CESAG

CENTRE AFRICAIN D'ETUDES SUPERIEURES EN GESTION

INSTITUT SUPE[illegible]TABIL[illegible]

DIPLOME D'ETUDES SUPERIEURES SPECIALISEES EN AUDIT ET CONTROLE DE GESTION

THEME :

LA SECURITE DU SYSTEME D'INFORMATION : CAS DE LA CNCAS

Présenté par :
Charles Le Bon YOUKOU
15ème Promotion
(Janvier 2006)

Sous la Direction de
Abdoulkadire DIAGNE
Directeur de mission
Système d'Information
[illegible]

SIGLES ET ABREVIATIONS

AFAI	: Association Française de l'Audit et du conseil Informatique
BSA	: Business Software Alliance
BSP	: Business Systems Planning
CA	: Crédit Agricole
CI	: Contrôle Interne
CISA	: Certified Information Systems Auditor
CLUSIF	: CLUb de la sécurité des Systèmes d'Information Français
CNCAS	: Caisse Nationale de Crédit Agricole du Sénégal
CNCC	: Compagnie Nationale des Commissaires aux Comptes
DESCOGEF	: Diplôme d'Etudes Supérieures de Comptabilité et de Gestion et Financière
FBI	: Federal Bureau of Investigation
GASP	: Globally Accessible Statiscal Procedures
IBM	: International Business Machines
IFAC	: International Federation of Accountants
IFACI	: Institut Français de l'Audit et du Contrôle Internes
ISACA	: Information Systems Audit and Control Association
MARION	: Méthode d'Analyse des Risques Informatiques Orientée par Niveaux
MEHARI	: Méthode Harmonisée d'Analyse de Risques
NTIC	: Nouvelles Technologies de l'Information et de la Communication
OECCA	: Ordre des Experts Comptables et Comptables Agréés
PPTP	: Point to Point Tunneling Protocol
RSSI	: Responsable de la Sécurité du Système d'Information
SAGAM	: Société Africaine Gestion Assistance Mission
SDLC	: System Development Life Cycle
SI	: Système d'Information
SSI	: Sécurité du Système d'Information
VPN	: Virtual Private Network

LISTES DES FIGURES ET TABLEAUX

A. Liste des figures

B. Liste des tableaux

LISTE DES ANNEXES

TABLE DES MATIERES

DEUXIEMME PARTIE

INTRODUCTION GÉNÉRALE

Contexte

La modernisation et le recours aux Nouvelles Technologies de l'Information et de la Communication (NTIC) si elles rendent les entreprises plus efficaces, les exposent aussi à de nouvelles vulnérabilités. En effet comme le soutien REIX (2002 : 415) « le recours étendu aux techniques informatiques a fortement accru les performances des systèmes d'information mais aussi leur vulnérabilité ». Qu'arriverait-il à une société de vente par correspondance si sa base de données « clients » était détruite ? Comment pourrait fonctionner une compagnie aérienne si son service informatique était en panne ? Le développement exponentiel des applications autour d'Internet n'a fait que multiplier les risques. La multiplication des relations inter organisationnelles, l'ouverture à tout individu d'un réseau universel a comme conséquence immédiate l'augmentation considérable des risques d'intrusion, donc de piratage ou de destruction par l'invasion de virus.

L'impératif de sécurité est donc un enjeu particulièrement grave qui nécessite une attention soutenue de la part des responsables d'entreprise. Le système d'information, nécessaire à toute entreprise qui s'inscrit dans une optique de performance, assiste les hommes au sein d'une organisation, en ce qu'il leur permet d'automatiser la majeure partie des fonctions d'exécution, de gestion et de prise de décision qui leur incombe. Pour WATERFIELD (1998)[1] : « une organisation pourra d'autant mieux gérer ses ressources que ses informations seront bonnes ». Ainsi, Mettre une information de qualité à la disposition de ceux qui savent l'utiliser facilite les performances de l'entreprise. Ces exigences de performance et de disponibilité de l'information au sein de toute organisation requièrent un suivi particulier du caractère opérationnel de la sécurité et des performances de son système d'information.

[1] WATERFIELD Charles ; RAMSING Nick (1998), Système d'information de gestion pour les institutions de microfinance : Guide pratique, CGAP,serie « outil technique », n°1, 22pages.

Problématique

Comme toute activité de l'entreprise, la sécurité informatique, qui est l'un des processus support les plus importants, contribue à l'amélioration de la compétitivité, à la recherche d'avantages compétitifs durables et au respect des lois, des règlements et des obligations contractuelles. L'ensemble des sécurités contribue à la maîtrise de l'entreprise (MAIDOUDOU, 1992 : 36).

Ainsi, toute entreprise doit assurer la disponibilité constante de tous ses outils, et particulièrement de son outil informatique dont elle est de plus en plus dépendante. L'entreprise doit aussi assurer l'intégrité de l'information qu'elle a stockée dans son système informatique. D'autre part, elle doit préserver la confidentialité de cette information car les risques d'accès ou de détérioration de ses données sont de plus en plus nombreux. Les risques auxquels sont exposés les systèmes d'information relèvent de la confidentialité, l'authentification, la non répudiation, la disponibilité, l'intégrité, l'efficience et l'efficacité.

L'explosion des délits informatiques est due au développement de l'informatique répartie et de l'informatique mobile, à l'émergence d'Internet pour les communications professionnelles, etc. Selon DUNSMORE (2002 :3) une enquête réalisée en 2000 par le CSI (computer Security Institute) avec la participation de l'agence de San Francisco du FBI, a démontré que 90% des entreprises interrogées ont connu un bris de sécurité informatique, 70% de ces entreprises ont subi des bris de sécurité sérieux (vols d'information propriétaire, intrusion, sabotage de données ou encore attaques provoquant un dénis de service); les ¾ de ces entreprises ont subi des pertes financières Il ressort de cette étude que 32% des entreprises ayant répondu (273 entreprises) ont été victimes d'un acte de malveillance interne, 18% d'un acte de malveillance externe. En outre, la majeure partie des attaques et sinistres a des causes internes. (ERNST & YOUNG, 2004).

La sécurité du système d'information s'intéresse à l'intégrité, la confidentialité et la disponibilité. Elle concerne les dysfonctionnements potentiels du système d'information du fait de phénomènes naturels, des accidents, des erreurs d'utilisation ou de manipulation des données et des malveillances.

Ainsi, force est de constater comme le mentionne Marc THORIN (2000), que l'ordinateur demeure un outil potentiellement dangereux, vulnérable aux erreurs involontaires et aux tentatives de fraude. Pour atteindre un niveau de sécurité adéquat, les entreprises se doivent d'avoir :

- ✓ Une organisation optimale répondant aux besoins du contrôle interne ;
- ✓ Un bon pilotage de cette organisation et un suivi régulier ;
- ✓ Un bon contrôle de la mise en oeuvre des exigences de sécurité ;
- ✓ Un bon suivi de son système d'information à travers des audits informatiques réguliers.

Cette dernière activité constitue un élément clé dans la sécurisation d'un système d'information. L'audit des systèmes d'information évalue l'exposition de l'entreprise aux sinistres informatiques. Des éléments de l'audit de la sécurité sont l'évaluation des risques informatiques liés à la sécurité physique du système d'information, à la sécurité logique, à la gestion des changements, à la continuité de l'activité, etc. L'audit informatique peut aussi avoir pour mission l'évaluation d'une partie ou de l'ensemble des processus informatiques - ce qui est généralement le cas- pour répondre à une demande précise du client. Les objectifs de l'audit de la sécurité informatique peuvent être le renforcement du contrôle interne, la fiabilisation des données, la recherche de fraude, etc.

La principale question qui découle de ce qui précède est la suivante : « Comment atteindre un niveau de sécurité optimal du système d'information dans une entreprise ? » Plus précisément, nous nous posons les questions suivantes :

- ✓ Comment détecter et quantifier les vulnérabilités du système d'information et les risques associés ?
- ✓ Comment parvenir à une sécurité efficace, efficiente et économique au sein d'un environnement informatique ?
- ✓ Comment mettre en pratique une méthode de management de la sécurité informatique adéquate ?
- ✓ Comment assurer la pérennité de la sécurité mise en place ?

Objectif de l'étude

L'objectif de ce mémoire sur *La sécurité du système d'information* est de cerner la méthode d'audit de la sécurité informatique dans l'optique de réduire l'exposition aux vulnérabilités, et menaces et de minimiser les risques. Notre but est de faire un diagnostic des états des lieux afin d'obtenir un bon système d'information, des informations (financières) fiables et crédibles pour un bon pilotage de l'entreprise et un gain optimal de compétitivité.

Les objectifs spécifiques d'un audit de sécurité sont :

- ✓ Etablir un état des lieux vis-à-vis des risques ;
- ✓ Elaborer des scénarii de réduction des risques ;
- ✓ Concevoir une politique de sécurité ;
- ✓ Mettre au point un programme de mise en œuvre de cette politique ;
- ✓ Elaborer des processus d'organisation et de contrôle de la sécurité.

Intérêts de l'étude

L'enjeu de notre étude est de montrer l'importance du système d'information dans le cadre de la sécurité au sein des entreprises. Car convaincu qu'un usage maîtrisé du système d'information, véritable outil stratégique, répond aux préoccupations des dirigeants que sont :

- ✓ Optimiser la performance globale de l'entreprise ;
- ✓ Améliorer le pilotage ;
- ✓ Améliorer la qualité du service client.

Pour les Auditeurs et les contrôleurs, ce mémoire est un outil pour la bonne maîtrise d'un Audit de la sécurité qui de nos jours s'impose dans toute organisation pour sa survie. L'étude réalisée fournit :

- ✓ la démarche et le déroulement d'une mission d'audit de la sécurité ;
- ✓ des outils et des méthodes pour la sécurité du système ;
- ✓ des informations sur la réglementation et quelques lois internationales.

Délimitation de l'étude

Notre étude vise le système d'information de toute l'entreprise. Cependant l'audit de la sécurité du SI porte essentiellement sur l'automatisation de l'entreprise et particulièrement l'informatique. Aussi nous travaillerons en étroite collaboration avec la Sous Direction de l'Informatique et de l'Organisation (SDIO) pour l'étude de la fonction informatique

Démarche méthodologique

Le sujet délimité à la fonction informatique nous développerons la SSI à travers deux parties :

- Une première partie théorique servira à exposer la revue littéraire sur les notions de l'information, du Système d'Information (SI), de la Sécurité du Système d'Information (SSI) et de la réglementation en vigueur. Par la suite nous montrerons la méthodologie et les outils de l'Audit de la sécurité, et nous présenterons notre modèle d'analyse.

- La seconde partie pratique présentera la CNCAS, l'audit sécurité au sein de la banque avec les travaux et les résultats effectués, et nous terminerons par une synthèse et des perspectives de mises en œuvre des recommandations.

PREMIÈRE PARTIE :

CADRE THÉORIQUE DE LA SÉCURITÉ DU SYSTÈME D'INFORMATION

INTRODUCTION

« La Sécurité Informatique pose un problème d'un ordre nouveau et qu'un simple ajout d'une serrure ne saurait résoudre » (Tall, 2004 : 1).

Pour MEILLAN (1993 : 11), « l'année des nouvelles technologies de l'information n'a pas engendré de perturbations particulières dans le fonctionnement social … ».

Deux opinions qui démontrent bien la problématique de la sécurité des systèmes d'information. Quant à REIX (2002), il nous fait savoir que la sécurité informatique est un enjeu considérable dont peu de responsables d'entreprise ont pris la mesure exacte ; les statistiques montrent que le risque s'accroît et peut mettre en cause la survie de l'entreprise.

La question de la sécurité des systèmes d'information est-elle un problème de gestionnaire ? Ou un problème de spécialistes, d'attitudes ou de comportements ?

Cette première partie de notre étude est essentiellement constituée d'une revue critique de la littérature et des théories existantes en matière d'audit de la sécurité des systèmes d'information.

Cette revue synthétique portera sur les notions suivantes :

- L'information ;
- Les systèmes d'information ;
- Le management de la sécurité de l'information ;
- Les normes et lois de la sécurité informatique.

Par la suite, la mise en œuvre de la sécurité du SI sera perçue à travers un audit de la sécurité. D'où la nécessité de la bonne maîtrise des méthodes et outils que nous livrent chercheurs et experts.

CHAPITRE 1 : NOTION DE LA SÉCURITÉ DU SYSTÈME D'INFORMATION

INTRODUCTION

Pour des soucis d'efficacité et de rentabilité, une entreprise communique aujourd'hui avec ses filiales, ses partenaires et va jusqu'à offrir des services aux particuliers, ce qui induit une ouverture massive à l'information. Par l'ouverture des réseaux, la sécurité devient un facteur décisif du bon fonctionnement de l'entreprise ou de l'organisation.

Il reste qu'une entreprise ou un organisme possède certaines informations qui ne doivent être divulguées qu'à un certain nombre de personnes ou qui ne doivent pas être modifiées ou encore qui doivent être disponibles de manière transparente à l'utilisateur. Ces informations feront l'objet d'une attaque si et seulement si des failles de sécurité existent et si le système abritant ces informations est vulnérable.

Par conséquent, selon REIX (2002 :402) « la sécurité d'un système d'information est sa non vulnérabilité à des accidents ou à des attaques volontaires, c'est-à-dire l'impossibilité que ces agressions produisent des conséquences graves sur l'état des systèmes ou son fonctionnement ». La sécurité de l'information est donc l'état de protection, face aux risques identifiés, qui résulte de l'ensemble des mesures générales et particulières prises pour assurer la confidentialité, l'intégrité et la disponibilité de l'information traitée, où :

- *La confidentialité* est le caractère réservé d'une information dont l'accès est limité aux seules personnes admises à la connaître pour les besoins du service.
- *L'intégrité* de l'information traitée garantit que celle-ci n'est modifiée que par un acte volontaire et légitime.
- *La disponibilité* est l'aptitude d'un système d'accéder à l'information dans des conditions définies d'horaires, de délais et de performances.

Toute entreprise se doit de protéger ses informations, le cas échéant la perte de ses informations provoqueraient :

- *Une perte financière* (exemple : destruction de fichiers client, récupération de contrats par un concurrent, etc.) ;
- *Une perte de l'image de marque* (exemple : piratage d'une banque, divulgation d'un numéro de téléphone sur liste rouge, etc.) ;
- *Une perte d'efficacité ou de production* (exemple : rendre indisponible un serveur de fichiers sur lequel travaillent des collaborateurs) ;

d'où l'intérêt pour une entreprise ou un organisme d'avoir une classification de ses informations suivant différents niveaux de sécurité. Ainsi on a les informations dites :

- ✓ *stratégiques* pour l'entreprise comme les offres de rachat, en général ce sont des informations manipulées au niveau de la direction de l'entreprise ou de l'organisation ;
- ✓ *critiques* comme le plan d'adressage de l'entreprise, la configuration des outils de sécurité, des plans de secours, etc. ;
- ✓ *internes* comme l'ensemble des informations propres à l'entreprise qui ne doivent pas être forcément de notoriété publique ;
- ✓ *publiques* comme les informations faisant l'objet de communiqué de presse ou les informations figurant que sur le site Web de l'entreprise ou de l'organisme (exemple du rapport annuel de gestion).

Mais ce travail de classification demande une réflexion qui doit être menée au sein de l'entreprise et de l'organisme en fonction de son système d'information. Ce système ne doit pas être vulnérable à une menace, une action ou un événement qui peut porter préjudice à la sécurité. Qu'entend t-on par système d'information ? Pourquoi mon système est-il vulnérable ?

1.1 NOTION DE SYSTÈME D'INFORMATION

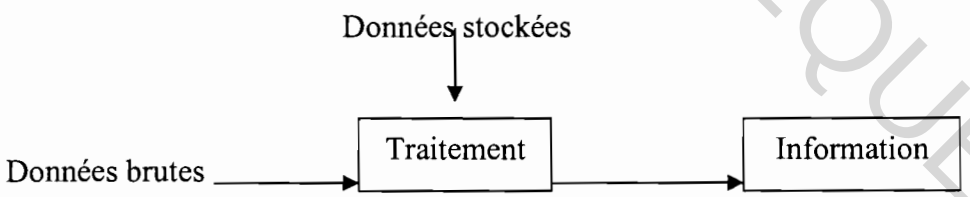
On entend par système d'information de l'entreprise, selon REIX (2000 : 1), un ensemble de ressources affectées à des fonctions d'acquisition, de stockage, de traitement et de diffusion de l'information. Pour ALTER (1996 : 2), un système d'information est un système qui utilise des technologies de l'information pour saisir, transmettre, structurer, retrouver, manipuler ou afficher l'information utilisée dans un ou plusieurs processus de gestion. Ces définitions mettent en évidence deux notions essentielles. Il s'agit d'une part de la notion d'ensemble de moyens (matériels, humains et financiers) et d'autre part de la notion d'information.

Pour ce qui est de la notion de l'information, au-delà de la définition technique du mot information : « données enregistrées, classées, organisées pour avoir une signification et une valeur propre au contexte et à l'instant » (Dictionnaire LE PETIT LAROUSSE ILLUSTRE : 1996 : 549), on parle de *l'information sensible* ou de *l'information stratégique*, expressions montrant que l'information ne prend son intérêt, par delà le système de communication et de traitement, que lorsqu'elle est replacée dans son contexte. Ce qui importe, c'est la bonne information au bon moment pour le bon utilisateur ; comme le soutiennent WATERFIELD & RAMSING (Février 1998) : « dans un environnement concurrentiel, l'organisation qui détient de meilleurs informations dispose d'un net avantage ».

Après avoir passé en revue les différents types d'informations, nous examinerons les finalités des systèmes d'information.

1.1.1. Notion d'information

La définition étymologique du mot *information* nous conduit au mot latin *informare* qui veut dire « mettre en forme ». Cette définition est approfondie par Davis (1986) pour qui l'information représente les données transformées sous une forme significative pour la personne qui les reçoit ; elle a une valeur pour ses décisions et ses actions.



Selon MAIDOUDOU (1992 :15), plusieurs critères sont utilisés pour caractériser l'information. En effet selon :

- ✓ <u>le type d'information :</u> on parle d'informations stratégiques, d'informations opératoires ou d'informations courantes. On distingue l'information destinée au grand

public, aux masses média, aux pouvoirs publics, aux clients, aux actionnaires, aux syndicats, aux fournisseurs, au personnel, à la direction, etc. ;

- ✓ la diffusion de l'information : l'information est soit publique ou interne à l'organisme, soit restreinte voire confidentielle ;
- ✓ le type d'utilisateur : l'information peut être destinée directement à l'utilisateur final ou à travers un intermédiaire impliqué ou neutre ;
- ✓ Le niveau d'élaboration : l'information est dite primaire, secondaire ou tertiaire ;
- ✓ Le média utilisé : information orale, écrite, graphique ;
- ✓ La nature de l'information : on parle d'information scientifique et technique, d'information économique (finance, marché, gestion), d'information juridique (législation, jurisprudence), d'information sociale, etc. ;
- ✓ La fréquence d'utilisation : l'information est dite vivante ou morte (classée) ;
- ✓ Les finalités de l'information : lorsque l'information permet de connaître le milieu puis d'agir sur le milieu.

Pour l'entreprise nous nous limiterons à *l'information utile* en nous basant sur les informations internes et externes. Les informations utiles sont celles qui informent sur la réalité et permettent d'apprécier son fonctionnement et son évolution. Celles qui informent sur l'environnement de l'entreprise et ses changements sont appelées informations externes.

L'information doit être adaptée aux utilisateurs tant par sa forme, son contenu que par le vecteur par lequel elle transite. En effet, la même information n'est pas utile à tous et chaque utilisateur a des besoins différents.

REIX (2000 : 63-64) soutient que l'information apparaît comme un élément de base du fonctionnement des organisations, et que pour faire face à l'ensemble de ces besoins fondamentaux en information, les organisations développent des activités de traitement de l'information (acquisition, communication, transformation, stockage, diffusion) essentielles pour leur survie.

Les attributs de la qualité de l'information se fondent donc sur son contenu, sa forme et son temps. Qu'est qu'un système d'information et qu'elles sont ses finalités ?

1.1.2. Le système d'information

La notion de système d'information est assez récente. Plusieurs définitions peuvent être reprises pour cerner la notion :

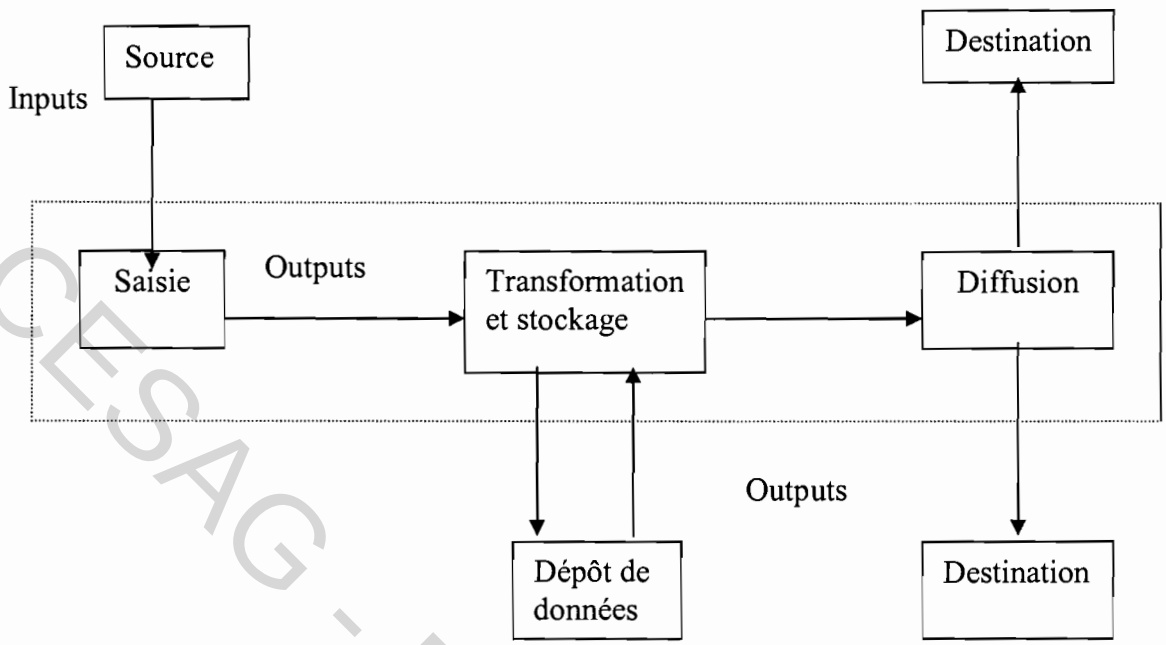
Lucas (1986) analyse le système d'information comme « l'ensemble des procédures organisés qui permettent de fournir l'information nécessaire à la prise de décision et/ou contrôle de l'organisation ».

Une définition simple est donnée par Dumoulin (1986) : « Ensemble des informations circulant dans l'entreprise, ainsi que les procédures de traitement et les moyens octroyés à ces traitements. »

Selon l'OECCA[2] (1960), au congrès national de Strasbourg : « de tout temps, en entreprise, les responsables à quelque niveau que ce soit ont recherché l'information qui leur était utile : à l'analyser, la classer, la traiter, la recouper et la combiner avec d'autres et enfin à la communiquer ». Le *système d'information* (ou *les systèmes d'information*) est donc un ensemble bien défini de tâches élémentaires qui permettent la saisie, le stockage, la transformation et la diffusion des données, comme l'indique la figure 1. A partir de ces définitions, il ressort que la fonction première d'un système d'information est de produire de l'information.

[2] OECCA : Ordre des Experts Comptables et Comptables Agréés.

Figure 1 : Un système d'information.



Source: Vital Roy 2000 (2004: 2)

Face à la masse croissante des données et à la répétition des traitements à opérer, les entreprises ont recours à l'informatique érigée en système décidant de l'information (quelle information produire ? A quel rythme ? Sous quelle forme ?)

