CESAG

Centre Africain d'études Supérieures en Gestion

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

Master Professionnel en Audit et Contrôle de Gestion (MPACG)

Promotion 4
2010-2012

Mémoire de fin d'étude

THEME

AUDIT D'UNE APPLICATION INFORMATIQUE DECENTRALISEE DE GESTION DES ENCAISSEMENTS: CAS DU SYTRIIS A LA SENELEC

Présenté par :

M. Bilyce Abel Angenor BAILLET

Dirigé par :

M. Alain SAWADOGO
PROFESSEUR ASSOCIE
CESAG

Avril 2012

DEDICACES

Je dédie ce mémoire à :

- mon père Monsieur BAILLET Benoît Sévérin, et ;
- toute ma famille ;

Pour les sacrifices consentis, la patience et les encouragements à mon endroit.
Qu'ils trouvent dans ce modeste travail l'aboutissement de leurs nombreux efforts.

PUISSE DIEU LES BENIR

REMERCIEMENTS

Je souhaite témoigner ma profonde gratitude et mes remerciements les plus sincères à mon directeur de mémoire **Monsieur SAWADOGO Alain** pour ses conseils et le temps qu'il m'a accordé pour la réalisation de ce rapport.

J'adresse également mes remerciements au **Directeur Général de la Société Nationale d'Electricité (SENELEC)** et ses plus proches collaborateurs, particulièrement à **Madame DIALLO Safietou et Monsieur NDOYE Mactar Chef du Département Audit Interne et Organisation**, pour les documents qu'ils m'ont fournis, nécessaires à la rédaction du présent mémoire. Ce travail est l'accomplissement d'une partie de mon rêve le plus lointain.

Au personnel de cette entreprise, je leur adresse tous mes remerciements pour l'accueil chaleureux, le soutien indéfectible tout au long de ce stage et les multiples conseils qui m'ont été donnés, enfin, la disponibilité totale dont ils ont fait montre pour répondre à toutes mes attentes.

Enfin, je remercie le corps professoral et administratif du CESAG pour le service rendu, et plus particulièrement **Monsieur YAZI Moussa Directeur de l'Institut Supérieur de Comptabilité, de Banque et de Finance** qui m'a été d'un soutien considérable dans la réalisation du présent rapport de fin d'études.

Soyez tous bénis.

LISTE DES SIGLES ET ABREVIATIONS

AC :	Application Controls
ACISSI :	Audit, Conseil, Installation et Sécurisation des Systèmes d'Information
AFAI :	Association Française de l'Audit et du conseil Informatiques
ANSSI :	Angence Nationale de la Sécurité des Systèmes d'Information
CAAT :	Computer-Assisted Audit Technique
CLUSIF :	Club de la Sécurité de l'Information Française
CMMI :	Capability Maturity Model Integration
COBIT :	Control Objectives for Information and related Technology
ERP :	Enterprise Resource Planning
FRAP :	Feuilles de Révélation et d'Analyse des Problèmes
GTAG :	Global Technology Audit Guide
IFACI :	Institut Français de l'Audit et du Contrôle Interne
IIA :	Institute of Internal Auditors
ISACA :	Information Systems Audit and Control Association
IT :	Information Technology
ITIL :	Information Technology Infrastructure Library
PC :	Personnal Computer
RSSI :	Responsable de la Sécurité du Système d'Information
SENELEC :	Société Nationale d'Electricité du Sénégal
SIC :	Système d'Information Clientèle
SMI :	Société de Marketing Industriel
SYTRIIS :	SYstème de Transfert d'Information Inter-Site
USB :	Universal Serial Bus

LISTE DES TABLEAUX ET FIGURES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ANNEXES

TABLE DES MATIERES

INTRODUCTION GENERALE

A l'heure du changement climatique et de la raréfaction des ressources énergétiques fossiles, les pouvoirs publics comme les investisseurs ont intérêt à déterminer quelles sources d'énergie seront les plus efficaces et les plus fiables pour soutenir la croissance à l'avenir. Dans cette perspective, de grands bouleversements s'annoncent. D'après l'Agence internationale de l'énergie, la majeure partie des infrastructures énergétiques qui existent aujourd'hui dans le monde devront être remplacées d'ici 2030 (World Energy Outlook, 2008 : 39).

De manière générale, on prévoit que les investissements annuels dans la production d'électricité renouvelable dépasseront les investissements dans les centrales à combustibles fossiles au cours de la période 2007-2030 (World Energy Outlook, 2008). Ainsi, en 2008, les investissements dans la production d'électricité à partir de ressources renouvelables ont considérablement augmenté. Les énergies renouvelables gagnant du terrain, les pouvoirs publics des pays d'Afrique pourraient prendre des mesures pour stimuler l'investissement dans ce seeteur et accroître les transferts de technologies propices à l'essor de ces formes d'énergies.

La stabilité des approvisionnements énergétiques est essentielle à une croissance économique soutenue et à la réduction de la pauvreté. Les énergies renouvelables sont abondantes et diversifiées, et elles ont pour avantage de diminuer la dépendance à l'égard des ressources finies ou importées. Elles comprennent notamment, mais pas uniquement, la biomasse, l'énergie solaire, l'énergie éolienne, l'hydroélectricité, l'énergie marémotrice et la géothermie. Elles renforcent la sécurité énergétique, en particulier dans les pays qui ne produisent pas de pétrole, créent des emplois et contribuent à la lutte contre la pauvreté en améliorant l'accès à l'énergie, notamment dans le cas des populations rurales ou isolées. Qui plus est, le marché des technologies énergétiques non polluantes est rentable.

Le secteur énergétique d'Afrique subsaharienne est aujourd'hui en situation de crise : sa capacité de production insuffisante, approvisionnement irrégulier, prix très élevés et accès au réseau électrique très limités. Caractérisée par la stagnation, la capacité de production énergétique de la région est inférieure à celle des autres régions. L'énergie africaine coûte deux fois plus que celle des autres régions en développement, et son approvisionnement n'est pas fiable. Dans plusieurs pays, la croissance des connexions des ménages au réseau électrique est inférieure à la croissance de la population, avec pour résultat que le taux d'électrification, déjà faible, est actuellement en déclin. Les manifestations de la crise actuelle sont les symptômes de problèmes plus profonds.

Par contre, pour ce qui est de l'électricité, l'Afrique de l'Ouest et l'Afrique subsaharienne en général sont très en retard comparée aux autres parties du monde. Elle produit très peu d'électricité et surtout, ne consomme pas assez d'électricité par rapport à ses besoins réels. Les

sociétés de distribution n'ont d'autres choix que les délestages pour pallier ce déficit de production énergétique. De même les réseaux électriques sont loin d'être à la hauteur des besoins des populations. Aujourd'hui, les délestages font partie de la vie des habitants des grandes agglomérations ouest-africaines et aucun pays ouest-africain n'échappe à ce phénomène.

Une société d'électricité est en relation directe avec sa clientèle. Les liens se nouent directement dans les agences, pour cela, il faut une gestion de qualité pour conserver sa clientèle. La gestion de qualité est devenue essentielle pour la survie des entreprises. Ces dernières cherchent plus d'innovations, d'efficience et de réactivité. Pour ce faire, il est nécessaire de s'ouvrir aux technologies de l'information et de la communication.

De nos jours, on peut affirmer, sans risque de se tromper, que la majorité des sociétés intègrent les IT (matériels informatiques, logiciel ou progiciel de gestion, internet, etc.) dans la gestion courante de leurs activités afin d'être plus performantes. Les technologies de l'information et de la communication, bien que bénéfique, exposent les organisations à de nombreux risques, auxquels le management doit faire face.

La mise en place d'un service d'audite interne pour certains ou la sous-traitance avec des cabinets d'audit externe pour d'autres, se présente comme une des réponses à ces besoins, car elle permet de maîtriser la qualité des processus métiers et des flux de traitement des données s'y rapportant.

Aujourd'hui, l'audit des états financiers d'une entreprise représente pour les auditeurs financiers un nombre de défis de plus en plus grand ; d'un côté l'évolution rapide des normes comptables et de l'autre l'automatisation croissante de la préparation des états financiers au moyen de systèmes d'informations toujours plus complexes. Il est donc logique que l'auditeur concentre son travail sur ces processus métiers et intègre le contrôle des applications correspondantes dans son approche d'audit.

La Société Nationale d'Electricité du Sénégal (SENELEC) n'a pas dérogé à cette règle. Depuis 2004, elle utilise une application de gestion du nom de SYTRIIS (système de transfert inter-site). En effet, le SYTRIIS est une application informatique de gestion implantée dans les différentes agences de la SENELEC à travers le pays afin de décentraliser les encaissements des factures et de venir en support au système de base vétuste.

Mais, lors de son implantation, la validation des modules n'a pas été auditée par le service d'audit, car ce dernier manquait de connaissances, de savoir-faire et de compétences nécessaires en son sein pour réaliser de tels contrôles. Actuellement, les commerciales (utilisateurs) rencontrent quelques difficultés en utilisant cette application, d'où notre intérêt pour ce sujet et le choix de ce thème.

En effet, l'application n'arrive souvent pas à apurer les caisses et effectuer leur déversement dans le système de base (SIC). Cela est dû soit à des défauts de conception (programmation), soit à la qualité du réseau (internet/intranet). Mais aussi à un manque de formation des agents, qui non seulement sont habitués à l'ancien système, mais également ont du mal à s'adapter à la nouvelle application.

Cette situation a pour conséquence immédiate l'arrêt des travaux qui peut aller d'une à trois journées, en fonction de la situation géographique de l'agence. Certains agents refusent carrément d'utiliser le SYTRIIS au profit du SIC vétuste, donc lent. L'activité d'encaissement se trouve donc ralentie, ce qui entraine des pertes financières et de temps à la société. En outre, les clients de la SENELEC sont mécontents de la qualité des services rendus.

Pour pallier ce problème, les informaticiens, en ce qui concerne l'aspect technique, corrigeaient les insuffisances au jour le jour. Il fallait attendre qu'un problème survienne pour le corriger au fur et à mesure (à titre correctif). L'entreprise avait également la possibilité d'acquérir un logiciel déjà existant et le configurer, mais le coût du renouvellement de la licence est très élevé (d'où le développement d'une application à l'interne). En outre, la SENELEC a recours à des audits externes et internes pour résoudre certains problèmes (audit comptable et financier, etc.), mais ces audits ne se penchaient pas spécifiquement sur l'aspect informatique qui soutient l'ensemble du processus métier.

L'audit en tant que levier de performance de l'organisation, doit s'imprégner des techniques d'audit informatique pour mieux contribuer à la création de valeurs dans un environnement de plus en plus informatisé. Les auditeurs internes de la SENELEC, lors de leurs différentes missions, doivent faire de l'audit des applications informatiques une de leurs priorités et l'intégrer dans leur plan d'audit.

Une question se pose à nous : comment réaliser un audit d'une application informatique de gestion ?

Pour mieux cerner le contour de cette interrogation, il est nécessaire de savoir :

- quel est l'intérêt d'un contrôle des applications informatiques pour la SENELEC ?
- quels sont les risques inhérents à l'utilisation d'une application de gestion comme le SYTRIIS ?
- quels sont les dispositifs de sécurité à mettre en place pour limiter l'impact de ces risques ?

- quels sont les référentiels à la disposition des auditeurs internes de la SENELEC pour leur permettre de réaliser l'audit du SYTRIIS ?
- quelle démarche suivre pour réaliser un tel audit ?

L'audit d'une application informatique décentralisée de gestion des encaissements nous permettra de répondre à ces questions. Notre étude allant dans ce sens, il s'agit dans le cadre de ce mémoire, de proposer une démarche d'audit des applications informatiques de gestion qui sera appliquée par le service d'audit interne.

L'objectif de notre étude est d'intégrer dans le fonctionnement du département d'audit interne de la SENELEC une dimension audit informatique en vue de le rendre pertinent et efficace dans la résolution des différents problèmes liés aux applications informatiques et aux technologies de l'information et de la communication en général.

Pour atteindre cet objectif, il nous faudra :

- identifier les risques inhérents aux applications informatiques ;
- répertorier les dispositifs et bonnes pratiques à mettre en œuvre pour circonscrire/maîtriser ces risques, et ;
- proposer une démarche d'audit ainsi que des référentiels à utiliser.

L'audit d'une application informatique qui a pour mission d'apprécier une application en production, couvre un large champ à savoir: 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. Mais aussi l'appréciation de la sécurité de l'infrastructure informatique nécessaire au bon fonctionnement de l'application.

Cependant, nous limiterons notre étude à l'appréciation des données opérationnelles, à la gestion des droits d'accès et enfin à la sécurité de l'infrastructure informatique nécessaire au fonctionnement de l'application.

L'intérêt d'une telle étude pour l'entreprise est de lui permettre d'évaluer et de situer sa maîtrise des risques des applications informatiques de gestion, lui proposer des dispositifs pour circonscrire les risques et proposer, au département de l'audit interne, une démarche pour le rendre apte à mener une mission d'audit informatique.

En ce qui nous concerne, ce sera pour nous l'opportunité de nous familiariser avec la notion d'application informatique de gestion, d'acquérir les connaissances, le savoir-faire et les compétences nécessaires pour réaliser une mission d'audit informatique. Cette étude est le point culminant de notre formation de deux (02) ans.

Ce thème sera traité en deux grandes parties :

- la première concernera les aspects théoriques de l'audit des applications informatiques de gestion qui comprend trois (03) chapitres à savoir : le système informatique et la sécurité, ensuite l'audit des applications informatiques de gestion et enfin la méthodologie de l'étude, et ;
- la seconde partie abordera l'aspect pratique qui se compose de trois (03) chapitres : la présentation de la SENELEC, la description du système informatique et de l'application SYRIIS et enfin la présentation des résultats, de leur analyse et les recommandations.

PREMIERE PARTIE : CADRE THEORIQUE

Introduction

Le système d'information est l'un des domaines de l'entreprise devant bénéficier d'une gestion de sécurité optimale. La montée en puissance de la cybercriminalité, les menaces de l'environnement internes et externes font peser des risques sur ce système stratégique pour l'entreprise. En effet, du fait de sa particularité de dispositif transversal, l'impact éventuel des risques qui l'affectent se répercute dans toute l'organisation. Sa sécurité doit être mise en œuvre de façon pointilleuse, et être évaluée régulièrement.

L'évaluation du système informatique en général, et de ses applications en particulier, implique de s'assurer que les procédures et les dispositifs de sécurité mis en place sont efficaces, et qu'ils sont en adéquation avec les normes et les référentiels de bonnes pratiques. Il s'agit de procéder à un audit.

Ainsi, nous consacrerons cette partie au système informatique et à la sécurité, puis à l'audit des applications informatiques de gestion et nous terminerons par notre méthodologie de travail.

CHAPITRE 1 : LE SYSTEME INFORMATIQUE ET LA SECURITE.

Introduction

Les entreprises modernes dépendent aujourd'hui, pour l'atteinte de leurs objectifs, de l'outil informatique. Quelques fois, le même ensemble prend le nom de système d'information. Il s'agit là de deux notions connexes que nous allons décrire pour mieux en cerner la nuance. Nous allons ensuite présenter les risques pouvant affecter ce système puis nous terminerons ce chapitre par la description des dispositifs relatifs à la sécurité de ces outils.

1.1 Description d'un système informatique

Selon GRAEVE & POTIER (2001 : 3), « le système d'information peut être considéré comme la moelle épinière de l'entreprise, de même que le système de pilotage en est le cerveau et que le système opérant en est les membres ». Nous pouvons donc affirmer dans ce cas que le système informatique en est la colonne vertébrale, car il est le support du système d'information.

1.1.1. Le système informatique comme support du système d'information.

Pour DAYAN & al. (2004), le système d'information ne se réduit pas au système informatique. En effet, dans l'esprit de nombreuses personnes s'est installée une confusion entre système d'information et système informatique. L'informatique reste un support et un véhicule privilégié de l'information formalisée. Elle est un moyen et seulement un moyen parmi d'autres.

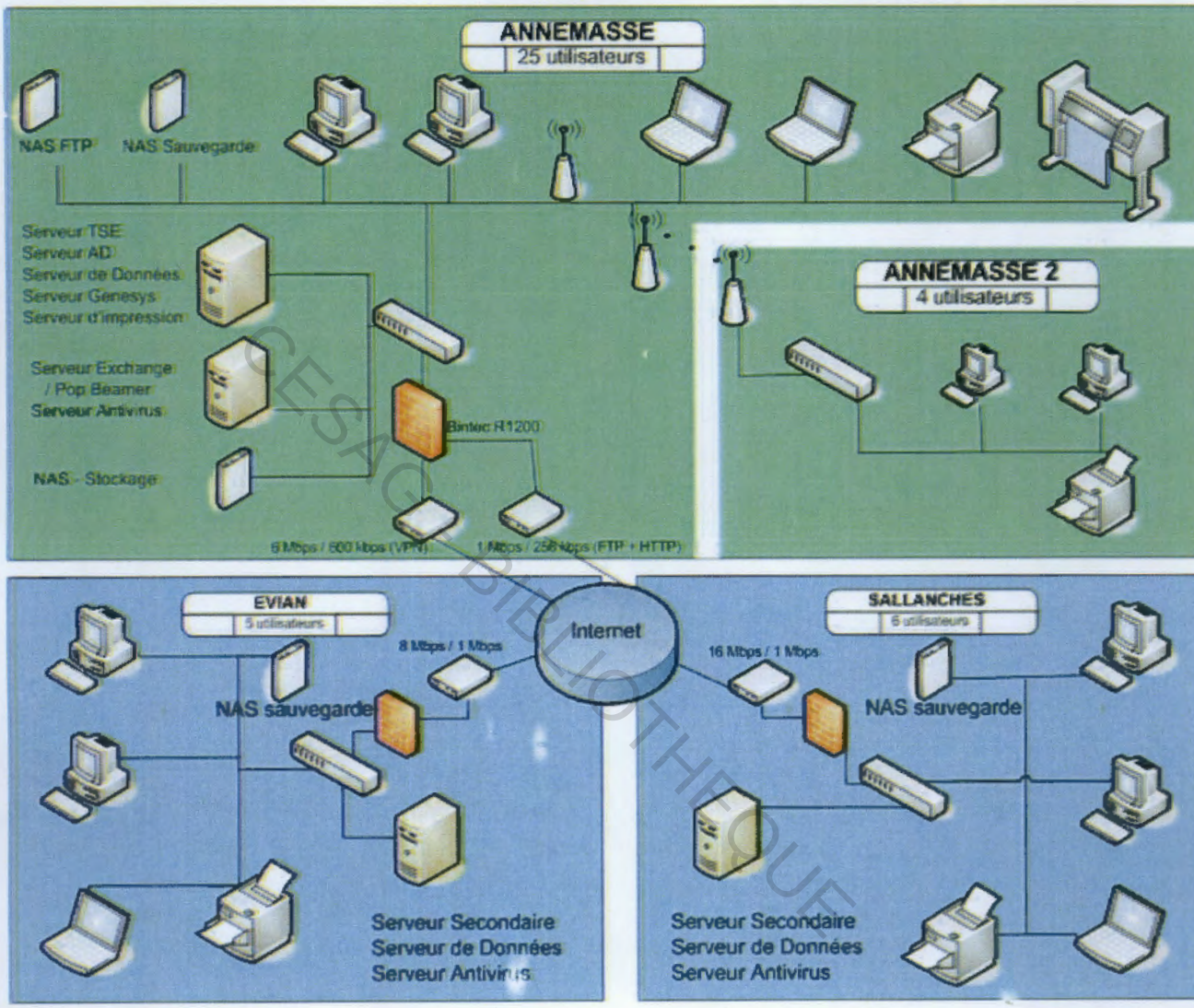
Selon LAUDON & al. (2002), bien que les systèmes d'information informatisés se fondent sur la technologie informatique pour traiter des données brutes et les transformer en informations ayant une signification, il faut bien distinguer un ordinateur et un logiciel, d'une part, et un système d'information d'autre part. Les ordinateurs et les logiciels connexes constituent le fondement technique, les outils et le matériel nécessaire pour stocker l'information et pour la traiter. Tandis qu'un système d'information est un ensemble organisé de ressources : matériel, logiciel, personnel, données, procédures...permettant d'acquérir, de traiter, de stocker des informations dans les organisations (REIX, 2005 : 1-5).

1.1.2. Architecture d'un système informatique.

Selon DAYAN & al. (2004 : 1075), « le système informatique est le support technique du système d'information de l'entreprise. Cela regroupe les moyens informatiques (serveurs et poste utilisateurs) et les moyens de communication (réseau) ».

Il faut retenir que le système informatique regroupe les postes de travail, les supports de stockage, les serveurs et les réseaux sans lesquels cet ensemble serait inopérant. La figure ci-après nous donne une vue de ces différents composants en réseau.

Figure 1 : Exemple d'éléments constitutifs d'un système informatique.



Source : PSI-INFORMATIQUE (2012).

Au vu de la figure 1, le système informatique est composé d'éléments divers, y compris les logiciels qui n'apparaissent pas sur le schéma. On a :

- **les serveurs :** selon YADAV & SINGH (2009 :36), un serveur est à la fois un ensemble de logiciels et d'ordinateur les hébergeant dont le rôle est de répondre de manière automatique à des demandes envoyées par des clients (ordinateur et logiciel) via le réseau. Les utilisateurs courants des serveurs sont le serveur de fichiers, d'impression, de base de

données, de courrier, ainsi que le serveur Web, le serveur d'applications, le proxy et le serveur de jeu ;

- **les postes utilisateurs ou ordinateurs :** ce sont les ordinateurs de bureau et leurs périphériques d'entrée/sortie, les ordinateurs portables, les ordinateurs de poches, les tablettes et les Smartphones qui permettent de ce connecter de n'importe quel lieu où une connexion réseau est disponible (DAYAN & al, 2004) ;
- **les équipements électroniques :** selon CARPENTIER (2009), c'est l'ensemble constitué par tous les appareils électroniques qui peuvent être intégrés au système informatique. Il s'agit principalement des imprimantes, des scanners, des vidéoprojecteurs, des appareils fax, des téléphones, des photocopieurs, des caméras numériques, des clés USB, des lecteurs MP3, des disques durs externes… ;
- **l'infrastructure réseau :** l'infrastructure réseau ou supports peuvent être des câbles dans lesquels circulent des signaux électriques, l'atmosphère (ou le vide spatial) où circulent des ondes radio, ou des fibres optiques qui propagent des ondes lumineuses, des modems et des antennes réseau. Elles permettent de relier « physiquement » des équipements assurant l'interconnexion des moyens physiques (YADAV & SINGH, 2009). Les équipements d'un réseau sont connectés directement ou non entre eux par des commutateurs (Switch), des concentreurs (hub) ou des routeurs (LAUDON & al, 2000) ;
- **la salle informatique ou data center :** selon la Société de Marketing Industriel (SMI, 2010) et YADAV & SINGH (2009), cette salle héberge tous les équipements spécialisés, nécessaires à la fourniture des ressources informatiques. On y trouve les serveurs, les calculateurs, les solutions de sauvegarde et de restauration des données, les baies de stockage, etc. dans la plupart des sociétés de taille moyenne, cette salle contient également les éléments critiques du réseau (commutateurs, routeurs…) ainsi que les points d'accès et équipements servant à connecter la société vers le monde extérieur (central téléphonique, accès internet…).

1.2 Les applications informatiques.

Il existe plusieurs manières de classer les applications informatiques. Nous retiendrons la classification de l'Association Française de l'Audit et du Conseil Informatiques (AFAI). Compte tenu de leurs profils de risque très différents, les types de programmes sont une caractéristique importante pour la planification et la réalisation de l'audit et doivent donc être documentés. Selon l'AFAI (2008), on distingue : les applications standards, les applications standards fortement adaptées et les développements internes :

- **les applications standards :** ce sont souvent des logiciels, utilisés ou vendus, qui ont été développés pour un nombre important d'entreprises et généralement vendus plusieurs fois. Les applications standard typiques sont, par exemple, des logiciels métiers spécifiques à des secteurs d'activité, des logiciels multifonctions tels que les logiciels bureautiques, les logiciels spécialisés tels que les systèmes de gestion intégrée ERP, les systèmes de gestion de marchandises et des inventaires, etc. L'avantage de ce genre d'application, du point de vue du contrôle interne, est qu'un grand nombre de développeurs et de clients travaillent sur l'application et donc contribuent à son amélioration permanente (conception, développement, test et documentation). Les applications standards au bénéfice d'une certaine maturité présentent généralement une multitude de contrôles intégrés pertinents ;
- **les applications standards fortement adaptées :** ce sont des progiciels dont le but principal est de mettre à disposition des fonctionnalités de base et des outils de création de processus, et dont le paramétrage permet la mise en place de solutions spécifiques qui répondent aux besoins de l'entreprise. L'auditeur est ici confronté à un grand défi dans la mesure où, même s'il dispose d'informations sur la fiabilité des composants des applications et systèmes éprouvés, il n'en a pas sur l'interaction de ces composants avec les éventuelles configurations et programmations supplémentaires dans l'environnement spécifique du client. En pareilles situations, l'auditeur devra prévoir davantage de temps pour l'identification des risques et l'évaluation des contrôles pertinents ;
- **les développements internes ou les applications dédiées :** ce sont des applications développées sur mesure pour une entreprise donnée ou pour répondre à un besoin spécifique (en interne ou à des entreprises tierces). En comparaison avec les applications standards, le logiciel dédié présente souvent plusieurs problèmes (développeurs moins qualifiés, solutions inabouties, etc.). Dans ce cas, l'auditeur n'est pas en mesure de s'appuyer sur les informations et les expériences généralement connues et doit adapter sa procédure d'audit à l'application concernée. Les applications développées en interne exigent généralement un travail de vérification plus important. En pareilles situations, la collaboration entre l'auditeur, le responsable de l'application et, le cas échéant, le développeur de l'application revêt une grande importance.

1.3 Les risques informatiques

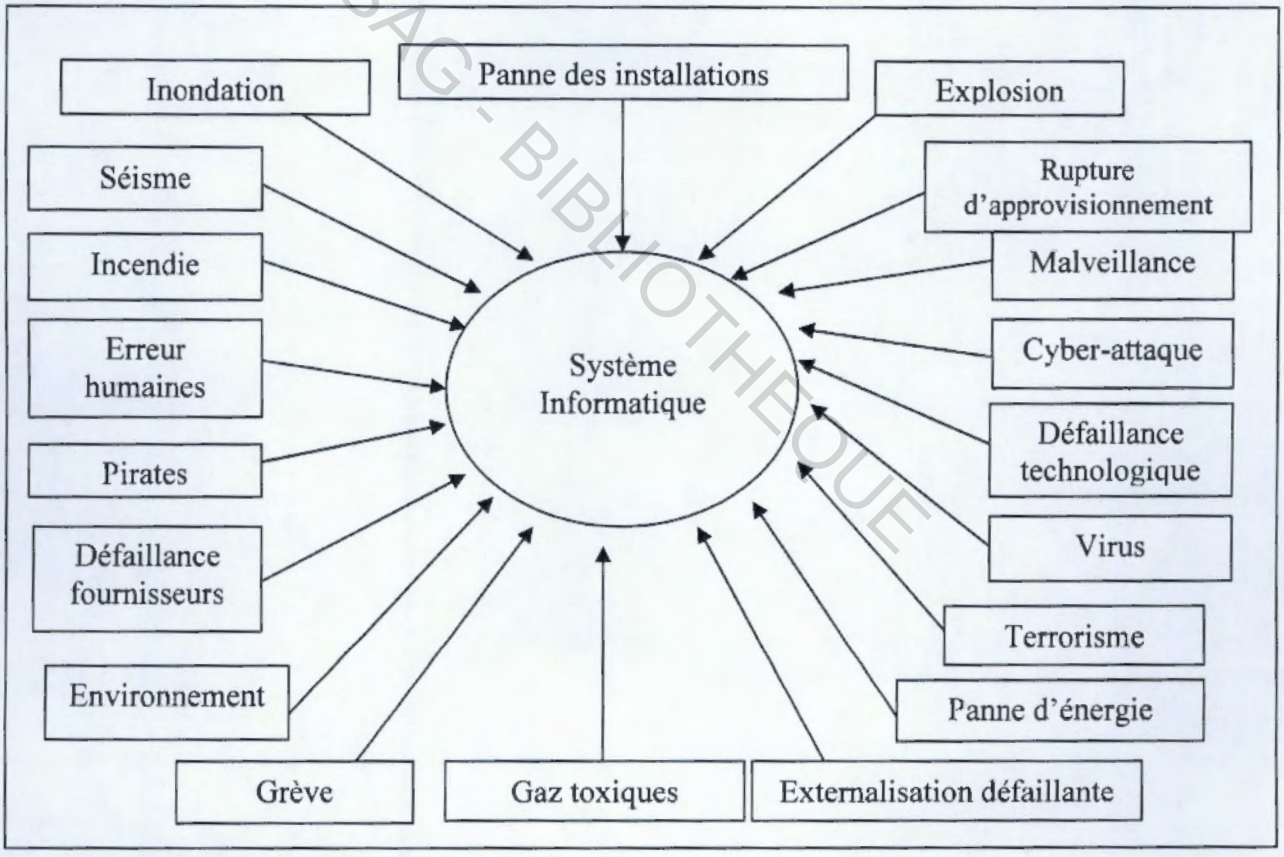
Tous les systèmes d'informations, quelles que soient leurs tailles, leurs structures, contiennent des failles. Nous définirons donc la notion de risque et nous présenterons les risques informatiques.

1.3.1. Définition du risque

Le risque opérationnel défini par le « nouvel accord de Bâle » est le risque de perte directe résultant d'une inadéquation ou d'une défaillance attribuable à des personnes, des procédures, des systèmes mis en place et à des évènements extérieurs. Selon l'IFACI (RENARD, 2010 : 155), « le risque est un ensemble d'aléas susceptibles d'avoir des conséquences négatives sur une entité et dont le contrôle interne et l'audit ont notamment pour mission d'assurer autant que faire se peut la maîtrise ».

Pour HAMZAOUI (2005 : 37), « le risque est un concept selon lequel la direction exprime ses inquiétudes concernant les effets probables d'un évènement sur les objectifs de l'entité dans un environnement incertain ».

Figure 2 : les risques inhérents du système informatique de l'entreprise.



