	0

Accéder à... |< Premier < Précédent Suivant > Dernier >|

démarrer 3 Explorateur ETATS INVENTAI 11:54

BIBLIOGRAPHIE

Ouvrage :

- ANGOT Hugues, FISCHER Christian, THEUNISSEN Baudouin (2004), Audit comptable, Audit informatique, Boeck université, 3ème édition, P. 279
- ANGOT Hugues, FISCHER Christian, THEUNISSEN Baudouin (1994), Audit comptable, Audit informatique, Boeck université, P. 253
- A.T.H. (1986), JOCELYN Michel, Audit opérationnel : Guide pour l'audit opérationnel et des systèmes d'information, édition Clet, P. 273
- BARRY MAMADOU (2004), Audit et contrôle interne, Edition Sénégalaise de l'Imprimerie Dakar, (Pages 267)
- DERRIEN Yann (1992), Les techniques de l'audit informatique, édition Dunod, Paris, P. 238
- GILLET Michelle & Patrick (2008), Manuel et applications, Dunod, P. 431
- HANOUZ René, Paul de Kervasdoué & Philippe Rosé (2007), La pérennité du SI, Dunod, Paris, P. 191
- IFACI (1993), Audit et contrôle des systèmes d'informations, module 1 : Management de l'audit et du contrôle interne, IFACI, P. 110
- IFACI (1993), Audit et contrôle des systèmes d'informations, module 2 : Les outils informatiques de l'audit, IFACI, P. 129
- IFACI (1993), Audit et contrôle des systèmes d'informations, module 3 : Gestion des ressources informatiques, IFACI, P. 126
- IFACI (1993), Audit et contrôle des systèmes d'informations, module 8 : Sécurité, IFACI, P. 126
- KPMG (1998), Audit informatique, collection comptable, P. 316
- RAFFEGEAU J. & RITZ A. (1993), Audit et Informatique, 2 è éd., Presses Universitaires de France, Paris
- RENARD Jacques (2009), Théorie et pratique de l'audit interne, 7 e édition, Eyrolles, P. 463

- Solange Ghernaouti-Hélie (2008), Sécurité Informatique et Réseaux, 2 e édition, Dunod, Paris, P. 341
- THORIN Marc (2000), L'audit informatique, édition HERMES Science, P. 184
- le Guide Pratique d'audit des technologies de l'Information de l'IIA sur « l'audit des contrôles applicatifs les contrôles » de juillet 2007

Mémoire et Codex :

- BOA Jean-Yves (2006), L'audit informatique en entreprise : cas de l'ASECNA, P. 88
- MOUMOUNI Moussa Boubacar (2002), Audit d'une Application Informatique de Gestion Clientèle : Cas de la Société Nigérienne d'Electricité (NIGELEC), P. 164
- NGUESSAN David Parfait (2004), Audit informatique dans une entreprise pétrolière : OXYGAZ Sénégal, P. 108
- SARR Ababacar (2003), Audit informatique, codex, P. 63
- SOW N'gary (2003), Audit interne et procédures, codex, P. 130
- TALL Mamadou (2003), Audit de la sécurité informatique, codex, P. 100

Sites Internet :

- L'Association Française de l'Audit et du Conseil Informatiques (2009), COBIT V4 et Val IT, www.afai.asso.fr
- Portail de la sécurité de l'information (2009), Risques, www.cases.lu
- Club de la sécurité de l'Information Français (2009), Gestion des risques, www.clusif.asso.fr
- Le monde informatique (2009), Oracle-Sun : naissance d'un contrepoids à IBM, www.lemondeinformatique.fr

- SENELEC (2009), Historique et note de Direction, http://intranet.electricite.sn/C5/Directions%202009/default.aspx