L'offre d'information est de loin supérieure à la demande, selon MOHAMED (2002 : 34-36). Cela conduit les entreprises à organiser en système structuré la collecte et le traitement de l'information de natures diverses, de manière à les rendre disponibles, au bon moment, au bon destinataire, avec pour objectif d'améliorer la performance de tous les membres, qu'il s'agisse d'activités stratégiques, d'activités opératoires ou d'activités de contrôles. Le système d'information de l'entreprise joue donc un rôle important voire primordial. En effet, la pérennité et le développement d'une entreprise dépendent de la qualité des décisions (stratégiques et/ou opérationnelles) de sa direction, ainsi que du bon fonctionnement de la mise en œuvre de ses moyens par le personnel. Un bon système d'information est celui qui peut donner des avantages concurrentiels à l'entreprise en l'informant sur son marché, ses clients, ses fournisseurs, ses concurrents. Ce système doit analyser en permanence les informations qui correspondent aux indicateurs de performance que l'entreprise s'est fixée

pour mesurer les adaptations nécessaires et les évolutions à moyen et à long terme. En outre, un bon système d'information doit favoriser le bon fonctionnement opérationnel, mesurer le rendement des hommes, des capitaux, des matériels et réguler le fonctionnement de l'entreprise.

Aussi, le système d'information de l'entreprise se compose de quatre éléments d'ensemble à savoir :

- ✓ Un ensemble de domaines de gestion : se caractérisant par la réalisation d'activités ou de processus présentant une certaine homogénéité ;
- ✓ Un ensemble de données nécessaires à la gestion : mémorisées dans des fichiers, ces données portent à la fois sur la préparation de l'action (données prévisionnelles) et la représentation et la mesure des faits réels (données d'observation) ;
- ✓ Un ensemble de base de modèles et d'outils : il s'agit de l'ensemble des algorithmes et des procédures formalisés sous forme de programmes et de manuels ;
- ✓ Un ensemble de règles et de principes de fonctionnement : les règles de fonctionnement définissent les principes et les modalités de réalisation des opérations.

Le système d'information est dépendant du métier, de la stratégie, de la structure et du style de direction spécifique à chaque entreprise. Il revient donc à la Direction générale, assistée éventuellement de son comité d'audit interne, de définir les règles que devront respecter les systèmes d'information. Trois principaux rôles sont assignés aux systèmes d'information à savoir : un support stratégique, un support à l'élaboration de décision d'affaire et un support pour les opérations d'affaires. (MAIDOUDOU, 1992 : 28).

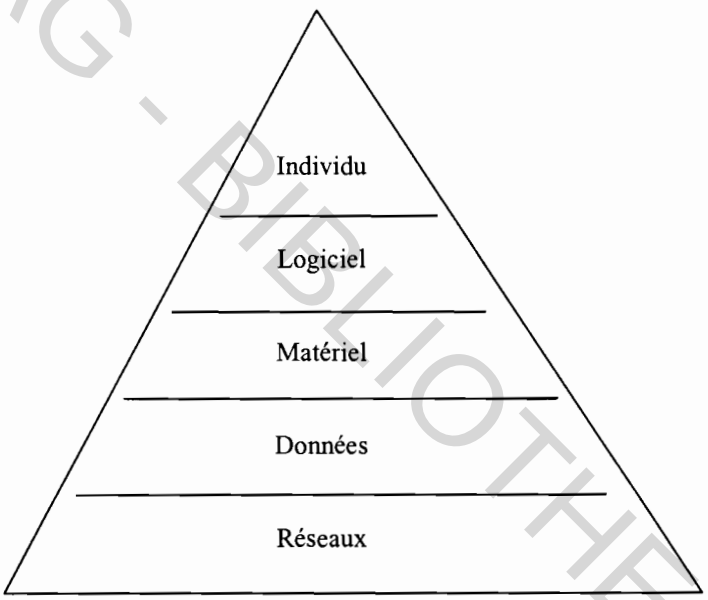
Le système d'information est une activité stratégique et également technique. Il doit permettre de connaître le présent, de prévoir, de comprendre et d'informer rapidement. Le système d'information doit être adapté à la nature (taille, structure) de l'organisation et être efficace (rapport qualité/coût). Les modes de fonctionnement et les méthodes de contrôles sont d'autant plus importants que la définition de la stratégie. Qu'en est –il de la conception, de l'organisation et de la mise en place d'un système d'information ?

1.1.3. L'organisation et la mise en place d'un système d'information

Un système d'information se perçoit comme un ensemble de ressources permettant d'acquérir, de traiter, de communiquer des informations. Il assiste l'homme au sein d'une organisation dans des fonctions d'exécution, de gestion et de prise de décision. Il sera réalisé physiquement grâce au personnel, aux procédures, aux données, aux logiciels et au matériel.

La figure 2 montre les différentes ressources en SI.

Figure 2 : les ressources en systèmes d'information.



Source : Vital Roy 2000 (2004:2)

Construire un système d'information consiste à répondre aux besoins en informations d'une entreprise en s'appuyant éventuellement sur des technologies spécifiques de traitement de l'information. Cette mise en place d'un système d'information est délicate à trois points de vue : technique (ordinateurs), économique (coûts) et sociologique (changements importants dans la répartition des tâches, des pouvoirs).

La démarche comprend deux étapes :

- Une première étape, axée sur la réalisation d'une ou plusieurs applications, dans un domaine bien délimité à l'intérieur de l'entreprise ;
- Une deuxième étape dite globale, stratégique, axée sur une réflexion à long terme, définissant les axes majeurs de développement du système d'information.

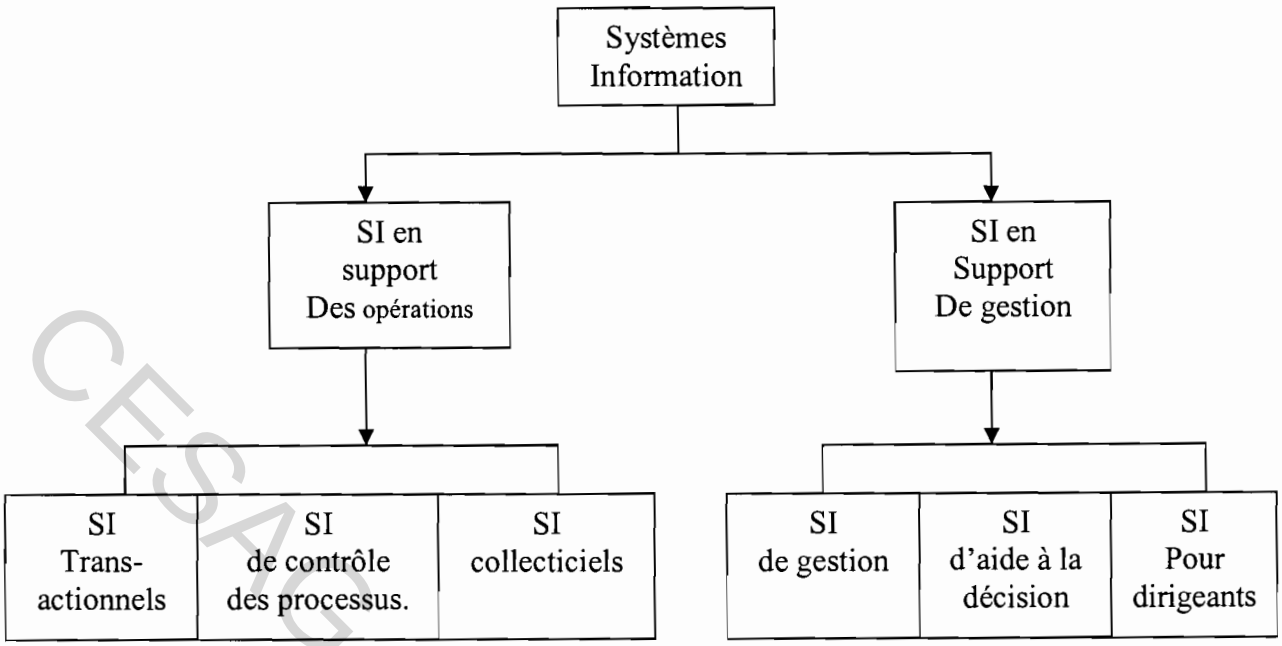
Tout système d'information doit être planifié. Cette planification doit être l'expression d'une attitude volontaire de l'entreprise ou d'une organisation pour préparer les évolutions. Elle doit se traduire par des objectifs clairement identifiés dans des documents susceptibles de mobiliser les différents acteurs concernés. Cette phase de planification présente donc le double aspect d'être un mécanisme d'allocation de ressources (financières et humaines) et un moyen pour motiver et coordonner les différents responsables concernés en les amenant à conduire une réflexion commune.

Le système d'information peut regrouper plusieurs sous systèmes d'information :

- Un système d'information en support des opérations : composé de système d'information transactionnels, de contrôle de processus, collecticiels[3]. (Figure 3) ;
- Un système d'information en support de gestion : composé de système information de gestion, d'aide à la décision, de tableaux de bords pour dirigeants. (Figure 3) ;
- Autres système d'information : système Expert (SE), SI de gestion des connaissances, SI en intelligence d'affaires, SI fonctionnels, SI stratégiques, etc. (Figure 4).

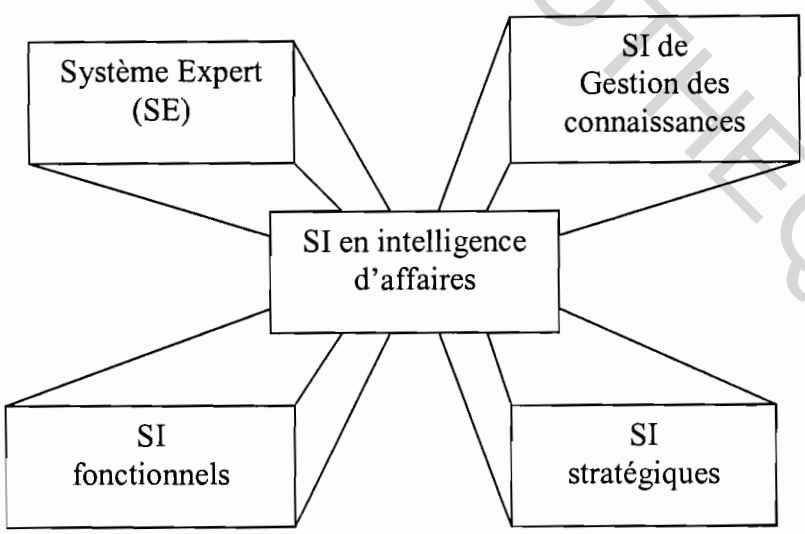
[3] Collecticiel : Un collecticiel est un système informatique qui assiste un groupe d'utilisateurs à la réalisation d'un projet commun, d'une tâche commune et qui fournissent une interface à un environnement partagé. Les membres du groupe collaborent à distance, soit au même moment (activité synchrone), soit à des moments différents (activité asynchrone). Favoriser la production est l'objectif principal dans le secteur du travail collaboratif assisté par ordinateur (CSCW Computeur Supported Collaborative Work). Facilter les apprentissages à distance est le but des systèmes de type CSCL (Computer Supported Collaborative Learning).

Figure 3 : Classification des SI selon les niveaux de gestion et d'opération



Source : Vital Roy 2000 (2004 :3)

Figure 4 : Autres classifications de SI



Source: Vital Roy 2000 (2004 :3)

Le système d'information nécessite pour sa mise en place un projet de SI. Cette mise en place de projet de système d'information peut se faire à travers plusieurs méthodes aussi nombreuses que variées. Nous nous limiterons à trois d'entre elles, les plus connues :

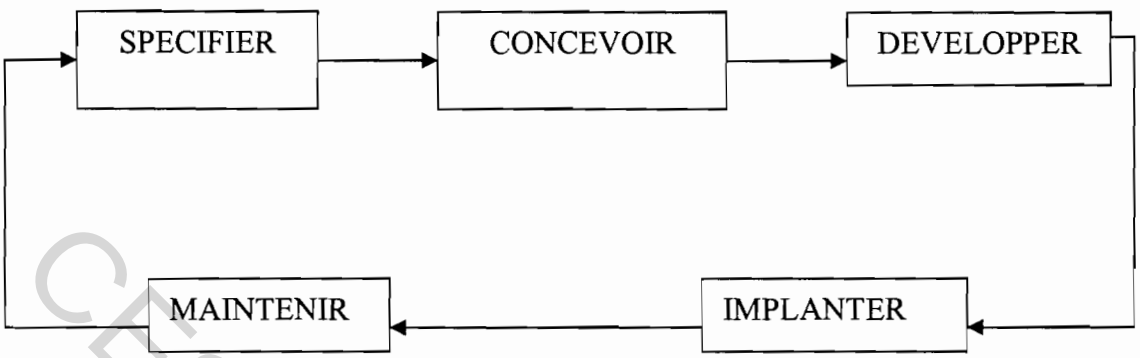
- ✓ La méthode fondée sur l'analyse des processus de gestion : la paternité de cette méthode appelée « Business Système Planning » (BSP) est attribuée à IBM. Le principe de cette méthode consiste à considérer l'entreprise comme un ensemble cohérent de processus qui doivent absolument se dérouler quelque soit l'organisation retenue, puis à définir l'ensemble des données qui permettront à ces processus de se dérouler ;
- ✓ La méthode fondée sur les facteurs clés de succès : le principe consiste à favoriser le développement des sous-systèmes d'information qui renforcent les facteurs-clés de succès de l'entreprise ;
- ✓ La méthode de l'approche par l'analyse concurrentielle : cette méthode proposée par M. PORTER, prend en compte le développement accéléré des technologies de l'information (informatique, télématique, bureautique, etc.). La stratégie de l'entreprise devient le centre du débat ; l'entreprise est soumise à différentes forces concurrentielles (concurrents, produits, les clients, les fournisseurs, etc.) et la question fondamentale est de savoir comment les technologies de l'information peuvent affecter l'équilibre de ces forces concurrentielles.

Le développement du système d'information se réalise par la mise en œuvre des projets d'informatisation, le System Development Life Cycle (SDLC). Le cycle de vie du projet traduit les activités de mise en œuvre suivantes :

- spécifier : définir les objectifs et les contraintes ;
- concevoir : définir les principes de solution ;
- développer : organiser la solution détaillée ;
- implanter : mettre en place les moyens de l'organisation ;
- maintenir : évaluer, adapter.

La figure 5 illustre le cycle de vie d'un projet informatique.

Figure 5 : Cycle de vie de projet d'informatisation



Source : MAIDOUDOU Abakar (1992)

A chaque étape de ce cycle de vie, des problèmes techniques (matériel, logiciel), humains (qui doit faire quoi ?), économiques (coûts) apparaissent.

En outre la construction d'un système d'information appelle d'autres impératifs que sont :

- ✓ *L'adaptabilité permanente du système* : savoir conduire l'évolution de l'environnement est une nécessité impérieuse ;
- ✓ *La sécurité garantie* (contrôle du système informatique ; contrôle de la méthodologie ; contrôle de sécurité générale ; contrôle des applications ; contrôles à la saisie des données ; autres contrôles des risques des erreurs de programmation, d'acheminement, par balance) ;
- ✓ *Son aptitude à se faire évaluer* (contrôle de la gestion ; Evaluation post-implantation, évaluation prévisionnelle, audits informatiques) ;
- ✓ *La participation des utilisateurs* ;
- ✓ *Le support des cadres ;*
- ✓ *La formulation claire des exigences ;*
- ✓ *La planification adéquate ;*
- ✓ *Des attentes réalistes.*

Il ressort de ce qui précède que le traitement automatisé de l'information doit être sûr. Pourtant l'ordinateur reste un outil potentiellement vulnérable et donc dangereux. Si l'entreprise souhaite pouvoir s'appuyer en toute confiance sur son système d'information, elle se doit impérativement de développer un bon management de la sécurité du SI.

1.2. LE MANAGEMENT DE LA SÉCURITÉ DU SYSTÈME D'INFORMATION

La sécurité du système d'information est indispensable pour toute l'entreprise et concerne tout le monde aussi bien les actionnaires, les partenaires, la direction générale, les utilisateurs que les informaticiens. Le management de la sécurité sert à définir les mesures de prévention et de protection à mettre en œuvre pour la pérennité de l'entreprise. Sa mise en œuvre nécessite une préparation à travers une évaluation exhaustive des risques potentiels, une mesure de l'efficacité des mesures proposées au regard de la persistance du risque, une décision de plan de mise en œuvre et une hiérarchisation des actions, une sensibilisation de tous les acteurs, un suivi à travers des tests récurrents de l'efficacité des mesures appliquées et constamment une réactualisation des procédures de sécurité ainsi qu'une mise à niveau du système en fonction des apports en logiciels et matériels.

1.2.1 Définition et objectifs de la sécurité du système d'information

Comment la Sécurité du Système d'Information (SSI) est elle perçue ? Nous nous proposons dans cette sous section de définir la SSI, de mêmes que les objectifs qu'elle vise.

A. Définition de la Sécurité du Système d'Information

L'information est indispensable à la bonne marche des organisations. A mesure que la Direction prend conscience des conséquences qu'implique la perte de données ou de possibilités de traitement, la sécurité tend à devenir une priorité absolue. Selon REIX (2002 :416) : « la sécurité d'un système d'information est sa non vulnérabilité à des accidents ou à des attaques volontaires, c'est-à-dire l'impossibilité que ces agressions produisent des conséquences graves sur l'état du système ou son fonctionnement ».

B. Les objectifs de la Sécurité du Système d'Information

Pour THORIN (2000 :45), un audit informatique n'a de sens que si sa finalité est définie quel que soit le type d'audit, notamment l'audit de la sécurité du SI. Cette finalité est de porter un jugement sur le management du SI et de l'existence des objectifs.

L'objectif de la sécurité des systèmes d'information est de garantir qu'aucun préjudice ne puisse mettre en péril la pérennité de l'entreprise. Cela consiste à diminuer la probabilité de voir des menaces se concrétiser, à en limiter les atteintes ou dysfonctionnements induits, et autoriser le retour à un fonctionnement normal à des coûts et des délais acceptables en cas de sinistre. Il importe de signifier que la sécurité ne permet pas directement de gagner de l'argent mais évite d'en perdre. Elle se présente d'une part comme une stratégie préventive qui s'inscrit dans une approche d'intelligence économique (réduction des coûts), et d'autre part comme une stratégie curative dans le cas de sinistre (les procédures mises en place permettent de redémarrer rapidement le système).

Pour ce qui concerne les données et les logiciels, la sécurité informatique implique qu'il faille assurer les propriétés suivantes:

- ✓ la *confidentialité* (aucun accès illicite): maintien du secret de l'information et accès aux seules entités autorisées;
- ✓ l'*intégrité* (aucune falsification): maintien intégral et sans altération des données et programmes;
- ✓ l'*exactitude* (aucune erreur);
- ✓ la *disponibilité* (aucun retard): maintien de l'accessibilité en continu sans interruption ni dégradation;
- ✓ la *pérennité* (aucune destruction): les données et logiciels existent et sont conservés le temps nécessaire;
- ✓ la *non répudiation* (aucune contestation).

Ces propriétés, en fonction de la valeur des ressources et de leur cycle de vie, doivent être garanties par des mesures de sécurité. Celles-ci, sont mises en oeuvre au travers d'outils particuliers, de procédures adaptées et de personnes. Elles sont gérées et validées par des procédures de gestion et d'audit. La sécurité repose donc sur un ensemble cohérent de

mesures, procédures, personnes et outils. D'où la nécessité de développer une politique de management adéquate.

1.2.2. LE MANAGEMENT DE LA SÉCURITÉ

Le management de la sécurité se conçoit à travers la mission de la sécurité, la définition d'une politique sécuritaire, sa réalisation et les conditions de succès de cette démarche sécurité.

A. La mission

La principale mission du management de la sécurité, selon Aud-IT (2004 :2), est d'évaluer les risque des SI nécessaires au fonctionnement des applications. Elle peut se résumer en cinq types d'actions génériques. Elle consiste à:

- Définir le périmètre de la vulnérabilité lié à l'usage des technologies de l'information et de la communication;
- Offrir un niveau de protection adapté aux risques encourus par l'entreprise;
- Mettre en oeuvre et valider l'organisation, les mesures, les outils et les procédures de sécurité;
- Optimiser la performance du système d'information en fonction du niveau de sécurité requis;
- Assurer les conditions d'évolution du système d'information et de sa sécurité.

L'efficacité de la sécurité d'un système d'information ne repose pas uniquement sur les outils de sécurité mais également sur une stratégie, une organisation et des procédures cohérentes. Cela nécessite une structure de gestion adéquate dont la mission est de gérer, mettre en place, valider, contrôler et faire comprendre à l'ensemble des acteurs de l'entreprise l'importance de la sécurité. Elle détermine également le comportement, les privilèges, les responsabilités de chacun. Elle spécifie, en fonction de facteurs critiques de succès qui permettent d'atteindre les objectifs de l'entreprise, les mesures et directives sécuritaires appropriées. Ces dernières doivent être cohérentes par rapport au plan d'entreprise et informatique. Pour cela, une vision stratégique de la sécurité globale de l'entreprise est nécessaire. Et le choix des mesures de

sécurité à mettre en place au sein des organisations, résulte généralement d'un compromis entre le coût du risque et celui de sa réduction. Il dérive de l'analyse à long, moyen et court termes des besoins et des moyens sécuritaires.

B. La définition d'une politique sécuritaire

La gestion de la sécurité est spécifique à la structure organisationnelle de l'entreprise et dépend de sa stratégie. Il existe donc autant de politiques, de procédures, d'outils de sécurité que d'entreprises et de besoins sécuritaires. Pour THORIN (2000 :57) la politique sécuritaire doit d'une part assurer la reprise du service dans des délais acceptables, et d'autre part rendre absolument impossible une défaillance permanente. La direction générale de l'entreprise est responsable de l'évaluation des risques, de l'établissement de la politique de sécurité et de la mise en place de la structure organisationnelle qui la mettra en oeuvre. Les risques et la politique font l'objet d'une évaluation et d'une actualisation. Une politique de sécurité offre une réponse graduée à un problème sécuritaire spécifique, en fonction de l'analyse des risques qui en est faite et de l'impact des risques sur l'entreprise. Elle doit exprimer l'équilibre entre les besoins de production et de protection.

C. La réalisation d'une politique sécuritaire

Une entreprise détermine des normes générales de sécurité qui s'appliquent à l'ensemble de ses systèmes et de son personnel. La démarche sécurité est un projet d'entreprise, dans la mesure où chacun est concerné par sa réalisation ; elle est analogue à celle de «qualité totale » (participation de tous). Sa validité sera renforcée si l'organisation développe une éthique d'entreprise et si elle stipule également ses exigences de sécurité envers ses partenaires externes.

Le CLUSIF (2004 :3) estime que pour la réalisation d'une politique sécuritaire, l'entreprise doit :

- Déterminer le périmètre (fonctionnel, géographique, organisationnel, etc.) ;
- Identifier les processus de la sécurité et leurs risques associés ;

- Déterminer les exigences (objectifs, référentiels, méthodes, etc.) nécessaires pour assurer la sécurité du processus ;
- Définir les mesures de sécurité nécessaires pour se conformer aux exigences exprimées.

D. Les conditions de succès d'une démarche sécuritaire

Selon l'étude de la Commission bancaire Française, la mise en place d'une démarche sécurité passe par la réalisation des points suivants:

1. une volonté directoriale;
2. une politique de sécurité simple, précise, compréhensible et applicable;
3. la publication de la politique de sécurité;
4. une gestion centralisée de la sécurité et une certaine automatisation des processus de sécurité;
5. un niveau de confiance déterminé des personnes, des systèmes, des outils impliqués;
6. un personnel sensibilisé et formé à la sécurité, possédant une haute valeur morale;
7. des procédures d'enregistrement, de surveillance et d'audit;
8. la volonté d'éviter de mettre le système d'information de l'entreprise en situation dangereuse;
9. l'expression, le contrôle et le respect des clauses de sécurité dans les différents contrats;
10. une certaine éthique des affaires et respects des contraintes légales (recensement des fichiers nominatifs, etc.).

Le management de la sécurité du système d'information exige une démarche globale de maîtrise des risques liés à l'usage de systèmes informatiques et de télécommunication et contribue à la protection des valeurs (ressources informatiques, informations). La difficulté de mise en oeuvre de solutions efficaces de sécurité provient du fait qu'elles doivent être à la fois d'ordre technologique, procédural, réglementaire, organisationnel, humain et managérial. Ces multiples facettes sont donc à intégrer de façon cohérente et doivent être acceptées et gérées

efficacement par l'ensemble des acteurs intervenant dans une opération. Ainsi le respect de normes et règlements internationales s'avère nécessaire voir primordiale.