Source : Nous même, à partir de DUGELAY (2003 : 17)

Comme nous le voyons sur la figure 2, les risques propres au système informatique ou risques inhérents sont d'une part les risques physiques, qui affectent le matériel informatique et d'autre part les risques logiques qui eux sont relatifs à la partie immatérielle du système informatique

(logiciels, données…), et ceci sans tenir compte du contrôle interne qui pourrait exister dans l'entité. Ces risques sont les suivants :

1.3.2. Les risques physiques et environnementaux.

Selon GODARD (2002) & ACISSI (2009), sans être exhaustif, les plus envisageables sont : les dégâts des eaux, le feu, l'électricité, les défauts de climatisation, les intrusions physiques et les phénomènes électrostatiques…il existe plusieurs modes de classification des risques informatiques. Nous retenons pour la présentation des risques physiques la nomenclature qui distingue les risques humains, environnementaux, électriques et les sinistres (CALE & TOUTTOU, 2007) :

- **les risques humains :** selon CARPENTIER (2009), la circulation des personnes non autorisées dans les locaux peut entraîner divers incidents : vols, pertes de confidentialité, sabotages, etc., avec des conséquences aisément imaginables (pertes de temps, pertes financières, pertes de réputation, indisponibilité du système informatique, etc.). La menace d'une attaque terroriste sur des sites stratégiques est hélas d'actualité. Elle entrainerait la destruction de l'infrastructure technologique ;
- **les risques environnementaux :** ici il s'agit des fluctuations de température, de l'hygrométrie et de la poussière. Ces éléments peuvent entraimer des incidents techniques de nature à ralentir l'activité. La survenance d'un tremblement de terre est une éventualité qui pourrait gravement affecter le système informatique du fait de la destruction des bâtiments et de la rupture des câblages (CLEUET & al, 2008b) ;
- **les risques électriques :** selon ROYER (2004), les risques liés à l'électricité proviennent surtout de : surtension, sous-tension, coupures de courant. Malgré la qualité du fournisseur, ces incidents sont difficilement prévisibles et ont un impact sur le système informatique (pertes de données, pannes d'équipements, etc.). La foudre peut être également être classée dans cette catégorie ;
- **les sinistres :** les sinistres sont principalement dus à l'eau et au feu :
    - pour l'eau, il s'agit de : rupture de conduite, infiltration, déclenchement de système anti-incendie, obstruction des évacuations d'eaux usagées, inondation…les causes sont nombreuses, tout comme les conséquences : courts-circuits, dangers d'électrocution, détérioration des équipements, corrosion des câbles et connecteurs (GODART, 2002) ;
    - les dégâts du feu peuvent entraîner la destruction partielle ou totale des équipements informatiques (centre informatique, câblage, atteinte physique aux équipements informatiques, etc.) et donc l'indisponibilité de tout ou partie de l'architecture durant une assez longue période. A noter qu'ils s'accompagnent

souvent des dégâts liés à l'eau du fait des tentatives d'extinction (CARPENTIER, 2009 et CLEUET & al, 2008b).

1.3.3. Les risques logiques.

Ce sont les risques qui affectent les personnes (social engineering), les logiciels, les données et les informations du système informatique. Ils sont le fait soit de personnes internes à l'organisation, soit le fait de personnes externes à travers les réseaux (internet, Wifi…). Selon CALE & TOUTTOU (2007) et ROYER (2004), l'être humain est le maillon le plus faible du système d'information. Il représente ainsi la plus grande menace pour la sécurité informatique. L'ignorance des menaces et des techniques des cybercriminels est un facteur aggravant des risques informatiques.

De nouvelles menaces apparaissent chaque jour. Nous allons présenter les risques les plus significatifs. On a :

- **les malwares :** selon ACISSI (2009) et CALE & TOUTTOU (2007), les malwares sont des programmes malveillants qui sont utilisés par les pirates pour commettre leurs forfaits. Ils sont de plusieurs types :
  - le « virus informatique » comme son équivalent biologique, s'installe au sein des programmes légitimes pour se reproduire et contaminer le plus de fichiers possible et ensuite déclenche l'action pour laquelle il a été crée ;
  - le « ver informatique » est différent du virus en ce sens qu'il est un programme autonome qui ce déplace dans les réseaux informatiques grâce à une faculté d'auto-duplication ;
  - le « cheval de Troie » est un logiciel se présentant sur une apparence bénigne (utilitaire, jeu, etc.), mais il recèle en son sein des fonctionnalités cachées lui permettant d'effectuer en toute discrétion du vol de fichiers, de la destruction de données, l'établissement d'une connexion à travers un pare-feu. Il permet à son concepteur de faire du chantage, de l'espionnage industriel et commercial, des détournements de fonds, prise de contrôle à distance, etc. ;
  - le « back door » est une fonctionnalité cachée incluse dans un logiciel ou système d'exploitation par un développeur ou un cheval de Troie qui permet à son concepteur d'avoir accès à certaines fonctions sans passer par le processus d'authentification (session utilisateur et mot de passe) ;
  - les « logiciels espions » permettent de voler des informations ou d'effectuer des tâches à l'insu de l'utilisateur un peu comme les chevaux de Troie. Il en existe de

plusieurs sortes (le spyware, le keylogger ou enregistreur de touche, l'adware, le rookit ou « kit de démarrage », le dialer, etc.) ;

- **les spam :** selon ACISSI (2009), le spam encore appelé pourriel, désigne l'envoi massif de courriers publicitaires dans les boîtes aux lettres électroniques à des personnes ne souhaitant pas recevoir ce type d'information. Il est de plus en plus utilisé pour effectuer de « *social ingeenering* » (technique que nous décrirons plus loin) ;
- **les facteurs humains :** selon ACISSI (2009), CALLE & TOUTTOU (2007) et GODART (2002), il s'agit ici :
    - des erreurs humaines commises par les informaticiens qui peuvent être lourdes de conséquence. Ces erreurs sont notamment des erreurs de conception, des erreurs de programmation, des erreurs de configuration ou des erreurs par négligence ;
    - du *social engeenering* ou ingénierie social qui consiste à exploiter la confiance humaine pour obtenir des informations (numéros de téléphone, organigramme, mot de passe, etc.) qui serviront à mener des attaques ou à faire effectuer certaines actions par les victimes en se faisant passer pour quelqu'un d'autre (service sécurité, administrateur système, etc.) ;
    - du *phishing* ou hameçonnage qui est une technique qui consiste à créer une réplique presque 100% parfait d'un site Web qui entreprend subrepticement d'extorquer à des utilisateurs leurs données d'accès personnelles (nom d'utilisateur, mot de passe, code PIN, etc.) au moyen d'un formulaire présenté sur le site Web contrefait ;
- **les atteintes à la disponibilité ou déni de service :** le déni de service est un type d'attaque qui a pour but de rendre indisponible un service ou d'en détériorer la qualité afin de l'empêcher de répondre aux demandes légitimes. Cette technique permet à son auteur de na pas rentrer par effraction dans le système cible, il utilise des canaux de communications généralement ouverts (ROYER, 2004) ;
- **les compromissions de l'information et les usurpations d'identité :** selon GODART (2002), il s'agit ici de vol d'informations confidentielles par cassage de messages cryptés ou cassage de mots de passe, le *snifing* ou encore la récupération de données effacées. L'information peut également être manipulée en modifiant le contenu des pages d'un site Web. Un pirate peut se « déguiser » et prendre l'identité d'une ressource qui est considérée comme étant de toute confiance (ACISSI, 2009) ;
- **les nouvelles menaces :** pour CALE & TOUITOU (2007), l'usage de téléphone sur IP et du Wifi sont désormais des cibles potentielles pour les cybercriminels faisant appel au déni de service. Les logiciels P2P (*peer-to-peer*), l'usage des clés USB, des iPOD, des disques durs externes ainsi que le téléchargement de fichiers (image, audio, vidéo, etc.) sont également de grands vecteurs de risque. Les usurpations d'identités, les intrusions, les

attaques par des vers, les écoutes et l'enregistrement des communications sont les risques associés à ces technologies. La possibilité de mettre en place un point d'accès Wifi pirate est aisé, il s'agit de la technique du « man in the middle ». Nous classons également dans cette catégorie les menaces liées à l'utilisation de logiciel sans licence d'exploitation et l'usage des copies de logiciel illégales.

A travers cette présentation non exhaustive des risques inhérents au système informatique, force est de constater que les menaces sont nombreuses et de diverses natures. Afin de s'en prémunir, l'entreprise doit mettre en place des dispositifs et des procédures de sécurité que nous allons présenter dans la section suivante.

1.4 La sécurité informatique

Selon l'IIA in GTAG 4 (2009 : 11), La sécurité informatique fait partie intégrante de tous les contrôles du système d'information. Elle s'applique à la fois à l'infrastructure et aux données, et c'est sur elle que repose la fiabilité des autres contrôles.

Selon ROYER (2004 : 55), le domaine couvert par la sécurité informatique est vaste. L'auteur la définit comme étant : « la protection contre tous les dommages subis ou causés par l'outil informatique ».

Selon GODART (2002 : 16-17), de manière plus concrète, une entreprise parle de sécurité pour protéger sa réputation, assurer la continuité de ses activités, protéger ses données stratégiques et ses propriétés intellectuelles, protéger les données privées de sa clientèle et de ses employés, se prémunir de la fraude, satisfaire aux exigences légales et éviter des pertes financières.

La sécurité informatique consiste aussi à s'assurer que les ressources matérielles ou logiciels d'une organisation sont uniquement utilisées dans le cadre prévu.

Selon le GTAG 4 (2009), l'ACISSI (2009), CARPENTIER (2009) et GODART (2002), les composantes universellement acceptées de la sécurité informatique sont :

- **la confidentialité :** c'est l'assurance que l'information n'est accessible qu'aux personnes autorisées, qu'elle ne sera pas divulguée en dehors d'un environnement spécifié. Ce principe traite de la protection contre la consultation de données stockées ou échangées. Les données doivent être cryptées, seuls les auteurs de la transaction possèdent la clé de compréhension. Les données confidentielles ne doivent être divulguées que lorsque c'est nécessaire, et doivent être protégées contre toute interception ou communication non

autorisée. La confidentialité a également trait au respect de la vie privée et des données personnelles ;

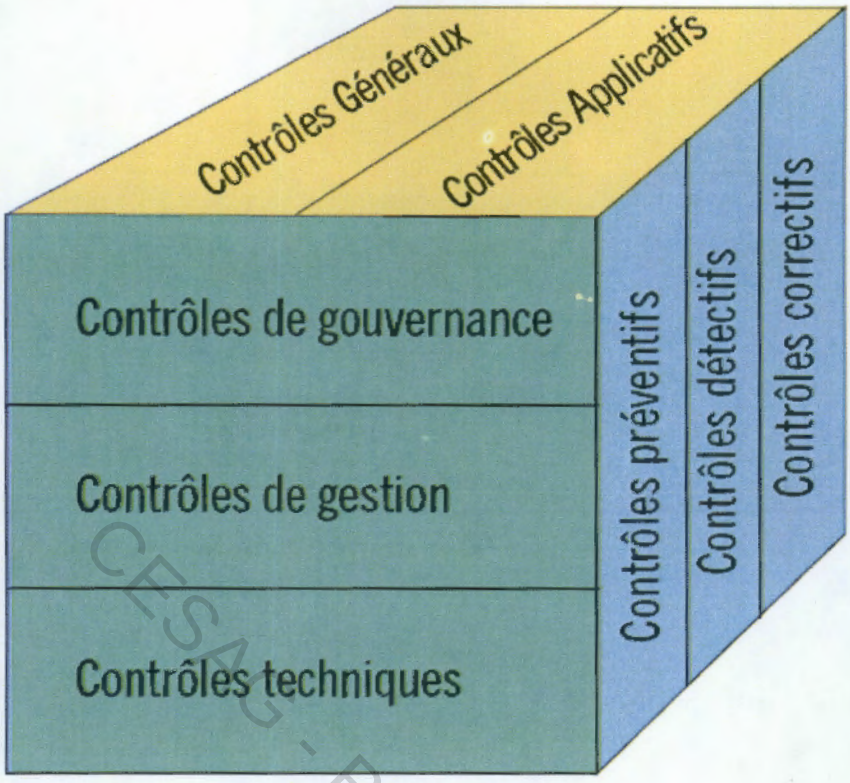
- **l'intégrité :** l'intégrité des données désigne des données correctes et complètes. elle est particulièrement importante pour la fiabilité du traitement de données financières et les communications financières. Ce principe garantit à chaque instant que les données qui circulent sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non) au cours de la communication ; la mise en œuvre de ce principe doit permettre de valider l'intégralité, la précision, l'authenticité et la validité des données ;
- **la disponibilité :** les données doivent être accessibles à l'entreprise, à ses clients et partenaires au moment, à l'endroit et de la manière requise. La disponibilité porte également sur la capacité de redémarrage du système d'information après une perte, une panne ou la corruption de données et de services du système d'information, ou encore après un sinistre majeur à l'emplacement où les données étaient situées. Il faut s'assurer du bon fonctionnement du système ;
- **la non-répudiation :** cette caractéristique assure le fait qu'une personne ou une entité ne puisse pas nier avoie effectué une activité. La non-répudiation de l'origine et de la réception des données prouvent que les données ont été reçues. Cela se fait par le biais de certificats numériques grâce à une clé privée. L'élément de la preuve de non-répudiation doit permettre l'identification de celui qu'il représente ; il doit être positionné dans le temps (horodatage), il doit préciser l'état ou le contexte dans lequel il a été élaboré ;
- **l'authentification :** c'est le moyen qui permet d'établir la validité de la requête émise pour accéder à un système. Elle assure l'identification d'un individu, d'une entité mais également l'origine de l'information ou de l'opération traitée par le système ;
- **la journalisation ou la preuve :** elle assure que tout accès à un système, tout accès à une information ainsi que toute opération exercée sur ceux-ci soit toujours enregistrée et répertoriée.

Ces caractéristiques doivent être mises en œuvre dans le cadre de la politique de sécurité qui est définie par les dirigeants de l'entreprise et la direction informatique et dont le rôle est le choix des solutions organisationnelles et techniques aux problèmes de sécurité informatique.

1.4.1. Les types de contrôle.

Selon le GTAG 1 (2009), on peut classifier les contrôles de manière à en comprendre les objectifs et à savoir où ils s'insèrent au sein du système de contrôle interne (figure 3). La compréhension de ces classifications permet à celui qui analyse les contrôles et à l'auditeur de mieux connaître leur position au sein du système de contrôle.

Figure 3 : Quelques classifications des contrôles.



Source: IIA in GTAG1 (2009:6).

Comme nous le voyons sur la figure 3, il existe plusieurs types de contrôles repartis en trois (03) principales catégories. Néanmoins, une classification courante des contrôles du système informatique, est de séparer les contrôles généraux des contrôles applicatifs :

- **les contrôles généraux :** les contrôles généraux (que l'on désigne également de contrôles d'infrastructure) s'appliquent à l'ensemble des composantes, processus et données d'une organisation ou d'un environnement système. Selon le GTAG 4 (2009 : 1), les contrôles généraux informatiques (CGTI) les plus courants sont les suivants :
  - contrôles d'accès logique à l'infrastructure, aux applications et aux données ;
  - contrôles du cycle de développement des systèmes d'applications informatisées ;
  - contrôles sur la gestion des changements dans les programmes ;
  - contrôles de sécurité physique sur le centre de traitement informatique ;
  - contrôles de sauvegarde et de restauration des systèmes et des données ;
  - contrôles de l'exploitation ;
- **les contrôles applicatifs :** selon le GTAG 4 (2009 : 2), ils portent sur l'étendue des processus de l'entreprise ou ses applications. Il s'agit, notamment, de la validation de données, de la séparation des taches (saisie d'une transaction et son autorisation, etc.), de

la balance des totaux de contrôle, de la journalisation des transactions et des rapports d'erreurs. Toutes les applications qui supportent les activités métier doivent être contrôlées. Pour toutes les applications que l'organisation développe ou acquiert, des normes doivent définir les types de contrôle à mettre impérativement en place tout le long des processus métier, ainsi que les contrôles spécifiques aux processus et données sensibles.

Le rôle d'un contrôle est primordial pour en évaluer la conception et l'efficacité. On peut différencier les contrôles préventifs, de détection et de correction.

1.4.2. La politique de sécurité de l'information

La politique de sécurité de l'information est le principal document de référence en matière de sécurité informatique ou sécurité d'un système d'information. Elle à pour objectif de définir la protection des systèmes d'information. Elle reflète la vision stratégique de l'organisation et montre l'importance qu'accorde le manager à son système d'information (ANSSI, 2010).

La politique de sécurité se présente sous la forme d'un ensemble de documents qui présentent de manière ordonnée les règles de sécurité, les directives, procédures, règles organisationnelles et techniques à appliquer et à respecter. Ces règles sont généralement issues d'une étude des risques des systèmes d'information (PILLOU, 2010).

1.4.3. La charte informatique

Selon EOX-PARTNERS (2009), c'est un document à forte connotation juridique qui est souvent associé au règlement intérieur de l'organisation. Elle est inspirée de la politique de sécurité informatique. La charte définit les règles d'utilisation de l'outil informatique ; elle définit aussi les responsabilités et les droits des utilisateurs (internes et externes). Selon CALE & TOUITOU (2007), la charte informatique à comme objectifs de fixer les droits et obligations des utilisateurs concernant l'usage des ressources informatiques en définissant les règles d'usage et de fonctionnement, d'informer les utilisateurs des moyens de contrôle mise en place pour surveiller et limiter l'utilisation des ressources informatiques et permettre une meilleure gestion des coûts et des risques liés à cette utilisation notamment en termes de sécurité, de responsabilité, d'image et de réputation.

1.4.4. Les acteurs de la sécurité du système d'information

Ce sont toutes les personnes qui jouent un rôle dans la prévention et la gestion des risques informatiques. On a :

- **la direction générale :** selon GRAEVE & POTIER (2001), la Direction Générale est le maitre d'ouvrage de la sécurité informatique. C'est la direction générale qui définit la politique de sécurité, affecte les budgets et définit toute la stratégie de sécurité de l'entreprise. De plus, elle est responsable du respect des prescriptions légales et règlementaires relatives à l'information, au respect et à la protection des propriétés intellectuelles et des œuvres produites et/ou utilisées au sein de l'entreprise ;
- **le directeur des systèmes d'information :** selon le GTAG 4 (2009), c'est le directeur des systèmes d'information qui porte la responsabilité globale de l'utilisation des outils informatiques au sein de l'organisation. S'agissant des contrôles des systèmes d'information, il a pour mission de comprendre les besoins de l'entreprise qui conduisent à la mise en œuvre de système d'information ; développer des partenariats SI avec les responsables métier afin de veiller à ce que la politique de système d'information soit cohérente avec la politique de l'entreprise, veiller au respect des règles, bénéficier des gains d'efficience sur les processus et atténuer les risques évalués ; concevoir un cadre de contrôle interne des systèmes, de le mettre en place et à jour ; planifier, trouver et maîtriser les ressources, etc. ;
- **le Responsable de la sécurité des systèmes d'information (RSSI) :** selon CARPENTIER (2009) et REIX (2005), le responsable de la sécurité du système d'information (RSSI) ou le responsable du système informatique est le maitre d'œuvre de la politique de sécurité informatique. Il établit des procédures spécifiques, limite les accès au réseau en cas d'informations stratégiques, s'assure de l'intégrité des données et veille régulièrement à ce que le réseau ne présente aucune faille. Il contribue à garantir la disponibilité du système d'information de l'entreprise, préserve son intégrité et sa confidentialité et assure la sécurité des transactions électroniques ;
- **le directeur chargé de la gestion des risques ou le Risk Manager :** selon le GTAG 4 (2009), le directeur chargé de la gestion des risques s'intéresse à la gestion des risques à tous les niveaux de l'organisation. Puisque les risques informatiques relèvent de cette fonction, il doit les prendre en considération, avec l'aide du directeur de la sécurité informatique. Il s'agit d'analyser et d'évaluer l'exposition aux risques informatiques, notamment les risques d'atteinte à l'intégrité des données (perte, détérioration, divulgation ou indisponibilité) ; d'évaluer les événements informatiques, comme les interruptions, sinistres et changements ; d'analyser et d'évaluer les risques opérationnels dans la mesure où ils sont affectés par les risques informatiques ; enfin, de suivre, d'assister et d'être la personne de référence pour toutes les activités liées à la maîtrise des risques informatiques ;
- **les acteurs de l'audit :** il s'agit ici de l'auditeur interne et des auditeurs externes :

- l'audit interne : selon le GTAG 4 (2009 : 17), l'audit interne est une composante essentielle du processus de gouvernance d'entreprise, que l'on ait recoure ou non à un groupe d'audit interne spécifique. Les auditeurs internes doivent généralement disposer d'une compréhension générale des Systèmes, mais qui sera plus ou moins approfondie selon la catégorie d'audit ou de supervision d'audit pour laquelle ils interviennent (Norme 1210.A3 de l'IIA) ;
- les auditeurs externes : selon le GTAG 4 (2009 : 18), des audits externes indépendants sont une obligation pour la plupart des organisations ; ils sont généralement effectués tous les ans. Les aspects que le service d'audit interne et le comité d'audit doivent prendre en considération sont les suivants : le champ des responsabilités de l'auditeur externe pour la compréhension et l'évaluation du système d'information et les contrôles informatiques qui y sont associés au cours des audits financiers ; la portée des responsabilités de l'auditeur externe dans l'examen des contrôles et systèmes informatiques au cours de n'importe quel agrément formel que peut exiger la législation ou la réglementation, tels que le système de contrôle interne portant sur les communications financières ou d'autres impératifs normatifs ;

- **le personnel :** selon REIX (2005) et GRAEVE & POTIER (2001), le personnel est l'utilisateur des ressources informatiques. Son rôle est d'appliquer les règles et principes définis dans la charte de sécurité informatique qui est un dispositif de contrôle interne. Une bonne sensibilisation du personnel aux problèmes de sécurité informatique réduit les risques qui pèsent sur le système d'information.

1.4.5. Les dispositifs de sécurité informatique

Nous présentons dans ce paragraphe les dispositifs qui peuvent être mis en place afin d'assurer la sécurité des actifs informatiques, du point de vue physique et du point de vue logique. Nous allons reprendre la nomenclature utilisée pour la présentation des risques afin d'associer chaque dispositif de sécurité au risque qu'il permet de maitriser :

- **les dispositifs de sécurité physique et environnementale :** ces dispositifs permettent d'assurer la protection physique du matériel informatique :
- **les risques humains :** les ordinateurs portables doivent être équipés de câbles en titane qui permettent de les fixer à une table, une armoire ou à une chaise. Une protection des bâtiments doit être mise en place notamment des dispositifs de contrôle d'accès (badges, biométrie, clé, etc.) et de détecter des déplacements et des intrusions. Les fenêtres doivent être en double vitrage blindé et les portes donnant sur l'extérieur doivent être blindées et

disposées d'une détection d'ouverture reliée à une alarme. Le premier rempart peut être un service de gardiennage qui identifie et filtre les visiteurs. La solidité des bâtiments et une bonne police d'assurances sont le dernier recours à une attaque terroriste (CALE &TOUITOU, 2007) ;

- **les risques environnementaux :** un double système de climatisation (principal et secondaire) doit être installé avec un contrat de maintenance 24h/24 et 7j/7. Des dispositifs de contrôle d'alerte pour les températures doivent être installés. La salle informatique doit être propre et correctement rangée (CLEUET & al, 2008a) ;
- **les risques électriques :** les bâtiments doivent être équipés de système évitant les remontées de foudre (paratonnerre, puits de terre, fusibles). Une double alimentation doit être prévue (groupe électrogène) et tous les postes doivent être équipés d'onduleurs adaptés. Les circuits d'alimentation du câble électrique doivent également être redondants (SMI, 2010) ;
- **les sinistres :** les dégâts des eaux se préviennent par le choix judicieux de la salle informatique qui ne doit pas être située en sous-sol (inondation) ou au dernier étage (infiltration). Les équipements doivent être surélevés et des tubes hermétiques doivent être utilisés pour les câblages d'alimentations et réseaux. Le plancher doit être compartimenté de façon à contenir et à diriger l'eau vers les systèmes d'évacuation (ROYER, 2004). Les dégâts du feu se préviennent en évitant de disposer au voisinage de la salle informatique des produits inflammables, en évitant des kyrielles de blocs de multiprises et en vérifiant régulièrement les circuits électriques. Des armoires ignifuges doivent être prévues pour le stockage des supports informatiques. Un système de détection d'incendie qui déclenche une alarme et/ou un mécanisme d'extinction (de préférence au gaz halon, Co2, FM200, etc.). Ce système doit couper l'alimentation électrique avant de déclencher le dispositif d'extinction. Des extincteurs doivent être disposés dans les bâtiments. Les installations stratégiques et complexes doivent être reliées par un dispositif d'alerte automatique à la caserne des pompiers la plus proche (CLEUET & al, 2008a et SMI, 2010).

Tous ces dispositifs doivent être entretenus et testés régulièrement par un personnel compétent et ces opérations doivent être consignées dans un registre.

- **les dispositifs de sécurité logique :** nous faisons une présentation de quelques dispositifs ou solutions suivant la présentation faites des risques logiques :
- **les malwares :** face à ces menaces, la solution de sécurité est l'usage d'un logiciel antivirus sur les postes clients, sur les serveurs, ainsi que sur les passerelles d'accès Internet, couplé à un dispositif pare-feu ou firewall (CLEUET & al, 2008a). De plus, il faudra scanner les supports externes avant de les consulter et s'assurer d'une mise à jour

permanente des logiciels. Il est aussi recommandé, pour chaque point névralgique retenu, d'utiliser différents antivirus afin d'augmenter les chances de détection ;

- **les spam :** tout comme les malwares, ces menaces peuvent être repoussées grâce à l'usage d'un logiciel antivirus qui intègre un module de filtre de courriers indésirables ;
- **les facteurs humains :** les erreurs humaines peuvent être détectées lorsque la séparation des tâches et des environnements est effective et que le personnel informatique est supervisé. Le *social engineering* et le *phising* se préviennent par la sensibilisation et une grande vigilance du personnel d'entreprise. La charte informatique trouve ici toute son utilité (ACISSI, 2009) ;
- **les atteintes à la disponibilité ou déni de service :** l'usage d'un proxy, d'un firewall, de sonde réseaux et la mise en place de réseau privé virtuel permettent de faire face à ce type d'attaque. Les contrôles d'admission réseau, le compartimentage du système informatique et l'usage d'un « *honey pot* » sont d'autres parades limitant les attaques au cœur du dispositif informatique (CALE & TOUITOU, 2007) ;
- **la compromission de l'information et l'usurpation d'identité :** une séparation des environnements études et exploitation de telle sorte que les personnes qui développent les applications et celle qui gèrent le fonctionnement des postes clients ne puissent pas accéder aux mêmes fichiers. Un deuxième dispositif consiste à la limitation des accès aux utilitaires et fichiers systèmes en instaurant des droits d'accès en fonction des tâches auxquelles le personnel utilisateur est affecté. Le troisième dispositif est l'usage de mot de passe « fort » qui doit comporter au moins huit caractères différents et qui doit être changé régulièrement et resté confidentiel (ACISSI, 2009 et ROYER, 2004) ;
- **les nouvelles menaces :** le wifi doit être fermé afin de ne pas diffuser des informations de nature à permettre une authentification par des pirates, un système de détection des intrusions propre au Wifi doit être installé, il doit permettre de signaler des interférences qui sont des indices de tentative de mise en œuvre d'un point d'accès pirate. L'usage des périphériques amovibles doit être limité, pour ceux dont l'usage est fréquent et indispensable, il faudrait privilégier lors des achats de ces périphériques, ceux disposants d'une autorisation d'accès par mot de passe (CALE & TOUITOU, 2007).

Ces dispositifs techniques comme nous le voyons font partie d'une gestion organisationnelle de la sécurité et dont ils ne sont qu'une composante.

1.4.6. Le plan de sauvegarde et le plan de secours informatique

Ces processus sont des éléments du plan de continuité d'activité. Leurs mises en place résultent de la dépendance de plus en plus grande des entreprises envers l'informatique. Ces processus ont

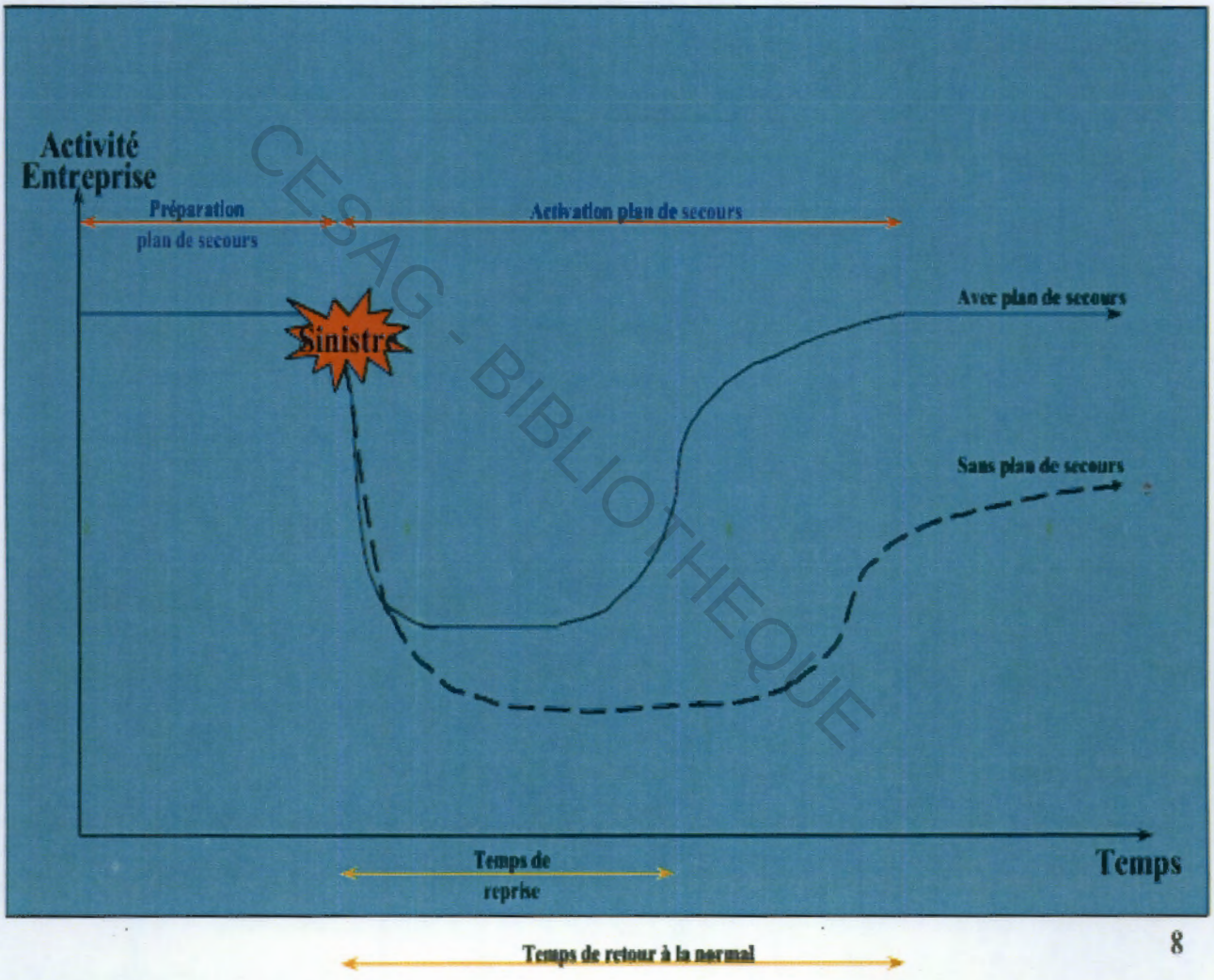
pour rôle de permettre à l'entreprise de continuer son activité en mode dégradé en cas de sinistre important, de récupérer des données effacées ou d'utiliser des versions antérieures des logiciels et informations du système informatique. Le contexte limité de cette étude ne permet pas d'aborder le sujet de façon exhaustive. Nous ferons une présentation sommaire de ces deux dispositifs de la gestion organisationnelle de la sécurité. On a :

- **le plan de sauvegarde :** selon BUTEL (2008) et LESSAUVEGARDES (2007), le plan de sauvegarde doit permettre de récupérer, de manière transparente, les informations indispensables au fonctionnement opérationnel de l'entreprise, voire vitales pour sa survie. Improvisation et sauvegarde sont deux mots antinomiques. En revanche, anticipation et sauvegarde sont étroitement liés. Un bon plan de sauvegarde doit être exhaustif, fiable, évolutif, cohérent et « auditable ». De façon concrète il est composé de trois éléments essentiels :
    - une analyse des besoins qui détermine ce qui doit être protégé, le degré de sécurisation et la facilité de récupération ;
    - les procédures et les règles générales qui s'appliquent pour chaque type de fichiers, de données, d'applications et de matériel ;
    - la documentation détaillée des actions à entreprendre pour sauvegarder les données, les méthodes et les outils employés, les fréquences de sauvegarde, le nombre de génération concernées, les supports utilisés, les procédures de marquage et d'identification, les documentations concernées, les règles de restauration ainsi que le lieu de stockage de sauvegardes (interne ou externe à l'entreprise) ;
- **le plan de secours informatique :** « Le plan de secours est l'ensemble des solutions étudiées par la Direction Générale de l'entreprise et par la Direction informatique pour reprendre l'activité informatique, après un sinistre total, dans des conditions qui permettent la survie de l'entreprise » (MENTHONNEX, 1995 : 211). Un plan de secours est composé de dispositifs élémentaires dont l'activation dépendra de l'évènement survenu et du contexte général. Ces dispositifs sont généralement classés par type d'activité : mobilisation des ressources nécessaires, secours des équipements informatiques, des réseaux et de la téléphonie, reprise des traitements, logistique, relogement, reprise des activités des services utilisateurs, communication de crise et dispositifs de post-reprise.