1.3. LES NORMES ET LES LOIS DE LA SÉCURITÉ

Les normes, règlements et lois sont importants pour le bon déroulement de la profession d'auditeur. Ils permettent de définir des principes fondamentaux et de préciser leurs modalités d'application concernant la démarche à suivre lorsque l'audit de la sécurité est réalisé. En outre il existe des lois répressives qui sanctionnent.

Dans le cadre de la sécurité informatique, plusieurs normes et lois ont vus le jour notamment la norme ISO/IEC 17799 : 2000, les normes professionnelles de la Compagnie Nationale des Commissaires aux comptes (CNCC) et plus particulièrement la norme CNCC 2-302, la lois du code des télécommunications du Sénégal et la loi Sarbanes-Oxley.

1.3.1. La norme ISO/IEC 17799 : 2000

La norme ISO/IEC 17799 : 2000 (anciennement BS 7799) propose des recommandations pour le démarrage, l'installation et la gestion de la politique de sécurité des informations et des systèmes d'information de l'entreprise.

Cette norme fournit des standards de contrôle de la sécurité des informations de très bonne qualité (best practice) structurés en domaine, par exemple la politique de sécurité, l'organisation de la sécurité, la sécurité physique, la gestion des télécommunications et des systèmes et le contrôle des accès. C'est un excellent outil pour la mise en place de la gestion de la politique de la sécurité des informations.

1.3.2. Les normes professionnelles

La Compagnie Nationale des Commissaires aux Comptes a entériné, en 2003, la transposition dans le référentiel français des normes d'audit internationales de l'IFAC (the International Federation of Accountants).

Les normes professionnelles d'Audit sont intégrées dans le Recueil « Normes professionnelles et Code de déontologie » paru en décembre 2000 et mis à jour en juillet 2002. Parmi les normes relatives à la mission d'audit, celles qui traitent de « l'appréciation du contrôle interne » sont au nombre de trois :

- évaluation du risque et contrôle interne (norme CNCC 2-301),
- audit réalisé dans un environnement informatique (norme CNCC 2-302),
- facteurs à considérer lorsque l'entité fait appel à un service bureau[4] (norme CNCC 2-303).

A. Les droits des personnes

Les droits des personnes dont les données (nominatives) sont enregistrées dans un traitement automatisé sont les suivants :

- droit d'être informé du traitement des données (loi du 6 janvier 1978, art. 27, al. 2) ;
- droit d'accéder et de rectifier les informations qui y sont contenues (art 34) ;
- droit de s'opposer au traitement des données (art. 226-18 du Code pénal lois européennes).

En plus du respect des droits des personnes énoncés ci-dessus, la loi prévoit une obligation :

- de déclaration des traitements (art. 226-16 du Code pénal),

[4] Un service bureau: un service spécialise qui assure un traitement de travail bien défini (sous-traitance), comme par exemple assurer tout le traitement : de la collecte des documents jusqu'à l'archivage des données électroniques, en passant par la numérisation, la reconnaissance des données, l'encodage et le contrôle qualité.

- de ne pas utiliser le traitement à d'autres fins que celles déclarées (art. 226-21 du Code pénal),
- de sécurité (art. 29 de la loi Informatique et Liberté du 6 janvier 1978 ; art. 226-17 du Code pénal ; art. 226-22 du Code pénal.)

B. La protection des logiciels

La protection des logiciels est réglementée par le Code de la propriété intellectuelle. Les logiciels mis à la disposition du public par la diffusion d'un support matériel sont soumis à l'obligation de dépôt légal à la Bibliothèque Nationale. Le dépôt est obligatoire et gratuit. Il est sanctionné par des peines d'amende allant de 1 500 à 75 000 euros (327 798 à 49 196 775 F. CFA).

Au niveau international, la BSA (Business Software Alliance) est une organisation qui représente les principaux développeurs de logiciels et du commerce électronique dans 65 pays. Elle a été fondée en 1988 et possède des bureaux aux Etats-Unis, en Europe et en Asie. Son action consiste à sensibiliser les gouvernements et les consommateurs à la lutte contre la fraude relative aux logiciels et le vol sur Internet. Cette association met à disposition (par téléchargement) des consommateurs et des entreprises un logiciel d'audit, GASP (Globally Accessible Statiscal Procedures) permettant d'identifier les copies illicites figurant sur un ou plusieurs ordinateurs. Les tableaux 1 et 2 suivants, présentent une synthèse des infractions par type de logiciels.

Tableau 1 : Logiciels téléchargeables

	Typologie	Infractions	Etendue de la protection
Logiciels libres (open source)	L'auteur fournit gratuitement le logiciel avec son code source.	En général le contrat de licence exclut l'exploitation commerciale du logiciel libre.	Les droits sont régis par les termes du contrat de licence. Le droit de paternité, au même titre que les autres droits moraux, a une durée illimitée.
Logiciels gratuits (freeware)	L'auteur a donné son accord pour la reproduction et l'exploitation du logiciel sans contrepartie.	Utilisation, copie et diffusion gratuites autorisées. Mais interdiction de modification sans le consentement de l'auteur.	Droits d'auteur limités au contenu.
Téléchargement possible	L'auteur a donné son accord avec des contreparties (conditions d'utilisation et/ou paiement demandé).	L'utilisation du logiciel sans respecter les conditions du contrat de licence ou sans payer le montant de la redevance constitue un acte de contrefaçon. L'auteur doit avoir exprimé les conditions dans lesquelles il consent à l'utilisateur un droit de reproduction et d'utilisation. A défaut, le téléchargement est un acte de reproduction et l'utilisation du logiciel sans droit constituerait nécessairement un acte de contrefaçon.	Les droits sont régis par les termes du contrat de licence.
Logiciels à l'essai (shareware)			
Logiciels du domaine public	Les auteurs ont renoncé à leur droit de paternité sur l'œuvre.	Aucune, libre disposition.	Pas de droits de paternité sur ces logiciels.

Source : CNCC, Juillet 2002.

Tableau 2 : Logiciels non téléchargeables

	Droits de l'utilisateur du logiciel	Droits de l'auteur du logiciel		Infractions	LOI	Sanctions
Logiciels commerciaux **Téléchargement Prohibé**	Droit d'utilisation Droit de décompilation du logiciel sous certaines conditions Droit à une seule copie de sauvegarde Droit de reproduction et de traduction du code pour les besoins de l'interopérabilité, dans les conditions stipulées par le Code de la propriété intellectuelle	Droits d'auteur accordé pour 70 ans	Droits moraux : Droit au nom Droit au respect de l'œuvre Droit d'autoriser ou nom la divulgation de son oeuvre	Contrefaçon et dommages et intérêts si l'auteur a subi un préjudice lié à l'utilisation sans licence.	Loi du 10 mai 1994 Loi du 5 février 1994	Responsabilité civile et pénale du dirigeant d'entreprise personne physique en plus de celle de la personne morale.
			Droits patrimoniaux : Droit d'exploitation (d'utilisation et d'usage) Droit de représentation Droit de reproduction Droit de traduction, d'arrangement, d'adaptation Droit de mise sur le marché à titre gratuit ou onéreux			

Source : CNCC, Juillet 2002.

C. L'archivage fiscal et le contrôle des comptabilités informatisées

L'archivage fiscal doit permettre à une entreprise de répondre à une demande d'information émanant de l'administration fiscale dans le cadre de la réglementation applicable (article 103

de la loi de finances pour 1990, complétée par la loi du 10 mai 1994 spécifique aux programmes développés par des prestataires).

Les instructions administratives, des 14 octobre 1991 et 24 décembre 1996 commentant ces dispositions, précisent les obligations incombant aux contribuables dont la comptabilité est informatisée et peuvent être résumées comme suit :

- mise à disposition de l'administration fiscale de tout élément d'information ou traitement concourant directement ou indirectement à la formation des résultats comptables ou fiscaux,
- tenue d'une documentation informatique :
  - ✓ décrivant le système d'information mis en œuvre au cours de la période vérifiée,
  - ✓ explicitant les règles de gestion des données et des fichiers mises en œuvre dans les programmes informatiques et ayant des incidences directes ou indirectes sur la formation des résultats comptables et fiscaux et des déclarations rendues obligatoires par le Code Général des Impôts.

D. Autres lois

Plusieurs lois spécifiques à chaque pays existent. Au Sénégal nous présentons, notamment, la loi portant code des télécommunications de décembre 2001. En effet, Depuis la fin de l'année 2001, le Sénégal s'est doté d'un nouveau code des télécommunications, à travers la loi n°2001-15 du 27 décembre 2001 portant code des télécommunications. Cette dernière abroge et remplace la loi n°96-03 du 22 février 1996 portant code des télécommunications qui, elle-même, s'est substituée à la loi n° 72-39 du 26 mai 1972 relative aux télécommunications.

Le nouveau code des télécommunications introduit les principales innovations suivantes :

- ✓ Clarification des principes de base devant désormais régir les activités de télécommunication.
- ✓ Meilleure cohérence des régimes juridiques applicables aux réseaux, services et équipements de télécommunications.
- ✓ Mise en place d'un organe indépendant de régulation chargé, sous l'autorité directe du Président de la République, de garantir l'exercice d'une concurrence saine et loyale, au

bénéfice des consommateurs, des opérateurs du secteur et, en général, de l'économie nationale.

La loi Sarbanes-Oxley aux Etats Unis, en ses articles 303 et 404, vise à mieux responsabiliser les dirigeants des entreprises cotées en matière de préparation et de présentation de l'information financière. Les directeurs généraux et les directeurs financiers ont ainsi pour obligation :

- de certifier personnellement la sincérité de leurs états financiers ;
- d'établir et de maintenir des procédures et des contrôles internes adéquats afin de garantir l'intégrité de l'information financière ;
- de maintenir une documentation de ces contrôles et de les transmettre au commissaire aux comptes ;
- de vérifier et d'évaluer régulièrement l'efficacité de ces contrôles afin de veiller à ce qu'ils soient en phase avec l'évolution de la réglementation et de l'activité de l'entreprise.

CONCLUSION

Ce premier chapitre nous a permis de bien percevoir la notion de la sécurité du système d'information (SSI), ainsi que les concepts d'information et de système ou des systèmes d'information (SI).

Il en est ressorti que la sécurité du SI est au cœur de la pérennité de l'entreprise. Car avec l'informatique, les entreprises ont à leur disposition un outil puissant, mais cet outil peut se révéler dangereux s'il n'est pas sécurisé. Il importe donc, que la Direction de l'entreprise élabore et mettre en place un bon mangement de la SSI pour pouvoir assurer la pérennité de l'information et de la communication, pouvoir offrir un niveau de protection adapté aux risques auxquels est exposée l'entreprise et mettre en œuvre les mesures, outils et procédures de sécurité, tout en optimisant la performance du SI et son développement.

L'apport des normes et lois internationales a montré que l'utilisation de l'informatique en audit ne saurait modifier les objectifs fondamentaux de la mission de l'auditeur.

CHAPITRE 2 : AUDIT DE LA SÉCURITÉ DU SYSTEME D'INFORMATION

INTRODUCTION

L'audit de la sécurité, à l'instar de tout audit, requiert une rigueur et une démarche appropriées. Et dans le souci d'atteindre les objectifs de certification plusieurs associations et clubs, notamment le CNCC et le CLUSIF, ont développé des techniques d'approche d'une mission d'audit informatique.

Ce second chapitre de notre partie théorique sera consacré à une analyse de la mission d'audit de la sécurité à savoir les objectifs et les travaux à réaliser, de la démarche et du déroulement d'une mission d'audit sécurité ainsi que des méthodes et des outils adéquats à utiliser. Aussi nous présenterons notre modèle d'analyse dans le cadre de notre étude sur la sécurité du système d'information à la CNCAS.

2.1 MISSIONS ET OBJECTIFS DE LA SÉCURITÉ DU SYSTEME D'INFORMATION

La sécurité du SI vise selon le CLUSIF (2003) à protéger les actifs informatiques de l'entreprise contre les risques et ce d'une manière qui est adaptée à l'entreprise, à son environnement et à l'état de son outil informatique.

Les missions d'audit de la sécurité visent à présenter les objectifs recherchés, la revue de l'organisation générale de la sécurité, l'analyse générale des risques, l'évaluation de la sécurité physique, l'évaluation des données et des traitements informatiques ainsi que l'examen des dispositifs de protection contre les risques et attaques venus du réseau interne ou d'Internet.

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

L'audit de la sécurité couvre toutes les composantes du système d'information. Il doit aboutir, en cas d'insuffisances décelées, à la proposition des mesures à mettre en place pour renforcer la sécurité. Les objectifs de l'Audit de la sécurité peuvent être perçus, selon la CNCC (2003:11) à travers les points suivants.

2.1.1 La revue de l'organisation générale de la sécurité

L'objectif de la revue de l'organisation générale de la sécurité vise à évaluer l'organisation informatique mise en œuvre pour assurer la sécurité :

- La politique générale et les plans de sécurité ;
- Le management et le pilotage de la sécurité ;
- La charte de sécurité ;
- Les procédures de gestion opérationnelle de la sécurité ;
- La sensibilisation et la formation du personnel à la sécurité informatique.

2.1.2 L'analyse générale du risque

La phase d'analyse du risque a pour objectifs selon la CNCC (2003 :30) la prise en compte de l'environnement informatique sur le risque inhérent et le risque lié au contrôle. Pour la Compagnie Nationale des Commissaires aux Comptes, les travaux consistent à évaluer les risques en tenant compte de l'identification potentiel et du système de contrôle interne mis en place par l'entreprise, et à en déduire la nature et l'entendu des contrôles substantifs à mener avec ou non l'aide de technique d'audit assistée par ordinateur.

Selon TALL (2004 : 18), il s'agit de faire l'analyse, des différents scénarios de risques auxquels l'entreprise ou l'organisation peut être exposés, avec la présentation pour chaque risque des aspects suivants :

- La description (la nature, l'origine, la cible, la matérialité) ;
- L'analyse de sa probabilité de survenance ;
- L'analyse de ses impacts.

L'analyse générale du risque recommande les aspects suivants :

- ✓ Les risques sur les ressources
- ✓ Les risques sur les logiciels de base et les traitements informatiques
- ✓ Les risques sur les données
- ✓ Les risques sur la conformité aux lois et contrats

2.1.3 L'évaluation de la sécurité physique

Cette évaluation consiste en la mesure du dispositif mis en œuvre pour assurer la sécurité de l'environnement physique. Cela se réalise à travers la revue de :

- la protection de l'accès physique à l'environnement informatique ;
- la protection et le contrôle de l'accès physique aux lieux de stockage des bandes (ou cartouches) magnétiques ;
- la protection des locaux contre les catastrophes naturelles ;
- la couverture des risques par un contrat d'assurance.

2.1.4 L'évaluation de la sécurité des données et des traitements informatiques

Les objectifs sont l'évaluation de l'organisation générale, des mesures et dispositifs mis en place pour assurer la sécurité des données et des traitements informatiques. Il s'agit des saisies des données, du traitement des données en temps différé, de la gestion rigoureuse des sauvegardes, de la reprise sur site extérieur, de l'accès aux applications et aux données, de la protection des données et de l'utilisation de méthode d'authenfication forte et de cryptographie.

Il s'agira donc de faire :

- L'évaluation de la production informatique ;
- L'évaluation des procédures de gestion des accès aux applications et aux données ;
- L'évaluation de la protection et de la confidentialité des données ;
- L'évaluation des autres dispositifs de sécurité.

2.1.5 L'examen des dispositifs de protection contre les risques et attaques venus du réseau

L'examen des dispositifs de protection contre les risques et attaques est une évaluation des mesures et des dispositifs mis en œuvre pour assurer la protection des systèmes informatiques contre les risques et attaques venus du réseau. Cela consiste en : la prévention des risques ; la détection des intrusions ; les réactions (ripostes) face aux attaques ; les tests de la vulnérabilité des dispositifs mis en place.

En effet il existe plusieurs manières pour un ordinateur de se mettre en liaison avec d'autres. L'ordinateur peut être isolé, c'est à dire qu'il n'y a pas de liaison fixe avec d 'autres machines, et donc l'échange de données ne peut se faire qu'à l'aide de support amovibles, disques durs amovibles, etc. L'ordinateur peut être en réseau d'entreprise (LAN, WAN) c'est à dire en contact permanent avec un groupe déterminé d'autres ordinateurs, dans un réseau d'entreprise. Enfin, l'ordinateur peut être en réseau global (Internet), c'est à dire en connexion permanente ou temporaire avec l'immense parc d'ordinateur mondial. Quel que soit le type de connexion, l'utilisateur expose son ordinateur à des dangers.

L'examen des dispositifs de protection contre les risques et attaques venus du réseau nécessite :

- Evaluation de la segmentation du réseau ;
- Evaluation des dispositifs de contrôle des accès réseau d'entreprise et Internet ;
- Evaluation des mesures et des dispositifs de sécurité de l'exploitation des réseaux ;

- Evaluation des mesures et des dispositifs de protection contre les programmes malveillants ;
- Evaluation des dispositifs de détection des intrusions et des tests de la robustesse des dispositifs de protection.

2.2 LES ETAPES DE L'AUDIT DE LA SÉCURITÉ

L'auditeur de la sécurité a une démarche adaptée aux caractéristiques environnementales.

L'informatique joue un rôle important dans toute organisation. Aussi une démarche s'impose tout au long des audits, notamment celui de la Sécurité du SI. Dans le cadre de sa mission, l'auditeur définit les objectifs à atteindre, ainsi que les ressources (matériels, logiciels, humains, financiers et juridiques). En effet, les systèmes d'information étant de plus en plus variés et mouvants d'une entreprise à l'autre, un programme standard de l'audit de la sécurité pourrait être inadapté.

L'IFACI (1993 :59), indique que lors d'un audit de la sécurité, l'auditeur doit définir le périmètre et les objectifs de la mission compte tenu des risques pour l'organisation. Il est possible de développer un programme d'audit de la sécurité en choisissant les aspects appropriés de ce module liés à la gestion de la sécurité, la sécurité physique et logique, et en les adaptant à l'environnement technologique de l'organisation. Aussi il appartient à l'auditeur d'examiner les domaines suivants :

- Les politiques, procédures et directives de sécurité ;
- Les programmes de sensibilisation et de formation à la sécurité ;
- La gestion et l'administration de la sécurité ;
- Les contrôles de sécurité physique, y compris l'accès et les risques liés à l'environnement ;
- Les contrôles d'accès (logique) logiciels, y compris ceux concernant les accès aux données et aux programmes, le contrôle de modification, les pistes d'audit, les caractéristiques du logiciel et le logiciel de contrôle d'accès.

La démarche présentée par IFACI ne prend pas assez en compte l'analyse des risques, qui est fondamentale pour notre étude sur la sécurité du SI.

THORIN (2000 :48) explique le déroulement de l'audit informatique en sept phases, à savoir :

- Le plan de travail
- La lettre de mission ou notre de service
- Une considération stratégique et tactique (Audit interne)
- Les ressources de l'auditeur
- Les travaux de l'audit
- Le rapport
- Le suivi de l'audit et l'assistance post-audit

Cette démarche d'audit, bien que détaillée, semble être spécifique à l'audit interne et généraliste.

Selon SARR (2004 : 1-11), l'audit de la sécurité étant l'examen de la sécurité du système d'information en tout ou partie pour porter un jugement à celui-ci, comme toute mission d'audit, connaît un programme d'action qui est le suivant :

- ✓ La définition des objectifs et des moyens ;
- ✓ La prise de connaissance du système ;
- ✓ L'analyse des risques ;
- ✓ L'évaluation du contrôle interne ;
- ✓ Les recommandations ;
- ✓ Le rapport.

La troisième démarche d'audit présentée, est une synthèse des deux précédente. Elle est à la fois précise et concise et permet de faire l'analyse des risques informatiques. Ainsi nous adopterons pour notre étude les différentes phases de cette dernière démarche.

2.2.1 La définition des objectifs et des moyens

Les objectifs et les moyens doivent être clairement définis et consignés sur un document appeler *la lettre de mission* ou *note de service* (pour une mission d'audit interne). Ce document précise le cadre de la mission, les objectifs, la durée, etc. Il émane de la hiérarchie de l'entreprise.

2.2.2 La prise de connaissance du système

L'auditeur ne peut effectuer efficacement une mission d'audit sans au préalable rassembler le maximum d'information relatif à l'entreprise et au système à étudier. L'auditeur situe l'organisation par rapport à son environnement concurrentiel, ses politiques et ses stratégies générales, ses produits, ses clients et ses fournisseurs. En collaboration étroite avec la direction de l'organisation, il définit les termes de références et obtient des informations portant sur l'historique, les objets de l'organisation, l'organigramme, le système, le cadre juridique et institutionnel, les ressources financières, matérielles et humaines.

2.2.3 L'analyse des risques

L'analyse des risques est une étape très importante de la démarche d'audit de la sécurité. En effet, l'analyse des risques fait apparaître les menaces, attaques et autres vulnérabilités, ainsi que les mesures de sécurité correspondantes. Aussi, l'auditeur devra tenir compte à la fois de la possibilité qu'un événement se produise et de l'impact de cet événement. Ainsi donc pour chaque type de risque, l'auditeur se posera les questions sur la survenance de ce risque et sur les conséquences matérielles et financières de ce risque. Le tableau d'analyse, suivant, nous présente quelques risques informatiques.

Tableau 3 : Quelques risques informatiques

Insuffisances	Risques	Techniques d'audit pour identifier les risques
Absence de stratégie de sécurité écrite ; Absence de procédures écrites limitant l'accès physique	Destruction des actifs entraînant une rupture de la continuité des traitement ; transfert d'information à la concurrence ; chantage sur le contenu confidentiel d'un support informatique volé ; perte financière.	Visite des locaux ; Entretiens ; se faire transmettre le plan de sécurité et de sauvegarde ; observations des entrées/sorties à la salle informatique
Absence de procédures de sauvegarde ; Climatisation défaillante ; Absence de procédures écrites pour la reprise à froid quotidienne ; Manque de plan de sauvegarde	Destruction des actifs entraînant une rupture de la continuité des traitements.	Observations ; Entretiens ; Visites des locaux ; Prise de connaissance des procédures de sauvegarde.
Rapports tendus entre informaticiens et utilisateurs	Développement des programmes sans relation avec les besoins des utilisateurs ; Informations « sauvage » ; configuration mal adaptée aux besoins ; Insuffisance de contrôles programmés.	Entretiens avec les utilisateurs et les informaticiens ; Examen des PV des réunions du comité informatique et des correspondances entre les informaticiens et les utilisateurs.
Insuffisance dans la séparation des tâches	Malversations, atteinte à la confidentialité, détournement des ressources, fraudes.	Prise de connaissance des organigrammes et des fiches de fonction ; Procédures de gestion de personnel.
Insuffisances dans les procédures de gestion du personnel informatique	IDEM + incompétence et inefficacité	Prise de connaissance des procédures de gestion du personnel informatique.
Mauvaise procédure de développement	Non fiabilité des applications ; Insuffisance de contrôles programmés et de sécurité	Entretiens, observations, manuels de procédure sur la méthodologie de développement
Mauvaise procédure de mise en exploitation	Non exhaustivité des données transférées, pertes de données.	IDEM+ examen des procès verbaux de transfert.

Source : TALL Mamadou (2004), *Audit de la sécurité Informatique*

2.2.4 L'évaluation du contrôle interne

Le contrôle interne tient une place de plus en plus grande dans les préoccupations des autorités du secteur bancaire. La réglementation bancaire impose à tous les établissements de crédit de se doter d'un système de contrôle et d'une fonction de contrôle interne. Le contrôle interne dans le cadre de la sécurité du système d'information englobe les procédures, les chaînes de traitement de données et les applications. L'évaluation du contrôle interne débouche sur un éventaire des forces et des faiblesses de la sécurité du système d'information.