Afin que leurs niveaux soient garantis, les dispositifs de secours doivent être accompagnés de dispositifs permanents tels qu'un plan de sauvegarde, la formation des acteurs (CLUSIF, 2003).

Le plan de secours aboutit assez souvent à une duplication de l'infrastructure informatique sur un autre site. Un contrat peut être également passé avec un fournisseur et/ou un assureur pour une fourniture de matériel en cas de survenance d'un sinistre lorsqu'on ne dispose pas d'un site de secours préalablement équipé. Selon CLEUET & al (2008 : 46), « cette démarche de remplacement des ressources matérielles du système d'information peut être complétée par des procédures, dites dégradées, permettant aux utilisateurs de travailler manuellement en l'attente d'une remise en service du système informatique ».

Figure 4 : Pourquoi un plan de secours ?



8

Source : BUTEL in (CLUSIF, 2008 :8)

Comme l'indique la figure 4, un plan de secours permet à une entreprise de retrouver assez rapidement son niveau d'activité tandis que sans plan de reprise, le retour au niveau d'activité d'avant sinistre est très lent et l'entreprise ne retrouve pas son niveau d'activité.

1.4.7. Les contraintes légales et réglementaires

De plus en plus de textes législatifs influent sur le cadre de contrôle interne que les organisations décident de mettre en œuvre. Cette partie résume ces obligations et l'incidence de certaines dispositions importantes qu'il convient de prendre en considération dans l'évaluation et la gestion des contrôles du système d'information.

L'acte uniforme portant Organisation pour l'Harmonisation en Afrique du Droit des Affaires (OHADA), en son article 22 relatif au traitement informatique de la comptabilité, reprend dans ses alinéas 1 à 7 les principes de la sécurité informatique que nous avons présentés plus haut qui sont : la confidentialité, l'intégrité, la disponibilité, la non-répudiation, l'authentification et la journalisation ou preuve. Le même acte en son article 24 évoque la conservation des pièces comptables pour une période de dix (10) ans, ce qui ramène à la sauvegarde et l'archivage des données.

En France, la loi n°85-660 du 3 juillet 1985 relative à la protection des logiciels et des progiciels protège la propriété intellectuelle des concepteurs contre la copie ou l'utilisation non autorisée. La loi n°88-19 du 5 janvier 1988 relative à la fraude informatique protège les propriétaires d'un système d'information contre une série d'actes de malveillance ou de piraterie qui sont : l'accès ou le maintien frauduleux dans un système informatique avec dommages, volontaires ou non, la modification ou la suppression de données, l'altération du système, l'entrave volontaire au fonctionnement d'un système informatique, l'introduction, suppression, modification intentionnelles du mode de traitement, des transmissions de données, la falsification de document informatique, l'usage de document falsifié (CLEUET & al, 2008a).

Aux Etats Unis, la loi Sarbanes-Oxley vise à réformer les pratiques comptables des sociétés privées cotées en Bourse, ainsi que d'autres processus du gouvernement d'entreprise, et à consolider les marchés des capitaux après les affaires Enron et WorldCom. Cependant, elle ne traite pas spécifiquement des contrôles des systèmes d'information, ce qui ne signifie pas pour autant que les examens de conformité qu'elle impose peuvent faire l'impasse sur les ceux-ci. Cette loi est neutre vis-à-vis de la technologie, mais l'implication est claire : les contrôles des systèmes sont critiques pour l'intégralité du système de contrôle interne d'une organisation.

Les Accords de Bâle II constituent un traité définissant des normes mondiales pour les pratiques de gestion du risque à l'échelle de l'entreprise dans le secteur financier, en vue d'y atténuer les risques de pertes. Ils sont axés sur le secteur bancaire, mais visent manifestement l'harmonisation

des normes entre tous les pans de ce secteur. Ils traitent de tous les aspects des activités bancaires : ressources humaines, processus, systèmes, gouvernance et gestion des fournisseurs.

Ces obligations légales et règlementaires et recommandations ci-dessus ne sont pas exhaustives.

Conclusion Chapitre 1

Le système informatique est stratégique pour l'entreprise car il constitue un processus transversal, support de tous les métiers. Cependant, il est sujet à de nombreux risques aussi bien physiques que logiques. La sécurité informatique qui est un dispositif de contrôle interne, technique et organisationnel, doit donc prémunir le système informatique de la survenance d'un risque qui pourrait mettre en péril la confidentialité, l'intégrité, la disponibilité du système et des informations traitées et donc la continuité d'exploitation de l'entreprise. Mais pour que ce dispositif soit fiable et efficace, il faudra qu'il fasse l'objet de contrôle et d'évaluation permanents. Ces contrôles doivent être réalisés aussi bien à l'interne (contrôle interne et audit interne) que par des compétences externes (auditeurs externes).

CHAPITRE 2 : L'AUDIT DES APPLICATIONS INFORMATIQUES

Introduction

Une entreprise doit implémenter les mesures nécessaires pour garantir la sécurité et la conformité des applications et donc des processus métiers. Chaque processus d'affaire, sous-processus ou activité doit donc être piloté d'une manière ou d'une autre pour atteindre les objectifs définis. On parle ici du terme «contrôles», qui désigne «tous les concepts, procédures, pratiques et structures d'organisation permettant de vérifier avec une assurance raisonnable la réalisation des objectifs d'entreprise et la prévention ou l'identification et la correction d'événements non désirables» AFAI (Guide d'audit des applications informatiques, 2008 : 34).

Le terme contrôle vient de l'anglais «control» et signifie, entre autres, commande, dispositif pour manœuvrer, mais également maîtrise, supervision, pilotage ou guidage, ce qui dépasse de loin le sens habituel et plutôt limité que l'on donne au terme contrôle. Chaque application et donc chaque processus commercial spécifique contient des contrôles qui garantissent la réalisation des objectifs définis. Ces contrôles sont appelés «contrôles applicatifs». Il s'agit par exemple de contrôles d'exhaustivité, d'exactitude, de validité et de séparation de fonction. Outre les contrôles liés aux applications, il existe des contrôles non liés aux applications, appelés également contrôles IT généraux. Il s'agit par exemple de contrôles dans le domaine des développements de système, des modifications, de la sécurité et de l'exploitation. Ces contrôles ne sont pas traités dans ce chapitre.

Dans le cadre des procédures d'audit orientées processus et basées sur l'utilisation d'applications informatiques, il est essentiel de prendre en compte tous les domaines importants, y compris les domaines IT spécifiques ayant une influence significative sur l'objectif de contrôle de l'auditeur. Pour y parvenir une approche de contrôle intégrée (auditeur et auditeur informatique) est nécessaire. L'absence de procédure concertée entre auditeurs et auditeurs informatiques (auditeurs IT) constitue à cet égard un risque élevé.

Il est évident que chaque type d'application exige des contrôles différents: chaque activité commerciale spécifique comporte des risques commerciaux différents, inhérents à cette activité et susceptibles d'empêcher l'atteinte des objectifs.

Pour mener à bien une mission, l'auditeur doit faire le choix d'une norme, d'un standard et d'un référentiel correspondant au domaine audité, puis définir ses objectifs d'audit et enfin décider d'une approche méthodologique (CLEUET & al, 2008b).

Afin de mener à bien sa mission et en toute efficacité, l'auditeur doit s'appuyer sur des normes, des standards et des référentiels considérés comme les bonnes pratiques dans le domaine. Nous nous appuierons sur les référentiels récemment publiés sur le sujet à savoir le:

- **CobiT and Application Controls**, publié en 2009 par l'ISACA, et ;
- **Global Technology Audit Guide (GTAG) n° 8 – Auditing Application Controls**, publié par l'Institute of Internal Auditors en juillet 2007.

Ces référentiels ci-dessus sont loin d'être exhaustifs.

2.1.Le modèle de l'ISACA : CobiT and Application Controls

Il est important de noter que l'ancienne version du CobiT mentionnait les contrôles applicatifs, mais ne les intégrait pas dans les 34 processus informatiques de base. Ces contrôles relevaient en effet des processus métiers. Ils n'étaient donc compris ni dans les Objectifs de contrôle, ni dans le Guide du management. Cependant, dans sa nouvelle version « CobiT and Application Controls », les contrôles applicatifs font l'objet d'un traitement spécifique (ISACA, 2009)[1]. Nous avons retenu les six (06) principaux Contrôles Applicatifs (AC) suivants :

2.1.1. AC1 : Source des données, Préparation et autorisation

Veiller à ce que les documents de base soient préparés par le personnel qualifié et autorisé suivant les procédures établies, en tenant compte de la séparation des tâches concernant la création et l'approbation de ces documents. Minimiser les erreurs et omissions dans la conception d'entrée une bonne forme. Détecter les erreurs et les irrégularités afin qu'elles puissent être signalées et corrigées.

Les principaux contrôles retenus sont :

- vérifier, par l'inspection des listes d'autorisation, que les niveaux d'autorisation sont correctement définis pour chaque groupe de transactions. Observer que les niveaux d'autorisation sont correctement appliquées ;
- inspecter et observer la création et la documentation des procédures de préparation des données, et se demander si et confirmer que les procédures sont bien comprises et les médias de source corrects soient utilisés ;
- lorsque cela est requis par les procédures, de savoir si et veiller à ce que la séparation des tâches entre donneur d'ordre et approbateur existe ;

[1] IT Assurance Guide: Using COBIT/COBIT Control Practices, 2nd Edition, Appendix VI -- Application Control © 2007 IT Governance Institute. All rights reserved. www.itgi.org.

- inspecter les documents, le suivi des transactions par l'intermédiaire du processus et, si possible, utiliser la collecte de preuves automatisées, y compris les données d'échantillonnage, des modules de vérification intégrés ou CAATS, de retracer les transactions afin de vérifier que les contrôles d'autorisation d'accès sont efficaces ;
- renseignez-vous si, et confirmer que la liste des personnes autorisées et leurs signatures est maintenu par les services compétents. Si possible, utilisez la collecte des preuves automatisées ;
- inspecter la liste des personnes autorisées et d'autres documents, et observer les processus et les procédures pour vérifier que les processus et les procédures utilisés pour maintenir la liste, sont opportun et efficaces ;
- renseignez-vous si, et confirmer que tous les documents sources comprennent des composants standards tels que les codes d'entrée prédéterminés et les valeurs par défaut pour réduire les erreurs, le temps de transaction et la date d'enregistrement pour assurer la surveillance, et de capturer les informations d'autorisation pour assurer la validité ;
- renseignez-vous si, et confirmer que, lors de la saisie des données, les documents sources sont passés en revue; les documents incomplets, non signés ou mal autorisés sont retournés aux initiateurs pour la correction et sont enregistrés, et les journaux sont revues périodiquement pour vérifier que les documents corrigés sont retournés par les initiateurs dans un temps opportun ;
- examiner les formes de documents sources et vérifier si elles sont utilisables, pour faciliter la prévention des erreurs, et permettre une préparation rapide et efficace.

2.1.2. AC2 : Source Collecte et d'entrée de données

Veiller à ce que la saisie des données soit effectuée en temps opportun par le personnel autorisé et qualifié. La correction et la nouvelle présentation des données qui ont été entrées à tort doit être effectuée sans compromettre les niveaux d'autorisation de transaction d'origine. Le cas échéant pour la reconstruction, conserver les documents sources originaux pour le laps de temps approprié.

Les principaux contrôles retenus sont :

- renseignez-vous si, et confirmer que les documents sources critiques sont numérotés à l'avance et les out-of-numéros de séquence sont identifiés et pris en compte ;
- renseignez-vous si, et confirmer que les messages d'erreur sont générés en temps opportun, les transactions ne sont pas traités à moins que ces erreurs soient corrigées ou correctement remplacées ;

- renseignez-vous si, et confirmer que les rapports sur les erreurs et les conditions sont examinées par un personnel compétent; toutes les erreurs sont identifiées, corrigées et vérifiées dans un délai de temps raisonnable, et les erreurs sont signalées jusqu'à ce qu'elles soient corrigées ;
- pour un échantillon de flux de transactions, savoir si et confirmer que la rétention de documents de base est définie et appliquée en fonction de critères établis pour la conservation des documents sources ;
- sélectionnez un ensemble de transactions critiques et:
    - comparer l'état actuel des contrôles d'accès sur l'entrée de transaction, d'édition, d'acceptation, etc. avec les critères établis, politiques ou procédures ;
    - vérifier si les documents sources critiques sont numérotés à l'avance ou que d'autres méthodes uniques d'identification des sources de données sont utilisées ;
    - inspectez la documentation ou rendez-vous grâce à des transactions afin d'identifier les personnes qui peuvent saisir, éditer, autoriser, accepter et rejeter des opérations et remplacer des erreurs ;
    - prenez un échantillon de transactions au sein de cet ensemble pour une période déterminée, et inspecter les documents de base pour ces transactions. Vérifiez que tous les documents sources appropriées sont disponibles ;
- identifier et examiner l'extérieur de leur séquence de nombres, les lacunes et les doublons à l'aide d'outils automatisés (CAATS) ;
- inspecter les transactions des documents, des traces à travers le processus et, si possible, utiliser la collecte de preuves automatisé, y compris les données d'échantillonnage, des modules de vérification intégrés ou CAATS, pour retrouver la trace des transactions afin de vérifier que les contrôles d'autorisation sont efficaces et que des preuves suffisantes sont enregistrées de manière fiable et examinées ;
- inspecter les documents, le suivi des transactions par l'intermédiaire du processus et, si possible, utiliser la collecte de preuves automatisés, y compris les données d'échantillonnage, des modules de vérification intégrés ou CAATS, pour retrouver la trace des transactions afin de vérifier que les messages d'erreur en temps opportun, les restrictions processus de transaction et les journaux d'erreur sont générés, appliqués et de recours efficaces ;
- inspecter l'erreur et out-of-bilan des rapports, des corrections d'erreurs, et d'autres documents afin de vérifier que les erreurs et out-of-équilibrer les conditions sont effectivement revues, corrigées, vérifiées et déclarées jusqu'à ce corrigé.

2.1.3. AC3 : Contrôle de l'exactitude, l'exhaustivité et l'authenticité

Veiller à ce que les opérations soient exactes, complètes et valides. Valider les données qui étaient entrées, et de modifier ou renvoyer pour correction au plus près du point d'origine que possible.

Les principaux contrôles retenus sont :

- inspecter les erreurs et out-of-équilibre des rapports, des corrections d'erreurs, et d'autres documents afin de vérifier que les erreurs et out-of-équilibre sont effectivement revues, corrigées, vérifiées et signalées jusqu'à ce qu'elles soient corrigées ;
- inspecter les corrections d'erreur, out-of-équilibre les conditions, les dépassements d'entrée et d'autres documents afin de vérifier que les procédures sont suivies ;
- sélectionner un échantillon de données de source d'entrée de documents de source. Utilisation de l'inspection, CAAT, ou toute autre collecte de preuves automatisés et des outils d'évaluation, de valider que les données d'entrée sont une représentation complète et exacte des documents sources sous-jacentes ;
- sélectionner un échantillon de processus de sources de données d'entrée. renseignez-vous si, et confirmer que les mécanismes sont en place pour s'assurer que les processus de sources de données d'entrée ont été effectuées en conformité avec les critères établis pour la rapidité, l'exhaustivité et l'exactitude ;
- renseignez-vous si, et de confirmer que les opérations d'édition et à défaut routines de validation font l'objet d'un suivi approprié jusqu'à ce qu'ils soient assainis.

2.1.4. AC4 : Intégrité du traitement et de la validité

Maintenir l'intégrité et la validité des données tout au long du cycle de traitement. Veiller à ce que la détection des transactions erronées ne perturbe pas le traitement des transactions valides.

Les principaux contrôles retenus sont :

- pour un exemple d'application, se demander si et confirmer que la séparation des tâches est en place. Vérifiez si la séparation des fonctions est mise en œuvre pour l'entrée, la modification et l'approbation des données de transaction ainsi que les règles de validation ;
- pour un échantillon de transactions de processus critiques, vérifier si les contrôles d'accès permettent de prévenir la saisie de données non autorisées. Avec des outils de recherche, identifier les cas où des personnes non autorisées sont en mesure de saisir des données ou modifier ;

- pour un échantillon de systèmes de transaction, vérifier si les comptes d'attente et les fichiers d'attente pour les transactions à défaut d'édition et des routines de validation ne contiennent que des erreurs des dernières années. Assurez-vous que les transactions défaillantes ont été correctement restaurées ;
- pour un échantillon de transactions, vérifiez que la saisie des données ne soit pas retardée par des transactions non valides ;
- pour les opérations très critiques, mettre en place un système de test qui fonctionne comme le système en direct ;
- vérifiez si la détection d'erreur et les rapports sont à jour et complètes et si elles fournissent des informations suffisantes pour corriger la transaction ;
- pour les opérations très critiques, mettre en place un système de test qui fonctionne comme le système en direct. Traitement des transactions dans le système de test afin de s'assurer que les transactions valides sont traitées de façon appropriée et en temps opportun ;
- veiller à ce que les erreurs soient signalées de façon appropriée et en temps opportun ;
- inspecter les messages d'erreur lors de l'entrée de données ou le traitement en ligne ;
- veiller à ce que les messages d'erreur soient appropriés pour le flux de transaction ;
- déterminer si les transactions à défaut d'édition et des routines de validation sont affichés à des fichiers de suspense ;
- vérifiez si les fichiers suspens sont correctement et systématiquement produits ;
- vérifiez si l'utilisateur est informé des transactions reportées à des comptes d'attente ;
- prendre un échantillon d'opérations d'entrée de données. utilisez l'analyse automatique et appropriée des outils de recherche pour identifier les cas où des erreurs ont été identifiées par erreur et les cas où des erreurs n'ont pas été détectées.

2.1.5. AC5 : Examen de sortie, la réconciliation et la gestion des erreurs

Établir des procédures et des responsabilités associées à s'assurer que la production est gérée d'une manière autorisée, livrée au destinataire approprié et protégé lors de la transmission; que la vérification, de détection et de correction de l'exactitude de la production se produit, et que les renseignements fournis dans la sortie est utilisé. Les principaux contrôles retenus sont :

- revoir les critères de conception et confirmer l'utilisation de processus de contrôle d'intégrité à la base, tels que l'utilisation des totaux de contrôle en-tête et / ou d'enregistrements de fin et l'équilibrage des outputs, pour contrôler les totaux produits par le système ;
- renseignez-vous si, et confirmez que les conditions détectées hors-bilan sont signalées au niveau approprié du management. Inspecter les rapports hors-bilan. Si possible, utilisez la

collecte des preuves automatisée pour rechercher toutes les erreurs de contrôle et vérifier qu'elles ont été correctement suivies et en temps opportun ;

- renseignez-vous si, et de confirmez que les stocks physiques de sorties sensibles sont pris à des intervalles appropriés. Veiller à ce qu'ils soient comparés aux registres d'inventaire et que les différences soient prises en compte. Assurez-vous que les pistes de vérification sont créées pour tenir compte de toutes les exceptions et les rejets de documents de sortie sensibles ;
- obtenir une liste de toutes les sorties électroniques qui sont réutilisées dans applications d'utilisateur final. Vérifiez que la sortie électronique est testée pour l'exhaustivité et l'exactitude avant que la sortie ne soit réutilisée et retraitée ;
- renseignez-vous si, et confirmez que la production est passée en revue de la vraisemblance et de l'exactitude. Sélectionner un échantillon représentatif de rapports de production et tester le caractère raisonnable et la précision de l'output. Vérifiez que les erreurs potentielles sont signalées et centralisées ;
- renseignez-vous si, et confirmez que les informations sensibles sont définies, convenues par le propriétaire du processus et traitées de façon appropriée. Il peut s'agir de sortie de l'application d'étiquetage sensible et, le cas échéant, l'envoi de sortie sensible à des dispositifs spéciaux de sortie à accès contrôlé.

2.1.6. AC6 : Authentification des transactions et l'intégrité

Avant de passer les données de transaction entre les applications internes et les entreprises / fonctions opérationnelles (dans ou en dehors de l'entreprise), s'assurer de leur bon traitement, de l'authenticité de la source et de l'intégrité de leur contenu. Maintenir l'authenticité et l'intégrité lors de la transmission ou du transport.

Les principaux contrôles retenus sont :

- exécutez un test par le biais du code d'un échantillon de demandes pour confirmer que les spécifications d'authenticité ont été appliquées. Vérifiez que ces spécifications ont été testés avec de bons résultats ;
- examinez les journaux d'erreurs pour les transactions qui ont échoué et vérifiez la cause.

2.2.Le modèle de l'IIA - Audit des contrôles applicatifs

Les contrôles applicatifs portent sur l'étendue des différents systèmes d'applications ou processus d'entreprise, dont les éditions de données, la séparation des fonctions, la balance des totaux de contrôle, la journalisation des transactions et les rapports d'erreurs. Les paragraphes qui suivent

décrivent les contrôles applicatifs courants avec les tests proposés pour chaque contrôle. Le tableau a été communiqué par le groupe AXA[2] (GTAG n°8, 2007 : 18-20).

2.2.1. Les contrôles des données en entrée

Ces contrôles servent principalement à vérifier l'intégrité des données entrées dans une application, que les données aient été entrées directement par le personnel de l'entreprise, à distance par un partenaire commercial ou via une application ou interface Web. La vérification de la saisie des données intègre la vérification que les limites spécifiées ne sont pas dépassées. Ces contrôles sont conçus pour apporter une assurance raisonnable que les données reçues pour un traitement informatique sont dûment autorisées et converties dans une forme assimilable par une machine, et que des données ne sont pas perdues, supprimées, ajoutées, dupliquées ou indûment modifiées. Les contrôles des entrées informatisés comprennent des procédures de vérification et de validation des données telles que les chiffres clés, le nombre d'enregistrements, les totaux de contrôle et les totaux financiers de contrôle, tandis que les routines d'édition informatisées, conçues pour détecter les erreurs de données, regroupent des contrôles de la validité des caractères, des contrôles des données manquantes, des tests de séquence et des contrôles de vraisemblance. Le tableau ci-après présente les contrôles des entrées et les tests préconisés.

[2] Tiré de Common Application Controls and Suggested Testing du Groupe AXA.

Tableau 1 : Contrôle des entrées et des accès /Contrôles de la transmission des fichiers et des données

Contrôles des entrées et des accès Ces contrôles permettent de vérifier que toutes les données d'entrée sont exactes, complètes et autorisées.		
Domaine	**Contrôle**	**Tests possibles**
Vérification et validation des données	• Contrôles de vraisemblance sur les valeurs financières. • Contrôles des formats et des champs requis, écrans d'entrée standardisés. • Contrôles de séquence (p. ex. éléments manquants), contrôle des limites et chiffres clés. • Contre-vérification (certaines politiques ne sont valides qu'avec certains codes de table premium). • Validations (p. ex. table en mémoire et menu déroulant des éléments valides).	• Tester des échantillons pour chaque scénario. • Observer les tentatives d'entrer des données incorrectes. • Déterminer qui peut passer outre les contrôles. • S'ils sont gérés par tables, déterminer qui peut altérer les modifications et les niveaux de tolérance.
Autorisation et agrément automatisés et contournement (*override*)	• Des droits d'autorisation (p. ex. pour les dépenses, le paiement des créances ou les crédits au-delà d'un certain seuil) sont accordés à des utilisateurs sur la base de leurs rôles et de leur besoin d'utiliser l'application. • Le pouvoir de passer outre (p. ex. l'autorisation de créances d'un montant inhabituellement élevé) est réservé à certains utilisateurs, sur la base de leurs rôles et de leur besoin d'utiliser l'application.	• Procéder à des tests sur la base des droits d'accès des utilisateurs. • Vérifier les privilèges d'accès pour chaque fonction ou transaction sensible. • Examiner les droits d'accès qui établissent et modifient des limites configurables d'agrément ou d'autorisation.
Séparation automatisée des fonctions et des droits d'accès	• Les individus qui décident, sont les fournisseurs agréés ne peuvent pas engager de transactions d'achat. • Les individus qui ont accès au traitement des créances ne doivent pas être en mesure de définir ou d'amender une politique.	• Procéder à des tests sur la base des droits d'accès des utilisateurs. • Examiner les droits d'accès qui établissent et modifient des rôles configurables ou des structures de menu .

Éléments en Attente	• Les superviseurs vérifient tous les jours ou une fois par semaine les rapports chronologiques faisant apparaître des nouveaux éléments des politiques dont le traitement est incomplet. • Les fichiers en attente pour lesquels les informations disponibles sont insuffisantes pour permettre un traitement de la transaction.	• Examiner le résultat du classement chronologique et la preuve des procédures d'examen par les superviseurs. • Cheminer dans un échantillon vers et depuis le rapport chronologique ou le fichier en attente.
Contrôles de la transmission des fichiers et des données Ces contrôles permettent de vérifier que les fichiers et les transactions transmis en interne ou à l'extérieur par voie électronique ont été envoyés par une source identifiée et traités exactement et complètement.		
Domaine	**Contrôle**	**Tests possibles**
Contrôles des transmissions des fichiers	• Contrôle de l'exhaustivité et de la validité du contenu, y compris la date et l'heure, la taille des données, le volume des enregistrements et l'authentification de la source.	• Observer les rapports de transmission et d'erreur. • Observer les paramètres de validité et d'exhaustivité et les réglages. • Examiner les droits d'accès à la définition et à la modification des paramètres configurables pour le transfert de fichiers.
Contrôles des transmissions des données	• Application de certains contrôles des entrées afin de valider les données reçues (p. ex. principaux champs, vraisemblance, etc.).	• Tester des échantillons pour chaque scénario. • Observer les tentatives d'entrer des données incorrectes. • Déterminer qui peut passer outre les contrôles. • S'ils sont gérés par tables, déterminer qui peut modifier les éditions et les niveaux de tolérance.

Source : Nous même, adapté du GTAG 4 (2009 : 18)

2.2.2. Les contrôles sur le traitement

Ces contrôles constituent un moyen automatisé de faire en sorte que le traitement soit complet, exact et autorisé. Ces contrôles sont conçus pour apporter une assurance raisonnable que le traitement des données s'est déroulé comme prévu, sans omission ni double décompte. Les contrôles du traitement sont en grande partie les mêmes que les contrôles des entrées, particulièrement pour les systèmes de traitement en ligne, ou en temps réel, mais sont appliqués pendant les phases de traitement. Ces contrôles sont les totaux intermédiaires, les rapports des

totaux de contrôle, les contrôles des fichiers et des opérateurs, tels que les labels externes et internes, les journaux système des opérations informatiques et les tests de vraisemblance.

Tableau 2 : Les contrôles du traitement

Contrôles du traitement Ces contrôles permettent de vérifier que les données d'entrée valides ont été traitées exactement et complètement		
Domaine	**Contrôle**	**Tests possibles**
Identification et validation automatique des fichiers	• Les fichiers à traiter existent et sont complets.	• Examiner le processus de validation et le fonctionnement du test.
Fonctionnalité automatique et calculs	• Calculs spécifiques effectués sur une ou plusieurs entrées et éléments de données stockés qui produisent d'autres éléments de données. • Utilisation des tables de données existantes (p.ex. fichiers maîtres ou données de référence telles que les barèmes).	• Comparer les valeurs d'entrée et de sortie pour tous les scénarios par cheminement et réexécution. • Examiner les contrôles de la maintenance des tables et déterminer qui peut modifier les éditions et les niveaux de tolérance.
Pistes d'audit et contournements/ *overrides*	• Suivi automatisé des changements apportés aux données, attribuant le changement à un utilisateur précis. • Suivi automatisé et mise en évidence des contournements des procédures normales.	• Examiner les rapports et les preuves des vérifications. • Examiner les droits de contourner les procédures normales.
Extraction, filtrage et communication des données	• La vraisemblance et l'exhaustivité des sorties des routines d'extraction sont contrôlées. • Allocation automatisée des transactions (p.ex. à des fins de réassurance, d'autres processus actuariels ou l'allocation des fonds). • Évaluation des données utilisées pour procéder aux estimations à des fins de communication financière.	• Examiner la conception de la routine d'extraction par rapport aux fichiers de données utilisés. • Examiner l'évaluation par les superviseurs du résultat de la routine d'extraction pour vérifier qu'un examen régulier est effectué et s'il existe des problèmes. • Examiner le bien-fondé d'un échantillon d'allocations. • Examiner le processus d'évaluation de l'exhaustivité et de la validité des données extraites.

Équilibre à l'interface	• Vérification automatique des données reçues depuis les systèmes en amont (p. ex. données sur les paies, les créances, etc.) par les entrepôts de données ou les grands livres. • Vérification automatique de la correspondance entre les soldes des deux systèmes. En cas de non correspondance, un rapport d'exception est généré et utilisé.	• Inspecter les rapports d'erreur à l'interface. • Inspecter les paramètres et les réglages de la validité et de l'exhaustivité. • Examiner les droits d'accès au réglage et à la modification des paramètres configurables sur les interfaces. • Examiner les preuves des rapports de correspondance, des vérifications et du traitement des fichiers contenant des erreurs.
Fonctionnalité automatique et classement chronologique	• Extraits de fichiers des listes de débiteurs afin de procurer à la direction des données sur les transactions par ordre chronologique.	• Tester des échantillons de transactions sur ces listes afin de valider le bien-fondé du processus de classement chronologique.
Contrôles des doublons	• Comparaison de chaque transaction aux transactions précédemment enregistrées afin de mettre les champs en correspondance. • Comparaison de chaque fichier avec les dates, heures, tailles, etc. attendus.	• Examiner les droits d'accès au réglage et à la modification des paramètres configurables sur les transactions ou les fichiers dupliqués. • Examiner le processus de manipulation des fichiers ou des transactions rejetés.

Source : Nous même, adapté au GTAG 4 (2009 :19)

2.2.3. Les contrôles des données en sortie

Ces contrôles portent sur ce qu'il advient des données et doivent rapprocher les résultats en sortie avec le résultat escompté, en confrontant les données de sortie aux données entrées. Ces contrôles sont conçus pour apporter une assurance raisonnable que les résultats du traitement sont exacts, et diffusés exclusivement au personnel habilité. Il convient de comparer et de rapprocher les totaux de contrôle sortis pendant le traitement, aux totaux de contrôle d'entrée et intermédiaires produits en cours de traitement. Il convient de comparer les rapports de modification générés par ordinateur pour les fichiers maîtres, aux documents source originaux afin de vérifier que l'information est correcte.

Tableau 3 : Contrôles des sorties/Contrôles des fichiers maîtres et des données de référence

Contrôles des sorties Ces contrôles permettent de vérifier que les données de sortie sont complètes, exactes et diffusées à qui de droit.		
Domaine	**Contrôle**	**Tests possibles**
Report dans le grand livre général	• Tous les reports des transactions individuelles et synthétisées dans le grand livre.	• Remonter jusqu'au grand livre général un échantillon de transactions synthétisées d'entrée et du grand livre auxiliaire.
Report dans le grand livre auxiliaire	• Tous les reports de transactions réussis dans le grand livre auxiliaire.	• Remonter jusqu'au grand livre auxiliaire un échantillon de transactions d'entrée.
Contrôles des fichiers maîtres et des données de référence Ces contrôles permettent de vérifier l'intégrité et l'exactitude des fichiers maîtres et des données permanentes		
Domaine	**Contrôle**	**Tests possibles**
Autorisation des mises à jour	• Droits d'accès aux mises à jour attribués aux utilisateurs seniors sur la base de leurs rôles et de leur besoin d'utiliser l'application	• Examiner les droits d'accès au réglage et à la modification des fichiers maîtres et des données de référence.

Source : Nous même, adapté au GTAG 4 (2009 :20)

2.2.4. Les contrôles d'intégrité

Ces contrôles surveillent les données en cours de traitement et les données stockées afin de veiller à ce qu'elles restent cohérentes et correctes.

2.2.5. La piste de contrôle de gestion

La trace des opérations réalisées, souvent appelée piste d'audit, permet à l'encadrement d'identifier les transactions et les événements enregistrés en suivant les transactions depuis leur entrée jusqu'à leur sortie et en sens inverse. Ces contrôles permettent également de vérifier l'efficacité des autres contrôles et de repérer les erreurs au plus près possible de leur source.

Conclusion Chapitre 2

L'audit des applications informatiques permet à l'entreprise de situer sa maîtrise et sa gestion des risques pesant sur son système informatique. Ceci permettra de se situer par rapport à un référentiel de bonnes pratiques tel que le GTAG ou d'autres, de prendre des mesures corrective et de se fixer des objectifs en matière d'application informatique.

Un modèle basé sur l'approche par les risques peut être envisagé. Le chapitre suivant sera consacré à l'élaboration d'un modèle d'analyse pour la conduite d'une mission d'audit des applications informatiques par le service d'audit interne.

CHAPITRE 3 : LE METHODOLOGIE DE L'ETUDE

Introduction

Les chapitres précédents nous ont permis de présenter le système informatique ainsi que la démarche d'audit des applications informatiques. Ce présent chapitre nous permettra de présenter notre modèle d'analyse qui nous servira de fil conducteur pour mener à bien la partie pratique de cette étude. L'élaboration d'une démarche référentielle d'audit des applications informatiques est l'objet de ce chapitre. Pour ce faire, le travail sera réparti en deux parties. La première consistera à la présentation de notre démarche référentielle, la seconde présentera les outils de collecte et d'analyse de données nécessaires à la conduite de notre mission d'audit d'une application informatique décentralisée.

3.1. Le modèle d'analyse

Dans notre démarche d'identification et d'évaluation des risques nous privilégierons l'approche par les risques qui permet de définir les domaines où les contrôles seront approfondis, d'identifier les cycles d'activité significatifs, de planifier des interventions intercalaires pour la réalisation de certains contrôles ou le suivi de certains éléments (situation de trésorerie, indicateurs clés, ...), et de définir un seuil de signification à partir duquel une anomalie pourra affecter l'image fidèle des comptes.

Concernant la démarche d'audit proprement dite nous retiendrons la démarche de l'IIA présentée dans le GTAG n°8 pour la partie spécifique de l'audit de l'application informatique. Le tableau suivant illustre nôtre modèle d'analyse.

Tableau 4: Modèle d'analyse

Préparation	Exécution	Conclusion	PLAN D'ACTION ET DE SUIVI
• **Familiarisation et cadrage (comprendre l'entreprise)** - Questionnaire de prise de connaissance (QPC) ; - Interviews ; - Analyse documentaire ; - Observation physique. • **Définir l'univers informatique** • **Identification et évaluation des risques** - Analyse documentaire ; - Interviews ; - Evaluation des risques; - Tableau des risques. • **Formalisation du plan d'audit** - Elaboration et communication du plan détaillé de la revue ; - Dossiers d'audit.	• **Réunion d'ouverture** • **Programme de vérification** - Questionnaire de contrôle interne (QCI) ; - Modèle de l'IIA (GTAG 8, 2009 : 9) : méthode de l'application unique. • **Travail sur le terrain** - **Contrôles généraux informatiques (CGTI) :** o Observation physique ; o Interviews ; o FRAP. - **Contrôles applicatifs** o Tests : ▪ Contrôle d'entrée et d'accès ; ▪ Contrôle du traitement ; ▪ Contrôle des sorties ; ▪ Traçabilité ; o FRAP	• **Projet de rapport** • **Réunion de clôture** - Entretien ; - Validation des constats et recommandations. • **Rapport définitif**	

Source : Nous même, inspiré du «The IT audit plan process » (GTAG 11, 2008 : 3).

3.2.Population de l'étude et les outils d'analyse.

Nous décrivons dans cette section, les techniques, les outils d'analyse et de collecte de données que nous utiliserons ainsi que la population cible sur laquelle nous allons appliquer notre démarche d'audit.

3.2.1. Population cible.

Notre principale mission est d'auditer l'application de gestion des encaissements de la SENELEC, décentralisée dans ses différentes agences. Pour ce faire, nous allons effectuer notre mission dans deux (02) agences (Agence de Vincent plateau et une autre au choix). Pour chaque agence nous allons cibler le chef d'agence et deux (02) cassiers. Ainsi, pour chaque individu nous allons effectuer l'audit de l'application de gestion installé sur leur poste (ordinateur). Bien entendu, tout audit d'une application doit également apprécier la sécurité de l'infrastructure informatique nécessaire au fonctionnement de celle-ci.

Nous allons également intégrer dans notre population cible, l'agent informaticien responsable du contrôle de la dite application.

3.2.2. Techniques, outils d'analyse et de collecte de données

Pour mener à bien notre mission, il nous faut collecter certaines informations aussi bien qualitatives que quantitatives afin de les analyser et faire des recommandations. Pour ce faire, nous allons utiliser les outils suivants :

3.2.2.1. Outils de collecte de données

Nous distinguons ici le questionnaire de prise de connaissance, l'interview, l'observation physique, le sondage statistique et le test sur l'application.

3.2.2.1.1. Le questionnaire de prise de connaissance (QPC)

Cet outil permet à l'auditeur d'avoir une vision d'ensemble de l'entité et du domaine audité. Il liste la documentation à se faire communiquer. Le questionnaire sera utilisé comme une check-list de documents et d'informations à obtenir dès le début de la mission. Le dépouillement des informations obtenues permettra de faire une présentation de l'entité, de se familiariser avec les procédures en place, etc.

3.2.2.1.2. L'interview

L'interview permet de recueillir des informations auprès de l'interlocuteur. Il a pour but d'une part de connaitre et comprendre les activités au sein de l'entreprise, et d'autre part d'avoir une idée des procédures de fonctionnement du système informatique et de déterminer les procédures de contrôle qui régissent le domaine audité. Il peut porter sur des questions ouvertes ou sur des questions ou des questions fermées. L'interview sera mise en œuvre pour obtenir des explications détaillées sur des faits et manquements relevés. Il s'agira principalement d'interviews semi-directifs et d'interviews sous forme de causeries pour tirer le maximum d'informations des différents interlocuteurs grâce à un guide d'entretien prévu à cet effet.

3.2.2.1.3. L'observation physique

C'est l'outil de validation par excellence lors d'une mission d'audit. Il permet de s'assurer de la réalité, de la permanence ou de la conformité des dispositifs de contrôle interne. Il nous permettra de faire l'état des lieux sur les dispositifs de sécurité logique et physique et environnementale, le contrôle de la sécurité et l'accès aux sites et locaux sensibles. Ceci grâce à un guide d'observation et de contrôle. Ce sera le principal outil de validation des dispositifs sécurité physique.

3.2.2.1.4. Le sondage statistique

Le sondage statistique sert au dépistage des dysfonctionnements, à l'appréciation de l'ordre de grandeur d'un phénomène ou à l'estimation des attributs dudit phénomène. Cet outil sera utilisé pour valider les réponses positives du questionnaire de contrôle interne. Il servira également de faire le tirage aléatoire de deux opérations saisies pour en vérifier l'exactitude, l'exhaustivité des opérations ainsi que le respect des procédures.

3.2.2.1.5. Le test sur l'application

Le test consiste à effectuer et à documenter les étapes manuelles et/ou automatiques du processus ou de la classe de transaction sur la base d'une transaction type servant d'exemple. Il sert à vérifier la compréhension du processus concerné, les risques et les contrôles réalisés. Il sera utilisé pour simuler une opération d'encaissement et de vérifier tout le long du processus que les différentes étapes sont respectées et sécurisées. Il servira également à vérifier que les contrôles applicatifs sont fonctionnels.

3.2.2.1.6. Site Web du département d'audit

Un certain nombre de départements d'audit se sont dotés d'un site Web. Ces sites fonctionnent généralement sur l'Intranet, mais peuvent aussi se trouver sur Internet. Les solutions Internet permettent le partage d'informations entre les organisations à l'échelle mondiale, mais posent des problèmes de confidentialité (GTAG 4, 2009 : 18). Il nous permettra de recueillir des informations nécessaires à la réalisation de notre mission d'audit.

3.2.2.1.7. Documentations mises à jour

Il s'agit de documentations régulièrement mises à jour et relatives aux différentes applications à auditer, mais aussi tout autres documents afférents à la politique informatique de l'organisation. Cet outil sera utilisé pour acquérir les connaissances nécessaires sur l'objet de notre audit.

3.2.2.1.8. Contrôles d'accès

Quelle que soit la méthode choisie pour déterminer l'étendue des contrôles applicatifs, il convient de procéder à un examen périodique des contrôles d'accès logiques aux modules ou aux applications. Dans la plupart des cas, les droits d'accès utilisateurs et administrateurs (lire, écrire et supprimer) sont conçus sur la base des outils et de la plateforme de sécurité inhérents à l'application. Cela permettra de vérifier si l'organisation se conforme à cette plateforme.

3.2.2.2. Outils d'analyse de données

Il s'agit de l'analyse documentaire, du tableau des risques, du questionnaire de contrôle interne et des FRAP.

3.2.2.2.1. L'analyse documentaire

Elle consiste à l'exploitation des documents de l'organisme faisant l'objet de l'étude. Il s'agit de consulter les documents obtenus ainsi que les informations collectées afin d'en tirer une connaissance plus approfondie. C'est donc une bonne technique de rapprochement pour la vérification des données. Cet outil sera utilisé tout le long de la mission, surtout dans la phase de préparation.

3.2.2.2.2. Tableau des risques

Ce tableau découpe l'activité (en fonction ou processus) objet de l'audit afin d'identifier les risques inhérents. Il permet d'associer à chaque tâche, les risques susceptibles de se produire et de proposer les meilleures pratiques ou dispositifs de contrôle interne pour y pallier. En fonction du degré d'affinement de l'analyse, il comprendra 3 à 8 colonnes. C'est à partir de ce tableau que l'auditeur précisera les objectifs de la mission.

3.2.2.2.3. Questionnaire de contrôle interne (QCI)

Cet outil est un questionnaire préétabli pour chaque fonction et chacun des objectifs de l'audit. Il liste également les principaux points de contrôle interne qu'il est généralement nécessaire de prévoir. Le questionnaire permet de relever les mesures du contrôle interne existant, de constater les lacunes et points forts du processus informatique mis en place. Les questions sont de types « fermées » et le questionnaire est conçu de sorte qu'un « non » équivaut à une lacune ou faiblesse ; et qu'un « oui » équivaut à une force qui devra ensuite être validée par sondage ou par observation physique. Il sera construit à partir des processus du GTAG que nous avons décrit plus haut.

3.2.2.2.4. La FRAP

C'est un outil d'analyse des anomalies rencontrées. Les FRAP servent pour l'ossature du rapport qui est élaboré à partir des observations y figurant. L'ossature du rapport est en quelque sorte un rassemblement des FRAP d'une manière cohérente et selon une logique de hiérarchisation des problèmes rencontrés, assortie d'un commentaire descriptif.

3.2.2.2.5. Test de cheminement

Un test de cheminement désigne l'analyse systématique (reconstruction) d'un processus et sert à comprendre et à vérifier ce dernier. Lors de cette vérification, l'auditeur suit les chemins à travers le processus définis par les conditions préalables et, le cas échéant, par les décisions prises par l'utilisateur. Il existe également un autre test qui permet de faciliter l'analyse des résultats du test par comparaison avec les résultats du test précédent après une maintenance ou une correction du programme : c'est le test de non-régression. Il sera utilisé pour mieux comprendre le processus d'encaissement sur le SYTRIIS et de vérifier s'il est conforme au processus décrit par le management.

3.2.2.2.6. Accélérateurs de tests

Il s'agit d'outils d'analyse de la sécurité, d'outils d'analyse de réseau, d'outils de piratage, d'outils d'analyse de la sécurité des applications (GTAG 4, 2009 : 19). Compte tenu de la limitation de nos ressources (techniques), nous n'aurons pas à utiliser ce genre d'outils.

3.2.2.3. Techniques de collecte de données

Il s'agit des techniques d'audit assistées par l'ordinateur, la méthode du processus d'entreprise et la méthode de l'application unique.

3.2.2.3.1. Techniques d'audit assistées par ordinateur

les techniques d'audit assistées par ordinateur recourent aux applications informatiques, telles que ACL, IDEA, VIRSA, SAS, SQL, Excel, Crystal Reports, Business Objects, Access, et Word pour automatiser et faciliter le processus d'audit (facilitateurs d'audit). Elles permettent d'instaurer la couverture requise pour un examen des contrôles d'une application, en particulier lorsque des milliers, voire des millions, de transactions sont effectuées durant une période de test (GTAG 8, 2009 : 13). Compte tenu de la limitation de nos ressources, nous n'aurons pas recours à ces techniques.

3.2.2.3.2. Méthode du processus d'entreprise

La méthode du processus d'entreprise (*business process*) est une approche de revue descendante (*top-down*), utilisée lorsqu'on veut évaluer les contrôles applicatifs présents dans tous les systèmes qui supportent un processus donné. Au cours des dernières années, cette méthode a gagné en importance au point de devenir la plus courante et la plus largement employée. Cette popularité s'explique principalement par une augmentation de l'utilisation des applications transactionnelles ERP (GTAG 8, 2009 : 9). Nous n'aurons pas recours à cette méthode, mais plutôt à la méthode suivante (méthode de l'application unique) car nous auditons une application décentralisée.

3.2.2.3.3. Méthode de l'application unique

L'auditeur utilise la méthode de l'application unique lorsqu'il veut examiner les contrôles applicatifs au sein d'une seule application, ou d'un seul module, au lieu de s'intéresser à l'ensemble du processus d'entreprise. Comme nous l'avons expliqué précédemment, il s'agit de la

méthode la plus efficace pour déterminer l'étendue de la revue dans un environnement non-ERP, ou non intégré, car l'auditeur peut plus facilement isoler l'application (GTAG 8, 2009 : 9).

Conclusion Chapitre 3

Ce chapitre nous a permis de présenter la démarche référentielle que nous utiliserons lors de la phase pratique. Il a également permis de présenter les différents outils qui nous serons nécessaires pour la réalisation de l'audit de l'application informatique décentralisée de gestion des encaissements de la SENELEC. Il marque l'achèvement de la revue de littérature et le passage à la partie pratique de notre étude.

Conclusion de la première partie

La revue de la littérature a permis de présenter le système informatique ainsi que l'audit des applications informatiques et notre modèle d'analyse.

L'inhérence des risques informatiques nécessite de leur accorder une attention particulière. Les entreprises qui exploitent de plus en plus les technologies de l'information pour la gestion de leur clientèle, comme la SENELEC, sont exposées à ces risques et donc concernées par cette assertion.

La mission de la SENELEC, les mutations technologiques en cours et la gouvernance du système informatique posent des exigences de performance. Cela passe par la connaissance du niveau de sécurité actuelle du système d'information. Et l'audit est le support sur lequel peut s'appuyer la SENELEC pour assurer la performance de son système et par conséquent de ses applications informatiques de gestion. Il attirera l'attention des dirigeants sur le niveau de sécurité et les menaces qui pèsent sur la performance de l'entité et permettra de définir des axes d'amélioration de ce processus hautement stratégique.

DEUXIEME PARTIE : CADRE PRATIQUE

Introduction Partie 2

La mondialisation impose aux entreprises africaines d'être plus performantes. Pour ce faire, celles-ci procèdent à l'automatisation de leurs processus métiers et à l'acquisition d'applications en adéquation avec leurs besoins. Cette automatisation n'est pas sans risques, d'où la nécessité de prendre des précautions pour en minimiser leurs impacts.

La sécurité de ces outils informatiques, particulièrement des applications nécessite une véritable prise de conscience et la mise en place de dispositifs techniques et organisationnelles adéquats.

La SENELEC, depuis plus d'une décennie, c'est lancée dans un important projet d'automatisation de ces activités. Ce qui la conduit même à développer certaines applications à l'interne pour être plus efficace. Cette politique expose l'entité à de nombreux risques qui doivent être maîtrisés. Et l'un des outils de maîtrise de ces risques est l'audit.

Dans cette partie du travail, nous procéderons à l'audit de l'application informatique de gestion des encaissements et d'édition des factures de la SENELEC, décentralisée dans toutes ces agences ; et nous finirons par la présentation des résultats et les recommandations. Mais tout d'abord nous procédons à la présentation de la structure et de son système d'information.

CHAPITRE 4 : PRESENTATION DE LA SENELEC

Introduction

La Société Nationale d'Electricité du Sénégal (SENELEC) est une société anonyme à capitaux publics majoritaires, qui intervient dans le secteur de l'énergie électrique, et dont le siège social est situé à la rue Vincent à Dakar. Avec un capital de plus de 125, 676 milliards de francs CFA, elle est l'une des grandes entreprises industrielles du Sénégal. En effet, elle est concessionnaire de la production, du transport, de la distribution et de la vente de l'énergie électrique ; mais également, de l'identification, du financement et de la réalisation de nouveaux ouvrages sur son périmètre. Elle dispose du monopole du transport de l'électricité sur l'ensemble du territoire ainsi que de l'exclusivité de la distribution sur son périmètre.

Il sera question dans ce chapitre de présenter la SENELEC à travers son historique, sa mission et objectifs, son organigramme ainsi que ses perspectives de développement.

4.1.Historique

La SENELEC est née de la fusion entre l'ex-société d'Electricité Du Sénégal et l'ex-société chargée de l'exploitation des ouvrages, la Société Sénégalaise de Distribution d'Energie Electrique, instituée par la loi n°83/72 du 05 juillet 1983.

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

Dans le cadre de la reforme du secteur de l'énergie, le gouvernement décide en janvier 1998, d'ouvrir le capital de la société au public, pour remédier à son problème de financement. Elle est ainsi transformée en société anonyme et le 31 mars 1999, son capital est ouvert avec comme partenaires stratégiques HYDRO QUBEC et ELYO.

Face à la persistance des difficultés dans la distribution de l'électricité, le gouvernement sénégalais décide de rompre avec ses partenaires stratégiques, après une concertation avec ceux-ci. La rupture est consommée et le 21 septembre 2000, et l'Etat sénégalais redevient l'unique actionnaire. Il faut noter que depuis sa création en 1984, la SENELEC a été l'un des moteurs les plus dynamiques du développement économique et social du Sénégal. De 604 000MWh en 1983,

ses ventes sont passées à 1 866 766MWh en 2008. Dans le même temps, sa pointe maximale du réseau de 99 MW à 407 MW et sa puissance installée de 184 MW à 476,8 MW.

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 tout en gardant le monopole du transport de l'électricité sur l'ensemble du territoire ainsi que de l'exclusivité de la distribution sur son périmètre.

Après avoir fait un bref historique de l'entité, nous passons à la présentation de sa mission et des ses objectifs.

4.2.Mission et objectifs

La SENELEC a une mission prioritaire qui est de fournir de l'électricité aux citoyens et aux industries afin de participer activement au développement du Sénégal. Pour ce faire, elle s'est fixée comme objectifs globaux l'accroissement du niveau d'électrification sur tout l'étendu du territoire et l'atteinte de l'autosuffisance énergétique. De plus, l'état attend maintenir le monopole du transport, de la distribution et de la vente d'énergie électrique sur l'ensemble du territoire.

4.3.Les services offerts

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

4.3.1. La production

Toute la production électrique du pays est d'origine thermique. Une grande partie du parc thermique fonctionne au pétrole. La SENELEC dispose de plusieurs zones de production. La puissance totale installée du parc de production est de 601,5 MW. Mais différentes contraintes dont la vieillesse de certains équipements, font que la puissance assignée du parc de production n'est que de 528,4 MW en 2006. Cette puissance est répartie comme suit :

- réseau interconnecté : 495 MW
    - production propre de Senelec : 327 MW (Centrales à vapeur : 91, Production Diesel : 164 et Turbine à Gaz : 72) ;
    - production privée : 168 MW (Diesel temporaire : 58, Hydroélectrique Manantali: 60, GTI : 50)

- réseau non interconnecté : 33,4 MW (Bel Air, Cap des Biches et les sites régionaux).

4.3.2. Le transport

La fonction du réseau de transport est d'acheminer l'électricité en haute tension (90 et 225 kV) des centrales où elle est produite vers les centres de consommation. Au Sénégal, Le réseau de transport comprend un réseau national (327,5 kms de lignes 90 kV) et un réseau supranational (945 kms de la ligne 225 kV).

4.3.3. La distribution

Alimenté à partir des postes HT/MT et MT/MT, les réseaux électriques diffusent l'électricité vers les autres utilisateurs : particuliers, administrations, industries et commerces. Les transits entre la production et les points de consommation constituent un processus complexe du fait de l'impossibilité de stocker l'électricité et de la nécessité de faire face à une demande variable à tout instant. Au cœur de ce processus se trouve le Dispatching de Hann, véritable centre d'aiguillage de l'électricité qui, 24 heures sur 24, veille au maintien de l'équilibre production/consommation. Le Dispatching est assisté par le Bureau Central de Conduite qui veille en permanence sur le réseau MT de Dakar.

4.4.La structure organisationnelle

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. Il 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. La SENELEC, pour pouvoir mettre en application ses projets de développement, s'est dotée d'une nouvelle structure organisationnelle depuis 2009 à travers la note de direction n° 013/2009 qui réglemente l'organigramme général et le fonctionnement de la SENELEC (voir annexe 1). La nouvelle organisation se présente comme suit :

- **la Direction Générale (DG) :** qui coordonne les activités de la SENELEC ;
- **la Direction Générale Adjoint (DGA)** : par la délégation du Directeur Général, supervise les structures de support suivantes qui lui sont directement rattachées :
    - 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 ;

- **la Direction de l'Audit Interne et du Contrôle de Gestion (DAICG) : e**lle 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 également 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. De plus, elle s'occupe du « *reporting* », de l'analyse des résultats, pour le Directeur Général, de l'élaboration du budget général de l'entreprise et du suivi de son exécution ;
- **la Direction du Contrôle Général (DCOG) : e**lle 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 également le respect des normes techniques de réalisation des ouvrages d'exploitation et de maintenance ;
- **la Direction des Ressources Humaines (DRH) : e**lle est chargée de la gestion prévisionnelle et de la gestion administrative centralisée des ressources humaines. Elle est aussi 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 Operations et Maintenances (O&M). Elle gère également les stocks de combustibles et lubrifiants mis à sa disposition ;
- **la Direction du Transport (DT) : e**lle 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) : e**lle a pour mission l'élaboration des politiques et la fixation des objectifs globaux dans le domaine de la distribution ; elle assure aussi la

maintenance et l'exploitation du réseau Moyenne Tension et Basse Tension de Dakar et de sa 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 ;
- **la Direction des Finances et de la Comptabilité (DFC) :** elle est responsable de l'enregistrement exact, exhaustif et de la traçabilité de toutes les transactions comptables et financières de la 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 aussi 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 ;
- **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 la SENELEC et ses clients et entre la SENELEC et les tiers avec l'appui des conseils. Elle joue le rôle de « risk manager » de l'entreprise.

4.5.Les perspectives de développement

Suite à de nombreuses difficultés rencontrées ces dernières années, l'Etat du Sénégal c'est vue dans l'urgence de prendre un certain nombre de mesures. Ceci dans l'intention d'accroitre la qualité des services de la SENELEC et d'asseoir sa politique de développement. En effet, les difficultés rencontrées étaient en grande partie d'ordre financier. Les principales causes étaient entre autres les créances non recouvrées auprès de la clientèle, le non reversement de la totalité de certains prêts souverains accordés par les institutions financières, la compense perçue avec du retard et/ou pour des montants insuffisants (entre l'Etat et la SENELEC), les pertes financières dues à la fraude, etc. Ceux-ci avaient comme conséquences des ruptures d'approvisionnement en combustible, l'absence de maintenance des équipements, le problème de renouvellement des investissements et des difficultés à payer les fournisseurs, qui à la fin, exigeaient un règlement au comptant.

Face à ces difficultés, une perspective de sortie de crise a été trouvée entre l'Etat et la SENELEC suite à une mission d'audit stratégique et technique du secteur de l'énergie au Sénégal, confiée à un cabinet international. Les recommandations formulées tournaient autour des principaux axes suivants : l'augmentation de la capacité de production à 150 MW, la maîtrise de la demande, le renforcement de l'image de marque et la restauration de la relation de confiance entre la SENELEC et sa clientèle, une restructuration financière, la restauration du mode de régulation tarifaire, une contre performance interne évaluée à 20% pour la SENELEC et 80% pour l'Etat, etc.

Ces recommandations ont été traduites, par l'Etat, en plan d'action appelé plan de relance et de restructuration du secteur de l'électricité : « Plan TAKKAL ». Ce plan qui se décline en cinq (05) volets, a été évalué à environ six cent cinquante (650) milliards de F CFA et doit se dérouler sur la période de 2011 à 2012.

En outre, depuis 2005, un projet informatique a été mis en œuvre et devait normalement être atteint sur trois (2005, 2006, 2007). Cet important projet informatique, qui devait soutenir le développement de l'activité de l'entreprise, à connu des difficultés faute de financement.

Conclusion Chapitre 4

La SENELEC a traversée des moments de difficultés, suite à divers facteurs financiers. Mais, vu le caractère stratégique du secteur de l'énergie dans le développement économique et social, l'Etat du Sénégal a pris un certains nombre de mesures. Ces mesures claires et précises, ouvrent des perspectives de développement pour faire de la SENELE le moteur de l'activité économique au Sénégal.

Après cette brève présentation de la structure organisationnelle et fonctionnelle de la SENELEC, nous passons à la description de son système informatique, plus précisément de son application de gestion des encaissements et d'édition des factures (le SYTRIIS), qui fera l'objet de notre audit.

CHAPITRE 5 : DESCRIPTION DU SYSTEME INFORMATIQUE : LE SYTRIIS

Introduction

Depuis 1998, la SENELEC s'est dotée d'un système d'information automatisé pour supporter ses activités et être plus performante. Ce système repose sur le logiciel standard « ORACLE APPLICATIONS », qui est fortement intégré (ERP) et qui couvre la majeure partie de ses activités.

Cependant, compte tenu du volume et de la complexité de certaines opérations, l'entreprise c'est dotée d'applications développées à l'interne en adéquation avec ses besoins. Parmi ces développements internes, nous avons le Système d'Information Clientèle (SIC), centralisé à Dakar et en connexion avec toutes les agences. Ce dernier est constitué de plusieurs applications dont le SYTRIIS. En effet, le SYTRIIS est une application informatique qui permet la gestion décentralisée des encaissements et d'édition des factures. Il est implanté dans toutes les agences et connecté au SIC.

Ce chapitre sera pour nous l'occasion de faire une brève présentation du système d'information de la SENELCE et de décrire son application SYTRIIS.

5.1.Le système d'information de la SENELEC

Il s'agit ici de présenter l'architecture du système d'information de la SENELEC ainsi que sa cartographie applicative.