L'objectif du contrôle interne (ensemble des procédures, instructions, règles ou formalités et des contrôles) est d'assurer à l'établissement ou faciliter :

- La sauvegarde de son patrimoine
- L'exactitude et la fiabilité de l'information comptable
- L'efficacité de la mise en œuvre de sa stratégie
- L'adhésion du personnel à la politique définie par la Direction Générale

2.2.5 Les recommandations

A la suite de l'évaluation de l'analyse des risques et de l'évaluation du contrôle interne, l'auditeur est appelé à formuler des recommandations chaque fois qu'un risque important est détecté. Il doit prendre en compte les points suivants :

- vérifier les contraintes financières ;
- s'assurer que les mesures préconisées atténuent suffisamment les risques ;
- s'assurer que les solutions (techniques) préconisées sont appliquées.

2.2.6 Le rapport

Le rapport est un document qui conclut la mission d'audit. Il est confidentiel et destiné à la direction de l'entreprise. L'auditeur établit un pré rapport qui est un projet de rapport. Après réception des observations sur le projet de rapport, il rédige le rapport final (définitif). Son contenu varie selon l'organisation ou le type d'audit. Dans le cas d'un audit de la sécurité, les

éléments du rapport sont les suivants : le cadre de la mission, les objectifs, l'étendu et les limites de la mission, les principaux interlocuteurs, l'état des lieux (diagnostic, estimation des risques, évaluation du contrôle interne, forces et faiblesses), les recommandations (les solutions préconisées, l'évaluation économique et le plan de mise en œuvre), la méthode d'approche employée, les résultats des travaux (de l'étude ou de la méthode) et les contrôles.

2.2.7. Le suivi de l'Audit sécurité

Pour le suivi de l'audit sécurité, la CNCAS soucieuse de la sécurité de son SI a commandité un Audit sécurité du 18 décembre 2001 au 21 décembre2001 pour l'évaluation de son système. Cet audit fut réalisé par le cabinet d'expertise comptable et d'audit DELOITTE & TOUCHE TOHMATSU qui dans son rapport à la Direction générale a émis plusieurs recommandations susceptibles de palier aux lacunes et améliorer le niveau de sécurité physique et logique de la banque.

Notre travail consistera donc à évaluer les recommandations mises en œuvre, celles en cours de réalisation et celles qui n'ont pas été prises en compte. Les menaces et attaques ne restent pas sans changer, alors il importe de s'appesantir sur le suivi des recommandations ou « follow up » indispensable à la SSI.

2.3 LES METHODES ET OUTILS DE LA SECURITE

L'utilisation de méthodes et outils d'Audit Informatique dans le cadre de la méthodologie d'Audit Sécurité s'avèrent important. Aussi dans le cadre de notre étude nous nous limiterons aux méthodes recommandées en ce qui est de la Sécurité du Système d'Information (SSI), les plus récentes de nos jours (avec leurs mises à jour) : Marion, Méhari, le Cobit et nous citerons quelques autres outils automatisés.

2.3.1 La méthode MARION

La Méthode d'Analyse des Risques Informatiques en Organisation par Niveaux (MARION) est l'une des techniques permettant de mesurer le niveau de sécurité d'une entreprise. Cette

méthode a été élaborer et conçue par le CLUSIF (Club de la sécurité Informatique). A partir de questionnaires, cette méthode attribue à chaque facteur étudié une valeur variant entre 1 et 4 avec :

- 1 = mauvais ;
- 2 = médiocre ;
- 3 = assez bon ;
- 4 = bon.

L'objectif minimal à atteindre est la valeur 3 ; tout résultat inférieur à 2 est mauvais, est considéré comme un risque, doit être étudié rapidement et amélioré. Le niveau de sécurité est évalué suivant 27 indicateurs (facteurs) répartis en 6 grands thèmes :

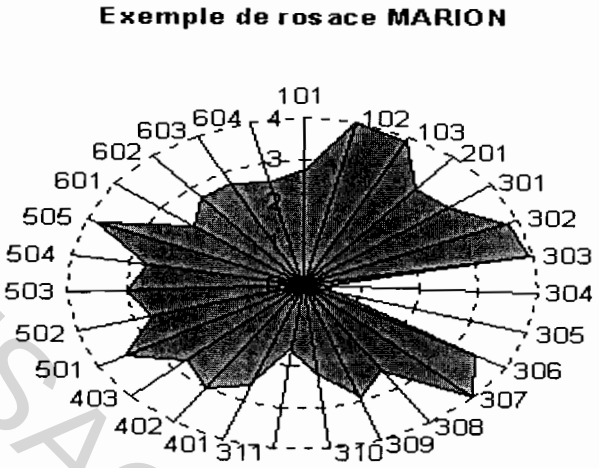
- La sécurité organisationnelle ;
- La sécurité physique ;
- La continuité ;
- L'organisation informatique ;
- La sécurité logique et d'exploitation ;
- La sécurité des applications.

Le déroulement de la méthode est composé de 4 phases :

- ✓ La phase de préparation : les objectifs de la sécurité sont définis ; le champ d'action est élaboré.
- ✓ La phase d'audit des vulnérabilités : phase du déroulement des questionnaires de la méthode et du recensement des contraintes propres à l'organisation. Le résultat des questionnaires permet d'obtenir la « rosace » propre à l'entreprise ou d'autres diagrammes tels que le diagramme différentiel ou les diagrammes relatifs aux risques.

La figure 6 présente un exemple de rosace MARION d'une entreprise.

Figure 6 :



Sources : www.clusif.asso.fr (2004).

- ✓ La phase d'analyse des risques : au cours de cette phase, les résultats sont exploitées et une répartition des risques en Risques Majeurs (RM) et Risques Simples (RS) est effectuée. Le système d'information est découpé en groupes fonctionnels spécifiques et hiérarchisé selon l'impact de la potentialité de risques. Selon le CLUSIF, la méthode identifie 17 types de menaces :

  1. accidents physiques ;
  2. malveillance physique (panne du SI) ;
  3. carence de personnel ;
  4. carence des prestataires ;
  5. interruption de fonctionnement du réseau ;
  6. erreur de saisie ;
  7. erreur de transmission ;
  8. erreur d'exploitation ;
  9. erreur de conception – développement ;

10. vice caché d'un progiciel ;
11. détournement de fonds ;
12. détournement de biens ;
13. copie illicite de logiciels ;
14. indiscrétion ;
15. détournement d'information ;
16. sabotage immatériel ;
17. attaque logique du réseau.

- ✓ La phase du plan d'action : elle consiste à analyser les moyens à mettre en œuvre pour atteindre la note « 3 » qui constitue l'objectif de sécurité de la méthode. Les tâches sont ordonnancées, on indique le degré d'amélioration à apporter et on détermine un chiffrage du coût de la mise en conformité.

La méthode MARION identifie rapidement les risques susceptibles d'amélioration, offre un moyen de comparaison de la sécurité du système d'information d'une entreprise par rapport à d'autres entreprises. L'une des limites de cette méthode est qu'elle pèche dans la mise en œuvre des recommandations.

2.3.2 La méthode MEHARI

La méthode MEHARI (MEthode Harmonisée d'Analyse de RIsques) développée par la commission METHODES du CLUSIF permet par une analyse rigoureuse et une évaluation quantitative des facteurs de risques propres à chaque situation, de concilier les objectifs stratégiques et les nouveaux modes de fonctionnement de l'entreprise avec une politique de maintien des risques à un niveau convenu. L'analyse des vulnérabilités fait partie de la méthode en soutien du management des risques.

Pour le CLUSIF (2004), la méthode MEHARI conjugue la rigueur d'une analyse des risques liés formellement au niveau de vulnérabilité du système d'information, à l'adaptabilité de la

gravité des risques étudiés. En effet, la présence (ou l'absence) de mesures de sécurité va réduire (ou non), soit la potentialité de survenance d'un sinistre, soit son impact. L'interaction de ces types de mesures concoure à réduire la gravité du risque jusqu'au niveau choisi.

La méthode MEHARI diagnostic 160 services de sécurités répartis en 12 domaines étudiés :

1. organisation de la sécurité ;
2. sécurité des sites et bâtiments ;
3. sécurité des locaux ;
4. réseau étendu (inter site) ;
5. réseau local ;
6. exploitation des réseaux ;
7. sécurité des systèmes et leur architecture ;
8. production informatique ;
9. sécurité applicative ;
10. sécurité dans les développements ;
11. protection et environnement de travail ;
12. juridique et réglementaire.

Le déroulement de la méthode se fait en trois (3) phases

- ✓ Phase 1 : phase d'établissement d'un plan stratégique de sécurité global.
- ✓ Phase 2 : phase d'établissement de plans opérationnels de sécurité réalisés par les différentes unités de l'entreprise.
- ✓ Phase 3 : Phase de consolidation des plans opérationnels globaux.

La méthode MEHARI spécifique à l'analyse des risques, est en évolution continue grâce aux professionnels du CLUSIF, elle est supportée par des logiciels (comme par exemple le logiciel RISICARE), est compatible avec les normes notamment ISO/IEC 17799 : 2000 et ISO/IEC : 13335. En outre MEHARI permet d'alimenter une politique de sécurité et des tableaux de bord sécurité. La nouvelle version en 2004 de la méthode MEHARI est MEHARI V3 (version 3), elle comprend selon :

- ✓ Un Classeur Excel « Base de connaissance ».
- ✓ Un Classeur Excel « Base des scénarios ».
- ✓ Un Manuel de référence des services de sécurité.

2.3.3 Le COBIT

Le COBIT ou Gouvernance, Contrôle et Audit de l'Information et des Technologies Associées, développé par l'ISACA et repris en version française par l'AFAI, aide à faire le lien entre les risques de gestion, les besoins en contrôles et les problèmes techniques.

Le COBIT est un modèle de référence en matière d'Audit et de maîtrise des Systèmes d'Information (SI). Il aide les dirigeants à comprendre et à gérer les risques liés à l'informatique. Il fait le lien entre les processus de gestion, les questions techniques, les besoins de contrôle et les risques.

Selon AFAI (Avril 2003), le COBIT est structuré en quatre grands domaines permettant de couvrir l'ensemble des pans métiers que revêt un Système d'Information :

- ✓ La Planification et l'Organisation (PO) ;
- ✓ L'Acquisition et la Mise en Place (AMP) ;
- ✓ La Distribution et le Support (DS) ;
- ✓ La Surveillance (S).

Le tableau suivant nous présente les 34 objectifs de contrôles généraux dictés par les quatre (4) grands domaines du COBIT.

Tableau 4 : Domaines et objectifs du COBIT

PLANIFICATION ET ORGANISATION	DISTRIBUTION ET SUPPORT
PO 1 : Définir un plan informatique stratégique	**DS 1 :** Définir et gérer des niveaux de services
PO 2 : Définir l'architecture de l'information	**DS 2 :** Gérer des services tiers
PO 3 : Déterminer l'orientation technologique	**DS 3 :** Gérer la performance et la capacité
PO 4 : Définir l'organisation et les relations de travail	**DS 4 :** Assurer un service continu
PO 5 : Gérer l'investissement informatique	**DS 5 :** Assurer la sécurité des systèmes
PO 6 : Faire connaître les buts et orientations du management	**DS 6 :** Identifier et imputer les coûts
PO 7 : Gérer les ressources humaines	**DS 7 :** Instruire et former les utilisateurs
PO 8 : Se conformer aux exigences externes	**DS 8 :** Assister et conseiller les clients
PO 9 : Évaluer les risques	**DS 9 :** Gérer la configuration
PO 10 : Gérer les projets	**DS 10 :** Gérer les problèmes et les incidents
PO 11 : Gérer la qualité	**DS 11 :** Gérer les données
	DS 12 : Gérer les installations
ACQUISITION ET MISE EN PLACE	**DS 13 :** Gérer l'exploitation
	SURVEILLANCE
AMP 1 : Trouver des solutions informatiques	
AMP 2 : Acquérir des applications et en assurer la maintenance	**S 1 :** Surveiller les processus
AMP 3 : Acquérir une infrastructure technologique et en assurer la maintenance	**S 2 :** Évaluer l'adéquation du contrôle interne
AMP 4 : Développer les procédures et en assurer la maintenance	**S 3 :** Acquérir une assurance indépendante
AMP 5 : Installer des systèmes et les valider	**S 4 :** Disposer d'un audit indépendant
AMP 6 : Gérer les changements	

Source : www.afai.asso.fr

Pour mettre les technologies de l'information sous contrôle et faire en sorte qu'elles soient alignées avec l'activité en lui fournissant les informations dont elle a besoin, le *Guide de Management* propose différents outils de gestion : les Facteurs Clés de Succès (FCS), le Modèle de Maturité (MM), les Indicateurs Clés de Performance (ICP), les Indicateurs Clés d'Objectifs (ICO).

Il existe un *Cadre de Référence* de COBIT, qui permet l'application de normes et de principes internationaux, ainsi que la recherche des meilleures pratiques pour conduire à la rédaction des Objectifs de Contrôle. Le *Guide d'Audit* de COBIT a pour objet de vérifier si les Objectifs de Contrôle ont été mis en œuvre de façon adéquate. Le management a besoin d'un outil comme le *Cadre de Référence* du COBIT pour s'auto évaluer, et faire des choix sur la

mise en place des contrôles, l'amélioration de son information et des technologies utilisées. C'est le but principal du *Guide de Management,* rédigé grâce à l'aide d'experts du monde entier en gouvernance des Technologies de l'Information (TI), gestion des performances, sécurité et contrôle de l'information. Il propose un ensemble d'outils destinés à aider le management à répondre à la question suivante :"*Quel est le bon niveau de contrôle sur mon informatique de manière à ce qu'elle aide mon entreprise à réaliser ses objectifs ?"*

2.3.4 Autres outils informatisés

Plusieurs organismes, associations, instituts ou clubs informatiques développent des outils notamment des projets, des logiciels et progiciels pour la sécurité du SI. Nous pouvons citer par exemple les logiciels ACL et le projet Nessus.

A. ACL

ACL[5] fournit une gamme complète de logiciels Business Assurance Analytics qui s'adressent aussi bien à des utilisateurs finals et aux équipes des différents services qu'aux solutions d'entreprise. Ces logiciels ont pour fonction de surveiller les contrôles des processus de gestion principaux.

Selon ACL (2005), les solutions logicielles ACL effectuent des tests et des contrôles complets et indépendants des données transactionnelles, permettant ainsi aux organisations de valider l'efficacité des contrôles en interne afin que leurs objectifs commerciaux et législatifs soient atteints. La flexibilité et l'évolutivité de la technologie ACL permettent aux organisations d'envisager plusieurs approches d'analyse de données : l'analyse de données ad hoc, la vérification régulière des contrôles dans le cadre d'une planification de plusieurs audits, des contrôles continus automatiques pour surveiller les applications impliquées dans les opérations quotidiennes des processus de gestion stratégiques.

[5] ACL, fournisseur de solutions d'accès aux données, d'analyse de données et de génération d'états intégrée, est leader en matière de conformité des contrôles, de détection des fraudes et de technologie analytique depuis 1987. Plus de 70 % des 500 entreprises répertoriées dans le magazine Fortune, la moitié des 500 plus grosses entreprises du monde, les quatre plus gros cabinets d'expertise comptable et des centaines d'organismes publics font appel à ACL afin de résoudre leurs problèmes commerciaux et de conformité.

La gamme des produits Business Assurance Analytics d'ACL permettent aux organisations de :

- Identifier les défaillances des contrôles de façon proactive et de minimiser leur impact financier ;
- Améliorer les méthodes de test des contrôles et de création de rapports d'exception ;
- Réduire les dépenses en matière de conformité à l'aide de contrôles financiers et de gestion plus efficaces ;
- Accroître la transparence des processus de gestion de manière continue ;
- Créer une base solide pour obtenir des états financiers fiables ;
- Obtenir un suivi concret de vos analyses à l'aide d'une piste de vérification complète.

B. Nessus

Nessus est un projet qui permet l'analyse des vulnérabilités du système d'information. Il est de nos jours le plus utilisé avec plus de 75.000 organisations à travers le monde. Et plusieurs grandes sociétés ont survécues par le biais de Nessus dans le cadre de l'Audit Sécurité des développements et des applications de leurs systèmes.

Nessus a été fondé et développé en 1998 par RENAUD[6] pour assurer la sécurité de la connexion Internet par :

- ✓ La vulnérabilité du SI ;
- ✓ La sécurité du contrôle ;
- ✓ Bonne exécution des techniques de communication.

Il importe de noter que de nos jours plusieurs autres projets, logiciels et progiciels existent en nombres considérables.

[6] Renaud est impliqué dans le monde de la sécurité informatique depuis plus de quatre ans. Il est le developpeur d'outils distribués sous license GPL tels que nstreams (outil facilitant le déployement d'un firewall), filterrules (outil déterminant la politique appliquée à un firewall) et hlfl (language de configuration de filtres de paquets). Il est le fondateur et actuel leader du projet Nessus, permettant d'évaluer aussi exhaustivement que possible la sécurité d'une machine ou d'un réseau entier, outil faisant aujourd'hui matière de référence dans le domaine. Nessus a gagné le *Well-Connected Award 2001* de Network Computing le 7 mai dernier à Las Vegas.

CONCLUSION

La seconde partie théorique nous instruit sur l'Audit de la sécurité du système d'information.

A travers les missions d'audit de la sécurité, l'auditeur informaticien étudie les objectifs recherchés : l'organisation générale de la sécurité, l'analyse générale des risques, l'évaluation de la sécurité physique et logique ; aussi il effectue l'examen des dispositifs de protection contre les risques et attaques.

Pour bien mener sa mission, l'auditeur informaticien suit une démarche enrôlée autour d'un programme d'action de cheminement logique bien défini. Cette démarche part de la définition des objectifs et des moyens pour s'achever sur l'établissement d'un rapport d'audit, après la prise de connaissance, l'analyse des risques, l'évaluation du contrôle interne et des recommandations effectuées. En outre un suivi de ses recommandations peut être fait à travers le « follow up ».

L'apport des méthodes et d'outils modernes, tels que MARION, MEHARI, le COBIT et autres outils informatisés est d'une importance capitale pour la collecte des données et une meilleure certification du degré d'assurance de sécurité acceptable. Nous utiliserons dans le cadre pratique de notre étude la méthode d'analyse des risques informatiques orientés par niveaux (MARION).

CHAPITRE 3 : LA MÉTHODOLOGIE DE RECHERCHE

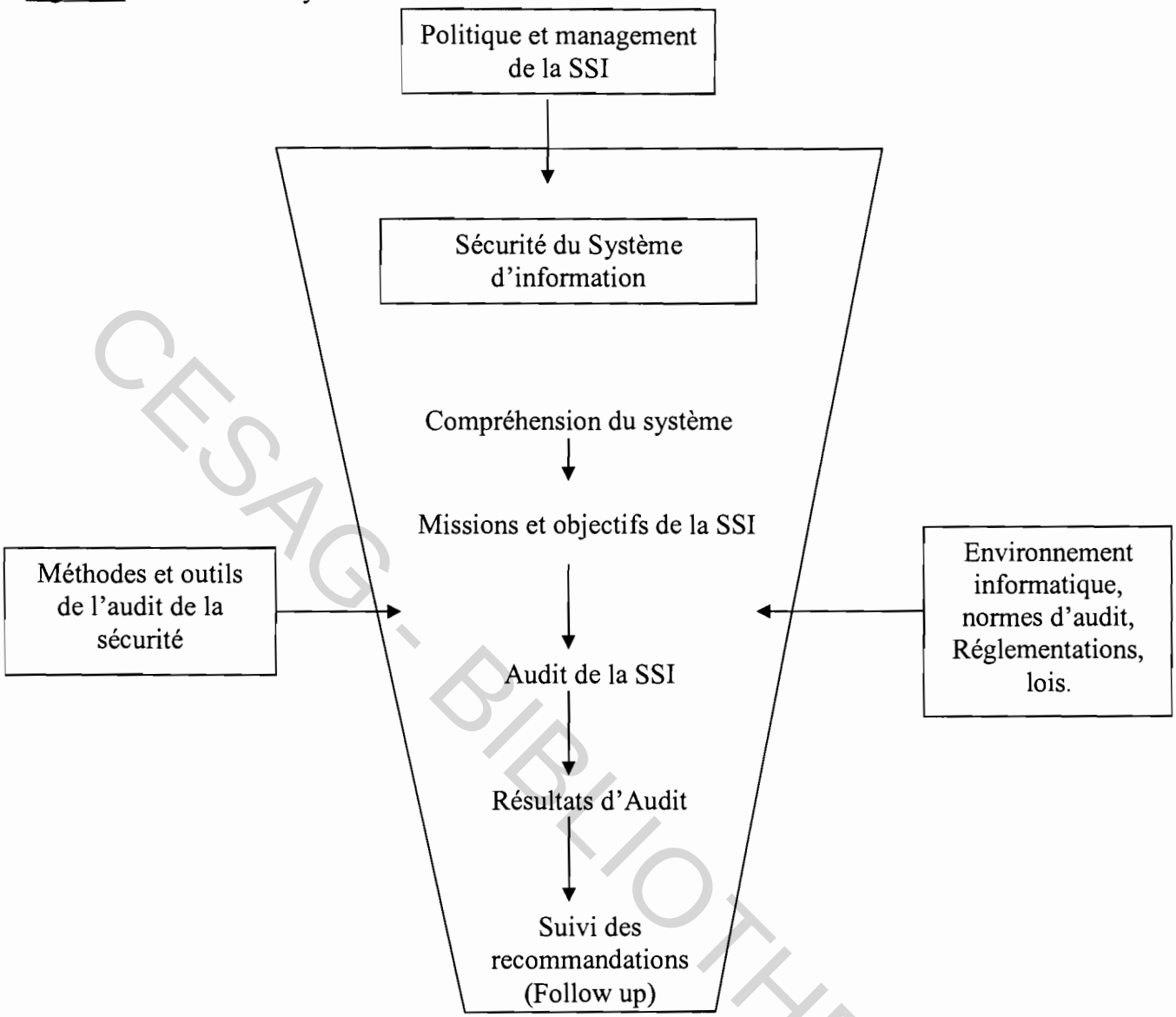
INTRODUCTION

La revue de littérature nous a permis de dresser le cadre théorique de notre étude. Ce cadre théorique servira de levier pour l'élaboration de la méthodologie à suivre pour atteindre les objectifs de l'étude. Il sera question pour nous d'élaborer le modèle d'analyse. Nous présenterons la population de l'étude, les outils de collecte des données et les méthodes d'analyse des données.

3.1 LE MODELE D'ANALYSE

L'analyse de la sécurité du système d'information nous a conduit à présenter une revue de littérature qui se résume de la manière suivante :

Figure 7 : Modèle d'analyse



Source : Nous-mêmes

La définition opérationnelle des variables dans le cadre de notre travail est faite de cinq dimensions de la variable dépendante et de trois variables indépendantes. Pour les dimensions de la variable dépendante nous avons :

- *la compréhension du système* : pour avoir les informations nécessaires à la maîtrise du système ;
- *Les missions et objectifs de la Sécurité du Système d'Information* : pour définir notre plan de travail ;
- *L'audit de la Sécurité du Système d'Information* : pour établir les états des lieux du système en fonctions des objectifs ;

- *Les résultats de l'audit* : pour affiner notre opinion sur la maîtrise de la sécurité du système de l'information au sein de l'entreprise ;
- *Le suivi des recommandations (follow up)* : pour s'assurer de la prise en compte des recommandations de l'audit et des mises à jour du système de sécurité.

Les variables indépendantes sont :

- *L'environnement informatique, les normes d'audit, les réglementations et lois* : qui affectent l'organisation et le fonctionnement de la sécurité du système d'information ;
- *Les méthodes et outils de l'audit de la sécurité* : qui permettent l'analyse des risques informatiques ;
- *Les politiques et managements de la SSI* : qui servent à définir les mesures de prévention et de protection à mettre en œuvre pour la pérennité de l'entreprise.

3.2 LA POPULATION DE L'ETUDE ET LES OUTILS D'ANALYSE

La population de notre étude est constituée du personnel des différentes directions de l'agence principale de la CNCAS de Dakar (siège social). Nous ferons des entretiens avec les responsables de l'entreprise et nous adresserons des questionnaires aux utilisateurs de l'outil informatique au sein de chaque direction. Le tableau 5 présente l'échantillon de l'étude.

Tableau 5 : Echantillon de l'étude

Libellé	**Effectif**	**Effectif total**
Direction Générale	1	7
Direction des Finances et de l'Information	10	19
Direction de l'Audit Général	6	10
Direction des Ressources Humaines et Logistique	2	5
Direction de la production	2	10
Délégué au crédit et au réseau	5	15
Total	**26**	**66**

Source : Nous-mêmes

Pour ce qui est des outils à utiliser, nous élaborerons deux types de questionnaires :

- ✓ un questionnaire de contrôle interne adressé au personnel des services informatique ;
- ✓ un questionnaire d'évaluation adressé aux utilisateurs des directions de notre échantillon.

En outre, un guide d'entretien servira pour les entretiens avec les responsables de l'entreprise.

La recherche documentaire consiste en l'exploitation des documents nécessaires à la connaissance et à la bonne compréhension du système d'information. Il s'agit du manuel de procédures, du business plan, des budgets prévisionnels, des notes de service, du rapport d'audit sécurité précédent, des rapports sur le contrôle et les activités d'audit, des rapports d'activités, des mémoires, etc.

L'observation physique concernera la visite des locaux au siège afin d'établir les états des lieux sur le dispositif de sécurité. Par la suite, des tests d'existence et de conformité nous permettront d'étayer notre opinion. Ces tests seront utilisés pour vérifier l'existence des procédures informatiques et en général du manuel des procédures, des mesures de sécurité, des méthodes et des outils d'audit. Enfin, l'inventaire physique nous permettra d'inventorier les matériels du système d'information.

3.3 LES METHODES D'ANALYSE DES DONNEES

Les données seront analysées par comparaison au modèle d'analyse qui constitue le référentiel dans le cadre de notre étude. Le cadre théorique nous a permis de définir les différentes phases d'audit de la sécurité et de collecte des données. Cette analyse nous permettra de faire le diagnostic physique et logique du SI de l'entreprise, de faire ressortir les forces et faiblesses ainsi que les risques potentiels et matériels. L'analyse de ces risques nous permettra de proposer des améliorations. Par la suite un suivi de l'audit des recommandations du dernier audit sécurité (2001) est envisagé.

CONCLUSION

L'audit de la sécurité du SI est d'une importance fondamentale pour toute organisation notamment la banque. La revue de littérature que nous avons faite, nous a permis de montrer cette importance au sein d'une entreprise. En effet, elle nous informe sur la notion de système d'information, du mangement de la SSI, l'apport des normes et lois de la sécurité informatique. Par ailleurs, l'audit de la sécurité à travers ses différentes phases nous conduit à une opinion sur l'état de la sécurité de l'organisation. Le modèle d'analyse tire sa source de cette revue, et nous avons définis des variables dépendantes et indépendantes de notre système d'analyse. La méthode de collecte des données et l'analyse des donnée nous permettrons d'apporter des amélioration au système et son suivi.

CONCLUSION DE LA PREMIÈRE PARTIE

L'environnement, la technologie, les risques et les fraudes informatiques ne restent pas sans changer. Il convient donc, en permanence, non seulement de surveiller les risques présents et d'ajuster les parades, mais aussi d'agir en prévision des risques nouveaux. L'analyse globale des risques doit être renouvelée périodiquement et un effort de sensibilisation au plus haut niveau de la hiérarchie est indispensable pour la prise de conscience en matière de sécurité.

La sécurité et le contrôle du système ou des systèmes d'information nécessitent de :

- ✓ Contrôler les coûts informatique et de télécommunication ;
- ✓ Vérifier que les règles en matière de SSI sont correctement appliquées et que la sécurité des systèmes d'information et du réseau est assurée ;
- ✓ Détecter toute anomalie de sécurité ou abus d'utilisation ;
- ✓ Etre à même de mener les enquêtes et contrôles appropriés.

La mise en œuvre d'un management de la sécurité, par la Direction Générale, est plus que nécessaire pour la survie de l'entreprise. Cette mise en œuvre de la politique de sécurité, des stratégies doit, cependant, respecter les normes et lois internationales.

Pour l'auditeur de la sécurité, l'utilisation de l'outil informatique ne change en rien les objectifs de sa mission à savoir la sincérité et l'intégrité des informations. Et pour le bon

déroulement de sa mission, une démarche logique et cohérente s'impose de même que le choix de méthodes de collectes de données et d'outils d'audit informatiques recommandées comme MARION, MEHARI, Le COBIT et les autres outils informatisés.

En réalité, la sécurité du système d'information (SSI) est une question d'esprit, de culture d'entreprise et de comportement : l'essentiel est de mettre en place une organisation adéquate, possédant correspondants et relais à tous les niveaux nécessaires, disposant de moyens de sensibilisation, de formation et de documentation. Le cas de la SSI de la CNCAS se révèle, dans le cadre de notre étude, comme une opportunité aussi bien pour la Direction Générale que pour le personnel.

A présent nous abordons la deuxième partie de notre travail pour tester les variables retenues dans le modèle d'analyse. Tenant compte de la limitation du domaine de notre étude, nous nous intéresserons d'avantage à la Sous Direction Informatique et Organisation.

DEUXIEME PARTIE :

CADRE PRATIQUE DE LA SECURITE DU SYSTEME D'INFORMATION A LA CAISSE NATIONALE DU CREDIT AGRICOLE DU SENEGAL

INTRODUCTION

Dans le cadre de notre étude sur *« la sécurité du système d'information »* nous avons effectué notre stage de fin de cycle à la Caisse National de Crédit Agricole du Sénégal (CNCAS). La CNCAS est une structure bancaire qui s'appuie sur un système d'information bancaire basé sur le progiciel DELTA-BANK pour le traitement de ses opérations. Elle procède à des audits réguliers pour remédier aux dysfonctionnements et faillites, comme le recommande la commission bancaire.

Les objectifs de l'audit de la sécurité du système d'information de la CNCAS sont les suivants :

- ✓ Etablir un état des lieux vis-à-vis des risques ;
- ✓ Elaborer des scénarii de réduction des risques ;
- ✓ Déterminer les orientations pour le renforcement de la politique de sécurité ;
- ✓ Mettre au point un programme de mise en œuvre de cette politique.

Les principaux sujets que nous abordons dans cette partie sont :

- La présentation de la CNCAS
- L'Audit de la sécurité à la CNCAS
- La synthèse et les perspectives de mise en œuvre des recommandations de l'audit.

CHAPITRE 1 : PRESENTATION DE LA CNCAS

INTRODUCTION

La Caisse Nationale de Crédit Agricole du Sénégal (CNCAS) dispose d'un système informatique moderne pour la gestion de l'information comptable et financière.

1.1 LA CAISSE NATIONALE DE CREDIT AGRICOLE DU SENEGAL (CNCAS)

Après une présentation générale de la banque nous dressons les caractéristiques de la fonction informatique en place.

1.1.1. Présentation générale de la banque

A. Présentation

Le Crédit Agricole (CA) ou Caisse Nationale de Crédit Agricole du Sénégal (CNCAS) est une société anonyme crée en Avril 1984. La banque a un capital de deux milliards trois cent millions de francs CFA (2 300 000 000 FCFA) décomposé en deux cent trente mille (230 000) actions de dix mille francs CFA (10 000 FCFA). Les actionnaires sont répartis de la manière suivante :

- L'Etat du Sénégal avec 24% ;
- L'Agence Française de Développement (AFD) avec 10% ;
- La Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO) avec 15% ;
- Les autres banques et établissements de la place avec environ 10% ;
- La Caisse Nationale de Crédit Agricole (CNCA) Paris avec 10% ;
- La Société Nationale de Recouvrement (SNR) avec 17,51% ;
- Le reste du capital est détenu par d'autres petits actionnaires (personnes physiques et morales) soit environ 13,49%.

Le siège social de la banque est situé à la place de l'indépendance : BP 3890 Dakar Sénégal ; Téléphone : (221) 839 36 36 ; Fax : (221) 821 26 26 ; Site Web : www.cncas.sn . Il importe de noter que dans un souci de dynamisme et de croissance, dans l'optique d'être une « banque universelle », la banque a acquis un nouvel immeuble pour le transfert du siège social.

La CNCAS est constitué de plusieurs réseaux comprenant les régions et repartis comme suite :

- Le réseau ouest : Dakar, Thiès, Mbour ;
- Le réseau nord : Saint Louis, Matam, Richard-Toll, Ndioum, Louga
- Le réseau sud : Ziguinchor, Sédhiou, Kolda ;
- Le réseau centre ouest : Kaolack, Diourbel, Tambacounda.

La CNCAS compte augmenter son nombre d'agence de 14 agences à 16 agences avec la création de l'agence de Fatick et celle de Dahra avant la fin de l'an 2007.

B. Missions et objectifs

La CNCAS a pour objectif principal de promouvoir le développement du pays par le biais de financement de projets dans le domaine Agricole (agriculture, élevage, pêche). La banque est le principal bailleur de fonds Sénégalais du monde rural. Elle participe au financement de la production et la commercialisation des produits agricoles à travers :

- les campagnes agricoles ;
- les grandes entreprises de collecte et de transformation ;
- les PME-PMI agricoles et de transformation ;
- l'artisanat urbain et rural ;
- l'aménagement rural (publics et privés).

En outre, la banque a d'autres vocations : la distribution du crédit au monde rural, la collecte de l'épargne rurale et les opérations classiques de banque (épargne bancaire et services financiers aux particuliers, consultation de comptes par téléphone et/ou Internet, etc.).

C. Les activités

Le rapport annuel de la commission bancaire 2002 de l'UEMOA indique que la CNCAS se positionne à la 7ème place sur les 11 unités que compte le secteur bancaire Sénégalais, avec 6,97% par rapport au résultat de l'ensemble des banques en termes du total de bilan.

Comme toute banque commerciale, la CNCAS mène deux activités principales à savoir la distribution de crédit et la collecte de l'épargne.

Pour ce qui est de la distribution de crédit, la banque offre les crédits suivants :

- Le crédit de campagne : pour financer la commercialisation des grands produits agricoles (Arachide, coton, riz) ;
- Le crédit à court terme : pour financer les intrants du monde rural (gasoil pour les motopompes, les semences et engrais, les achats de bêtes, les fonds de roulement) ;
- Le crédit à moyen et long terme : pour financer les équipements des agriculteurs, pêcheurs et éleveurs en matériels.

Quant à la collecte de l'épargne, la CNCAS y participe à travers l'ouverture de comptes bancaires. La banque offre :

- Des comptes à vue pour les dépôts à vue (DAV) ;
- Des comptes à termes pour les dépôts à terme (DAT) ;
- Des livrets d'épargne et de crédit.

La banque permet à ses clients de gérer leurs comptes en leur délivrant des carnets de chèques, en mettant à leur disposition des services de gestion des comptes par téléphones (AGRICALL) et par Internet avec la création d'un site web : www.cncas.sn permettant d'effectuer toute opération licite sur les comptes. En outre, la banque place auprès de sa clientèle des émissions d'emprunts des collectivités publiques, des organismes ou sociétés privés. La banque effectue, également, des opérations de ventes et d'achats de traveller's chèques Américain Express au niveau des guichets de Dakar, Mbour, Saint Louis et

Ziguinchor. Lancé depuis le 14 Novembre 2001, le produit *Moneygram*, transfert rapide d'argent, s'est bien développé sur tout le réseau.

La CNCAS entretient d'étroites relations avec des institutions de micro finances, des ONG et des projets tels que :

- Le Projet National de Lutte contre la Pauvreté (PNLP)
- Le Projet KASSACK Nord (PKN)
- Le Projet d'Appui à la Pêche et à l'Elévage (PAPEL)
- Le Projet d'Organisation et de Gestion Villageoises (POGV)
- L'ONG AFRICARE
- L'union des mutuelles (signatures de convention).

D. L'organisation de la CNCAS

Le personnel de la CNCAS se compose de 173 personnes dont 73% d'hommes et 27% de femmes. Ce personnel se réparti de la manière suivante :

- 1 hors cadre
- 42 cadres
- 101 gradés
- 29 employés.

La Sous Direction Informatique et Organisation ne représente que 4% des ressources humaines de la banque. Ce ratio est faible pour le milieu bancaire dont la norme est le double (8%).

La banque dispose au sommet d'un Conseil d'Administration mené par un président du Conseil d'Administration. Elle est dirigée par un Directeur Général assisté de quatre (4) conseillers techniques :

- Un attaché de direction chargée des études et du développement
- Un directeur de l'audit général
- Un sous directeur de la cellule recouvrement et contentieux

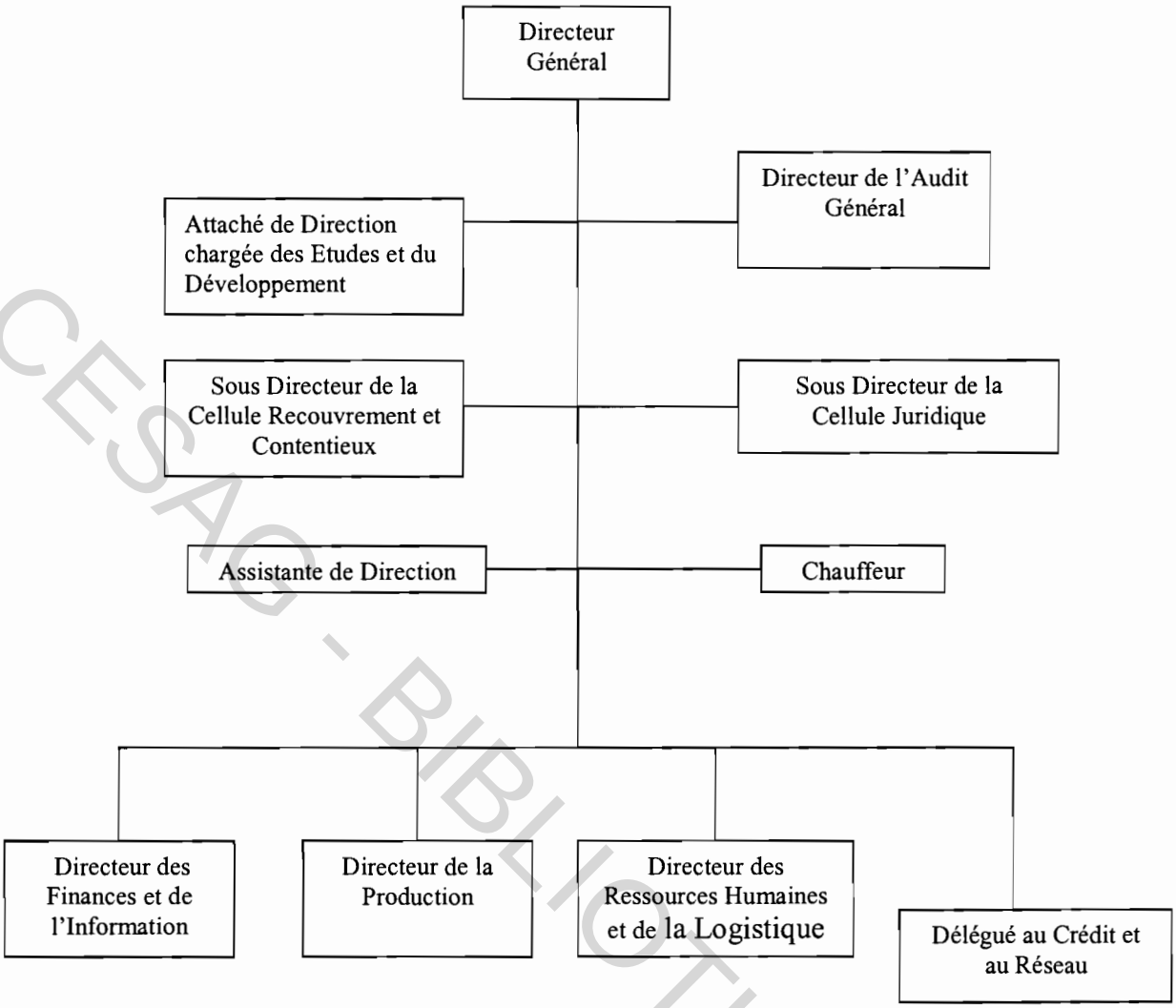
- Un sous directeur de la cellule juridique.

Le Directeur Générale est à la tête d'une équipe de trois directeurs et d'un délégué :

- Le directeur des finances et de l'information
- Le directeur de la production
- Le directeur des ressources humaines et de la logistique
- Le délégué au crédit et au réseau.

La figure 8 présente la structure de la Direction Générale.

Figure 8 : Organigramme de la Direction Générale

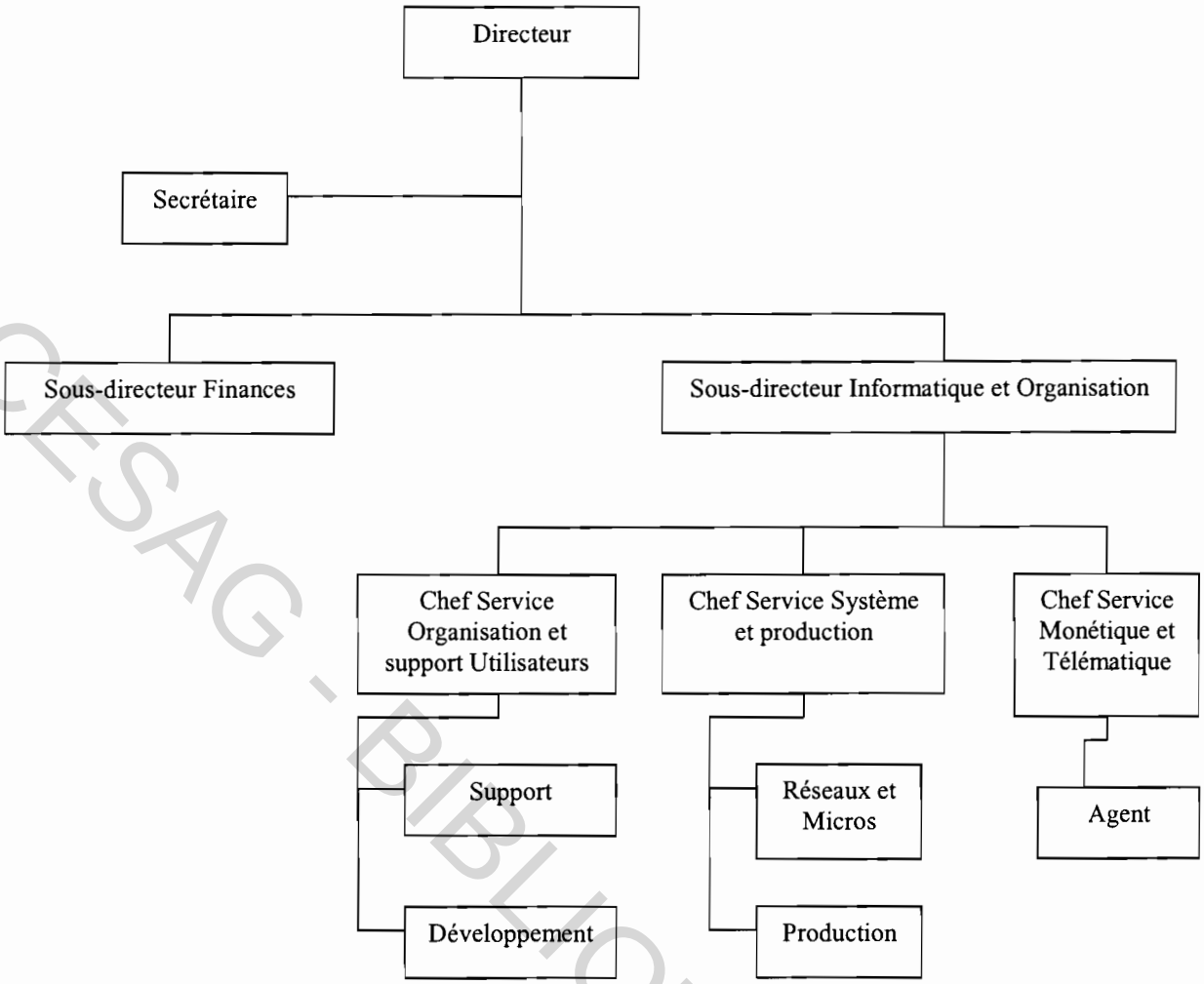


Source : CNCAS.

1.1.2. Présentation de la fonction informatique

La Direction des Finances et de l'Information de la CNCAS est composée d'une sous direction des finances et d'une sous direction de l'informatique et de l'organisation. La fonction informatique est organisée en trois services. La figure 9 présente l'organisation de la Sous Direction Informatique et Organisation.

Figure 9 : Organigramme de la Sous Direction de l'Informatique et de l'Organisation.



Source : CNCAS

La Sous direction Informatique et Organisation a pour mission principale de doter la banque d'outil et de traitement de services en informatique modernes pour le bon fonctionnement de ses activités de banque moderne et universelle. Aussi les différentes tâches assignées à ses services sont :

- *Le service organisation et support utilisateurs* : assure le traitement des travaux informatiques, administre les programmation, effectue les mises à jour, développe les application, les documente, rédige les guide utilisateurs, assiste les utilisateurs, et gère les mots de passe.

- *Le service systèmes et production* : administre la sécurité physique et logique, les serveurs, la base de données, les maintenances, conçoit les applications, effectue les sauvegardes, transfères les données et suit les contrats de maintenances.
- *Le service monétique et télématique* : assure la gestion des moyens de paiements électronique (cartes électroniques) et des services de la banque à distance par le canal du site web ou par le téléphone (Agricall)[7].

1.2. LE SYSTÈME INFORMATIQUE DE LA CNCAS

La CNCAS s'est doté d'un système informatique pour le traitement de ses activités bancaires. La Direction et les responsables informatiques doivent définir la politique de même que les stratégies informatiques.

1.2.1 Politiques et stratégies informatiques

Les objectifs stratégiques du Conseil d'Administration et de la Direction Générale sont de développer la CNCAS pour qu'elle soit la banque leader dans l'accompagnement du développement des régions du Sénégal. L'atteinte de ses objectifs stratégiques passe par une constante amélioration de son système d'information. Ainsi la CNCAS a commandité un audit de la sécurité du système d'information en Décembre 2001-Janvier 2002 afin d'améliorer sa sécurité. En outre, la CNCAS améliore son SI par l'achat de machines plus performantes, une réorganisation du service informatique avec un léger accroissement de l'effectif, un turn over plus adapté et une motivation salariale.

1.2.2. Environnement informatique

Notre revue de l'environnement informatique concerne l'architecture matérielle et logique de la CNCAS.

[7] Agricall : serveur vocal, permet de consultez en toute liberté son compte avec et de s'informer des derniers mouvements en ligne, sans vous déplacer.