5.1.1. Architecture du système d'information

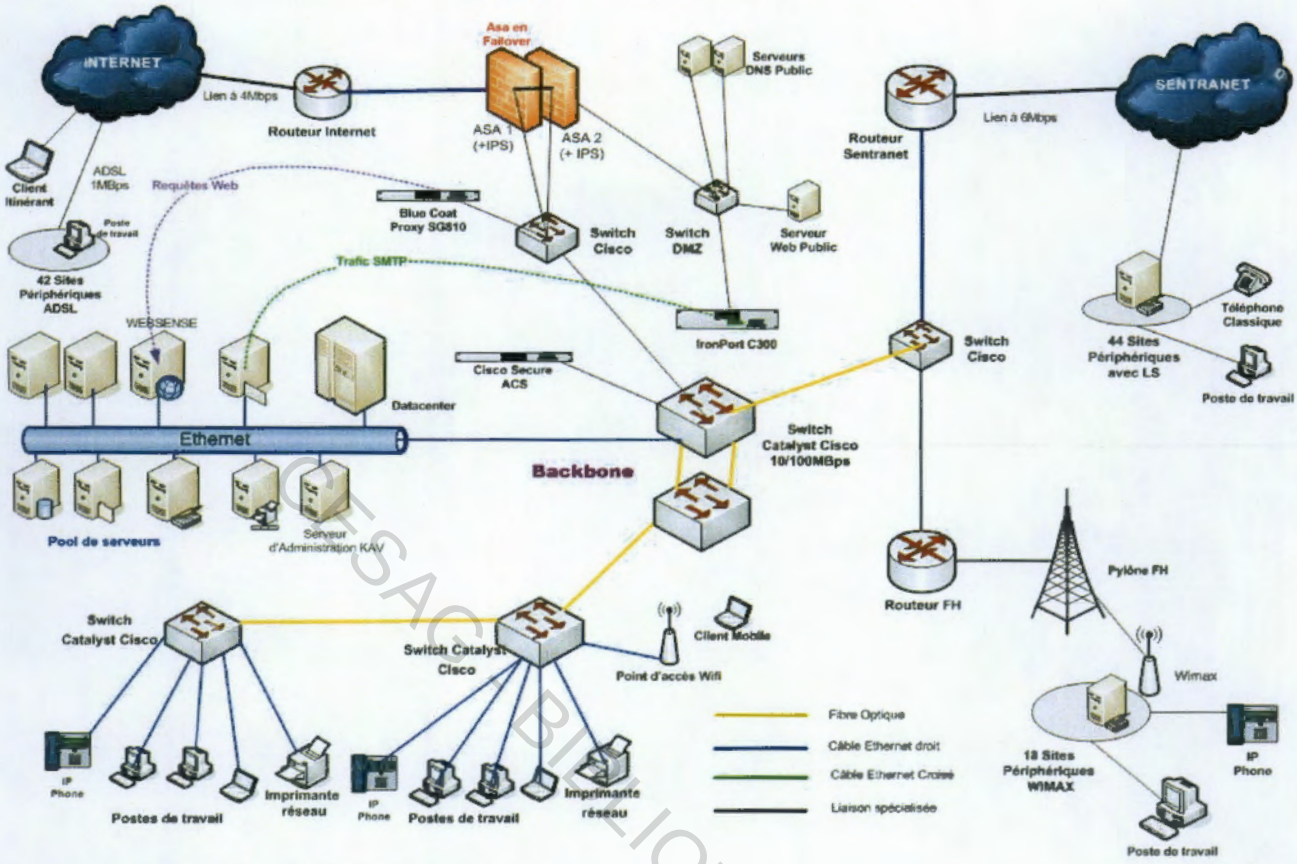
La SENELEC a opté pour la solution SENTRANET VPN Haute Disponibilité. Le SENTRANET est le réseau de transport sécurisé de la SONATEL, pour les accès permanents utilisant le protocole TCP/IP à très haut débit. Néanmoins, elle dispose de deux types de liaisons :

- les 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, et ;
- d'un réseau FH (Faisceau Hertzien) avec des liens allant de 8Mbits au niveau des agences de Dakar à 155Mbits au niveau de Hann, Cap des biches et Vincens.

Il faut noter, que l'entité dispose également d'une liaison internet de 4MB/s. Son réseau est ouvert au monde extérieur grâce au réseau IP. Pour empêcher toutes intrusions non autorisées, la

SENELEC a installé le système de protection réseau PIX Firewall Cisco, comme le décrit la figure suivante.

Figure 5: Présentation du système d'information de la SENELEC



Source : Cahier des charges 2012 de la DSI.

Au vu de la figure 5, le système d'information est composé d'éléments divers. 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 ;

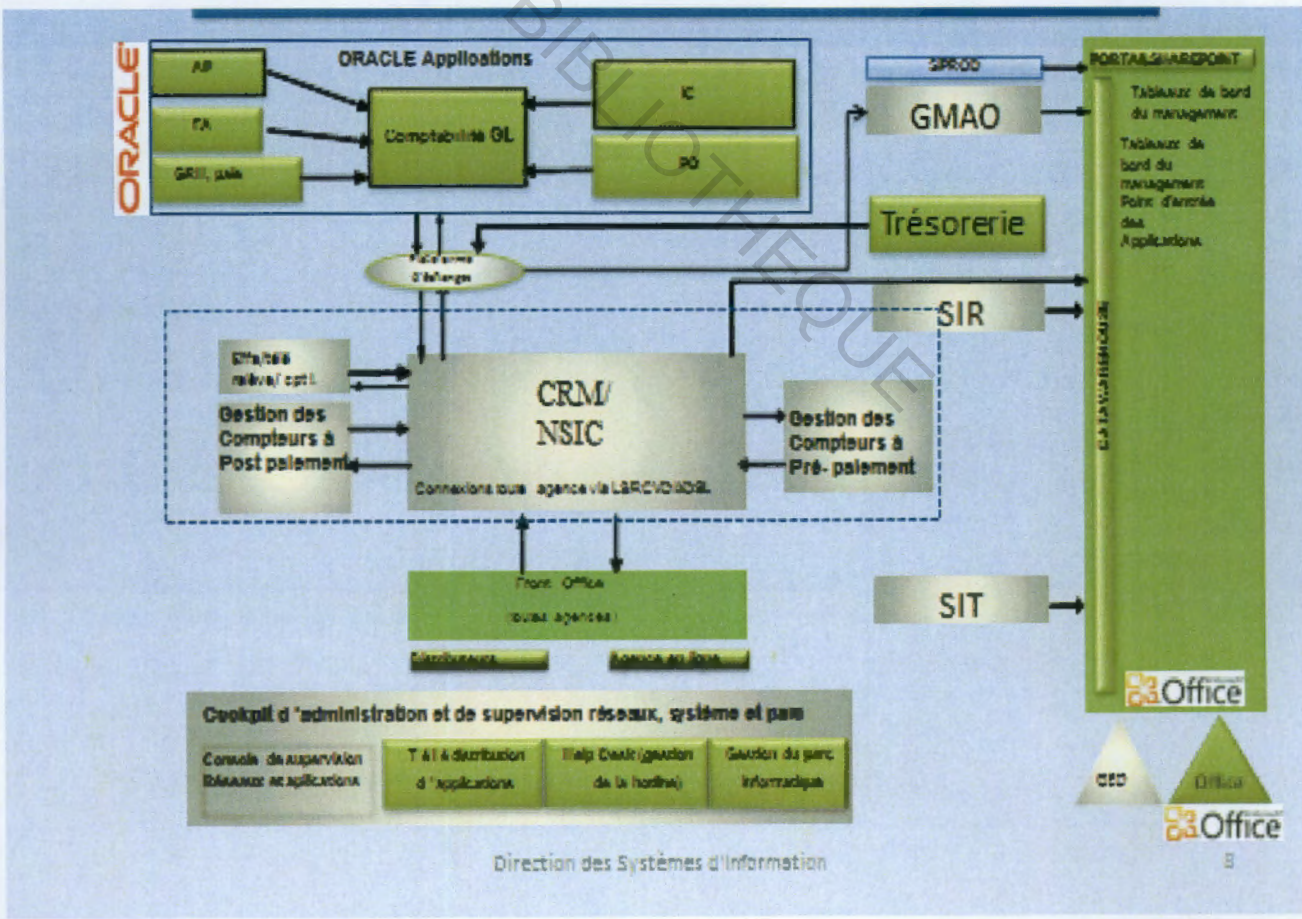
- double lien fibre Optique entre le bâtiment DCC et le siège ;
- liaisons FH entre les sites Vincens, Hann, Mbao et Cap des biches.

Le patrimoine informatique de la SENELEC est bien fourni aussi bien en matériel qu'en logiciels. Pour sa gestion, elle utilise différents types de logiciels (les logiciels systèmes, les progiciels acquis et les logiciels développés en interne).

5.1.2. Architecture applicative du système d'information

Depuis 1998, l'entreprise s'est dotée d'un logiciel standard : « ORACLE APPLICATIONS ». C'est un ERP (Enterprise Resource Planning) qui sert de base à l'ensemble du système d'information de la structure. En outre, compte tenu du volume de ses opérations et de la complexité de certaines d'entre elles, la SENELEC a développé à l'interne une application du nom de SIC (Système d'Information Clientèle) en adéquation avec ses besoins. En effet, cette application lui permet de suivre les revenus clients à partir de ses différents modules. La figure suivante nous donne de plus amples information sur le système applicatif.

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



Source : Dossier d'audit DSI (2012).

Au vu de la figure 6, on constate que le système applicatif de la SENELEC tourne autour des principales applications suivantes :

- l'ERP ORACLE : qui 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), et ;
- le Système d'Information Clientèle (SIC) : qui comprend plusieurs modules dont le SYTRIIS.

Cependant, de façon exhaustive le Système applicatif actuel est composé des principales applications suivantes :

Tableau 5 : Liste actuelle des applications à la SENELEC

Applications	
Oracle GL – Gestion des comptabilités	CENTRAL PARC – Gestion du matériel roulant
Oracle AP – Gestion des fournisseurs	DANILES COURRIER – Gestion électronique du courrier
Oracle FA – Gestion des immobilisations	Datawarehouse – Système d'aide à la décision pour le Commercial
Oracle IC – Gestion des stocks	RADAR : fourniture des éléments de reporting à la Direction Commerciale.
Oracle PO – Gestion des achats	Système d'Information Clientèle
Oracle HR – Gestion des ressources humaines	SYTRIIS – Décentralisation des impressions de factures et de leur encaissement
Oracle Payroll – Gestion personnalisée de la paie	Système de Prépaiement (Woyofal)
Oracle Discoverer	SIPROD – Système d'information de la production
ECASH – Gestion de la trésorerie	Portail d'entreprise – Intranet
EMATCHER – Rapprochement bancaire	Site WEB – Senelec

Source : Nous même.

La cartographie des applications montre les interactions existant entre ces différentes applications (standard et développement interne) utilisées par la SENELEC.

5.2.Description de l'application SYTRIIS

Le SYstème de Transfert d'Information Inter-Site (SYTRIIS) est une application qui permet la décentralisation des fonctionnalités d'édition et d'encaissement. Il a été implanté en 2004 pour venir en support au système de base de gestion de la clientèle (SIC) qui connaissait plusieurs dysfonctionnements (lenteur dans le traitement des opérations, etc.) dus à sa vétusté (implanté depuis 20ans).

Pour le SYTRIIS, les échanges d'information entre les différents sites se faisant sur la base de règles de routage paramétrables, sont parfaitement sécurisés. Ce système regroupe plusieurs composantes, à savoir : la base de données, les services de conduite de flux, le service de transport de données inter-site, les applications et le serveur d'abonnement IP. Toutes ces composantes du système peuvent être regroupées en trois grandes catégories : système, éditique et caisse.

5.2.1. La composante « système »

La composante « système » constitue l'infrastructure de conduite des flux d'informations entre les sites centraux et les différents sites décentralisés. Elle assure : les services de routage, la remise et la réception des données avec acquittement, la gestion des ruptures de liaison inter-site, et le schéduling (ordonnancement) des services de conduite de flux.

5.2.1.1. Le routage de l'information

Il s'agit ici de présenter les types de mouvements SYTRIIS, la route (comment les flux de données circulent), la carte de routage de l'information et les conteneurs des données inter site (fichier FME).

5.2.1.1.1. Les types de mouvements SYTRIIS

Les flux SYTRIIS sont référencés par grandes catégories, appelées type de mouvement. Le type de mouvement précise la nature du flux de données ainsi que les règles de routage d'information qui doivent lui être appliquées. Chaque type de mouvement précise :

- **la classe émissaire** renfermant l'ensemble des règles de gestions fonctionnelles à appliquer (détermination de la clé de routage, contrôle de la cohérence fonctionnelle des flux, etc.) ;
- l'autorisation de circulation des flux d'informations correspondantes entre les sites SYTRIIS ;
- l'origine interne (crée par SYTRIIS) ou externe (crée hors SYTRIIS) des flux d'informations correspondantes, et ;
- les fichiers de description pour les chargements en bloc des flux d'informations correspondantes dans les bases SQL SYTRIIS (Bulk copy).

Comme types de mouvements nous avons : la facture base tension (FACBT), la facture moyenne tension (FACMT), l'écriture (ECRIT) et l'encaissement SYTRIIS (ENCAI).

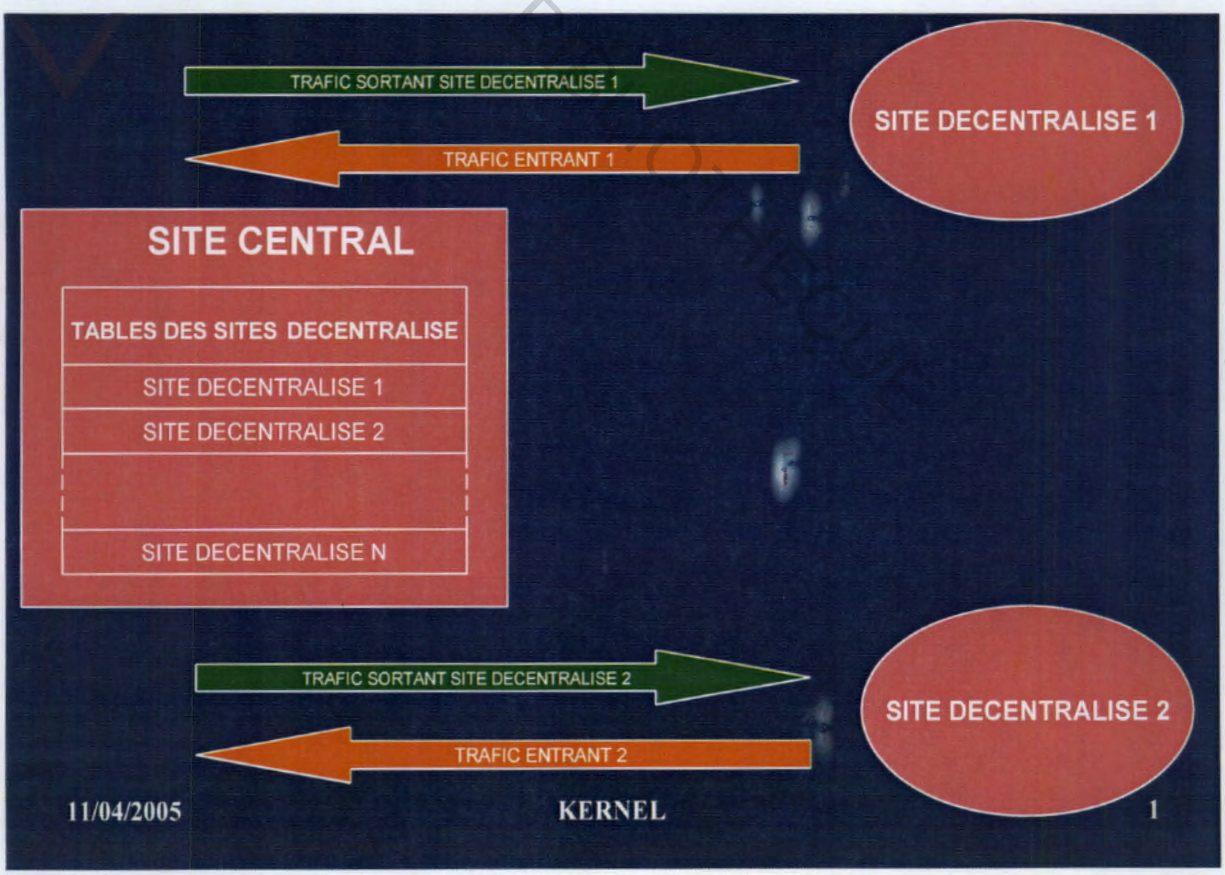
5.2.1.1.2. La route SYTRIIS

La route SYTRIIS est le support reliant le site central à un site décentralisé donné. Elle permet l'acheminement des flux d'informations sur les liaisons informatiques ayant des débits variés (33 Kb/s, 1 Mb/s, 100 Mb/s etc.). La route SYTRIIS est créée suite à la configuration du site central et l'activation du site décentralisé. Par site décentralisé, est créée :

- une route spécialisée dite **route de trafic sortant (RTS)** pour le trafic des flux d'informations allant du site central vers un site décentralisé donné, et ;
- une route spécialisée dite **route de trafic entrant (RTE)** pour le trafic des flux d'informations allant du site décentralisé vers le site central.

La route SYTRIIS, constituée de deux extrémités (origine et miroir), est à fonctionnement uni directionnel ; la circulation de l'information se faisant de l'extrémité d'origine vers l'extrémité miroir jusqu'à la parfaite synchronisation des deux extrémités, comme le montre la figure suivante :

Figure 7 : Organisation des routes SYTRIIS



Source : Guide d'utilisateur (KERNEL, 2012 : 6).

5.2.1.1.3. La carte de routage de l'information

La résolution du routage de l'information se fait par les services de conduite des flux du site central SYTRIIS, sur la base des deux éléments suivants:

- la clé de routage fonctionnel portée par les flux d'informations, et ;
- la carte d'adressage des sites décentralisés appelée carte de routage.

La carte de routage dont le paramétrage est externalisée, précise pour chaque clé de routage, l'adresse de la ou des routes à référencer dans le cadre du transfert des informations. SYTRIIS prévoit deux types de cartes de routage :

- **la carte de routage individuel :** elle précise les règles de routage de l'information dans le cadre des mouvements devant être traités par les centres, et ;
- **la carte de routage regroupé :** elle précise les règles de routage de l'information dans le cadre des mouvements (facture) devant être traités par les centres dits de regroupement (bordereaux factures).

Une même clé de routage peut être présente dans les deux types de cartes de routage. Lors des traitements de transfert de données, les flux d'informations pour lesquels aucune route n'est prévue dans les cartes de routage sont rejetés en « route non résolue ». Ils ne sont pas transférés par SYTRIIS. Les deux scénarios de routages de l'information ci-dessous décrits sont possibles :

- une même information peut être routée vers des destinations distinctes (de façon indépendante en route regroupée et individuelle), ou ;
- plusieurs informations distinctes peuvent être routées vers la même destination.

Cette disposition de paramétrage donne à l'entreprise la possibilité de prendre en compte toutes les configurations possibles de distribution de son information.

5.2.1.1.4. Les conteneurs de données inter site (fichier FME)

Les fichiers de message SYTRIIS (FME) contiennent les données devant être transportées d'un site SYTRIIS à l'autre. Ils sont transmis par le biais des routes SYTRIIS et leur contenu est crypté.

Le paramétrage de SYTRIIS permet de maîtriser le poids de chaque fichier FME en octet, de s'adapter au débit de la liaison et au sens du trafic correspondant à chacune des routes SYTRIIS. Le dimensionnement des fichiers FME est fait au moyen de l'outil IOF.

5.2.1.2. Les transferts d'information (Transfert asynchrone)

Les transferts asynchrones permettent aux sites SYTRIIS de communiquer avec un faible couplage. Ceci assure leur fonctionnement, même dans des conditions de ruptures de liaison. La nature **asynchrone** des transferts permet de déployer des sites SYTRIIS sur des postes mobiles (portable). Ces sites effectueront les opérations de synchronisation avec le site central en se connectant au réseau de l'entreprise (connexion LAN, RAS, etc.). Lors d'un transfert, lorsqu'une rupture de liaison se produit, l'infrastructure des services SYTRIIS la détecte automatiquement et suspend le transfert en cours. Le transfert suspendu est automatiquement relancé dès le rétablissement de la liaison.

5.2.1.2.1. Le fichier instruction

Les fichiers d'instructions permettent de sérialiser les chargements des fichiers de données SYTRIIS. Chaque fichier d'instruction précise les informations suivantes :

- la séquence de chargement (séquence qui sera contrôlée par SYTRIIS) ;
- le type de mouvement traité, et ;
- la localisation du fichier de données a charger.

Il contient également les informations de contrôle de la cohérence fonctionnelle du fichier à charger. La présence du fichier instruction est indispensable au chargement des fichiers de données par SYTRIIS. Le lot de fichiers à charger est mis à la disposition de SYTRIIS de la façon suivante :

- positionnement du fichier de données (copie dans le répertoire mentionné par le fichier instruction) ;
- copie du fichier instruction dans le répertoire des fichiers instruction SYTRIIS.

Cet ordre doit être scrupuleusement respecté afin d'éviter que le système ne tente de traiter un fichier de données en cours de copie et donc indisponible. La séquence de chargement permet de sérialiser la prise en charge des fichiers de données SYTRIIS en garantissant que chaque chargement effectué par le système correspond à celui attendu. Elle est définie par type de mouvement et pour l'ensemble des opérations d'émission normales et réémission (cas d'incohérence). Lorsque la séquence de chargement n'est pas conforme à celle attendue, SYTRIIS met le transfert en anomalie et le signale par une notification.

5.2.1.2.2. Les déversements fonctionnels

Les données transférées par le système SYTRIIS sont mise à la disposition des applications utilisatrice qu'après qu'elles aient été déversées dans les tables fonctionnelles correspondantes. Le déversement des informations ne s'effectue que si SYTRIIS constate que la réception de l'information est cohérente.

5.2.1.2.3. Les soumissions et réceptions des fichiers

Cette séquence dépend de la nature du type de mouvement (FACBT, etc.). Lorsqu'un lot cohérent (fichier instruction et donnée) est soumis au système SYTRIIS pour transfert, le déclenchement des opérations de transfert se fait automatiquement.

5.2.1.2.4. Trace de l'encaissement SYTRIIS

La consultation des sessions de caisse sur le site décentralisé, permet d'identifier la date de validation de celle-ci, ainsi que le numéro du transfert (qui correspond au label du fichier) vers le site central qui a assuré le transfert de cet encaissement. Le numéro du fichier de transfert de la session de caisse est affiché au bas de l'état **Session de caisse**, lorsque la session a été validée et prise en compte par les services de transfert SYTRIIS.

5.2.1.3. Surveillance du trafic d'informations (SAF)

Cette application dispose d'une surveillance de trafic d'information intégrée. Le Superviseur de transfert de Fichier (SAF) permet de suivre à l'échelle de l'entreprise les opérations de transfert de fichier inter site. L'état des fichiers transférés est actualisé de façon automatique en fonction de l'avancement des opérations. Il permet le suivi des transferts qu'il s'agisse d'émission ou de réception, qu'on soit sur le site central ou sur un site décentralisé. La mise en « inconsistance » des transferts de façon à permettre l'épuration des opérations inachevées est également possible grâce à cet outil.

5.2.2. La composante « caisse »

La « caisse-sytriis » permet l'exécution de l'ensemble des fonctionnalités liées à un poste de caisse (ouverture/fermeture de caisse, encaissements, etc.) de façon autonome. Le principe de la caisse est d'enregistrer toutes les opérations d'encaissement et de décaissement avec les contraintes de fiabilité et de sécurité requises par ce type de transactions. La caisse autonome assure l'ensemble des opérations présentées dans le tableau ci-dessous :

Tableau 6 : Les opérations pris en charge par la CAISSE-SYTRIIS

Opérations	Sous opérations
Opération de déclarations de caisse	Déclaration/activation poste de caisse
	Configuration poste de caisse
Opération de gestion de session de caisse	Ouverture/fermeture de session
	Validation de session
Opération d'encaissement	Encaissement facture
	Encaissement écriture
	Encaissement divers
	Encaissement frais de coupures
	Annulation encaissement
	Transfert de fond
Opération de contrôle de caisse	Synthèse de caisse
	Journal de caisse
	Session de caisse
	Edition bordereau de chèque

Source : Nous même.

5.2.2.1. Les opérations de déclarations de caisse

Il existe des conditions préalables au fonctionnement du poste de caisse. Pour qu'un poste de travail puisse fonctionner en tant que caisse il faut au préalable :

- qu'il ait été déclaré comme poste de caisse auprès du site central SYTRIIS, et ;
- qu'il ait été configuré en poste de caisse, après avis positif à la demande de déclaration auprès du site central.

5.2.2.2. Les opérations de gestion de session de caisse

La session de caisse est le regroupement logique et cohérent des opérations effectuées sur une caisse durant une journée calendaire donnée, entre deux actions d'ouverture et de fermeture de caisse. Elle permet un repérage précis des écritures de caisse (Date, auteur, poste de caisse, etc.).

La gestion des sessions de caisse s'effectue suivant le principe décrit ci-dessous :

- si la caisse, ou plus précisément la session de caisse n'est pas fermée, et si sa date d'ouverture correspond à la date du jour, alors les opérations de caisse, se poursuivent sur la même journée de caisse : **on dit que la session de caisse est réactivée ;**

- si la caisse, ou plus précisément la session de caisse n'est pas fermée, et si sa date d'ouverture est différente de la date du jour, un message informe l'utilisateur de la nécessité de fermer la caisse pour la dernière journée ouverte ;
- si la caisse, ou plus précisément la session de caisse est fermée, une nouvelle session de caisse est créée et la caisse est ouverte.

Toute ouverture de nouvelle session de caisse est subordonnée à la fermeture de la session précédente. Toute session de caisse ne peut s'étendre au-delà d'une journée calendaire : le système impose, qu'elle soit fermée.

5.2.2.3. Les opérations d'encaissement

Il existe diverses sortes d'opérations d'encaissement, dont les plus courantes sont :

- **encaissement écriture :** ce type d'encaissement concerne les soldes d'écritures débiteurs disponibles sur le site décentralisé après réception quotidienne des lots des écritures provenant du site central (synchronisation des écritures ou déversement fonctionnel du fichier écriture). Cette transaction permet d'effectuer le règlement des écritures inscrites dans le compte d'un client donné. Les éléments ou opérations engagés dans les encaissements sont automatiquement soldés. Le solde du compte d'écritures est automatiquement actualisé ;
- **encaissement facture :** cette transaction permet d'effectuer le règlement de factures d'énergie client (BT, MT). Les factures engagées dans les encaissements sont automatiquement soldées, en temps réel. Le solde du compte polices locales est automatiquement actualisé. Les encaissements partiels sur facture ne sont pas permis. L'encaissement sur facture ne tient pas compte de la date d'échéance de la facture. Il signale l'état échu de la facture sans bloquer le déroulement de l'opération ;
- **encaissement frais de coupures :** cette transaction permet d'effectuer le règlement des frais de coupure. Le montant des frais de coupure est paramétré. Il peut être redéfini à tout moment sur le site décentralisé ;
- **encaissement divers :** cette transaction permet d'effectuer le règlement de factures (commande, travaux, ...) émises dans le cadre de l'exécution de prestations de services. Les opérations d'encaissements divers, passe sur un compte général appelé « DIVERS » ;
- **transfert de fonds :** cette transaction permet d'effectuer soit une sortie de caisse, c'est-à-dire un transfert de fonds vers une autre caisse ou une banque ; soit une entrée de caisse c'est-à-dire réceptionner un fond venant d'un transfert inter caisse ;

- **annulation encaissement :** cette transaction permet d'annuler un encaissement. L'annulation d'encaissement, ne se fera uniquement que sur les encaissements de la session ouverte.

5.2.2.4. Les opérations de contrôle de caisse

Cette rubrique comprend les opérations suivantes :

- **journal de caisse :** cette transaction permet d'éditer les journaux détaillés et synthétiques de caisse pour une période donnée ;
- **session de caisse :** la transaction de consultation des sessions de caisse permet d'obtenir les états suivants : l'état synthétique de caisse, l'état de session de caisse et le bordereau de chèques ;
- **synthèse de caisse :** cette transaction permet de consulter et éditer les informations de synthèse de caisse ;
- **clôture de session de caisse :** la clôture de session de caisse permet de mettre fin à une session de caisse. Elle permet de contrôler l'équilibre de la caisse par rapprochement du solde informatique de celui déclaré par le caissier. Cette clôture donne lieu à un rapprochement entre les mouvements de la session de caisse pris en compte par le système, le fond de caisse et la déclaration du solde de la session de caisse ;
- **édition bordereau de chèque :** cette transaction permet d'éditer un bordereau récapitulatif des chèques encaissés par banque et par type de chèque. Le bordereau de chèque est éditable à tout instant, dès lors que la session de caisse est clôturée.

5.2.3. La composante « éditique »

Cette composante permet la gestion des éditions, du paramétrage (dessin des maquettes d'états), jusqu'à la production des états de façon autonome. Elle se focalise sur les domaines suivants : le design des documents, l'acquisition des datas, la gestion, la composition dynamique ainsi que l'impression des documents, la programmation multi canal et la vérification de l'authenticité des documents produits.

5.3.Les différents acteurs du système informatique

En application de la note de Direction n°013/2009 du 25 mai 2009 (voir annexe 6), les principaux acteurs du système informatique sont :

- **l'Etat Major :** qui comprend l'Expert Organisation et Méthode, l'Expert Sécurité et l'Assistant Gestion et Logistique ;
- **département Développement des Services (DDS) :** il gère le développement et la maintenance des applications par l'élaboration et le suivi du respect des normes de développement informatique. Il définit les besoins en termes de plateformes de génie logiciel. Il veille sur la cohérence des modèles de données de l'entreprise et participe à la formation des utilisateurs. Il comprend deux (02) services : le Service Avant-projets et Urbanisation (SAU) et le Service Développement d'Application (SDA), et ;
- **département Exploitation des Services (DES)** : il joue le rôle de support. Il procède à la mise en œuvre des applications et outils définis par le SDA ; Il définit les stratégies systèmes (serveurs et postes de travail) ; veille sur la fiabilité et la sécurité de stockage des informations et assiste les utilisateurs. Il définit les moyens à mettre en œuvre pour l'attente de cette mission par la définition des besoins en matière de licences de systèmes d'exploitation. Il comprend deux (02) services également : le Service Production et Support utilisateur (SPS) et le Services Infrastructure et Réseaux informatiques (SIR).

Conclusion Chapitre 5

Le système informatique de la SENELEC est divers et très varié. Ce chapitre nous a permis de nous faire une idée sur l'ensemble des applications de l'entité, d'explorer le SYTRIIS et de présenter les principaux intervenants. Cette description achevée, nous passons au déroulement de nos travaux d'audit ainsi qu'à la présentation des résultats obtenus et aux recommandations proposées. C'est l'objet du prochain et dernier chapitre de notre étude.

CHAPITRE 6 : RESULTATS, ANALYSE DES RESULTATS ET RECOMMANDATIONS

Introduction

L'ultime chapitre de cette étude est l'occasion de faire une présentation du déroulement de nos travaux d'audit et d'effectuer une synthèse des forces et des faiblesses constatées. Chaque faiblesse et/ou force donne lieu à des recommandations qui devraient permettre de les corriger et de renforcer les dispositifs existants. Le suivi et l'application desdites recommandations nécessite qu'un plan d'action soit mis en œuvre pour assurer une prise en compte efficace et méthodique des solutions retenues.

6.1.Le déroulement de la mission d'audit

Cette narration reprendra les points les plus significatifs de notre méthodologie ainsi que les outils retenus. Il est donc question ici de la mise en œuvre de notre modèle d'analyse.

6.1.1. La préparation et le cadrage de la mission

Cette phase a débuté avec la prise de connaissance de l'entité (voir annexe 6) par le déroulement de notre questionnaire de prise de connaissance. Cela a permis, dans un premier temps, d'identifier les stratégies, les objectifs de l'entreprise et de comprendre les principaux risques liés aux activités de l'organisation. Elle a également permis de nous familiariser avec l'environnement interne et externe de la SENELEC, ce qui nous a permis d'effectuer la présentation de la structure (structure organisation, système d'information, etc.) et d'identifier les départements impliqués dans le processus que nous avons audité (chapitre 4 et 5). C'était également l'occasion de comprendre comment les opérations commerciales et les fonctions des services informatiques supportent les activités de l'organisation.