A. Architecture matérielle

L'architecture matérielle de la CNCAS se compose de :

1. Postes de travail utilisateurs

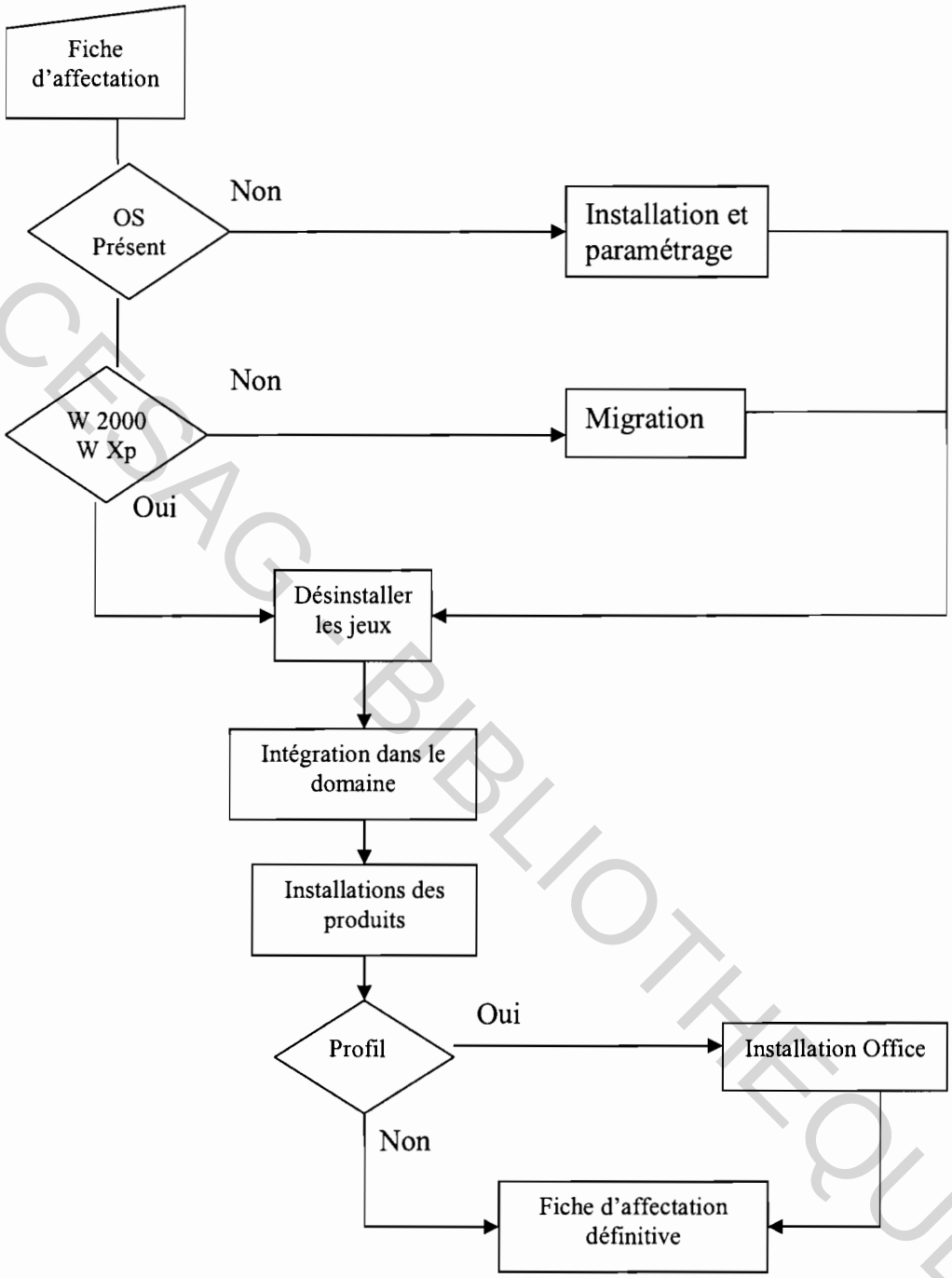
- ✓ Au siège de la CNCAS : deux (2) serveurs IBM RS/6000 (AIX), 100 postes utilisateurs sous Windows 2000Pro/XP Pro (dont un micro chèque et 56 micros DELTA-BANK) ;
- ✓ Dans les agences : 101 postes utilisateurs sous Windows 2000 Pro/XP Pro (dont 9 micro chèques et 61 micro DELTA-BANK).

Les postes de travail maintiennent une organisation homogène des machines de sorte à en faciliter la maintenance logicielle et à gérer au mieux les évolutions futures. Les produits installés sur les postes de travail (en réseau) sont :

- ➢ Le logiciel 4js (interface avec le logiciel bancaire DELTA-BANK) ;
- ➢ La gestion de l'inventaire;
- ➢ La télédistribution logicielle;
- ➢ La prise en main à distance des ordinateurs;
- ➢ Le logiciel antivirus.

La Figure 10 présente le processus de déploiement des postes de travail à la CNCAS.

Figure 10 : Processus de déploiement des postes de travail à la CNCAS



Source : CNCAS.

2. Les serveurs

Nous avons à la CNCAS deux typologies de serveurs :

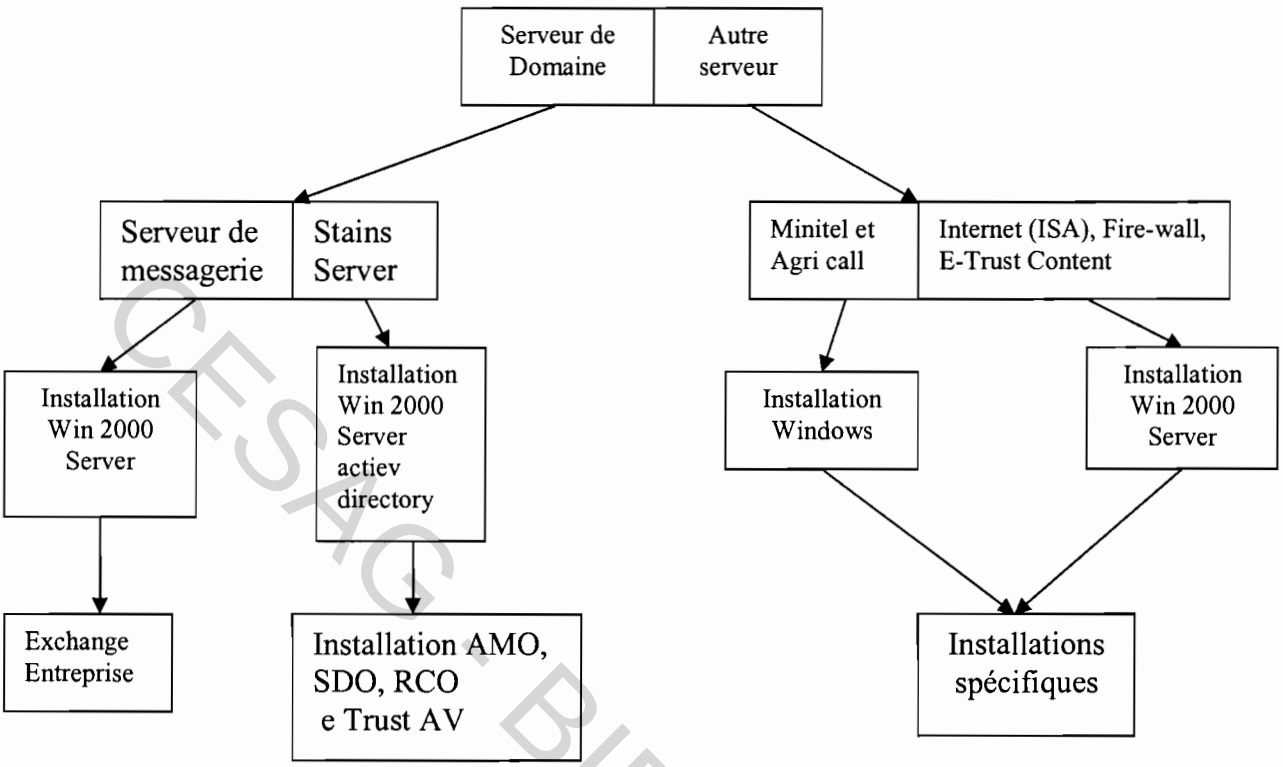
- ✓ Les serveurs de domaines : leur rôle principal est de gérer les accès des utilisateurs et d'assurer également des tâches secondaires comme la protection contre les accès externes provenant d'Internet. Ils canalisent et contrôlent les accès des utilisateurs vers Internet et gèrent le serveur Web de la banque. Nous pouvons citer :
  - ➢ Le serveur de messagerie qui renferme en son sein Win 2000 server, Microsoft Exchange 2000, le service annuaire, etc.
  - ➢ Le serveur des agences appelé *Staging server* qui a la gestion de AMO, SDO, RCO, Antivirus e-trust.
  - ➢ Le serveur IBM RS/6000 qui permet de faire tourner le progiciel DELTA-BANK.

Les autres serveurs ou serveurs spécifiques : ils ont une fonction particulière, les principaux serveurs au sein de la CNCAS sont :

- ➢ Le serveur Minitel et le serveur Agricall : ils renferment Windows 95/98 et les logiciels spécifiques que sont Minitel et Agricall. Ces serveurs permettent de fournir des informations aux clients abonnés sur leurs comptes que ce soit sous une forme d'interrogation écrite ou vocale.
- ➢ Le serveur Internet : renferme Windows 2000 server, ISA server couplé à e-trust content Inspection.
- ➢ Le serveur FIRE-WALL : joue un rôle de protection contre les attaques et menaces externes. Il renferme Windows 2000 server et un chekpoint.

L'analyse du déploiement des serveurs à la CNCAS est schématisée à la figure 11.

Figure 11: Déploiement des Serveurs à la CNCAS



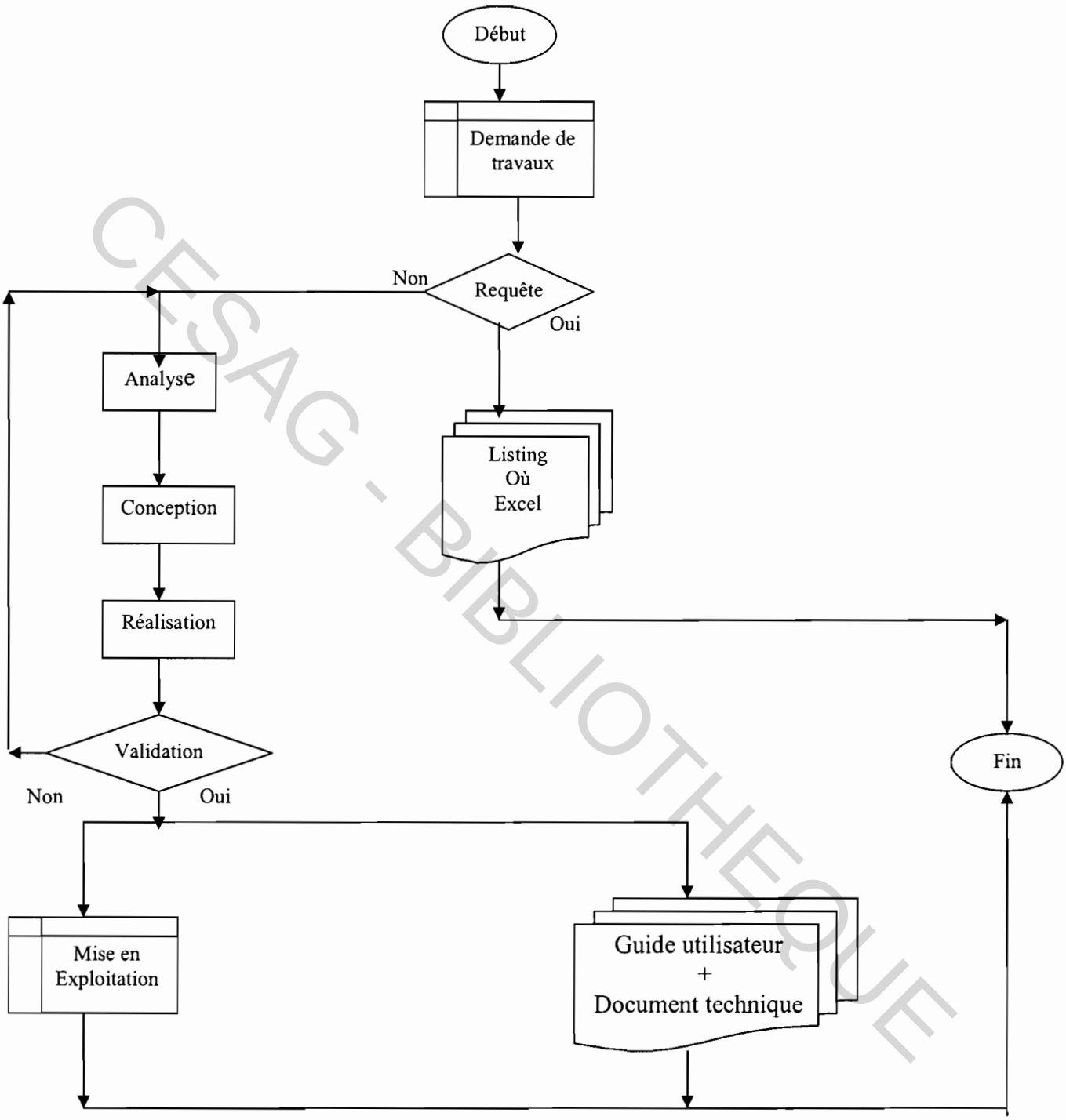
Source : CNCAS.

B. Architecture logiciel

La CNCAS s'est dotée d'un progiciel bancaire « DELTA-BANK » qui lui permet de prendre en charge toute activité opérationnelle.

Le service informatique de la CNCAS assure les processus et chaînes des traitements spécifiques ayant pour objectif principal de pallier aux insuffisances et manquements détaillés dans le progiciel DELTA-BANK. Le personnel informatique reste attentif aux demandes de travaux que leurs soumettent les utilisateurs. L'analyse du développement de demandes de travaux est schématisée à la figure 12.

Figure 12: Développement de demandes de travaux informatiques.



Source : CNCAS.

Ce système assure la gestion interne de l'ordinateur et ses différents organes (périphériques, mémoire, etc.). Il offre une vision normalisé de l'ordinateur et indépendante de l'électronique interne. Ses caractéristiques sont d'être multitâches, multi utilisateurs, possède une mémoire virtuelle avec une mise à disposition d'une mémoire étendue ainsi qu'une interactivité (une centaine de commandes).

UNIX permet la connexion LOGIN qui protège l'accès machine à travers deux types d'information à fournir :

- 1. LOGIN-NAME : Identifiant de compte ;
- 2. LOGIN-PASSWORD : Mot de passe sécurisé.

INFORMIX est le gestionnaire de base de données sur lequel fonctionne DELTA-BANK. La banque possède la version 9.21.

1.2.3. Le réseau informatique

A la CNCAS, l'architecture du réseau informatique est de type CLIENT/SERVEUR et chaque agence attaque le progiciel DELTA-BANK par l'intermédiaire du réseau IP de la SONATEL (Société National de Télécommunication) du Sénégal via son routeur. La CNCAS a choisi de fonctionner dans une architecture de base de données centralisée en concentrant l'ensemble des ressources au Siège.

Chaque agence de la CNCAS accède ainsi à sa base INFORMIX et au module agence de DELTA-BANK. En plus du module agence, un module site control est chargé de la consolidation des données traitées par l'ensemble des agences (Dakar y compris).

La CNCAS dispose d'un réseau LAN (Local Area Network) et d'un WAN (Wide Area Network) basés sur le protocole TCP/IP :

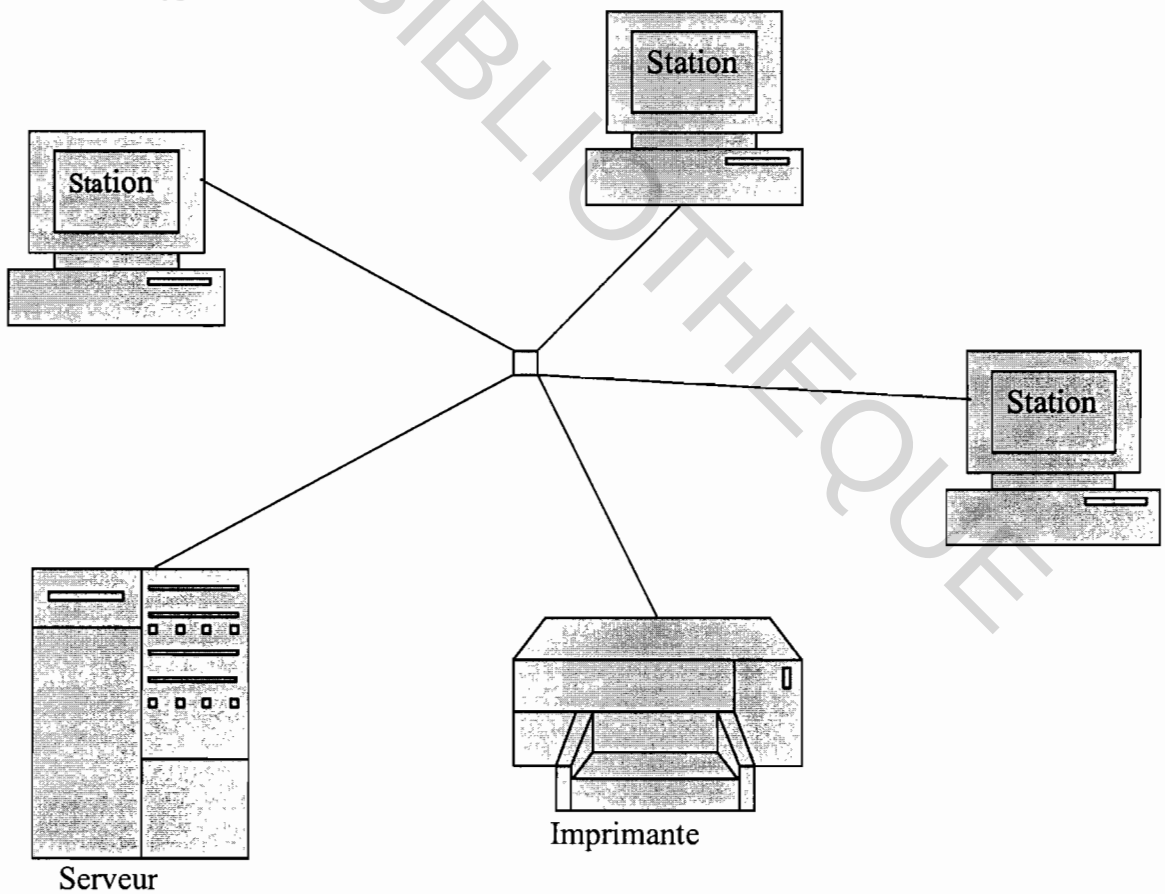
- Le réseau LAN, au siège, est constitués de serveurs UNIX et Windows, et des postes de travail, interconnectés par des câbles RJ45 constituant un réseau à 10Mb ;

- Le WAN permet l'interconnexion des réseaux locaux entre les agences et le siège. Il a pour principales fonctions :
    1. la télétransmission des agences vers le siège ;
    2. la mise à jour en temps réel des bases de données des agences qui sont localisées au Siège.

L'architecture du WAN est basée sur des routeurs de type CISCO, sur des LS à 256 Kbs entre Dakar et le réseau IP de la SONATEL et des LS de 64 Kbs entre le réseau IP de la SONATEL et les agences.

La topologie réseau utilisée à la CNCAS est de type « étoile » avec un réseau ETHERNET en 10 base T comme l'indique la figure 13 suivante :

Figure 13 : Réseau de type « étoile » à la CNCAS.



Source : CNCAS.

1.3. LA SÉCURITE DU SI DE LA CNCAS

L'analyse de la sécurité du système d'information de la CNCAS a porté sur cinq volets : la sécurité logique, la sécurité physique, la sécurité réseau, les logiciels anti-virus et la messagerie.

1.3.1 La sécurité logique

Dans le volet sécurité logique, nous avons analysé la gestion des accès à trois niveaux :

- ✓ les habilitations à DELTABANK/INFORMIX ;
- ✓ la connexion au réseau UNIX ;
- ✓ la sécurité sur le réseau au niveau utilisateur.

A. Les habilitations à DELTA BANK/INFORMIX

La gestion des habilitations dans DELTA se fait au niveau des tables de paramétrages de DELTA. Ainsi les utilisateurs déclarés se voient attribuer un code utilisateur qui leur permet de se connecter à DELTA. Le deuxième niveau de contrôle se fait dans les programmes qui sont mis à leur disposition. Le contrôle des habilitations de l'utilisateur s'effectue en fonction de plusieurs critères :

- ✓ Le gestionnaire du client ;
- ✓ Le profil du client ;
- ✓ Le type de compte ;
- ✓ Le chapitre comptable du compte.

Les différents droits qu'un utilisateur peut avoir sur un programme sont :

- ➢ « » pour non autorisé ;
- ➢ « c » pour création ;
- ➢ « i » pour interrogation ;

- « m » pour modification ;
- « s » pour suppression ;
- « * » pour toutes les options.

Pour organiser l'accès aux applications bancaires des utilisateurs dans la limite de leurs autorisations il existe trois types de profiles :

- ✓ Le profil « gestionnaire » ou « décisionnaire » : ce sont les utilisateurs qui prennent les décisions, qui valident ou ignorent certaines opérations ;
- ✓ Le profil « métier de la banque » : en fonction du profil, l'utilisateur peut faire certaine transaction et d'autres lui sont interdites ;
- ✓ Le profil «stagiaire » ou « consulting » : uniquement pour des consultation et/ou édition.

La connexion à DELTA se fait à travers un émulateur en tapant le code utilisateur sans le mot de passe. A ce stade, il faut préciser que le code utilisateur DELTA correspond en fait à un utilisateur du système UNIX qui a un mot de passe nul. Cet utilisateur n'a pas dans son fichier «profile » (fichier de paramètres utilisateur UNIX) que ses variables d'environnement et une instruction pour exécuter DELTA avec son nom de login. Ce n'est qu'une fois que son « profile » est exécuté que l'utilisateur voit se présenter la fenêtre de login de DELTA avec son nom de login déjà inscrit et il n'a plu qu'à saisir son mot de passe pour accéder aux menus qui lui ont été attribués.

Le mot de passe sous DELTA est compris entre quatre et six caractères. Les options de sécurité se trouvent dans le choix et la gestion du mot de passe qui est limitée, et la seule option disponible est la limitation de la durée de validité. Tout utilisateur créé se voit affecter un mot de passe sur six caractères « xxxxxx » qui lui permettra uniquement d'accéder au progiciel DELTA lors de la première connexion. Ensuite le système lui demandera de rentrer et de valider un mot de passe personnel dont le nombre de caractère devra être compris entre quatre et six caractères. Ce mot de passe à une durée de vie limitée de six mois et peut être modifié à volonté par l'utilisateur. Six jours avant la date d'expiration du mot de passe, l'utilisateur sera informé, à chaque connexion de la fin de validité de son mot de passe. Si

aucune action de modification du mot de passe n'est entreprise par l'utilisateur durant cette période, le code utilisateur sera automatiquement désactivé par le système au bout de six jours. Le code ne pourra plus être utilisé.

La déconnexion automatique de DELTA intervient qu'au bout d'une heure, ce délai est long et constitue un inconvénient dans le cadre de la sécurité.

A. La sécurité UNIX

Les différents comptes qui sont utilisés sous UNIX, outre les comptes directement liés à DELTA sont *root, informix, mls* et *trans* qui sont utilisés par tous les membres de la sous direction de l'informatique et organisation. L'identifiant UNIX root utilisé par tout le monde est un compte très dangereux dans le cadre de la sécurité car offre tous les privilèges qui ne devrait être utilisé que pour les travaux de maintenance.

B. La sécurité sur le réseau au niveau utilisateur

En ce qui est de la sécurité sur le réseau au niveau utilisateur, nous notons que les machines des utilisateurs tournent sous Windows. Au niveau utilisateur, il n'y a pas d'authentification sur le réseau. Seules les machines tournant sous NT demandent une authentification locale. Il importe de relever que les écrans des machines ne sont pas systématiquement verrouillés.

1.3.2 La sécurité physique

La sécurité physique se caractérise par les dispositions prises par l'entreprise pour accéder au service informatique, les mesures de sécurité relatives aux matériels informatiques et autres accessoires.

L'accès à la Sous Direction de l'Informatique et à la salle des machines est protégé par des portes fermées à serrure sans loquet à l'extérieur. Aucune personne ne saurait y pénétrer que si un membre du service ne lui ouvre pas la porte ou s'il possède une clé de la serrure.

Concernant les prises, elles sont protégées par un onduleur de 20KVA et il existe un groupe électrogène en cas de coupure d'électricité. Et dans la salle des serveurs, il existe un deuxième onduleur de secours de 2KVA.

Quant au dispositif de lutte contre les incendies, nous avons recensé des détecteurs de fumée, un plafond fait de polystyrène (ignifuge) ainsi que la présence à plusieurs endroits d'extincteurs au sein de l'entreprise et notamment à la sous direction informatique.

1.3.3 La sécurité réseau

La CNCAS dispose d'une connexion Internet (64K) via le fournisseur SONATEL MULTIMEDIA. Tous les utilisateurs se connectent via un routeur CISCO 1700. La banque s'est dotée d'un FIRE-WALL pour se protéger des dangers suivants :

- Malveillance ;
- Vol d'information ;
- Perte de confidentialité ;

Le siège est relié aux agences via le réseau IP qui s'appuie sur le protocole PPTP (Point to Point Tunneling Protocol) qui régie les VPN (Virtual Private Network). Cette connexion est sûre, à priori, étant donné que le réseau Sentranet de la SONATEL est sécurisé.