Dans un second temps, cela nous a permis de définir l'univers informatique. Nous avons identifié les objectifs clés de l'entreprise et les processus, les applications informatiques importantes qui supportent les processus d'affaires, les infrastructures nécessaires pour les applications, les modèles de l'organisation des services supports des TI, et le rôle des techniques de soutien tel que les dispositifs de réseau. C'est ainsi que nous avons limité nos investigations au processus d'encaissement des factures, et les applications qui interviennent dans ce processus sont le SIC et le SYTRIIS. Néanmoins, notre mission se déroulant dans un site décentralisé (agence), l'application qui nous concerne directement est le SYTRIIS ; le SIC étant implanté au siège pour le traitement des données issues du SYTRIIS et l'édition des FME. L'étape de familiarisation a également été l'occasion de faire connaissance avec le personnel et les principaux responsables,

grâce à des interviews visant à mieux comprendre le fonctionnement des différents services (voir annexe 3) ; et d'effectuer une visite des locaux.

Ensuite, après avoir eu une compréhension des processus de soutien des services et des objectifs de mise en œuvre du système informatique, nous avons procédé à un inventaire exhaustif de l'environnement informatique (voir annexe 6). Cet inventaire, à son tour, a constitué la base de l'évaluation des vulnérabilités qui peuvent avoir une incidence sur les contrôles internes. Cette étape a conduit à l'élaboration du tableau des risques (voir annexe 7). L'analyse du tableau des risques qui est au cœur de notre démarche (approche par les risques), répertorie les risques opérationnels et identifie les meilleures pratiques. Ce tableau est également le guide de mise en œuvre des tests que nous concevrons pour la recherche d'éléments probants.

Les informations et les analyses acquises par la compréhension de l'organisation, l'inventaire de l'environnement informatique et l'évaluation des risques se jettent dans la dernière étape, la formalisation du plan d'audit. L'objectif de ce plan est de déterminer où concentrer l'assurance de l'auditeur et le travail de consultation pour assurer la gestion de l'information objective pour gérer les risques (informatiques) de l'organisation et de l'environnement de contrôle.

Du fait de l'absence d'auditeur informatique, notre champ d'investigations n'a pu s'élargir à d'autres domaines comme l'analyse des données, etc. Néanmoins, les objectifs généraux définis dès le début de la mission et les objectifs spécifiques figurant dans le tableau des risques conduisent à déterminer le champ d'action suivant.

Tableau 7 : Champ d'action des travaux d'audit

Lieu, local ou emplacement	Population cible
▪ Salle informatique (siège) ▪ DSI (Etat major, SDA et SPS) ▪ Agence Vincens	• Expert sécurité, salle des serveurs. • Deux (02) agents. • Chef d'agence, deux (02) cassiers, deux (02) caisses-sytriis, deux (02) ordinateurs et les locaux abritant les caissiers.

Source : Nous même.

La phase de préparation s'achève avec la définition du champ d'action. Nous passons à la phase d'exécution de la mission.

6.1.2. La réalisation de la mission d'audit : les travaux sur le terrain

Cette phase a consisté à la finalisation du questionnaire de contrôle interne et à son administration auprès des principaux acteurs impliqués dans le processus. Nous avons ensuite procédé à l'élaboration d'un programme de travail et à la conduite des travaux de vérifications sur le terrain. Le contexte de l'étude n'a pas permis d'effectuer une réunion d'ouverture classique. Toutefois, avant de procéder à une quelconque opération, une sensibilisation a été effectuée auprès de chaque personne rencontrée, notamment en ce qui concerne les objectifs de l'étude et la méthodologie. Le planning d'audit est présenté dans le tableau ci-après.

Tableau 8 : Programme d'audit

Objet	Service/lieu	Nature des travaux
Questionnaire de contrôle interne	- Etat major -SDA -SPS -Agence Vincens	-**s'informer** en administrant le **QCI** aux personnes concernées : l'expert sécurité, le responsable du service SDA ou un agent, le responsable du service SPS ou un agent, le chef d'agence vincens/deux (02) caissiers. - **s'informer** par des **interviews**, afin d'éclaircir les zones d'ombre issues de l'administration du QCI. - **s'assurer de la vraisemblance** des réponses issues du QCI et les **confirmer** par un **test d'existence**.
Sécurité logique	-PC utilisateurs -Caisse-sytriis	-**simuler une opération d'encaissement** depuis l'accès à l'application « caisse-sytriis » jusqu'à l'édition du reçu d'encaissement. -**effectuer** les contrôles d'entrées et des accès, les contrôles de traitement de données et les contrôles de sorties.
Sécurité physique	-Salle informatique -Salle technique -Locaux abritant les caissiers	**Inspecter** pour les différents locaux : la qualité des murs ; la qualité des portes, des fenêtres et du vitrage ; l'étanchéité (humidité au plafond, sol et mur) ; le positionnement de la salle des serveurs ; le système de détection incendie ; les extincteurs ; l'alarme automatique ou manuelle ; la protection des câblages ; l'arrivée multiple du courant électrique ; les onduleurs et batteries-relais redondant ; la climatisation ; la protection des supports de sauvegarde.

Source : Nous même.

6.1.2.1. . Mise en œuvre des tests de fonctionnement des contrôles internes

Il s'agit ici de la mise en œuvre de notre programme de vérification. Nous effectuerons les contrôles, les inspections et les tests nécessaires.

6.1.2.1.1. Administration du QCI et entretien avec les personnes ressources

Nous avons procédé comme suit :

- **pour les questionnaires de contrôle interne :**
  - finalisation des questionnaires de contrôle interne après la prise de contact avec les audités ;
  - dépôt d'un exemplaire du QCI auprès des auditées au moins une (01) semaine avant chaque rencontre. Il faut noter que chaque personne concernée par l'audite recevait un questionnaire spécifique en relation avec son domaine de compétence ;
  - rencontre avec les audités une (01) semaine après réception du QCI. Il s'agissait ici d'échanger avec eux sur des questions mal comprises ou de recevoir des explications plus approfondies sur certains points ;
  - revue et analyse des informations obtenues ;
  - synthèse des données. ;

- **pour les interviews :**
  - finalisation du guide d'entretien après la prise de contact avec les audités ;
  - fixation des rendez-vous avec les différents responsables concernés 3 jours avant ;
  - administration du guide d'entretien aux audités pendants au moins 30 minutes par entretiens ;
  - revue et analyse des informations obtenues ;
  - synthèse des données.

Des questionnaires de contrôle interne ont été administrés à l'expert sécurité, à deux (02) agents de la SDA, à un (01) agent de la SPS et au chef d'agence Vincens ainsi qu'à deux (02) de ses caissiers. Des entretiens ont également été sollicités. Il faut noter qu'après tous ces travaux, nous avons vérifié la véracité des informations obtenues par des observations sur le terrain et des tests d'existence présentés dans les sections suivantes.

6.1.2.1.2. Observation et inspection des locaux et des dispositifs de sécurité

L'objectif ici est de s'assurer de la sécurité physique des infrastructures abritant les outils nécessaires au bon fonctionnement de l'application SYTRIIS. C'est ainsi que nous avons procédé à l'inspection de la salle des serveurs, des locaux des caissiers et des installations informatiques de façon générale. Nous avons procédé aux vérifications suivantes :

- vérification de la qualité des murs à l'intérieur et à l'extérieur : solidité, protection des cloisons et positionnement de la salle ;
- vérification de la qualité des portes, des fenêtres et du vitrage ;
- vérification de l'étanchéité : l'humidité au plafond, au mur et au sol ;
- vérification du système de détection d'incendie ;
- vérification de l'alarme automatique/manuelle ;
- vérification des extincteurs fixes (automatiques) et des extincteurs mobiles, avec la dernière de contrôle et d'évaluation de ces derniers ;
- vérification de la protection des câblages extérieurs ;
- vérification de l'arrivée multiple du courant électrique ;
- vérification de la présence des onduleurs et des batteries-relais redondant ;
- vérification de la présence des climatiseurs dans les salles sensibles ;
- vérification de l'organisation et de rangement des locaux ;
- vérification des supports et du lieu de stockage des sauvegardes de données.

6.1.2.1.3. Contrôle applicatifs et tests sur le SYTRIIS

Il s'agissait ici de réaliser les contrôles applicatifs sur le SYTRIIS avec les tests proposés pour chaque contrôle (modèle de l'IIA, chapitre 2). Nous avons procédé par la méthode de l'application unique qui consiste à isoler l'application afin d'effectuer les contrôles applicatifs correspondants, ensuite nous avons simulé une opération d'encaissement pour effectuer les tests.

- **contrôles des entrées et des accès :** ces contrôles permettent de vérifier que toutes les données d'entrée sont exactes, complètes et autorisées. Tests :
    - observer les tentatives d'entrer des données incorrectes ;
    - déterminer qui peut passer outre les contrôles ;
    - procéder à des tests sur la base des droits d'accès des utilisateurs ;
    - vérifier les privilèges d'accès pour chaque fonction ou transaction sensible ;
    - examiner les droits d'accès qui établissent et modifient des limites configurables d'agrément ou d'autorisation ;

- s'ils sont gérés par tables, déterminer qui peut altérer les modifications et les niveaux de tolérance ;

- **contrôles de la transmission des fichiers et des données :** ces contrôles permettent de vérifier que les fichiers et les transactions transmis en interne ou à l'extérieur par voie électronique ont été envoyés par une source identifiée et traités exactement et complètement. Tests :
  - observer les rapports de transmission et d'erreur ;
  - observer les paramètres de validité et d'exhaustivité et les réglages ;
  - examiner les droits d'accès à la définition et à la modification des paramètres configurables pour le transfert de fichiers ;

- **contrôles du traitement :** ces contrôles permettent de vérifier que les données d'entrée valides ont été traitées exactement et complètement. Tests :
  - comparer les valeurs d'entrée et de sortie ;
  - examiner le processus d'évaluation de l'exhaustivité et de la validité des données extraites ;
  - inspecter les rapports d'erreur à l'interface ;
  - inspecter les paramètres et les réglages de la validité et de l'exhaustivité ;
  - examiner les droits d'accès au réglage et à la modification des paramètres configurables sur les interfaces ;
  - examiner les preuves des rapports de correspondance, des vérifications et du traitement des fichiers contenant des erreurs ;
  - examiner les droits d'accès au réglage et à la modification des paramètres configurables sur les transactions ou les fichiers dupliqués ;
  - examiner le processus de manipulation des fichiers ou des transactions rejetés ;

- **contrôles des sorties :** ces contrôles permettent de vérifier que les données de sortie sont complètes, exactes et diffusées à qui de droit. Tests :
  - remonter jusqu'au grand livre général un échantillon de transactions synthétisées d'entrée et du grand livre auxiliaire.

6.1.2.2. Validation et évaluation des résultats

Il s'agit ici de la validation et de l'évaluation des résultats issus de nos vérifications et tests. De l'entretien avec l'expert sécurité et des différentes inspections réalisées en sa présence, nous avons pu nous faire une idée sur le dispositif de sécurité mis en place comme le présente les tableaux ci-après :

Tableau 9 : Identification et évaluation des dispositifs de sécurité informatique

IDENTIFICATION ET EVALUATION DES DISPOSITIFS DE SECURITE INFORMATIQUE		
Section	**Oui/ Force apparente**	**Non/Faiblesse apparente**
Sécurité physique		
Infrastructures physiques	x	
Qualité des murs et des fenêtres	x	
Détection d'intrusion (alarmes, gardiennage)	x	
Protection incendie		
Dispositif détection/extinction	x	
Protection électrique		
Un onduleur avec batterie est en place sur chaque serveur		x
Climatisation	x	
Contrôle des accès		
Contrôle des accès (jour/nuit)	x	
Conditions de fonctionnement		
Hygiène-propreté	x	
Rangement des locaux informatiques		x
Proximité d'autres risques		x
Maintenance du matériel		
Des contrats existent pour les serveurs	x	
Plan de secours informatiques		
Existence et documentation	x	
Tests de sécurité	x	
Sécurité logique		
User-id et mot de passe au démarrage	x	
User-id et mot de passe à l'entrée des applications	x	
User-id et mot de passe sont personnels	x	
Renouvellement régulier des mots de passe		**En cours**
Gestion des profils d'accès sur les données bureautiques	x	
Antivirus sur serveur et postes	x	
Mise à jour antivirus	x	
Verrouillage des configurations	x	
Procédure de sauvegarde		
Stockage externe	x	
Contrôle de relecture	x	
Sauvegarde des postes individuels (PC)		x

Source : Nous même, adapté de CLEUET et al (2008a :58-59).

Tableau 10 : Evaluation des dispositifs de sauvegarde

EVALUATION DES DISPOSITIFS DE SAUVEGARDE				
Questions				**Réponses**
En fonction du contexte et de la configuration informatique, combien de jours sont nécessaires pour remplacer celle-ci suite à un vol ou à un incendie ?				Indéterminés
Combien de jours d'arrêt informatique peut-on tolérer ?				0 jour
Sait-on travailler en mode « manuel » en se référant à des procédures dégradées ?				Oui
Niveau de risque en cas de sinistre				
Application	**Conséquence d'un arrêt (en jours)**			**Mesures dégradées**
	Faible	**Importante**	**Vitale**	
Système d'Information Clientèle			x	Oui
SYTRIIS – Décentralisation des impressions de factures et de leur encaissement		x		Oui
Délai de reconstruction du système informatique				Jours
Récupération d'un serveur				Un jour
Configuration OS, outils et réseau				Un jour
Restauration des applications, données				Un jour
Récupération hub				Un jour
Installations et câblages				Plusieurs semaines

Source : Nous même, adapté de CLEUET et al (2008a :57-59).

Les autres entretiens ont permis de se faire une idée sur les procédures de contrôles applicatifs et de gestion des incidents, le processus d'encaissement sur la « caisse-sytriis » et les différents niveaux d'habilitation.

Outre ces entretiens, nous avons procédé également à des analyses des documents mis à notre disposition lors des différentes rencontres de prise de contact et de prise de connaissance de l'organisation. C'est ainsi que nous avons reçu de la Direction Commerciale et de la Clientèle (DCC) un récapitulatif des incidents informatiques rencontrés par leurs agents sur les six (06) derniers mois. La synthèse de ce récapitulatif, nous donne le tableau suivant :

Tableau 11 : Synthèse des incidents relatifs aux mois de janvier à mars 2012

synthèse des incidents relatifs aux mois de janvier à mars 2012			
Applications	**Description**	**Cause**	**Nombre d'apparition en 03 mois**
SYTRIIS	session non transférée	lenteur du réseau internet	**1**
	synchronisation SYTRIIS	lenteur du réseau internet	**9**
	Mise à jour fichier SYTRIIS	lenteur du réseau internet	**10**
	Configuration SYTRIIS et transfère docs	Incapacité du chef d'agence à le faire	**1**
	Non apurement de sessions SYTRIIS	lenteur du réseau internet	**11**
	Non déversement dans le SIC d'une session SYTRIIS	lenteur du réseau internet	**6**
	Instabilité du réseau SYTRIIS	Coupure d'électricité	**1**
	Erreur base de donnes SYTRIIS	Erreur de configuration	**1**
	Sessions non validées.	lenteur du réseau internet	**3**
	Problème visualisation du journal de caisse	Problème de configuration	**3**
	Activation SYTRIIS facturation	Incapacité du chef d'agence à le faire	**1**
SIC	Mot de passe S I C	Incapacité du chef d'agence à le faire	**6**
	Attribution modules SIC	Incapacité du chef d'agence à le faire	**7**
	Fermeture de sessions	Plantage de la machine	**1**
	Réinitialisation mot de passe viplet	Incapacité du chef d'agence à le faire	**12**
	Problème lenteur	lenteur du réseau internet	**4**
	Changement de localité (mot de passe agent)	Incapacité du chef d'agence à le faire	**3**
	Activation et création de matricules pour contractuels de l'agence…	Incapacité du chef d'agence à le faire	**1**
	Relance	lenteur du réseau internet	**2**
	Problème accès SIC	lenteur du réseau internet	**2**
	Édition différée	Arrêt du système	**1**
Anti-virus	Problème virus	Absence d'anti-virus	**2**

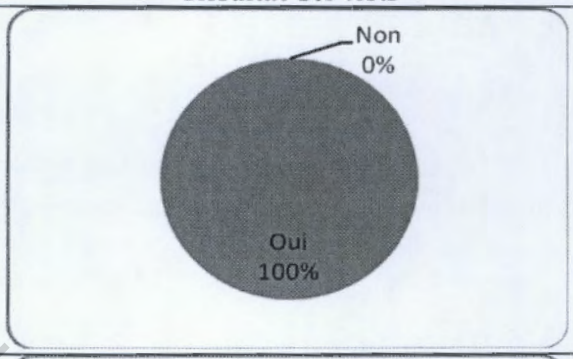
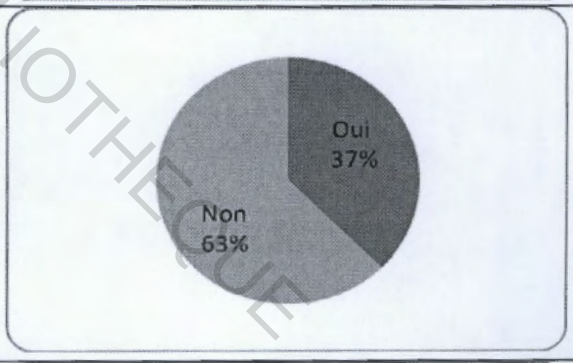
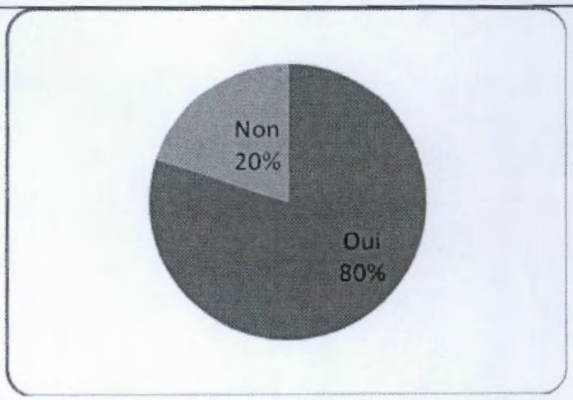
Source : Nous même.

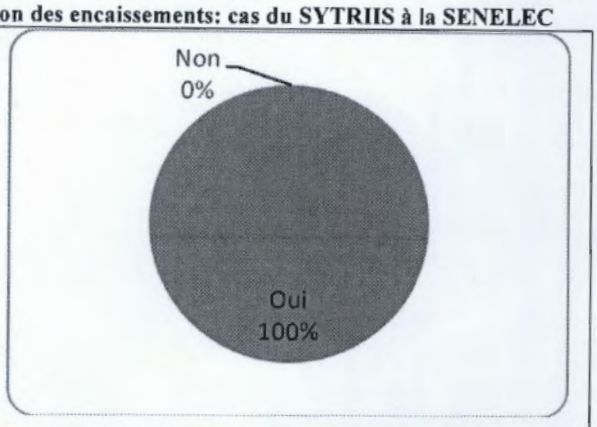
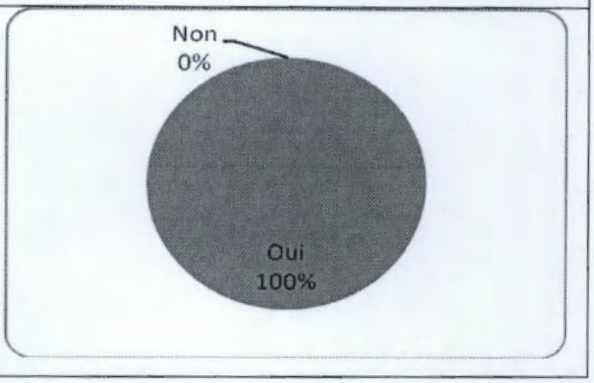
Les vérifications se sont déroulées à trois niveaux : un test de confirmation du questionnaire de contrôle interne (test d'existence) ; ensuite une inspection des infrastructures informatiques (salle des serveurs) et des locaux ; et enfin les contrôles applicatifs sur le SYTRIS avec les tests pour chaque contrôle, tel que proposés par l'IIA (voir chapitre 2).

6.1.2.2.1. Test d'existence

Le questionnaire de contrôle interne (voir annexe 4) a été conçu de telle sorte qu'une réponse négative équivaut à une faiblesse apparente. En ce qui concerne une réponse positive, elle équivaut à une force apparente qui devra faire l'objet d'une confirmation par des tests de conformité (test d'existence). Pour ce faire, nous avons procédé à un sondage statistique qui consiste à sélectionner de manière aléatoire cinq (05) échantillons de réponses positives (trois pour les contrôles applicatifs sur le SYTRIIS et les deux autres pour les contrôles IT généraux) pour ensuite réaliser les tests suivants.

Tableau 12: Tests de confirmation du questionnaire de contrôle interne (réponses positives)

Tests	Résultat des tests
Droit d'accès à la salle des serveurs : Vérifier que seules les personnes habilitées ont accès à la salle des serveurs. • Population cible : 6 • Echantillon : 2	
La charte de sécurité : Vérifier que la charte de sécurité est disponible à tous les utilisateurs de l'informatique et qu'ils en connaissent le contenu. 1. Population cible : 80 2. Echantillon : 16	
Contrôle d'entrée et d'accès à SYTRIIS : Vérifier que les agents responsables d'une caisse-sytriis disposent de mots de passe et qu'ils sont les seules à les connaître. • Population cible : 8 • Echantillon : 5 Certains agents communiquent leur droit d'accès aux stagiaires pour certaines tâches en cas d'absence ou pas.	

Contrôle d'entrée et de traitement des données: Vérifier que les données saisies et traitées (opérations d'encaissement) sont correctes et exhaustives. • Population cible : 20 • Echantillon : 10 La caisse-sytriis dispose d'un contrôle automatique des données (introduction d'un code figurant sur la facture traitée), ce qui réduit les erreurs de saisie.	
Traçabilité des données traitées : Vérifier que sur les reçus (données traitées par la caisse-sytriis) figure la date, l'heure, la taille des données, le volume des enregistrements et l'authentification de la source (automatisé). • Population cible : 20 • Echantillon : 10	

Source : Nous même.

6.1.2.2.2. Résultats issus de l'inspection des infrastructures informatiques et des locaux

Il s'agissait ici de procéder à l'inspection (contrôles IT généraux) de la salle des serveurs, des locaux qui abritent les « caisses-sytriis » ainsi que des dispositifs de sécurité.

Tableau 13 : Inspection des locaux et des dispositifs de sécurité

Points observés	Constats
Qualité des murs	Murs solide à l'intérieur et à l'extérieur, cloisons de protection pour chaque serveur dans la salle serveur.
Qualité des portes, des fenêtres et du vitrage	-Porte en aluminium vitré pour la salle serveur et les locaux des caissiers ; -Simple vitrage des portes et des fenêtres de la salle serveur.
Etanchéité (humidité au plafond, sol et mur)	Aucune trace d'humidité au plafond, au mur et au sol dans les deux salles (serveurs et caisse).
Positionnement de la salle des serveurs	Située au 3ème étage et complètement isolée, avec une porte hermétiquement fermée.
Système de détection incendie	Détecteur de fumée avec déclenchement automatique des extincteurs et de l'alarme dans la salle des serveurs, mais pas dans les locaux des caissiers.
Alarme automatique ou manuelle	Alarme automatique pour la salle des serveurs et manuelle pour le reste des locaux.

Extincteurs	Extincteurs fixes avec système de déclenchement automatique (salle serveurs) et extincteurs mobiles à certains endroits (salle serveurs et locaux). Ils sont vérifiés régulièrement.
Protection des câblages	Câbles dans les goulottes dans l'ensemble des locaux.
Arrivée multiple du courant électrique	Courant du secteur et groupe électrogène avec déclenchement automatique en cas de coupure.
Onduleurs et batteries-relais redondant	-Onduleur défectueux dans la salle des serveurs ; -absence d'onduleurs pour les postes fixes.
Climatisation	-Trois climatiseurs dans la salle des serveurs, température acceptable et constante ; -absence de climatiseur dans les locaux des caissiers.
Rangement des locaux	Bon rangement de la salle des serveurs et des locaux en général.
Présence de poussière	Absence de poussière dans la salle serveurs, ce n'est pas le cas dans les locaux des cassiers.
Protection des supports de sauvegarde	Aucun dispositif particulier
Lieu de stockage des sauvegardes	Stockées dans la salle serveurs

Source : Nous même.

6.1.2.2.3. Résultats issus des contrôles applicatifs et des tests sur le SYTRIIS

Il s'agissait ici de réaliser les différents contrôles et tests sur l'application SYTRIIS.

Tableau 14 : Tests sur le SYTRIIS

Contrôles	Tests	Constats
Contrôles des entrées et des accès	observer les tentatives d'entrer des données incorrectes	Le système rejette automatiquement les données incorrectes.
	déterminer qui peut passer outre les contrôles	Le chef d'agence et les agents du service production et support utilisateur (SPS) en fonction de leur habilitation.
	tests sur la base des droits d'accès des utilisateurs	Un droit d'accès utilisateur est demandé pour accéder à l'ordinateur et à la « caisse-sytriis ».
	vérifier les privilèges d'accès pour chaque fonction ou transaction sensible	Privilège réservé au chef d'agence pour l'attribution des droits, le contrôle des caisses et pour leurs apurements.
	examiner les droits d'accès qui établissent et modifient des limites configurables d'agrément ou d'autorisation	Ce droit est attribué au responsable du SPS.
	déterminer qui peut altérer les modifications et les niveaux de tolérance	Le chef d'agence et les agents du SPS en fonction de leur habilitation.

Contrôles du traitement	comparer les valeurs d'entrée et de sortie	il faut noter qu'après la saisie du numéro de police et le choix du mode de règlement, le montant est calculé automatiquement. De plus, il existe au code à deux lettres au bas de la facture qui permet, après sa saisie, de vérifier automatiquement l'exactitude des montants facturés. D'où il y a rarement une différence entre les données entrées et celles sorties.
Contrôles des sorties	remonter jusqu'au grand livre général un échantillon de transactions synthétisées d'entrée et du grand livre auxiliaire.	Après validation de l'opération et édition du reçu de caisse, l'encaissement est automatiquement enregistré dans le journal de caisse avant son déversement plus tard dans le grand livre général.

Source : Nous même.

Les anomalies constatées dès la phase de préparation et lors de l'administration du questionnaire de contrôle interne (réponses négatives), de même que les dysfonctionnements observés lors de l'inspection des installations IT généraux ainsi que de l'application SYTRIIS, conduisent à des analyses au travers des FRAP (voir annexe 8).

6.2. Synthèse de la mission de l'audit de l'application SYTIIS

Cette section présente les forces et les faiblesses du processus audité. La présentation se fera sous forme de tableau (voir tableau 14 ci-après) sur la base des questionnaires de contrôle interne et des entretiens effectués. Toutes les réponses positives ou éléments existants seront considérés comme des forces. Tandis que, les réponses négatives ou éléments non mis en place seront considérés comme des points faibles et feront l'objet de recommandations.

Tableau 15 : Tableau des points forts et des points faibles du système informatique

Eléments	Points forts	Points faibles
Contrôles applicatifs du SYTRIIS	-Des droits d'autorisation sont accordés à des utilisateurs sur la base de leurs rôles et de leur besoin d'utiliser l'application ; -Le pouvoir de passer outre (attribution des caisses-sytriis, etc.) est réservé à certains utilisateurs (Chef d'agence), sur la base de leurs rôles et de leur besoin d'utiliser l'application ; - Les superviseurs vérifient tous les jours ou une fois par semaine les traitements effectués ; - Le contrôle de l'exhaustivité et de la validité du contenu, y compris la date et l'heure, la taille des données, le volume des enregistrements et l'authentification de la source (automatisé) ; - Application de certains contrôles des entrées afin de valider les données reçues ; - Suivi automatisé des changements apportés aux données, attribuant le changement à un utilisateur précis ; - Suivi automatisé et mise en évidence des contournements des procédures normales ; -Vérification automatique des données reçues depuis les systèmes en amont (données sur les encaissements) par les entrepôts de données ou les grands livres ; -Vérification automatique de la correspondance entre les soldes des deux systèmes (SYTRIIS et SIC). En cas de non correspondance, les fichiers sont rejetés « incohérents » ; -Il existe un contrat de service pour les solutions informatiques qui ont été acquises ; -Il existe une documentation utilisateur, un dossier d'exploitation, et un dossier de maintenance ; -La documentation est de qualité et facilement compréhensible ; - Cette documentation prévoit des illustrations des différents écrans de saisies et écrans de sorties ; et les rubriques sont bien expliquées ; - L'accès au SYTRIIS est sécurisé ; -Les procédures de contrôle et	-La vraisemblance et l'exhaustivité des sorties des routines d'extraction ne sont pas contrôlées ; - Les utilisateurs n'ont pas été formés sur SYTRIIS et n'ont pas assistés à son paramétrage ; -Il n'est pas opéré un contrôle de la fiabilité des données et de leur degré de réponse aux attentes et besoins des utilisateurs (maintenance effectuée qu'en cas d'incident) ; -Les documentations ne sont pas régulièrement mises à jour en cas de changement, de modification ou de mise à jour du module ; -Cette documentation n'est pas communiquée aux utilisateurs concernés ; -Les procédures de contrôle et d'autorisations ne sont pas connues de tous ; - Les contrôles de sauvegarde ne sont pas régulièrement réalisés ; -Souvent les droits d'accès de certains agents qui changent d'environnent (mutation de poste, etc.) ne sont pas supprimés par le chef d'agence responsable (laxisme ou oubli) ; - Problème récurent de formation des agents (caissiers) qui ne savent pas souvent comment utiliser l'application ou corriger certains incidents (apprentissage sur le tas) ; - Absence de politique de contrôle des applications et des équipements informatiques. Les interventions sont effectuées en cas d'incidents exposés par les utilisateurs ; - Absence de mission d'audit (informatique) périodique ; - Absence de mise à jour des connaissances des utilisateurs ; - Pas de transfert de connaissance ; - Souvent les mots de passe de certains agents absents sont communiqués à leurs collègues pour continuer le travail ; -Absence de rapport sur l'application

	d'autorisations des accès sont formalisées ; - La politique de sauvegarde existe avec une périodicité des sauvegardes connue et automatisée ; -Collaboration avec les développeurs pour la résolution de certains incidents ; - sauvegarde des données trois (03) fois par jour et une (01) fois en fin de semaine ; - Possibilité de travailler en mode dégradé (en mode manuel).	SYTRIIS ; - Lenteur dans le traitement des opérations (déversement des caisses-sytriis dans le SIC) dans certaines agences, due à l'instabilité du réseau (internet) ; -Obsolescence du SIC (Vétusté de l'application installé depuis 20 ans), ce qui entraine la lenteur dans le traitement des opérations ; - Certaines agences préfèrent utiliser le SIC au détriment du SYTRIIS (défaut de maîtrise de l'application).
Contrôles IT généraux	-La politique de sécurité informatique (physique et logique) est formalisée au niveau de l'organisation ; -La DSI a élaboré un document officiel ou charte sur la sécurité qui décline cette politique en actions et procédures concrètes ; -Un expert sécurité, qui a une vision globale (aspects physiques et aspects logiques) de l'organisation ainsi que de l'environnement informatique, est désigné pour des raisons d'efficacité au niveau de l'organisation ; -La charte de sécurité est disponible à tous les utilisateurs de l'informatique ; -Une identification de l'ensemble des risques et menaces en relation avec la sécurité physique des données et équipements informatiques (accès aux locaux d'exploitation, protection physique des équipements, mesures de sécurité contre les intempéries, incendies,...) est effectuée ; -L'accès aux locaux abritant le matériel informatique (serveurs et autres) est limité aux seuls administrateurs du système informatique ; -Sécurité physique : infrastructures, qualité des murs et fenêtres ; - Dispositif de détection/extinction ; -Antivirus sur serveurs et postes et mise à jour ; - Stockage externe et contrôle de relecture périodique ;	-Des séances de formation et/ou de sensibilisation ne sont pas organisées ; -Cette charte ne prévoit pas des mesures de sanctions à l'égard des personnes qui l'enfreignent ; -La liste des risques et menaces n'est pas connue par tous les utilisateurs de l'informatique et des systèmes d'information ; - le plan de secours existe, mais n'est pas fonctionnel (absence de site de secours) ; - Absence de sauvegarde des postes individuels (PC) ; - L'onduleur pour les serveurs est défaillant ; -Absence de renouvellement régulier des mots de passe.