Au niveau du siège et des agences, les routeurs d'interconnexions ont chacun en plus du port Serial pour Liaison Spécialisée (LS), un port RNIS de back up. Le back up RNIS se fait sur un serveur d'accès de la SONATEL qui se trouve dans une région autre que celle de l'agence backupée (exemple de l'agence de Dakar et de Saint Louis).

1.3.4 Les mesures de sauvegarde

A la CNCAS, les procédures de sauvegarde sont journalières, hebdomadaires et mensuelles :

- ✓ La sauvegarde journalière vise à garder une image fidèle des données quotidiennes d'exploitation. La sauvegarde journalière de données est réalisée en deux exemplaires : une première sauvegarde est réalisé en utilisant les fonctionnalités de Delta-Bank et une

seconde sauvegarde est réalisé en utilisant un script spécifique après les traitements de fin de journée de Delta- Bank.

- ✓ La sauvegarde hebdomadaire vise à garder une image fidèle des données et systèmes de chaque serveur départemental. Ces sauvegardes sont réalisées chaque semaine en un exemplaire par serveur.
- ✓ La sauvegarde mensuelle vise à garder une image fidèle des données systèmes AIX (exploitation et back up) et une image complémentaire des données bancaires du serveur d'exploitation au dernier jour du mois. Ces sauvegardes sont réalisées chaque mois en deux exemplaires pour les données bancaires et en un exemplaire système par serveur.

1.3.5 Les antivirus

Les logiciels anti-virus qui sont installés à la CNCAS sont :

- ➢ Avp ;
- ➢ Norton 2004;
- ➢ Mc Afee.

La gestion de ces logiciels est individuelle.

1.3.6 La messagerie

A la CNCAS, la messagerie actuelle est hébergée chez SONATEL MULTIMEDIA et se compose de cinquante (50) adresses disponibles sous la forme login@cncas.sn

La banque agricole a acquis un serveur de messagerie Lotus Notes sous linux.

CONCLUSION

Ce chapitre de la partie pratique a été consacré à la présentation de la CNCAS afin de permettre une meilleure compréhension de l'architecture et de la sécurité informatique mise en place. Cette présentation nous permet d'entamer l'évaluation de la sécurité du SI de la CNCAS.

CHAPITRE 2 : AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION DE LA CNCAS

INTRODUCTION

Le but de notre stage est d'appliquer les connaissances théoriques acquises. Ainsi, à la suite de la partie théorique sur la SSI, nous avons mis œuvre les connaissances acquises au service de la CNCAS qui a bien voulu nous recevoir pour ce stage.

La CNCAS ayant été présenté dans le chapitre précédent, ce chapitre sera consacré à la présentation de l'audit de la sécurité à la CNCAS, des travaux effectués, des résultas de ses travaux et du suivi des recommandations de l'audit sécurité réalisé précédemment.

2.1 MISSION ET OBJECTIFS

La CNCAS vise à être une banque moderne de proximité (par rapport à la clientèle) et universelle d'ici l'an 2007. Aussi les responsables de la banque entendent se doter de moyens adéquats pour perfectionner son système d'information de même que son fonctionnement.

La Direction Générale insère dans sa politique et management de la sécurité des audits sécurité ayant pour mission l'évaluation de la SSI. Les objectifs des audits de la sécurité étant :

- ✓ Etablir un état des lieux vis-à-vis des risques ;
- ✓ Etablir des scénarii de réduction de risques ;
- ✓ Concevoir une politique de sécurité adéquate ;
- ✓ Mettre au point un programme de mise en œuvre de cette politique ;
- ✓ Elaborer des processus d'organisation et de contrôle de la sécurité.

Cependant dans le cadre de notre étude, nous nous limiterons aux objectifs relatifs à la l'état des lieux, à la conception d'une politique de sécurité et la perspective de mise en œuvre de cette politique.

2.2 AUDIT DE LA SECURITE A LA CNCAS

Dans le cadre de notre étude, nous avons réalisé l'évaluation de la Sécurité du Système d'Information (SSI) de la CNCAS.

L'objectif de cet audit sécurité était de dresser un état des lieux complet du niveau actuel de l'ensemble de la SSI sur le plan de l'organisation, de l'architecture, de la sécurité physique et logique, et de la formation sécurité.

2.21 Organisation générale de la sécurité

Nous avons observé une absence d'outils et de structures de pilotage nécessaire à une bonne gestion : absence de tableaux de bords internes, de reporting vers la direction ; absence d'indicateurs de service entre maîtrise ouvrage et maîtrise d'œuvre.

L'organisation générale de la CNCAS révèle également une absence de structure de décision associant la direction générale et les directions utilisatrices. Néanmoins il existe des comités de gestion où sont débattus les problèmes de sécurité de l'entreprise.
L'absence d'outils de pilotage et de suivi du service informatique (tableau de bord, reporting, indicateurs de service) peut entraîner un risque d'une gestion biaisée du service, ainsi que des prises de décisions inadéquates. Cela est d'autant plus crucial qu'il n'existe pas de comité permanent de gestion et de sécurité au sein de l'entreprise. Les problèmes de sécurité, la qualité des services et la satisfaction des utilisateurs et des clients sont grandement concernés.

Quant aux procédures au sein de la CNCAS, elles ont été formalisées, élaborées et mise en œuvre avec la contribution du Cabinet Mazard & Guérard en 2003. Elles sont à la disposition des agents au sein des différents services. L'utilisateur a également la possibilité de consulter le manuel de procédures par le biais de l'informatique en réseau, ce qui présente un avantage.

Cependant, les procédures d'exploitation informatique, indispensables au bon fonctionnement du SI, ne sont pas toutes formalisées. Ces procédures sont : la politique de sécurité, la séparation des fonctions, la procédure d'habilitation, le plan de secours, la protection de

l'information, les règles de sécurité liées aux nouvelles technologies, la charte sécurité, le plan qualité.

L'absence des procédures relatives au bon fonctionnement du SI ne permet pas l'efficacité des contrôles et le bon fonctionnement des services.

Recommandations :

1. Instauration d'une charte sécurité pour la sensibilisation et la prise en compte des règles fondamentales de sécurité générale pour l'entreprise ;
2. Instauration d'un schéma directeur informatique et des outils de pilotages de la fonction informatique (objectifs informatique, tableaux de bord, reporting, management des ressources informatique) ;
3. Instauration d'un comité permanent chargé des problèmes de sécurité et qui comprendrait le Directeur Général, le délégué à l'informatique et à l'organisation (responsable informatique), les représentants des fonctions utilisatrices, l'Audit Général, le responsable juridique et du contentieux ;
4. Désignation d'un responsable de la sécurité du SI (RSSI) pour l'organisation et la gestion de la sécurité dans l'entreprise ;
5. Création d'une Direction Informatique détachée de la Direction Financière et rattachée à la Direction Générale pour une meilleure gestion de la fonction informatique.
6. Développement des procédures d'exploitation pour un bon fonctionnement du service informatique

2.2.2 Architecture

A. Architecture technique

L'architecture du système est de type clients/serveurs et chaque agence attaque le progiciel DELTA BANK par l'intermédiaire du réseau IP de la SONATEL via son routeur.

La CNCAS dépend d'un seul fournisseur d'Internet (SONATEL MULTIMEDIA), elle court un risque de quasi dépendance en cas de rupture totale ou d'arrêt total en cas de défaillance de ce dernier.

Nous constatons que le nombre de PC est satisfaisant et nous avons constaté le renouvellement des postes utilisateurs avec l'acquisition de machines de marque DELL muni d'écran plat.

La lutte anti-virale est assurée par les logiciels anti–virus AVP, NORTON et Mc Afee. Leur gestion est individuelle. Cependant, nous constatons que les utilisateurs ne sont pas assez avertis pour effectuer les mises à jour.

Recommandations :

7. Programmation périodique des contrôles pour assurer la régularité des contrôles et assurer la concordance des données traitées.

B. Architecture applicative et développement

Nous avons constaté que les informaticiens ne prennent pas le temps d'élaborer des cahiers de charges et que les dossiers de conceptions et de modélisation sont succincts. Les modifications sur demande ne sont pas documentées et la documentation les concernant n'est pas mise à jour. En outre, les utilisateurs n'interviennent pas à aucun moment dans l'élaboration de l'application. Il n'existe pas de protocole entre le service informatique et les utilisateurs. Cela peut engendrer un risque de non adaptabilité, d'incompréhension et de non application. Il existerait donc un risque supplémentaire de vulnérabilité du SI.

L'exploitation et l'administration étudiées ont concerné le progiciel DELTA-BANK. Il s'est agit de répertorier les tâches pour l'exploitation du logiciel et leur segmentation. Ces tâches sont relatives aux clôtures de fin de journée, états financiers trimestriels (balance comptable, déclaration à la banque centrale, contrôle des risques), la réinitialisation des soldes des comptes de charges et de produits en fin d'année et les extractions de données pour alimenter les serveurs de banque en ligne tels que Minitel, Vocal et le Web.

En pratique, l'agent de l'équipe d'exploitation est chargé du redémarrer l'instance INFORMIX avec le script « reinit » et il lance les éditions, le journal des mouvements, l'état des comptes débiteurs, le rapport d'activités, les comptes en dépassement, les bordereaux de compensation. Il achemine également les serveurs Minitel, Vocal et Web à l'aide du script

« extract _don » pour les transférer dans les répertoires de chargement des serveurs avec la commande « rcp » d'unix.

Quant à l'administration des accès aux ressources des serveurs, elle est assurée par un agent de l'équipe réseau qui vérifie les droits des utilisateurs en fonction des fiches utilisateurs. Il octroie les autorisations demandées, modifie les autorisations spécifiées et supprime celles accordées ; ensuite il édite une nouvelle fiche utilisateur qu'il classe.

En ce qui concerne l'administration swift, l'agent de l'équipe administration swift vérifie si l'utilisateur est déjà créé, sinon il effectue les opérations de création, de modification ou de suspension de l'utilisateur.
Il importe de noter qu'à la première connexion, un contrôle technique est fait pour obliger l'utilisateur à changer de mot de passe. Par la suite, l'agent édicte une fiche utilisateur définitive qu'il classe.
Nous constatons que pour la création d'utilisateur, la norme de codifications des utilisateurs du serveur d'exploitation établie de la CNCAS est :

- Le code utilisateur est codifié sur quatre lettres ;
- Le code utilisateur permettant d'accéder au serveur d'exploitation (logging) est créé en minuscules ;
- Le code utilisateur permettant d'accéder au progiciel bancaire est créé en majuscules.

Il n'existe pas d'équipe pour un développement spécifique du progiciel DELTA BANK grandement exploité par tous. Cette situation peut entraîner un risque d'efficacité. En effet des difficultés dans l'adaptation du progiciel DELTA BANK surviennent pour certaines applications, créant ainsi une insatisfaction chez les utilisateurs et/ou la clientèle.

Le verrouillage sur DELTA BANK est nécessaire car l'entreprise encourt un risque de vulnérabilité en s'exposant à l'exploitation de ses données par des intrus de mêmes qu'aux pirates informatique. Ce verrou conduirait à un bon mappage des utilisateurs sur DELTA-BANK.

Recommandation :

8. Amélioration des applications du progiciel DELTA BANK en y associant les utilisateurs.

2.2.3 Sécurité

A. Sécurité physique

Les visites des locaux ont permis de déceler l'existence de plusieurs mesures de lutte contre les incendies, notamment des détecteurs de fumée, des extincteurs d'incendie. Les différents services sont parés contre les dégâts des eaux. Les installations, la planification du site, la topographie analysées permettent de constater la très faible probabilité d'inondations ou de tremblement de terre et une accessibilité en cas de mauvais temps. Nous avons également noté la présence d'un groupe électrogène qui assure la relève en cas de coupure d'électricité.

Bien qu'il existe du matériel de lutte contre les incendies, ceux-ci sont en nombre insuffisant. La CNCAS doit donc renforcer son matériel. Elle court un grand risque de perte matériel, immatériel et financière en cas de sinistre

Le contrôle des accès à L'entreprise est assuré par la société de gardiennage SAGAM, qui le fait par le contrôle des pièces d'identité de tous les visiteurs étrangers à la banque, à la porte d'entrée du personnel. Les agents de sécurité sont également présents à plusieurs endroits de la banque, notamment dans le hall où se trouvent les guichets ouverts à la clientèle. La salle machine, quant à elle, est sécurisée à l'aide de serrures dotées de crochet sans loquet extérieur.

La protection de l'accès du service informatique et de la salle machine doit être amélioré. La société court le risque de perte de données, vols, de malveillance et de dénis de service. En effet le dispositif actuel est susceptible d'être contourné par connivence avec un membre interne au service informatique et sans laissé de trace. La CNCAS doit s'équiper d'une porte à puce électronique ou à accès avec un code qui marquerait l'identité des utilisateurs, de même que les forçats.

Les sauvegardes et l'archivage des documents se font de manière journalière, hebdomadaire et mensuelle. Les documents qui remplissent la correcte exécution sont rangés dans un coffre ignifugé. La vérification est faite par le responsable informatique. Il importe de préciser que les sauvegardes hebdomadaires ont un exemplaire qui est transféré à l'agence de Thiès qui sert de secours (back up).

Recommandation :

9. Améliorations des mesures et outils de sécurité.

B. Sécurité logique

La CNCAS dispose d'une connexion Internet de 64 k via le fournisseur SONATEL MULTIMEDIA. Tous les utilisateurs se connectent via un routeur CISCO 1700. Le Siège est reliée aux 12 agences via le réseau IP qui s'appuie sur le protocole PPTP (point to Point Tumeling Protocol) qui régie les VPN (Virtuel Private Network). A priori, cette connexion est sûre s'il est prouvé que le réseau sentranet de la SONATEL est sécurisé.

La CNCAS dispose d'un réseau LAN et d'un WAN basés sur le protocole TCP/IP. Au siège, le LAN est constitué de serveurs RS/6000 interconnectés par des câbles RJ45 et constituent un réseau à 10Mb. Le WAN permet l'interconnexion des réseaux locaux entre les agences et le siège. L'architecture du WAN est basée sur des routeurs de type CISCO, sur les LS à 256Kbs entre Dakar et le réseau IP de la SONATEL et des LS (Liaisons Spécialisées) de 64 Kbs entre le réseau IP de la SONATEL et les agences.

La sécurité de la connexion à Internet est assurée par la mise en place d'un fire-wall. Cela permet à la banque de se protéger des dangers tels que la malveillance, le vol d'information, la perte de confidentialité, la perte d'intégrité des données.

La messagerie est hébergée chez SONATEL MULTIMEDIA et se compose de cinquante adresses disponibles dans la forme login@cncas.sn .

Recommandation :

10. Mise en place d'un autre serveur NT ou LINUX qui aurait la charge de valider les utilisateurs sur le réseau, ce qui permettrait une meilleure gestion des droits entre différents postes du réseau.

2.2.4 Formation sécurité

Le personnel de la CNCAS n'est pas imprégné de la sécurité de l'entreprise. La société de gardiennage SAGAM (Société Assistance Gardiennage Africain Mission) assure la sécurité

physique du personnel et du patrimoine de la CNCAS et des anti-virus sont installés au sein de chaque poste utilisateur. Mais, le personnel n'est pas informé sur les mises à jour, les mesures de sécurité et il n'existe pas de formation sur la sécurité.

Le manque de formation du personnel informatique et des utilisateurs y compris les contrôleurs du département Audit Général conduit l'entreprise à s'exposer d'avantages aux sinistres. En effet, personne ne sait ce qu'il devrait faire en cas de survenance d'un sinistre. Le risque de perte (matériels, humaines, financières et immatériels) est donc élevé.

Recommandations :

11. Instauration d'un planning de formation pour le personnel informatique, les utilisateurs ainsi qu'une documentation adéquate des applications informatiques ;
12. Instauration de formation pour des contrôleurs de l'Audit Général afin d'assurer des missions d'audit sécurité régulières.

2.3. RESULTAT DE L'AUDIT DE LA SECURITE

2.3.1 Travaux effectués

Pour mener à bien notre étude nous nous sommes appuyés sur les différents outils suivants : les entretiens, les questionnaires d'audit informatique, l'observation physique et le suivi de recommandations. Ces travaux nous ont permis de bien comprendre les activités et l'organisation de la CNCAS et de faire l'état des lieux de sa SSI.

A. Les entretiens

Au sein de la CNCAS, nous avons rencontré une Direction et un personnel de qualité, dynamiques et dévoués, qui ont bien voulu se mettre à notre disposition et contribuer à la réussite de l'étude. Ainsi, les entretiens réalisés ont pu avoir lieu sans difficultés et nous avons rencontré :

- ✓ Le Directeur des Finances et de l'Information : l'entretien a porté sur l'organisation générale du service informatique, de la sécurité et de l'opportunité de notre étude. Il a affirmé être satisfait de son système informatique qui répond aux besoins des banques et

établissements financiers modernes. Cependant il continue d'œuvrer pour l'amélioration du système et son développement par l'acquisition de nouveaux matériels adaptés.

- ✓ Le Sous Directeur de l'Informatique et de l'Organisation : malgré le poids de ses responsabilités, il a bien voulu nous recevoir à plusieurs reprises et nous a assuré de sa grande collaboration tout au long du déroulement de notre étude. Les entretiens ont porté sur le système informatique de la banque dont il a une bonne maîtrise. Il travaille en continu à son amélioration, notamment en mettant en œuvre les recommandations du dernier Audit Sécurité du SI de la banque, effectué en Décembre 2001-Janvier 2002 par le Cabinet Deloitte &Touche Tohmatsu.

- ✓ Le chef de Service Systèmes et Production : l'entretien a porté sur l'organisation de son service, la gestion des mots de passe, l'installation des réseaux et la sécurité informatique. Il a une bonne connaissance de l'informatique de la CNCAS et s'emploie à répondre aux besoins de la banque. Il déplore, cependant, l'étroitesse des bureaux et de la salle machine et souhaite un espace plus grand dans les nouveaux locaux du siège.

- ✓ Le Sous Directeur de l'agence de Dakar : l'entretien a été très enrichissant ; il a porté aussi bien sur la sécurité générale, la politique et la stratégie de la banque que sur les aspects techniques des besoins des agents. Il ressort de cet entretien que la banque a bien un comité de sécurité qui ne fonctionne pas. Les questions liées à la sécurité du SI sont cependant abordées lors des réunions du comité de direction et du conseil d'administration. Et d'autre part, l'apport des utilisateurs doit être d'avantage pris en compte et une plus grande collaboration avec le service informatique est de mise. Il mentionne que le progiciel DELTA BANK est bon mais se doit d'être en phase avec les besoins et travaux des agents.

- ✓ Les utilisateurs : nous avons rencontré des utilisateurs de l'ensemble des quatre directions que compte la CNCAS. D'une manière générale, les utilisateurs sont satisfaits du progiciel DELTA BANK et des prestations du service informatique. Bien que considérant le niveau de sécurité du SI comme satisfaisant, ils déplorent cependant le manque de formation informatique, notamment sur la sécurité du SI.

B. Les questionnaires

Dans le cadre de la collecte des informations nous avons administrés trois types de questionnaires : un questionnaire d'audit informatique basé sur la méthode MARION, un questionnaire de contrôle interne relatif au service informatique et un questionnaire d'évaluation adressé aux utilisateurs de l'outil informatique.

1. Le questionnaire MARION

Ce questionnaire nous a permis de dérouler la méthode MARION (cf. la première partie, chapitre 2.3.3.A.). Le responsable informatique a bien voulu répondre aux questions de la méthode MARION portant sur les 27 facteurs clés du système de sécurité (Annexe I).

2. Le questionnaire de contrôle interne au service informatique

Ce questionnaire est spécifique à l'organisation de la fonction informatique, la gestion des ressources informatique, de l'environnement d'exploitation et du logiciel de base.

Ce questionnaire porte sur :

- ✓ l'organisation de la fonction informatique : l'étendu du contrôle, la séparation des tâches, la formation, l'aspect financier de la planification des ressources, l'acquisition de matériels et de logiciels et les modalités de gestion des contrats et de l'assurance.

- ✓ La gestion des ressources informatiques : l'installation, les pannes du système, la planification du site et la sécurité physique, les aspects techniques et mécaniques, l'évaluation et l'adaptation des performances, la gestion des ressources machine, la disponibilité du système, le plan de secours, l'exploitation informatique, le contrôle des entrées et sorties, la diffusion des états, la gestion des supports, les secours, reprises et la gestion des modifications et des incidents.

- ✓ L'environnement d'exploitation : l' infocentre, l'exploitation en temps partagé, le traitement coopératif, l'informatique départementale, l'informatique individuelle.

✓ Le logiciel de base : la sécurité du système, l'intégrité du système, la responsabilité, l'efficacité et la compétence, la performance du système, la fiabilité et la pérennité du système, la reprise du système et la possibilité d'extension du matériel.

3. Le questionnaire d'évaluation des utilisateurs

Ce questionnaire d'évaluation permet aux utilisateurs de l'outil informatique d'apporter leurs appréciations sur la performance des machines, du système, du réseau et des prestations du personnel informatique à travers leurs compétences et leur disponibilité. Il a été adressé à trois ou quatre agents des différentes directions que compte la CNCAS et également à la Direction Générale, soit environ dix huit personnes. Des questions et un rating (Annexe II) portent sur les points suivants :

- L'organisation de la sécurité
- La formation
- L'informatique individuelle
- L'environnement d'exploitation.

A la fin du questionnaire, le répondant (l'utilisateur) est invité à relever les points forts, les points faibles et à mentionner d'éventuelles suggestions.

C. Les observations physiques

L'observation physique pratiquée concerne la visite des locaux et l'exploitation documentaire.

1. La visite des locaux

Cette visite des locaux a été réalisée sur l'ensemble de l'organisation générale de la sécurité de la CNCAS et notamment au sein de la Sous Direction de l'Informatique. Nous relevons :

✓ Au niveau de la sécurité générale : la présence d'une société de gardiennage SAGAM (Société Africaine Gardiennage Assistance Mission) avec des agents armés assurant la sécurité du patrimoine et du personnel. La société SAGAM contrôle les accès des entrées et sorties de toute personne étrangère à la banque. En outre, la présence de

plusieurs détecteurs d'incendie, d'extincteurs à différents endroits de la banque a été observée.

- ✓ Au niveau de la sécurité de la sous direction informatique : l'accès à la sous direction et à la salle machine est protégé par des portes fermées à serrure sans loquet extérieur. La salle des serveurs est étroite et ne dispose pas de dispositif de sécurité. Cette salle est encombrée, le nombre d'extincteurs est à accroître et la porte qui donne accès n'a pas de serrure.

2. L'exploitation documentaire

Nous avons eu à exploiter dans le cadre de notre étude sur la SSI plusieurs documents à savoir le manuel de procédures, le budget prévisionnel 2004 et le rapport d'Audit sécurité du dernier audit sur les SI. Nous relevons ce qui suit :

- ✓ Au niveau du manuel de procédures : il fut élaboré par le cabinet d'expertise comptable Mazars & Guérard en 2003. Il décrit plusieurs procédures, notamment celles sur la fonction informatique, la sécurité informatiques, les sauvegardes, le paramétrage. Cependant des procédures importantes dans le cadre de la SSI restent à être élaborées comme la politique de sécurité, le plan de secours, la charte sécurité et un plan qualité.
- ✓ Au niveau du budget prévisionnel 2004 : ce document porte sur l'ensemble des activités de la CNCAS. Aussi bien les agences et le siège de Dakar y sont concernés. La fonction informatique est développée à travers le budget d'investissement 2004 et le budget prévisionnel de recrutement 2004.
- ✓ Au niveau du dernier Audit sécurité de la SI : ce document a été réalisé par le cabinet d'expertise comptable et d'audit Deloitte Touche Tohmatsu. Il nous a permis de bien comprendre la SSI de la CNCAS.

D. L'évaluation du contrôle interne

Nous avons évalué le contrôle interne à travers le périmètre couvert par les procédures, des tests de cheminement sur les procédures et la grille d'analyse de séparation des tâches.

1. La description des procédures

A partir du manuel de procédures, mis à notre disposition, et des entretiens avec les responsables et les intervenants dans la fonction informatique, nous avons constaté que les procédures sont respectées et sont conformes au manuel de procédures.

2. Le test de cheminement d'existence de la procédure

L'objectif est de s'assurer que la description est conforme à la réalité.