Source : Nous même.

La présentation des forces et des faiblesses issues de l'audit de l'application SYTRIIS achevée, il convient de formuler des recommandations en vu de renforcer les dispositifs déjà existant. Les recommandations seront formulées en fonction de la présentation du tableau des forces et de faiblesses (Contrôles IT généraux et contrôles de l'application SYTRIIS).

6.3.Les recommandations

Ces recommandations devraient être mises en œuvre par le management en les transcrivant en procédures formalisées pour les faire appliquer aussi bien au niveau organisationnel, managérial que technique.

6.3.1. Recommandation sur les contrôles IT généraux

Le management gagnerait à :

- veiller à ce que la charte de sécurité informatique soit diffusée à tous les utilisateurs de l'informatique et qu'elle soit respectée et appliquée ;
- veiller à ce que des séances de formation et/ou de sensibilisation soient organisées dans ce cadre ;
- veiller à ce que cette charte prévoit des mesures de sanctions à l'égard des personnes qui l'enfreignent ;
- veiller à ce qu'une identification de l'ensemble des risques et menaces en relation avec la sécurité physique des données et équipements informatiques (accès aux locaux d'exploitation, protection physique des équipements, mesures de sécurité contre les intempéries, incendies,...) soit effectuée, et ;
- veiller également à ce que cette liste des risques et menaces soit connue par tous les utilisateurs de l'informatique et des systèmes d'information ;
- procéder périodiquement à des examens auprès des utilisateurs du système d'information afin de suivre les progrès réalisés et de déceler les problèmes éventuels (contrôle préventif et de détection) et ne pas attendre à ce qu'un incident subvienne pour apporter des mesures correctrices ;
- veiller à ce que le plan de secours existant soit mis en œuvre et que le site de secours soit fonctionnel ;
- veiller à ce que les données soient sauvegardées sur l'ensemble des postes individuels (PC).

6.3.2. Recommandation sur l'application SYTIIS

Le SYTRIIS en lui-même n'a pas de défauts de conception et fonctionne bien. Bien vrai qu'au début de son implantation les utilisateurs rencontraient quelques incidents, mais ces derniers ont tous été réglés. Néanmoins, certaines anomalies sont toujours constatées. Cependant elles sont en général liées soit à la réticence de certains agents (agence) vis-à-vis de l'application par manque de maîtrise, soit à l'instabilité très fréquente du réseau entrainant aussi bien la lenteur du système (dans certaines agences) que des difficultés d'apurement des caisses-sytriis (déversement des encaissements de la caisse-sytriis dans le SIC). Face à cela, il serait souhaitable de :

- veiller à ce que des séances de formation soient organisées pour les nouvelles recrues ;
- sensibiliser et former les agents (agences) encore réticents sur le SYTRIIS et des perspectives qu'il offre ;
- veiller également à la mise à jour des connaissances des utilisateurs et favoriser le transfert de connaissances entre agents (ancien agent ou non) ;
- veiller à ce que toutes les agences, quelle que soit la zone, utilisent l'application SYTRIIS pour uniformiser les pratiques ;
- mettre en place une procédure pour évaluer régulièrement et ré-authentifier les droits et accès des utilisateurs au système ;
- veiller à ce que les agents qui changent d'environnement voient leurs droits d'accès immédiatement supprimés ;
- veiller à ce que le renouvellement régulier des mots de passe soit effectué ;
- veiller à ce que les actifs informatiques (applications et équipements) soient analysés périodiquement ;
- veiller à ce qu'un contrôle de la fiabilité des données et leur degré de réponse aux attentes et besoins des utilisateurs soit opéré ;
- doter la Direction d'audit interne de compétences nécessaires pour effectuer des missions d'audit des systèmes d'informations périodiquement (à titre préventif) ;
- acquérir ou développer une nouvelle application de gestion de la clientèle, qui répond aux besoins spécifiques de l'organisation et des utilisateurs, en vu de remplacer le SIC qui est obsolète ;
- mettre en place un mécanisme ou des seuils d'alerte pour assurer le suivi des altérations ou obsolescences pouvant affecter le système d'information notamment à cause du progrès technique ;
- enfin, augmenter le débit du réseau (intranet et internet) de la SENELEC pour le rendre plus performant. Ce qui permettra de résoudre le problème de lenteur dans le traitement des opérations (encaissements, etc.) et de réduire le nombre de fichiers « incohérents ».

Conclusion chapitre 6

Au cours de notre mission d'audit, nous avons procédé au déroulement de notre programme de vérification tel qu'il est présenté dans notre modèle d'analyse. Lors de l'administration des questionnaires de contrôle interne, des interviews, des observations physiques, des analyses documentaires et des tests effectués, nous avons relevé des forces et des faiblesses apparentes qui ont fait l'objet d'analyse et de recommandation pour les améliorer.

Ces recommandations doivent être matérialisées dans un plan d'action et de suivi qui doit être mis en œuvre, compte tenu de certaines priorités, du budget disponible et de la disponibilité des différents protagonistes.

Conclusion de la deuxième partie

Cette partie a été l'occasion pour nous de présenter la SENELEC, son système d'information, les mesures de sécurité appliquées et les dispositifs mis en place pour sécuriser son application de gestion des encaissements et d'édition des factures. Les informations reçues et collectées ont permis la mise en œuvre de notre démarche référentielle et la conduite de l'audit de l'application informatique décentralisée SYTRIIS.

Cet audit permettra à la Direction Générale de SENELEC de corriger certaines défaillances constatées sur le plan organisationnel, fonctionnel et pratique.

CONCLUSION GENERALE

Au terme de notre étude, on peut affirmer, sans risque de se tromper, que la majorité des sociétés intègrent les IT (matériels informatique, logiciel ou progiciel de gestion, internet, etc.) dans la gestion courante de leurs activités afin d'être plus performantes. Les IT, bien que bénéfiques, exposent les organisations à de nombreux risques, auxquels le management doit faire face. L'audit est l'un des outils les plus fiables dont disposent les dirigeants pour réduire ces risques afin d'atteindre une assurance raisonnable.

L'audit des états financiers d'une entreprise représente pour les auditeurs financiers un nombre de défis de plus en plus grand ; d'un côté l'évolution rapide des normes comptables, de l'autre l'automatisation croissante de la préparation des états financiers au moyen de système d'information toujours plus complexes.

La qualité de l'information financière dépend dans une large mesure de la qualité des processus métiers et des flux de traitement des données s'y rapportant. Il est donc logique que l'auditeur concentre son travail sur ces processus métiers et intègre le contrôle des applications correspondantes dans son approche d'audit.

Les travaux effectués, nous ont permis d'acquérir une certaine connaissance du processus audité. Les interviews, les analyses et les observations effectuées, ont permis d'orienter nos investigations qui ont aboutie sur le recensement de points forts, mais aussi de points faibles.

Comme points forts, nous pouvons retenir qu'il existe une réelle volonté de la part du management d'assurer le développement du système informatique. Cette volonté s'est matérialisée par la mise en place d'un plan de développement informatique, qui a permis d'acquérir d'importants moyens matériels et technologiques dont le développement de certaines applications à l'interne (SYTRIIS, etc.). Mais faute de moyen financier, de manière générale, ce plan de développement connait un ralentissement dans sa mise en œuvre.

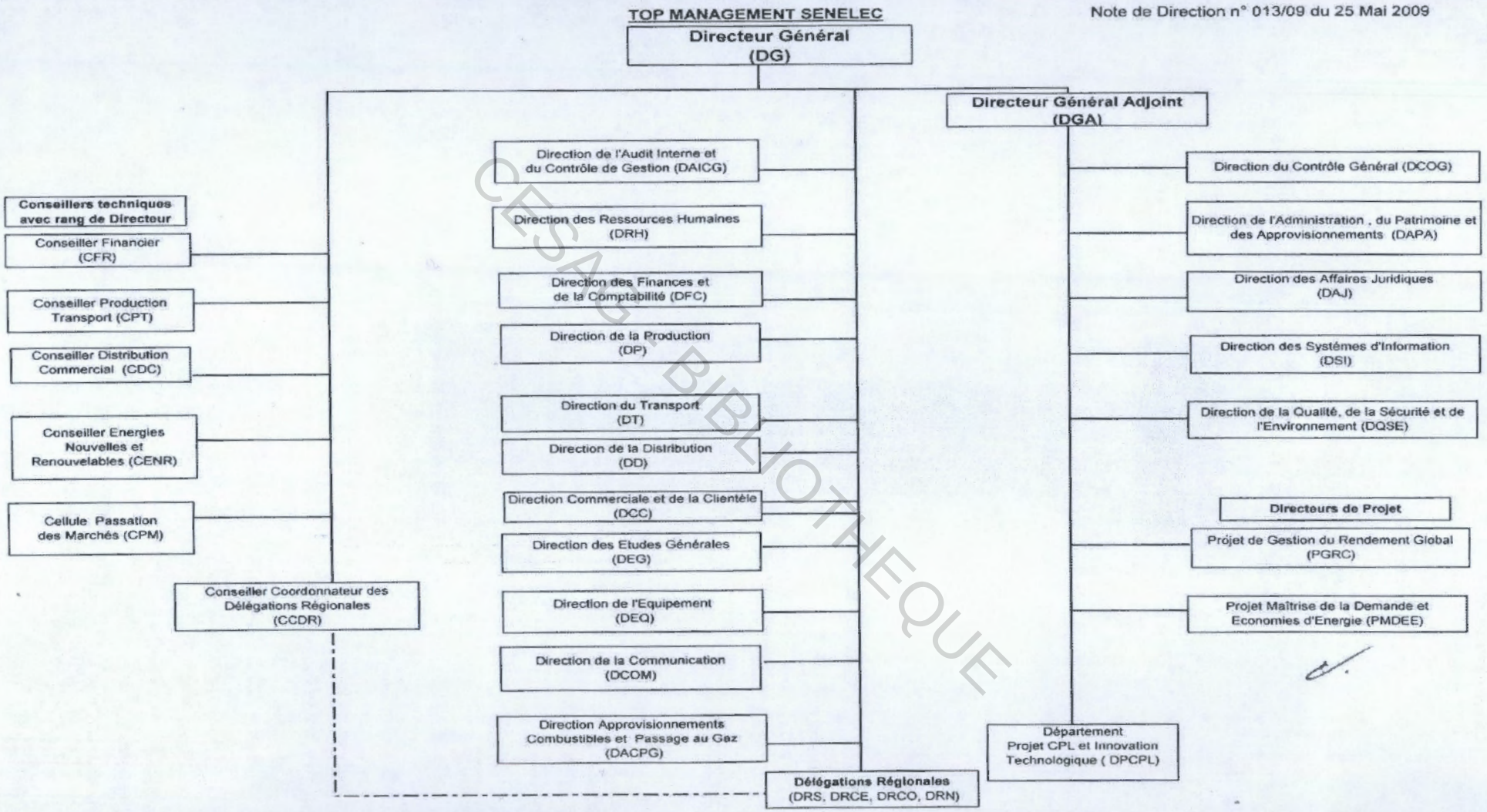
Comme points faibles, nous pouvons relever la vétusté de l'application SIC qui entraine la lenteur du système informatique de gestion de la clientèle. Même si l'implantation de l'application SYTRIIS a permis de réduire le nombre d'erreur et de décentraliser certaines opérations, force est de constater que le SIC est toujours un maillon faible. De plus, lors de son implantation, l'application SYTRIIS avait souvent quelques difficultés pour apurer certains encaissements. Ce qui amenait les caissiers à les apurer manuellement le lendemain avec l'aide de la DSI. Mais il faut noter que ce problème de conception a été progressivement

réglé par le service informatique. Les faiblesses restantes sont liées soit à la sécurité physique du matériel ou à la sécurité logique telle que la non suppression du droit d'accès d'un agent affecté dans un autre service ou une autre agence ; soit à la qualité du réseau (internet faible).

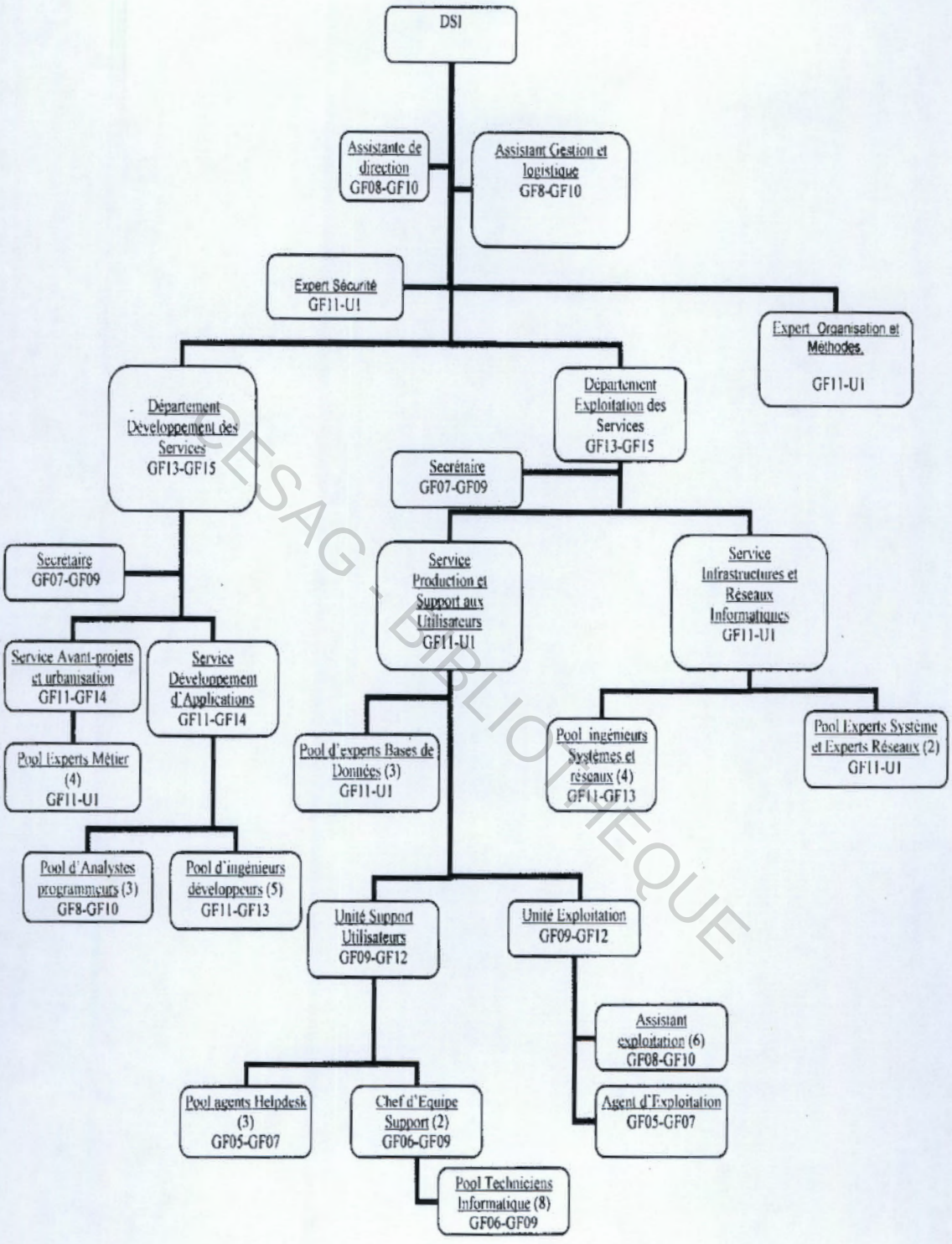
Suite à tout ce qui précède, nous avons proposé des recommandations pour améliorer certains points forts et réduire les maillons faibles. La principale recommandation, pour nous, est de doter le service d'audit interne de compétences nécessaires en audit informatique pour lui permettre de réaliser lors de ses missions, des contrôles IT généraux et les contrôles applicatifs. Car l'audit interne reste un outil de choix entre les mains du management pour ce prémunir des risques et donc assurer l'intégrité, la confidentialité et la disponibilité du système d'information et des données traitées.

ANNEXES

Annexe 1: organigramme de la SENELEC



Annexe 2: organigramme détaillé de la DSI



Annexe 3: Guide d'entretien

Guide d'entretien du personnel de l'agence de Vincens	
Questions	**Réponses**
Quelles sont les missions dévolues à votre service?	
Quelles sont les bureaux et sections sous votre responsabilité?	
Combien d'ordinateur votre service dispose t'il?	
Disposez-vous d'une application spécifique? Si oui laquelle?	
Une brève description du SYTRIIS	
Comment l'utilisez-vous?	
Quelles sont les opérations prises en charges par cette application?	
Quelles sont les difficultés rencontrées lors de son utilisation ?	
Comment faites vous pour y remédier ?	
Connaissez-vous les risques informatiques liés à l'utilisation de cette application (Riques physiques/risques logiques)?	
Installez-vous des antivirus su vos postes ? Des mesures de sécurité particulières sont elles définies pour vos matériel, infrastructures et réseau ?	
Qui a la charge de la protection/entretient de votre système d'information?	
Quel appui votre service apporte au service informatique?	
Quelles prestations le service informatique vous fournit-il?	
Comment vos données sont-elles sauvegardées?	
Existe-il des missions d'audit ou de contrôles ? Si oui, qui les effectuent?	
Les recommandations sont elles prises en compte ?	
Nous voulons procéder à l'audit du SYTRIIS : Quels conseils vous nous donnez pour qu'elle puisse aboutir ?	
Note de fin: Rappel des réponses données…/ Nous vous remercions d'avoir bien voulu nous recevoir.	

Annexe 4: Questionnaire de contrôle interne

Questions relatives à la sécurité informatique

QUESTIONNAIRE DE CONTROLE INTERNE	Système informatique	Folio 1/11

AUDIT DE LA SECURITE DU SYSTEME INFORMATIQUE

OBJECTIFS DE CONTROLE :

- S'assurer que les risques informatiques sont évalués et gérés.
- S'assurer de la gestion de la sécurité du système informatique.
- S'assurer de la gestion de l'environnement physique.

QUESTIONNAIRE DE CONTROLE INTERNE	DSI/Agence Vincens	Folio 2/11

OBJECTIFS DE CONTRÔLE:

- **s'assurer que les risques informatiques sont évalués et gérés.**

N°	QUESTIONS	OUI	NON	N/A	COMMENTAIRES
1	Un référentiel de gestion des risques existe-t-il dans l'entreprise ?		X		
2	Existe-t-il un référentiel de gestion des risques informatiques ?	X			Charte d'audit
3	Le contexte de risque informatique est-il : 3.2.2.1 compris ? 3.2.2.2 communiqué ?	X	X		
4	Les principaux évènements ou menaces sont-ils identifiés ?			X	Pour la salle des machines oui, toutes les dispositions de sécurité sont prises et régulièrement testées. Pour le reste, on intervient en cas d'anomalies.
5	Existe-t-il un processus d'identification qui tient compte : 1. de la probabilité ? 2. des conséquences ?		X X		
6	Existe-t-il un processus de réponse aux risques informatiques ?		X		
7	Un plan d'action de gestion des risques est-il en place ?		X		

QUESTIONNAIRE DE CONTROLE INTERNE	DSI /Agence Vincens	Folio 3/11

OBJECTIFS DE CONTRÔLE:

B- s'assurer de la gestion de la sécurité du système informatique

B-1: Gestion de la sécurité informatique

N°	QUESTIONS	OUI	NON	N/A	COMMENTAIRES
1	Existe-t-il un comité de pilotage de la sécurité informatique ?		X		C'est la responsabilité de l'expert sécurité
2	Les membres de ce comité sont-ils issues des principaux services fonctionnels de l'entreprise ?			X	
3	Est-ce que l'entreprise dispose d'une charte informatique ?	X			
4	La politique de sécurité couvre-t-elle : 1. la responsabilité du conseil d'administration ? 2. la direction générale ? 3. les cadres intermédiaires ?	 X X	X		
5	Existe-t-il des standards et procédures de sécurité détaillés ? ▪ politique de sécurité des ordinateurs de bureau et ordinateurs portables ? ▪ politique d'utilisation d'internet ? ▪ politique de sécurité du courrier électronique ? ▪ contrat de conformité aux règles de sécurité informatique ?	 X X X X			
6	L'entreprise dispose-t-elle d'une structure organisationnelle et hiérarchique de la sécurité informatique ?	X			

QUESTIONNAIRE DE CONTROLE INTERNE	DSI /Agence Vincens	Folio 4/11

OBJECTIFS DE CONTRÔLE:

B- s'assurer de la gestion de la sécurité du système informatique

B-2: Gestion des identités/ gestion des comptes d'utilisateurs

N°	QUESTIONS	OUI	NON	N/A	COMMENTAIRES
1	Les actions des utilisateurs (internes, externes, temporaires) sont-elles identifiables sans ambigüité ?	X			
2	Les systèmes sont-ils configurés pour imposer l'authentification avant d'autoriser l'accès ?	X			
3	Lors de l'attribution d'une identité, les droits sont-ils validés par le management responsable du processus ?	X			
4	Des mécanismes de fourniture d'accès et de contrôle d'authentification sont-ils utilisés pour contrôler : ▪ L'accès logique sur tous les utilisateurs ? ▪ Les processus système et les ressources informatiques ?		X X		
5	Existe-t-il une procédure pour évaluer régulièrement et ré-authentifier les droits et accès aux systèmes et applications ?		X		
6	Les politiques, les standards et procédures de gestion des comptes utilisateurs s'étendent-ils à tous les processus et utilisateurs des systèmes ?	X			

QUESTIONNAIRE DE CONTROLE INTERNE	DSI /Agence Vincens	Folio 5/11

OBJECTIFS DE CONTRÔLE:

B- s'assurer de la gestion de la sécurité du système informatique

B-3: Prévention, détection, neutralisation des logiciels malveillants/ Sécurité des réseaux/ Echange des données sensibles

N°	QUESTIONS	OUI	NON	N/A	COMMENTAIRES
1	Une politique de prévention contre les logiciels malveillants a-t-elle été mise en place ? Est-elle documentée et communiquée dans l'ensemble de l'entreprise ?	X X			
2	Un logiciel de protection est-il : ▪ Distribué ? ▪ De façon centralisée (version et correctifs) ? ▪ A l'aide d'un processus centralisé de configuration et de gestion modifications ?	X			Centralisé
3	L'usage des mots de passe est-il généralisé sur tous les postes et pour l'ensemble des utilisateurs ?	X			
4	Les fonctions de conception de la sécurité facilitent-elles les règles de mot de passe : ▪ Longueur maximum ? ▪ Caractères ? ▪ Expiration ? ▪ Réutilisation ?	X			
5	Une politique de sécurité réseaux ▪ Est-elle mise en place ? ▪ Est-elle à jour ?		X		
6	Les données sont-elles chiffrées avant leur transmission hors de l'entreprise ?		X		

QUESTIONNAIRE DE CONTROLE INTERNE	DSI /Agence Vincens	Folio 6/11

OBJECTIFS DE CONTRÔLE:

B- s'assurer de la gestion de la sécurité du système informatique

B-4: Sauvegarde et archivage des données

N°	QUESTIONS	OUI	NON	N/A	COMMENTAIRES
1	Est-ce qu'il existe une procédure de sauvegarde des données clairement définie ?	X			
2	Disposez-vous d'armoire appropriée pour la conservation des supports de sauvegardes ?	X			
3	Procédez-vous de façon périodique à des tests de relecture ?		X		
4	Les supports sont-ils conservés dans des lieux suffisamment éloignés des sites sensibles ?		X		
5	Est-ce qu'il existe un plan de secours et de reprise en cas de sinistre import ?	X			Mais pas encore opérationnel
6	Un périmètre de sauvegarde est-il défini ? concerne t-il : • Les données ? • Les applications et logiciels ? • La fréquence de sauvegarde ?		X		
7	La sauvegarde concerne-t-elle : - Les serveurs ? - Les postes individuels ?	X			

QUESTIONNAIRE DE CONTROLE INTERNE		DSI /Agence Vincens			Folio 7/11
OBJECTIFS DE CONTRÔLE: **C- s'assurer de la gestion de l'environnement physique** C-1: sélection du site et agencement					
N°	**QUESTIONS**	**OUI**	**NON**	**N/A**	**COMMENTAIRES**
1	Est-ce que les sites physiques où se trouve l'équipement informatique ont été choisis en fonction d'une stratégie technologique conforme aux exigences du métier ?	**X**			
2	Est-ce qu'une politique de sécurité, tenant compte notamment de la situation géographique, du voisinage, de l'infrastructure et des risques (vol, température, incendie, fumée, eau, explosion, etc.) est définie ?	**X**			
3	Est-ce qu'une procédure a été définie et mise en place pour identifier les risques et menaces potentiels vis-à-vis des sites informatiques de l'entreprise et pour évaluer régulièrement l'impact métiers, en tenant compte des risques liés aux sinistres d'origine naturelle ou humaine ?		**X**		
4	Est-ce que le choix et l'agencement du site tient compte des lois et règlementations applicables (normes de construction, réglementations en matière d'environnement, d'incendie, de génie électrique, de santé, hygiène et sécurité, etc.) ?	**X**			

QUESTIONNAIRE DE CONTROLE INTERNE	DSI /Agence Vincens	Folio 8/11

OBJECTIFS DE CONTRÔLE:

C- s'assurer de la gestion de l'environnement physique

C-2: mesures de sécurité physique

N°	QUESTIONS	OUI	NON	N/A	COMMENTAIRES
1	Est-ce qu'une politique a été définie et mise en place pour contraindre les sites informatiques de respecter les mesures de sécurité physique et de contrôle d'accès ?	X			Mais pas tout temps respectée
2	Si oui, cette politique est-elle régulièrement étudiée pour s'assurer qu'elle demeure pertinente et à jour ?		X		
3	Est-ce que l'accès aux informations sur les sites informatiques sensibles et à leurs plans de conception est limité ?	X			
4	Est-ce que les signes extérieurs et autres formes d'identification des sites informatiques sensibles sont discrets et n'identifient pas le site de façon évidente depuis l'extérieur ?			X	
5	Est-ce que l'élaboration des mesures de sécurité physique tient compte des risques liés aux métiers et aux opérations ?	X			
6	Le cas échéant, les mesures de sécurité physique incluent-t-ils : - Des systèmes d'alarme ? - La consolidation des bâtiments ? - Une protection des câbles ?	X			
7	Est-ce que les mesures de prévention, de détection et de correction de la sécurité physique sont régulièrement testées pour vérifier leur conception, leur application et leur efficacité ?	X			
8	Est-ce que la conception du site	X			

	tient compte du câblage physique des télécommunications et des conduites d'eau, branchements électriques et conduites d'égout ?				
9	Est-ce que les mesures de prévention, de détection et de correction de la sécurité physique sont régulièrement testées pour vérifier leur conception, leur application et leur efficacité ?		**X**		
10	Un processus est-t-il mis en place pour s'assurer que les périphériques de stockage contenant les informations confidentielles sont physiquement détruits ou nettoyés ?	**X**			
11	Est-ce que les sites particulièrement sensibles sont fréquemment contrôlés (y compris le weekend et pendant les congés) par le personnel de sécurité ?		**X**		

QUESTIONNAIRE DE CONTROLE INTERNE	DSI /Agence Vincens	Folio 9/11

OBJECTIFS DE CONTRÔLE:
C- s'assurer de la gestion de l'environnement physique
C-3: accès physique

N°	QUESTIONS	OUI	NON	N/A	COMMENTAIRES
1	Est-ce qu'un processus a été mis en place pour gérer les demandes et l'octroi d'accès aux infrastructures informatiques ?	X			
2	Est-ce qu'un processus permet de journaliser et de surveiller tous les points d'accès aux sites informatiques ? Et d'enregistrer tous les visiteurs, y compris les sous-traitants et les fournisseurs ?	X			
3	Est-ce qu'un règlement impose aux visiteurs d'être accompagnés ?		X		
4	Les individus qui ne portent pas de signe d'identification approprié sont –ils signalés au personnel de sécurité ?		X		
5	Est-ce qu'un règlement impose au personnel de porter en permanence un signe d'identification visible ? Evite-t-on l'émission de cartes d'identification ou de badges sans autorisation appropriée ?	X X			
6	Est-ce l'accès aux sites informatiques sensibles est limité par le biais d'une protection péri-métrique (clôtures/murs et dispositifs de sécurité sur les portes intérieures et extérieures) ?	X			

QUESTIONNAIRE DE CONTROLE INTERNE	DSI /Agence Vincens	Folio 10/11

OBJECTIFS DE CONTRÔLE:

C- s'assurer de la gestion de l'environnement physique

C-4: protection contre les risques liés à l'environnement

N°	QUESTIONS	OUI	NON	N/A	COMMENTAIRES
1	Est-ce qu'un processus permet d'identifier les sinistres d'origine naturelle ou humaine qui pourraient se produire dans la zone où sont situées les infrastructures informatiques sensibles ?		X		
2	Est-ce qu'une politique décrit comment l'équipement informatique, y compris l'équipement mobile et hors site, est protégé contre le vol et les menaces environnementales ?		X		
3	Est-ce les installations informatiques sont placées et fabriquées de façon à minimiser et limiter le risque de menaces environnementales ?	X			La salle des serveurs se situe au 2ème étage
4	Est-ce que les sites informatiques sont situés dans des bâtiments qui minimisent l'impact du risque environnemental (vol, air, feu, fumée, eau, vibrations, terrorisme, vandalisme, etc.) ?	X			
5	Est-ce qu'une politique a été mise en place pour garantir un nettoyage régulier à proximité des activités informatiques ?	X			

QUESTIONNAIRE DE CONTROLE INTERNE	DSI /Agence Vincens	Folio 11/11

OBJECTIFS DE CONTRÔLE:

C- s'assurer de la gestion de l'environnement physique

C-5: gestion des installations matérielles

N°	QUESTIONS	OUI	NON	N/A	COMMENTAIRES
1	Existe-t-il une procédure étudiant la nécessité de protéger les installations informatiques contre les conditions extérieures et les pannes de courant et incidents électriques ?	X			
2	Est-ce que l'entreprise se préoccupe des onduleurs ? Répondent-ils aux exigences de disponibilité et de continuité des activités ?		X X		
3	Est-ce que dans les installations accueillant des systèmes informatiques sensibles, plusieurs entrées d'alimentation électrique sont disponibles ?	X			
4	Est-ce que l'entrée physique du courant est séparée ?			X	
5	Est-ce que les câbles extérieurs au site informatique sont enterrés ou disposent d'une protection adapté ?				
6	Est-ce qu'un processus a été mis en place pour s'assurer que la maintenance du matériel et des sites informatiques est effectuée selon les spécifications et la périodicité recommandées par les fournisseurs ?	X			
7	Est-ce que la maintenance est uniquement effectuée par le personnel autorisé ?	X			
8	Est-ce qu'un processus a été mis en place pour informer le personnel sur les exercices d'évacuation en cas d'incendie et les exercices de secours, pour que tous les employés sachent quoi faire en cas d'incendie ou d'incident similaire ?		X		

Questions relatives aux applications informatiques

QUESTIONNAIRE DE CONTROLE INTERNE				DSI /Agence Vincens	Folio 1/1
OBJECTIFS DE CONTRÔLE:					
N°	**QUESTIONS**	**OUI**	**NON**	**N/A**	**COMMENTAIRES**
Identifier, recenser et lister toutes les applications informatiques opérationnelles au niveau de l'organisation auditée.					
1	Parmi ces applications, faire la distinction entre les applications qui ont été développées en interne, et celles qui ont été acquises ?	X			
2	Comment est opéré le choix de l'une ou l'autre option et quels sont les critères qui sont pris en compte ?			X	
3	Pour les applications développées en interne, a-t-il été élaboré un cahier des charges définissant les besoins fonctionnels des utilisateurs ?	X			
Décrire la procédure suivie pour l'acquisition de solutions informatiques.					
4	Dans les cas où la solution informatique a été acquise, existe-t-il un contrat de service ? Les utilisateurs ont-ils été formés au produit et ont-ils été assistés pour son paramétrage ?	X X			
5	Le paramétrage a-t-il été réalisé dans les règles de l'art ?	X			
6	Existe-t-il, pour chaque application, un document décrivant l'analyse fonctionnelle et les besoins des utilisateurs ?	X			
7	Décrire, pour chaque application informatique, les principales fonctionnalités et leur degré de réponse aux besoins des utilisateurs ?	X			
8	Est-il opéré un contrôle de la fiabilité des données et leur degré de réponse aux attentes et besoins des utilisateurs ?		X		Intervention qu'en cas d'anomalies
9	Ce contrôle, se base-t-il sur :		X		

	1. des entretiens avec le personnel informatique ainsi qu'avec certains utilisateurs ? 2. des contrôles de documents ou d'états pour la validation des réponses ?				
10	Pour chaque application informatique, existe-t-il une documentation utilisateur, un dossier d'exploitation, et un dossier de maintenance ? Ces documentations sont-elles régulièrement mises à jour en cas de changement de versements et sont-elles conservées en lieu sûr ?	X	X		
11	Cette documentation est-elle communiquée aux utilisateurs concernés ?	X			
12	Cette documentation est-elle de qualité et est-elle facilement compréhensible ?	X			
13	Cette documentation prévoit-elle des illustrations des différents écrans de saisies et écrans de sorties ? Toutes les rubriques sont elles bien expliquées ?	X X			
14	Les accès aux applications informatiques sont-ils sécurisés ?	X			
15	Les applications informatiques sont-elles évolutives ? Sont-elles mises à jour régulièrement (dès que les procédures ou réglementations changent, les données en entrées ou en sorties ont été modifiées) ?	X X			
16	Ces évolutions, modifications et mises à jour sont-elles reprises dans des documents utilisateurs ?		X		
17	Les procédures de contrôle et d'autorisations des accès sont-elles formalisées et connues de tous ?	X			
18	La politique de sauvegarde est-elle connue de tous ? est-elle appliquée ?		X		
19	Quelle est la périodicité des sauvegardes informatiques ?				Chaque fin de journée et en fin de semaine

20	Des contrôles de sauvegarde sont-ils régulièrement réalisés ?	X			
21	Ces sauvegardes informatiques sont-elles rangées en lieu sur ?	X			

Annexe 5 : Note de direction portant organisation de la DSI

Senelec

Direction Générale

Dakar, le 26 MAI 2010

NOTE DE DIRECTION N°..039.../2010

Portant Structures de la Direction des Systèmes d'Information

En application de la Note de Direction n°013/2009 du 25 mai 2009 portant modifications dans la répartition des fonctions et missions au niveau du Top Management de la SENELEC, la Direction des Systèmes d'Information (DSI) est désormais composée d'un Etat-Major et de deux Départements.

ETAT MAJOR

- **Expert Organisation et Méthodes :**

1. Elaboration des plans d'amélioration de la qualité à soumettre au Directeur
2. Validation de toutes les mises en production avec les « métier »
3. Suivi de l'efficacité et de la qualité des prestations par la mise en place et le suivi d'indicateurs
4. Réception des demandes d'amélioration
5. Contribution à l'amélioration de la qualité des services fournis aux utilisateurs par des actions d'information et de formation

- **Expert Sécurité :**

1. Conseil à la Direction sur le plan de la politique de sécurité globale des systèmes d'information
2. Proposition d'orientations et objectifs de sécurité
3. Déclinaison des objectifs validés en plan d'action
4. Définition des indicateurs de sécurité
5. Définition des règles de contrôle d'accès au SI
    a. Gestion des habilitations
    b. Gestions des accès distants
    c. Gestion des accès physiques
6. Animation du réseau de correspondants sécurité des systèmes d'information

- **Assistant Gestion et logistique :**

1. Suivi des contrats de services et des licences
2. Suivi budgétaire
3. Administration des achats

DEPARTEMENT DEVELOPPEMENT DES SERVICES (DDS) :

Il gère le développement et la maintenance des applications par l'élaboration et le suivi du respect des normes de développement informatique. Il définit les besoins en termes de plateformes de génie logiciel.

Il veille sur la cohérence des modèles de données de l'entreprise et participe à la formation des utilisateurs.

Il comprend deux services :

Service Avant-projets et Urbanisation (SAU):

1. Gestion de l'interface avec les métiers
2. Assistance à l'élaboration de cahiers des charges
3. Urbanisation : Privilégier la Construction de Solutions autour d'une Architecture capable d'accueillir des incréments successifs au fur et à mesure de la maturation des besoins venant des MAO (métiers)
4. Assister les métiers à peser objectivement les 2 scenarii classiques:

a. Solution-Progiciel ou Solution Spécifique.
b. Activité à prendre en charge ou externalisation

5. Etude de faisabilité des solutions à apporter aux besoins « métier »
6. Conception des applications et production de dossiers complets de développement

- **Service Développement d'Application (SDA):**

1. Développement des applications à partir des dossiers réalisés par SAU
2. Réalisation de tous les travaux de maintenance des applications
3. Formation des utilisateurs

DEPARTEMENT EXPLOITATION DES SERVICES (DES) :

Le Département Exploitation joue un rôle de support. Il procède à la mise en œuvre des applications et outils définis par le Département Développement et Urbanisation ; il définit les stratégies systèmes (serveurs et postes de travail) ; veille sur la fiabilité et la sécurité de stockage des informations et assiste les utilisateurs (helpdesk). Il définit les moyens à mettre en œuvre pour l'atteinte de cette mission par la définition des besoins en matière de licences de systèmes d'exploitation.
Il comprend deux services :

- **Service Production et Support Utilisateurs (SPS):**

1. Administration du système (postes de travail)
2. Application de la politique de sécurité des postes de travail
3. Mise en production des applications et outils transmis par le Département Développent des services
4. Conception et élaboration de l'architecture des systèmes de gestion de bases de données
5. Planification et mise en œuvre des extensions des systèmes de gestion de bases de données et des systèmes de gestion de fichiers
6. Assistance aux utilisateurs et gestion du helpdesk
7. Installation et maintenance des bases de données
8. Elaboration et mise en œuvre des procédures formalisées de sauvegarde des informations vitales de l'entreprise afin d'assurer les reprises en cas de sinistre.

- **Service Infrastructure et Réseaux Informatiques (SIR) :**

1. Administration du système (serveurs)
2. Définition des besoins en matière de licences de systèmes d'exploitation
3. Gestion de l'annuaire d'entreprise et de son fonctionnement (à travers Exchange et SharePoint)
4. Définition des stratégies systèmes (groupe gestions des postes de travail)
5. Définition des besoins en matière d'équipements de réseaux LAN
6. Gestion de la configuration du déploiement des réseaux
7. Définition de plans d'adressage
8. Application de la politique de sécurité du réseau
9. Gestion des points d'entrées et de sorties du réseau d'entreprise
10. Paramétrage des IOS

La présente Note de Direction qui annule et remplace la note 037/2010, prend effet dès sa signature.

LE DIRECTEUR GENERAL

SOCIETE D'ELECTRICITE Directeur Général SENELEC

Seydina KANE

Diffusion Générale

2/3

Annexe 6 : Questionnaire de prise de connaissance

QUESTIONNAIRE DE PRISE DE CONNAISSANCE		
OBJECTIF : avoir une vision d'ensemble de l'entité, du système d'information et de la sécurité informatique	**Réf**	**OBSERVATIONS**
Se faire présenter l'entité	**A**	
Missions, activités, produits, organisation, statuts, etc.	AA	**Ok**
Historique	AB	**Ok**
Appartenance à un groupe	AC	**Ok**
Obtenir l'organigramme général	AD	**Ok**
Prendre connaissance du système informatique	**B**	
L'organisation générale	BA	**Ok**
Les missions, l'effectif	BB	**Ok**
Les méthodes de travail	BC	**Ok**
Examiner le manuel de procédures	BD	**N'as pas été mis à notre disposition**
Visite des principaux locaux	BE	**Ok**
Documents à obtenir	**C**	
Manuels de procédures	CA	**N'as pas été mis à notre disposition**
Charte informatique		**Ok**
Statuts	CB	**Ok**
Rapport annuel/Rapport d'activité	CC	**Ok**
Etat récapitulatif du matériel informatique	CD	**Ok**
Organigramme détaillé	CE	**Ok**
Fiches de poste des différents protagonistes	CF	**Incomplet**
Schémas descriptifs des systèmes (Applicatif, réseau, etc.)	CG	**Ok**
Documentations sur le SYRIIS (implantation, cours de caisse, situation des incidents (janvier, février et mars), etc.)	CH	**Ok**

Annexe 7 : Tableau des risques

Tâches/ Opérations	Objectifs	Risques	Bonnes pratiques
Gestion et évaluation des risques	-Protéger l'atteinte des objectifs informatiques ; -Protéger tous les actifs et être comptable ; -Montrer clairement les conséquences des risques liés aux objectifs et aux ressources informatiques pour l'entreprise.	-Réponse aux risques non efficace ; -Confiance excessive dans les contrôles insuffisants existants ; -Perte d'actifs informatiques ; -Non détection de l'impact d'un risque informatique sur l'entreprise.	-Plan d'action de gestion des risques ; -Cartographie des risques ; -Fonction de gestion des risques (RSSI, risk manager) ; -Mise en place d'une action de sensibilisation à la valeur des actifs informatiques ; -Approche élargie de la gestion des risques informatiques.
Gestion de la sécurité informatique	-S'assurer que les règles et les procédures de sécurité sont clairement définies et connues de tous ; -Maintenir l'intégrité de l'information et de l'infrastructure de traitement.	-Données et actifs informatiques non protégés ; -Disparités entre les mesures de sécurités prévues et appliquées ; -Mesures de sécurité mises en échec par les parties prenantes et les utilisateurs.	-Protection des actifs informatiques critiques ; -Plan de sécurité informatique ; -Charte de sécurité informatique.
Gestion des identités/ Gestions des comptes d'utilisateurs	S'assurer que les données critiques et confidentielles ne sont pas accessibles à ceux qui ne doivent pas y accéder.	-Dénie de service ; -Modification non autorisée des données ; -Perte de confidentialité ; -Reconfiguration non autorisée des systèmes ; -Compromission de la sécurité logique.	-Mot de passe, outil de gestion d'accès ; -Verrouillage des configurations ; -Limitation de l'accès au panneau de configuration ; -Existence de procédure d'attribution, de suppression et de mise à jour des mots de passe.
Prévention, détection, neutralisation des logiciels malveillants	S'assurer de la protection des accès logiques aux systèmes d'information.	-Extraction non autorisée de données ; -Systèmes et données exposées aux attaques de virus ; -Contre mesures inefficaces ; -Faille de sécurité.	-Pare-feux ; -Logiciels anti-virus ; -Limitation des téléchargements ; -Application des correctifs et patchs de sécurité ; -Sonde réseaux, honey pot ; -Compartimentage du système informatique.

Sécurité des réseaux/ Echange des données sensibles	S'assurer que les transactions métiers automatisées et les échanges d'information sont fiables.	-Divulgation d'informations confidentielles ; -Systèmes et données exposés aux attaques de virus ; -Contre mesures inefficaces ; -Faille de sécurité ; -Mise en péril de l'architecture de sécurité globale ; -Attaques des cybers pirates.	-Pare-feux, logiciels anti-virus ; -Serveurs proxy ; -Limitation des téléchargements ; -Cryptographie ; Application des correctifs et patchs de sécurité ; -Sonde réseaux, honey pot ; -Compartimentage du système informatique.
Sauvegarde et archivage des données	S'assurer que les services et l'infrastructure informatique peuvent résister à une panne due à une erreur, à une attaque délibérée ou à un sinistre, et se rétablir.	-Perte d'image ; -Risque financier ; -Risque juridiques ; -Arrêt de l'activité compromise.	-Procédures de sauvegarde des données définies ; -Procédures d'archivage des données ; -Armoire sécurisée de protection des supports de sauvegarde ; -Contrôle de relecture des archives ; -Conservation des données conforme aux délais légaux d'archivage ; -Plan de secours et de reprise.
Mesures de sécurité physiques/ Accès physique	S'assurer que les services et l'infrastructure informatique peuvent résister convenablement à une panne due à une erreur, à une attaque délibérée ou à un sinistre, et se rétablir.	-Vol du matériel informatique ; -Accès non autorisé aux sites sensibles ; -système configuré sans autorisation ; -Attaques terroristes.	-Inventaire physique ; -Service de gardiennage ; -système de détection d'intrusion ; -Protection des câbles réseaux ; -Contrôle d'accès aux bâtiments ; -Gardiens armés et sensibilisés.
Gestion des installations matérielles	Protéger tous les actifs informatiques et en être comptable.	-Destruction des bâtiments ; -Destruction du système ; -Coupures d'électricité ; -Risques électriques ; -Incendie/ feu	-Contrat d'assurance du matériel ; -Plan de reprise ; -Groupes électrogènes ; -Onduleurs avec batteries-relais ; -Capteur de fumée ; -Extincteur à poudre ; -Extincteur automatique d'incendie.

Annexe 8 : Feuilles de Révélation et d'Analyse des Problèmes

Constats	Causes	Conséquences/Risques	Recommandations
Contrôles IT généraux			
1- Des séances de formation et/ou de sensibilisation ne sont pas organisées sur les risques informatiques et leurs conséquences.	- Absence de ligne budgétaire ; -Méconnaissance des biens fondés de cette pratique ; -Négligence.	En cas de d'anomalies ou de catastrophe, les agents ne sauront que faire, ce qui pourrait aggraver l'ampleur de la situation.	Procéder périodiquement (par semestre ou par an) à des formations et/ou sensibilisations sur les risques informatiques et leurs conséquences.
2- La charte informatique ne prévoit pas des mesures de sanctions à l'égard des personnes qui l'enfreignent.	-Laxisme dû au peu d'importance accordé par les dirigeants à la sécurité informatique ; -Méconnaisse des conséquences d'une telle passivité sur l'organisme et ses activités.	- Sabotage des installations ; - violation de la charte et de ses règlements sans être inquiété ; - Tentative d'outrepasser les limitations de l'accès au panneau de configuration pour commettre des malversations.	Les dirigeants doivent, en collaboration avec l'expert sécurité et les différents responsables, mettre en place des sanctions en vue de dissuader les malintentionnés.
3-La liste des risques et menaces n'est pas connue par tous les utilisateurs de l'informatique et des systèmes d'information.	Laxisme dû au peu d'importance accordé par les dirigeants à la sécurité informatique.	-Pilotage à vu ; -Prise de risque due à l'ignorance	Une liste des risques et menaces informatiques doit être élaborée par l'expert sécurité et validée par les autorités compétentes, pour ensuite être communiquée à tous les utilisateurs de l'informatique et des systèmes d'information.
4-le plan de secours existe, mais n'est pas fonctionnel (absence de site de secours).	-Absence de ligne budgétaire ; -Laxisme.	-Perte de données en cas de catastrophe ; -Arrêt des activités ; -Perte financière ; -Chômage technique.	Procéder dans de brefs délais à l'activation du site de secours, car ça y va de la survie de l'organisation.
5-Absence de	Toutes les sauvegardes	-Perte de données en cas	Permettre à ce que les

sauvegarde des postes individuels (PC).	sont faites sur le serveur en temps réel	de coupure ou de d'anomalie ; -Reprise à zéro d'un travail déjà fait et qui a été perdu.	agents puissent enregistrer certaines données sur le poste ou sauvegarder certains fichiers sources.
6- L'onduleur pour les serveurs est défaillant.	- Absence de ligne budgétaire ; - Méconnaisse des conséquences.	- variations et interruptions de tension ; - Perte de travaux en cours non sauvegardés ; - Peut endommager le matériel informatique	Vu l'importance d'un serveur dans une organisation et le rôle que joue un onduleur, il sera nécessaire de le remplacer dans de brefs délais.
7-Absence de renouvellement régulier des mots de passe.	Méconnaisse des conséquences d'une telle passivité sur l'organisme et ses activités.	-Sabotage ; -Piratage ; -Malversation ;	Procéder au renouvellement des mots de passe au moins une fois par mois.
Contrôles applicatifs du SYTRIIS			
1- La vraisemblance et l'exhaustivité des sorties des routines d'extraction ne sont pas contrôlées.	-Dû au fait que le système, lors des saisies, possède deux niveaux de contrôle (manuel/automatique) ; - le volume d'opérations traité et le nombre de clients.	-Erreur de fichier remit au client.	Quel que soit le degré de contrôle manuel/automatique à la saisie ou le volume d'activité ou encore le nombre de clients, les caissiers doivent vérifier à la sortie les reçu remis à la clientèle.
2- Les utilisateurs n'ont pas été formés sur SYTRIIS et n'ont pas assisté à son paramétrage.	-les caissiers présents lors de l'installation du SYTRIIS, avaient reçu une formation et assistés pour son paramétrage. Cela n'a pas été le cas pour ceux qui sont venus après ; -Absence de politique de transfert des connaissances entre anciens et nouveaux agents (apprentissage sur le tas).	-Mauvaise manipulation ; -Perte de données ; -Difficulté pour réaliser les paramétrages de routines (toujours contacter le service informatique) ; -réticence vis-à-vis de l'application.	Prévoir une ligne budgétaire pour permettre aux nouvelles recrues de suivre une formation adéquate, sur le SYTRIIS, avant d'occuper leurs postes.
3- Il n'est pas opéré	Absence d'audit	-utilisation d'application	Avant tout

un contrôle de la fiabilité des données et de leur degré de réponse aux attentes et besoins des utilisateurs (maintenance effectuée qu'en cas d'incident).	ponctuel ou programmé des applications, afin de déterminer l'adéquation besoins utilisateurs et applications adaptées.	qui ne répond pas aux besoins de ses utilisateurs ; -Manque d'efficacité et de problème de performance ; -lenteur dans les traitements des données ; -Perte financière, due au fait qu'on paie des applications chères et qui ne répondent pas aux besoins de ses utilisateurs.	acquisition ou développement d'une application procéder au préalable à des contrôles et vérifier si cette application répond aux attentes et aux besoins des utilisateurs. Pour ne pas payer cher des applications qui ne serviront pas et de sur croix vont ralentir l'activité de l'organisation.
4- Les documentations ne sont pas régulièrement mises à jour en cas de changement, de modification ou de mise à jour du module.	-Opérateurs étrangers et difficiles à contacter ; -coûts très élevés de la mise à jour.	-Documentation dépassée et reflétant pas l'image fidèle de l'application mise à jour ; -Problème pratique pour les agents qui vont l'utiliser.	À défaut de mettre à jour la documentation, il sera judicieux d'exiger de l'opérateur la nouvelle documentation.
5- Cette documentation n'est pas communiquée aux utilisateurs concernés.	-Absence de politique de transfert des connaissances.	- l'agent peut être confronté à des problèmes sans toutefois pouvoir les résoudre lui-même faute de documentation. Il aura toujours recours au service informatique même pour des incidences mineures.	Transférer une partir des compétences aux caissiers qui pourront résoudre sur le champ les problèmes mineurs pour éviter des pertes de temps inutiles. Distribuer le guide de l'application aux agents.
6- Les procédures de contrôle et d'autorisations ne sont pas connues de tous.	Manque de communication des procédures aux agents par la hiérarchie.	-Pilotage à vue ; -ralentissement de l'activité, parce que ne maîtrisant pas les procédures.	Veiller à ce que le SI mis en place dans la structure puisse rendre disponibles toutes les informations nécessaires aux agents dans la bonne

			marche de leurs activités.
7- Les contrôles de sauvegarde ne sont pas régulièrement réalisés.	Absence de procédure de contrôle de sauvegarde de données.	-Perte de données.	Mise en place de procédure de contrôle de sauvegarde des données. Ces contrôles doivent être réguliers pour éviter les pertes de données.
8-les droits d'accès de certains agents qui changent d'environnent (mutation de poste, etc.) ne sont pas supprimés par le chef d'agence responsable.	-laxisme ; -oubli.	-Un agent malintentionné peut commettre des fraudes via le compte de l'agent muté ;	Veiller à ce que les agents qui changent d'environnement voient leurs droits d'accès immédiatement supprimés.
9- Problème récurrent de formation des agents (caissiers) qui ne savent pas souvent comment utiliser l'application ou corriger certains incidents (apprentissage sur le tas).	Absence de ligne budgétaire pour les formations ou la mise à niveau des connaissances des agents.	-Difficulté rencontrées dans le travail ; -réticence vis-à-vis de l'application, faute de maîtrise ; -ralentissement dans l'exécution des tâches.	Veiller à ce que des séances de formation soient organisées pour les nouvelles recrues.
10- Absence de politique de contrôle des applications et des équipements informatiques. Les interventions sont effectuées en cas d'incidents exposés par les utilisateurs.	-Absence de procédure de contrôle des applications à l'interne ; - Méconnaisse des conséquences d'une telle passivité sur l'organisme et ses activités.	-Ralentissement des activités de l'organisation ; -Multitude d'incidents constatés ;	Doter la Direction d'audit interne de compétences nécessaires pour effectuer des missions d'audit des systèmes d'informations périodiquement (à titre préventif).
11- mots de passe de certains agents	Permettre aux agents d'être plus efficace.	- Problèmes de confidentialité ;	Veiller à ce que le renouvellement

absents sont communiqués à leurs collègues pour continuer le travail.		-Fraude en usurpant l'identité de l'agent absent.	régulier des mots de passe soit effectué.
13- Absence de rapport sur l'application SYTRIIS.	Aucun audit ou évaluation ne sont effectués pour déterminer l'état des applications.	-Problème de performance de l'application ; - régression de l'application lors des mises à jour ou de nouveaux paramétrages.	Procéder à des audits ponctuels ou programmés des applications ou évaluer régulièrement l'application (Semestre).
14- Lenteur dans le traitement des opérations (déversement des caisses-sytriis dans le SIC) dans certaines agences.	- Obsolescence du SIC ; - instabilité du réseau (internet).	-lenteur dans le traitement des opérations ; -Perte de données.	Mettre en place un mécanisme ou des seuils d'alerte pour assurer le suivi des altérations ou obsolescences des applications ; Augmenter le débit du réseau (intranet et internet) de la SENELEC pour le rendre plus performant.
15- Certaines agences préfèrent utiliser le SIC au détriment du SYTRIIS (défaut de maîtrise de l'application).	Faute de maîtrise du SYTRIIS.	Lenteur dans le traitement des données.	Veiller à ce que toutes les agences, quelle que soit la zone, utilisent l'application SYTRIIS pour uniformiser les pratiques. Sensibiliser et former.

BIBLIOGRAPHIE

Ouvrages

- BITTERLI R. Peter et al. (2008), *Guide d'audit des applications informatiques*, Copyright ISACA Switzerland Chapter, suisse, 48 pages.
- Institute of Internal Auditors in GTAG 1 (2009), *Les contrôles des systèmes d'information*, Copyright par l'Institute of Internal Auditors, 47 Maitland Avenue, Altamonte Springs, Florida 32701-4201, 66 pages.
- Institute of Internal Auditors in GTAG 4 (2009), *Management de l'audit des systèmes d'information*, Copyright par l'Institute of Internal Auditors, 47 Maitland Avenue, Altamonte Springs, Florida 32701-4201, 33 pages.
- Institute of Internal Auditors in GTAG 8 (2009), *Audit des contrôles applicatifs*, Copyright par l'Institute of Internal Auditors, 47 Maitland Avenue, Altamonte Springs, Florida 32701-4201, 32 pages.
- Institute of Internal Auditors in GTAG 11 (2008), *Developing the IT audit plan*, Copyright par l'Institute of Internal Auditors, 47 Maitland Avenue, Altamonte Springs, Florida 32701-4201, 36 pages.
- Association Française de l'Audit et du Conseil Informatiques, *COBIT*, 3ème édition, 88, rue de Courcelles, 75008 Paris, 18 pages.
- ACISSI (2009), *Sécurité informatique : ethical hacking, apprendre l'attaque pour mieux se défendre*, Editions ENI, Paris, 355 pages.
- AfAI (2008),
- CALE Stéphane et TOUITOU Philipe (2007), *la sécurité informatique : réponses techniques, organisationnelles et juridiques*, Lavoisier, Paris, 282 pages.
- CARPENTIER Jean-François (2009), *la sécurité informatique dans la petite entreprise : état de l'art et bonnes pratiques*, Editions ENI, Paris, 277 pages.
- CLEUET Fabien et al. (2009), *Audit des systèmes d'information*, Vol.1 (2) INTEC/CNAM, Paris, 162 pages.
- CLEUET Fabien et al. (2009), *Audit des systèmes d'information*, Vol.2 (2) INTEC/CNAM, Paris, 152 pages.
- CLUSIF (2010), *Menaces Informatiques et Pratiques de Sécurité en France*, Edition 2010, CLUSIF, Paris, 102 pages.
- CLUSIF (2003), *Plan de Continuité d'Activité : Stratégie et Solutions de secours du S.I.*, Dossier Technique, CLUSIF/COMMISSION TECHNIQUE DE SECURITE LOGIQUE, Paris, 58 pages.

- DAYAN Armand (2008), *Manuel de gestion Vol.1*, 2ème édition, ELLIPSES/AUF, Paris, 1088 pages.
- GODART Didier (2002), *Sécurité informatique : risques, stratégies et solutions*, Edipro, Paris, 334 pages.
- GRAEVE Jean et POTIER Jean (2001), *Système d'information, Management et Acteurs*, les éditions SAPIENTIA, Paris, 135 pages.
- HAMZAOUI Mohamed (2005), *Audit : gestion des risques d'entreprise et contrôle interne : normes ISA 200, 315, 330 et 500*, Editions Village Mondial, Paris, 242 pages.
- IFACI (2009), *Normes, The Institute of Internal Auditors*, Paris, 66 pages.
- LAUDON C. Kenneth, LAUDON P. Jane et GINGRAS Lin (2000), *Les systèmes d'information de gestion*, Pearson Education/ Village Mondial, Paris, 784 pages.
- LY Henri (2005), *L'audit technique informatique*, Lavoisier/HERMES SCIENCE, Paris, 230 pages.
- MENTHONNEX Jean (1995), *Sécurité et qualité informatiques*, Nouvelles orientations, Presses Polytechniques et Universitaires Romandes, Lausanne, 422 pages.
- MOREAU Franck (2002), *Comprendre et gérer les risques*, Editions d'Organisation, Paris, 222 pages.
- REIX Robert (2005), *Systèmes d'informations et management des organisations*, 5ème édition, LIBRAIRIE VUIBERT, Paris, 486 pages.
- ROYER Jean Marc (2004), *Sécuriser l'informatique de l'entreprise : enjeux, menaces, prévention et parade*, Edition ENI, Paris, 422 pages.
- SCHICK Pierre (2007), *Mémento d'audit interne, Méthode de conduite d'une mission*, DUNOD, Paris, 217 pages.
- THORIN Marc (2000), *L'audit informatique*, HERMES SCIENCE, Paris, 184 pages.
- VOLLE Michel (2004), *Lexique du système d'information*, Club des maîtres d'ouvrages des systèmes d'information & Michel VOLLE, GNU Free Documentation, Paris, 23 pages.
- YADAV S. Chandra et SINGH S. Kunar (2009), *An Introduction to Client/Server Computing*, New Age Internationnal, Varanasi, 212 pages.
- MORLEY Chantal, BIA-FIGUEIREDO Marie et GILLETTE Yves (2011), *Processus Métiers Et Systèmes D'information : Gouvernance, management, modélisation*, 3ème édition, DUNOD, Paris, 319 pages.

Articles

- CLUSIF (2009), *Sécurité des applications Web, Les Dossiers Techniques*, Club de la sécurité de l'information Française, Paris, pages 9-20.
- KPMG Maroc (2007), *Manuel d'audit Interne pour les Inspections Générales des Ministères pour l'USAID*, Projet de Gouvernance Locale au Maroc, pages 204-216.

Sources Internet

- Aud-IT (2011), *Audit informatique – audit des systèmes d'information, Evaluer les risques informatiques, risques des systèmes d'information*, www.aud-it.ch/audit%20informatique.html.
- ANSSI (2007), *politiques de sécurité des systèmes d'information (PSSI)*, sécurité-info, www.securite-informatique.gouv.fr/gp_article51.html.
- CLUSIF (2010), www.clusif.asso.fr, www.clusif.asso.fr/fr/production/mehari/.
- EOX PARTNERS SAS (2010), *charte informatique et Politique de sécurité*, www.eoxpartners.fr/charte_informatique_politique-sécurite-eox_partners.php.
- LESSAUVEGARDES (2007), *Construire son plan de sauvegarde*, www.lessauvegardes.com/lscom/2007/10/15/construire-son-plan-de-sauvegarde/.
- SOCIETE DE MARKETING INDUSTRIEL (2010), *Sécurité : Eviter aussi les risques physiques*, www.acheteursinfo.com/actualites_securite.html.