Au sein du service informatique, nous avons conduit un test de cheminement sur les demandes de travaux de la part des utilisateurs. La procédure qui nous a été décrite est conforme à la réalité car les différentes étapes du processus ainsi que les documents afférents ont été respectés.

3. La grille de séparation des tâches

La grille d'analyse des tâches indique pour chacune des tâches, les personnes (fonction dans l'organisation) habilités à les effectuer. Nous avons rempli notre grille de séparation des tâches avec l'aide des responsables de la fonction informatique.

Tableau 6 : la grille d'analyse des tâches

N°	Tâches	Nature	Personnes habilitées			
			DFI	SDIO	RSO	RSP
1	Administre la fonction informatique	A	×	×		
2	Administre la sécurité physique	C				×
3	Administre la sécurité logique	Ex				×
4	Administre les programmations	D			×	
5	Administre les serveurs	A				×
6	Administre la base de données	A				×
7	Administre les maintenances	A				×
8	Met à jour les applications	D			×	
9	Développe les applications	D			×	
10	Documente les applications	D			×	
11	Rédige les guides utilisateurs	D			×	
12	Assiste les utilisateurs	D			×	
13	Etudie les cahiers de charges	A	×	×		
14	Exploite les applications	C				×
15	Effectue les sauvegardes	Ex				×
16	Stocke les sauvegardes sur le site	Ex				×
17	Stocke les sauvegardes hors site	Ex				×
18	Transfère les données	Ex				×
19	Gère les mots de passe et les autorisations d'accès	A			×	
20	Entretient les équipements	A				×
21	Suit les contrats de maintenances	A				×

Source : Nous-mêmes

Avec pour :

- DFI : Directeur des Finances et de l'Information
- SDIO : Sous Directeur Informatique et Organisation
- RSO : Responsable Support et Organisation
- RSP : Responsable Système et Production.

La nature des différentes tâches :

- A : Administration (autorisation)
- C : Conception
- Ex : Exécution
- D : Développement (utilisation)

L'analyse de la grille de séparation des tâches indique que d'une manière générale, la CNCAS maîtrise la séparation des tâches. En effet au niveau des responsables Informatique (DFI et SDIO), nous notons qu'il n'y a pas de cumul de tâches ; de même qu'au niveau du Responsable du Support et de l'Organisation (RSO) qui assure les fonctions de développeur et de gestionnaire des mots de passe, des autorisations d'accès qui ne sont pas cumulatives. Cependant, le Responsable des Systèmes et Production (RSP) qui administre la sécurité physique et logique, effectuent également les sauvegardes des donnés et les contrôles. Ces deux tâches sont cumulatives et sont à corriger. En outre, nous notons un chevauchement des tâches du Directeur des Finances et de l'Information avec celles du Sous Directeur Informatique et Organisation.

2.3.2 Méthode d'Analyse des Risques Informatique Orientés par Niveaux (MARION)

Cette méthode a été utilisée pour permettre d'apprécier le niveau de sécurité de la CNCAS en 27 points que nous déterminons au tableau 7.

Il s'agit sur la base du questionnaire MARION (Annexe I) d'attribuer des notes variant de 0 à 4 à différents niveaux de sécurité, avec :

- 0 = néant
- 1 = mauvais
- 2 = médiocre
- 3 = assez bon
- 4 = bon.

Cette analyse a été faite avec le concours du responsable informatique. Les résultats obtenus à partir de la notation du questionnaire MARION, rempli par le responsable informatique, sont consignés dans le tableau suivant :

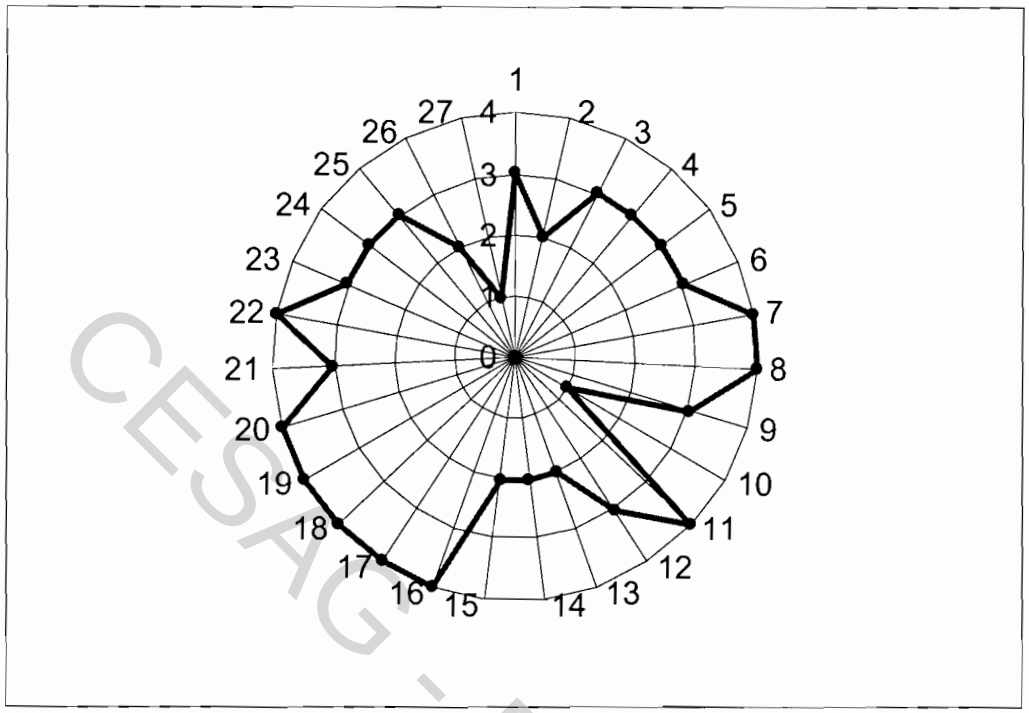
Tableau 7 : Risques informatiques par niveau

N°ordre	Risques Informatiques par Niveau	Notes	N°ordre	Risques Informatiques par Niveau	Notes
1	Appréciation générale de la sécurité	**3**	15	Plan informatique	**2**
2	Organisation générale	**2**	16	Fiabilités des matériels et logiciels de base	**4**
3	Contrôles permanents	**3**	17	Sécurité des télécommunications	**4**
4	Réglementation et audit	**3**	18	Protection des données	**4**
5	Facteurs socio économiques	**3**	19	Archivages	**4**
6	Environnement de base	**3**	20	Sauvegardes	**4**
7	Contrôle des accès	**4**	21	Suivi de l'exploitation	**3**
8	Consignes	**4**	22	Maintenance	**4**
9	Sécurité incendie	**3**	23	Procédures de révision	**3**
10	Dégâts des eaux	**1**	24	Méthodes d'analyse programmation	**3**
11	Amélioration fiabilité de fonctionnement	**4**	25	Contrôles programmés	**3**
12	Systèmes et procédures de secours	**3**	26	Micro informatique	**2**
13	Protocoles utilisateurs/informaticiens	**2**	27	Réseau de micros.	**1**
14	Personnel informatique	**2**			

Source : Résultats du questionnaire MARION.

Ce résultat nous a permis de construire la rosace MARION de la CNCAS à la figure 14.

Figure 14 : Rosace Marion de la CNCAS



Source : Résultats du questionnaire MARION

Nous pouvons conclure avec la méthode MARION que la CNCAS dispose globalement d'un bon niveau de maîtrise des risques informatiques. Cependant, il existe des points faibles qui nécessitent une amélioration :

- l'organisation générale de la sécurité est à parfaire (2) ;
- défaut de protection par rapport aux dégâts des eaux (10) ;
- les protocoles utilisateurs/informaticiens et le plan informatique ne sont pas définis et des réels efforts doivent être mis en œuvre pour la formation du personnel informatique et des utilisateurs (13 – 14 – 15) ;
- la maintenance du micro informatique doit être mieux suivi (26) ; Protection des micro-ordinateurs insuffisante (27).

2.4 Suivi de l'Audit Sécurité

Cette méthode a été utilisée pour apprécier la mise en œuvre des recommandations du dernier audit sécurité sur la SI réalisé en Décembre 2001, ainsi que les risques résiduels associés à l'absence de mise en oeuvre de certaines recommandations.

Notre travail a consisté à recenser les recommandations du dernier audit sécurité, analyser les recommandations prises en compte par l'entreprise, leur effectivité. Par la suite, nous avons analysé les recommandations non prise en compte de même que les risques afférents.

Cette analyse a été également faite avec le concours du responsable informatique. Les résultats sont les suivants :

Tableau 8 : Suivi des recommandations ou « Follow up » de l'Audit Sécurité du SI de Décembre 2001 à la CNCAS

Recommandations	**Prise en compte ou non OUI/NON**	**Nos recommandations**
1. Augmenter les effectifs de l'équipe d'au moins un ingénieur et deux analystes programmeurs	OUI	Aucune
2. Elaborer des fiches de postes plus précises permettant d'instaurer une réelle séparation des fonctions.	OUI	Aucune
3. Mettre en place un comité informatique (Direction, directions utilisatrices, direction informatique.	OUI	Aucune
4. Mettre en place des procédures d'audit informatique conformes au standard professionnel.	OUI	Aucune
5. Prévoir une extension de personnel au niveau de l'équipe informatique.	OUI	Aucune
6. Renforcer la motivation : - Améliorer les conditions salariales des membres de l'équipe informatique - Proposer un programme de formation plus adapté aux exigences du domaine informatique ; - Alléger la charge de chacun en procédant à des recrutements.	OUI	Aucune
7. Mettre en œuvre les procédures de développement.	OUI	Aucune
8. Recruter un organisateur bancaire.	NON	Amélioration de la gestion des habilitations (cohérence)
9. Formaliser les besoins des utilisateurs jusqu'au niveau des spécifications fonctionnelles.	NON	Meilleure élaboration de dossiers de conception et de modification en tenant compte des besoins des utilisateurs

10. Elaborer et mettre en œuvre une méthodologie de gestion de projet.	NON	Instauration d'une meilleure gestion de projet (informatique)
11. Prévoir l'acquisition d'un second routeur de série 3600.	NON	Rendre fonctionnelle la ligne secondaire (RNIS) qui existe déjà afin de répartir les charges et d'assurer une meilleure disponibilité de la liaison siège agence.
12. Rédiger l'ensemble des procédures d'exploitation.	OUI	Aucune
13. Mettre en place une vraie politique des habilitations de DELTA	OUI	Aucune
14. Faire un développement spécifique sur DELTA pour pouvoir augmenter la qualité de la gestion de la sécurité.	NON	Améliorer la qualité et la gestion des applications de DELTA BANK
15. Activer la journalisation de certains évènements dans le système UNIX, pour un bon suivi utilisateurs.	OUI	Aucune
16. Créer des comptes personnels distincts avec les privilèges adéquats pour l'équipe informatique (sur le serveur UNIX)	OUI	Aucune
17. Verrouiller la case nom de login sur DELTA, pour un bon mappage des utilisateurs sur DELTA.	NON	Idem à 14.
18. Se mettre à jour pour les licences Windows et bureautique.	OUI	Aucune
19. Séparer les deux serveurs et les placer dans deux endroits différents.	OUI	Aucune
20. Prévoir l'adjonction d'un nouveau climatiseur et aussi désengorger la salle machines	OUI	Aucune
21. Mettre des extincteurs dans le périmètre du département informatique et assurer le suivi et la maintenance.	OUI	Aucune
22. Mise en place d'un serveur DHCP et installation d'un serveur NT ou LINUX	NON	Améliorer la gestion des droits entre les différents postes réseau.
23. Mise en place d'un Fire-wall	OUI	Aucune
24. Acquérir une licence d'Anti-virus serveurs et postes clients.	OUI	Aucune
25. Projet de mise en place d'un serveur de messagerie avec Lotus Notes sous Linux.	OUI	Aucune

Source : Résultats des entretiens et du QCI

Nous pouvons conclure à l'aide du follow up réalisé, que la CNCAS a, d'une manière générale, bien tenue compte des recommandations du dernier audit sécurité sur la SI.

En effet, nous notons que 72% des recommandations ont été prises en compte et effectivement réalisées. Sur les 28% des recommandations non prises en comptes, 43% sont en cours de réalisation pour l'année 2005. Pour ce qui est des recommandations non encore effectuées, des risques y sont afférents.

Les risques associés sont les suivants :

- La non formalisation des besoins et de fait la non prise en compte des besoins des utilisateurs peut entraîner un risque d'insatisfaction,
- La non acquisition d'un second routeur de série 3600 peut entraîner des difficultés de reprise de la liaison siège-agence en cas de coupure totale de la liaison principale ;
- La non mise en place d'un serveur DHCP et d'un serveur NT ou Linux peut entraîner des difficultés pour assurer la sécurité des postes connectés en réseau.

CONCLUSION

Ce deuxième chapitre pratique permet de dérouler l'Audit de la sécurité du SI à la CNCAS, les travaux effectués, les résultats ainsi que le suivi réalisé sur les recommandations du dernier audit sécurité précédent.

Il ressort que la CNCAS a une bonne connaissance de la sécurité informatique de son système. Cependant des zones de faiblesses sont à améliorer pour l'organisation et le fonctionnement de la fonction informatique en particulier et de toute la banque en générale.

CHAPITRE 3 : SYNTHESE ET PERSPECTIVES DE MISE EN ŒUVRE DES RECOMMANDATIONS

INTRODUCTION

Les résultats des travaux d'Audit de la sécurité du SI nous ont permis de déceler les points forts, les points faibles et de proposer des recommandations pour l'amélioration de la sécurité du système d'information à la CNCAS. Dans le but de bien faire comprendre nos recommandations aux destinataires, nous envisageons des perspectives de mise en œuvre.

3.1 SYNTHESE

Il ressort de l'audit de la sécurité du SI à la CNCAS des points forts et des faiblesses du système.

3.1.1 Les principales forces

- ✓ Bonne prise de conscience des insuffisances de la SSI par le SDIO
- ✓ Bonne compétence et bonne qualification du personnel informatique
- ✓ Existence d'un groupe électrogène de secours pour une relève immédiate de l'alimentation en cas de coupure d'électricité
- ✓ Existence d'un système de détection de fumée et de matériels de pour lutte contre les incendies
- ✓ Existence d'un système de sécurité pour l'accès physique au sein de l'entreprise assurée par de vigiles de la société SAGAM qui opèrent des contrôles
- ✓ DELTA BANK, le progiciel utilisé est adéquat et facile à utiliser
- ✓ Bon suivi des sauvegardes journalières, hebdomadaires et mensuelles
- ✓ Bonne protection des données et du patrimoine
- ✓ Bonnes procédures d'archivages
- ✓ Bonne maintenance de l'outil informatique
- ✓ Bonne gestion des autorisations et des habilitations
- ✓ Bonne gestion des mots de passe
- ✓ Les outils de travail sont performants et adéquats
- ✓ Résultats satisfaisants de la SSI (Marion ; follow up)

3.1.2 Les principales faiblesses

- ✓ Absence de politique sécuritaire
- ✓ Absence de charte de la sécurité
- ✓ Absence d'un responsable de la sécurité du système d'information (RSSI)
- ✓ Absence d'un comité permanent chargés des problèmes liés à la sécurité
- ✓ Absence de conduite de projet informatique
- ✓ Absence de maîtrise générale des procédures de secours et de reprise en cas de sinistre
- ✓ Absence de procédures d'exploitation
- ✓ Absence de police d'assurance couvrant spécifiquement la sécurité informatique
- ✓ Absence de planning de formation pour l'actualisation des connaissances pour le personnel informatique
- ✓ Absence de formation sur la sécurité informatique adressée aux utilisateurs
- ✓ Dépendance d'un seul fournisseur (SONATEL MEDIA) pour la fourniture d'Internet
- ✓ Absence d'audits sécurité effectués périodiquement sur le SI
- ✓ Absence de protocoles de liaisons utilisateurs–informaticiens, pas de prise en compte des préoccupations des utilisateurs.

3.1.3 Les principales recommandations

A la suite de ces constats et de l'analyse des risques de la SSI à la CNCAS, pour améliorer le système nous avons proposé les recommandations suivantes :

❖ **Au niveau de la Direction Générale**

Aux dirigeants de la banque qui sont en amont de toutes décisions, nous recommandons :

- ✓ L'instauration d'une charte sécurité
- ✓ L'instauration d'un schéma directeur informatique et des outils de pilotages de la fonction informatique
- ✓ L'instauration d'un comité permanent chargé des problèmes de sécurité

- ✓ La désignation d'un responsable de la Sécurité du Système d'Information (RSSI)
- ✓ La création d'une Direction Informatique ou d'une délégation détachée de la Direction Financière

❖ **Au niveau de la Direction Informatique**

Les responsables informatiques ont un rôle capital dans le cadre de la sécurité du système d'information. Ils ont en charge toute la fonction informatique de la banque et ils sont les spécialistes (ingénieurs et techniciens informatique) capables de l'amélioration du système informatique. A la suite de l'audit sécurité, ils doivent :

- ✓ Développer les procédures d'exploitation
- ✓ Améliorer les applications du progiciel DELTA BANK
- ✓ Améliorer les mesures et outils de sécurité.
- ✓ Instaurer un planning de formation pour le personnel informatique et d'une documentation informatique adéquate.

❖ **Au niveau de la Direction de l'Audit Général**

Les auditeurs et contrôleurs de la CNCAS jouent un rôle fondamental dans la sécurité du système d'information. En effet ils établissement et ils conduisent les audits de la banque, notamment les audits de la sécurité informatique. La Direction de l'Audit Général doit :

- ✓ Instaurer des formations pour des contrôleurs de l'Audit Général
- ✓ Programmer de manière périodique des contrôles, notamment sur la sécurité.

3.2 PERSPECTIVES DE MISE EN ŒUVRE DES RECOMMANDATIONS

Les recommandations devront être faisables et économiques pour l'entreprise. La Direction Générale devra prendre les mesures efficaces, tout en mettant en œuvre les recommandations, pour assurer la continuité de son exploitation, l'exactitude des données et la protection de son patrimoine gage de pérennité pour son entreprise. Il s'agit de déterminer les modalités de mise en application effective de certaines recommandations formulées ci-dessus, étant donné que certains autres recommandations sont développées en annexe, notamment la charte de la sécurité (annexe III) et la désignation d'un RSSI (annexe IV).

3.2.1 Au niveau de la Direction Générale (DG)

Nous prenons en compte les recommandations relatives à la création d'une direction informatique et celle relative à l'instauration d'un schéma directeur et des outils de pilotage de la fonction informatique.

- **Création d'une Direction Informatique**

L'analyse des tâches, à partir de la grille de séparation des tâches, à révéler un chevauchement des responsabilités du Sous Directeur Informatique et Organisation et celles du Directeur des Finances et de l'Information. Ainsi donc, vu l'importance de la fonction informatique pour le système d'information bancaire, nous suggérons une création de deux directions distinctes à savoir la Direction Informatique et la Direction Financière et Comptable.

La Direction Informatique pourra garder la même organisation, la même structure et les mêmes charges que celles existantes à la Sous Direction Information et organisation. Cependant, le Directeur Informatique sera directement rattaché à la Direction Générale et non à la Direction des Finances et de l'Information qui devrait devenir une Direction Financière et Comptables suivant les nouvelles recommandations de la commission bancaire. Un recrutement de part et d'autre n'est pas nécessaire.

La mise en place d'une telle réorganisation demandera de la part de la Direction Générale, qui prendra la décision, une sensibilisation des agents par rapport à la mission et aux objectifs de sécurité du SI assignés à la nouvelle orientation de la banque. Elle améliorera l'organisation et le suivi des travaux informatiques, de la sécurité générale et en particulier du personnel informatique dans la prise de décision.

- **Instauration d'un schéma directeur informatique et des outils de pilotage de la fonction informatique**

Il s'agira pour la Direction Générale de mettre en place un schéma directeur informatique et des outils de pilotage de la fonction informatique, notamment le contrôle de gestion de l'informatique, les tableaux de bords informatiques, Le re-engineering du système d'information et La performance et l'assurance qualité des systèmes d'information.

➢ **Le schéma directeur informatique**

Pour une meilleure gestion de la fonction informatique tel que le pilotage rigoureux de la gestion des projets informatique, la Direction Générale doit mettre en place un schéma directeur de la fonction informatique, à savoir : classer les projets par priorité, désigner des équipes en charges de chaque projet, fixer des dates de début et de fin de projet, fixer les charges de travail (jours/homme). Par ailleurs, faire une étude de faisabilité pour chaque projet avant son inscription dans le plan annuel; mettre en place un comité permanent constitué de membres des différentes directions et faire le point périodiquement (tous les trimestres par exemple) sur l'avancement des projets, la qualité des services, la satisfaction des utilisateurs et notamment sur la sécurité du système.

➢ **Le contrôle de gestion de l'informatique.**

Dans les entreprises, le contrôle de gestion selon BOISVERT (1991 :30), pris au sens de la direction, consiste en la production des informations nécessaires aux gestionnaires pour fixer des objectifs pertinents, élaborer de bonnes stratégies et les mettre en œuvre de façon efficace et efficiente. Ayant pour objectif d'éclairer et de soutenir les différents services, le contrôle de gestion se trouve au centre de leur bonne gestion, de leur performance et intervient à tous les niveaux. Le contrôle de gestion de l'informatique, est plus que nécessaire pour faciliter le management de ce domaine de plus en plus primordial à l'entreprise. Les deux aspects à mettre en place par la Direction Générale sont :

- ✓ L'analyse des coûts informatiques
- ✓ Le budget informatique

➢ Les tableaux de bords informatiques

Le tableau de bord représente pour l'utilisateur un instrument de mesures des performances par rapport aux objectifs de motivation et de suivi des actions correctives, qui lui sont fixés, sur la base d'un diagnostic et d'une mise en exergue des points faibles. Le tableau de bord est personnel et nécessite après l'identification de son utilisateur la prise en compte de ses besoins et attentes. La mise en place d'un tableau de bord nécessite la détermination des facteurs de performances : il s'agit d'identifier l'ensemble des tâches ou actions considérées comme facteurs de performance, de déterminer leur unité de mesure et de leur attribuer une valeur quantifiable. Le tableau de bord est un instrument d'aide à la décision qui permet de mieux expliquer à la direction et aux utilisateurs ce que fait l'informatique et de déterminer sa contribution à la création de la valeur ajoutée dans l'entreprise.

La DG, avec le concours de la DIO, pourra mettre en place les tableaux de bord suivants :

- ✓ Le tableau de bord de l'exploitation
- ✓ Le tableau de bord des services utilisateurs
- ✓ Le tableau de bord administratif
- ✓ Le tableau de bord informatique de la direction générale

Vu le développement rapide des technologies de l'information et partant des besoins d'information, les tableaux de bords doivent être perpétuellement mis à jour.

➢ Le re-engineering du système d'information

Le re engineering informatique est une réalité que nul n'ignore. La caducité du matériel et des applications informatiques est courante dans les entreprises. Tout système informatique devient désuet au fil de quelques années et ne correspond plus aux attentes et besoins non seulement des utilisateurs, mais également des clients qui reçoivent les services de ce système. Les besoins changeant et le matériel évoluant devenant de plus en plus performant et technique, entraîne un renouveau permanent des processus des organisations et du re engineering du système d'information existant.

La direction doit préalablement vérifier l'opportunité et les dangers de cette action avec les informaticiens, analyser son impact financier en évaluant sa rentabilité, son budget et la

situation financière de l'organisation avant d'entériner la décision de changement. La DG avec le concours de la Direction Informatique doit alors déterminer avec précision les frontières des processus, établir le calendrier de mise en œuvre qui détermine les délais maximums et minimums d'obtention des premiers résultats d'une action de re engineering des systèmes d'information.

Le service informatique doit être compétent pour réussir les phases les plus délicates, l'implémentation et le pilotage du changement. La DG se doit d'expliquer au personnel la nécessité du changement en anticipant et en gérant les résistances, puis les sensibiliser afin de les faire participer pendant toutes les étapes du re engineering.

- **La performance et l'assurance qualité des systèmes d'information.**

L'évaluation de la performance du système d'information est l'une des nouvelles techniques recommandées en gestion d'entreprise. C'est une technique d'évaluation interne à l'organisation fondée sur des objectifs précédemment fixés qui constituent son référentiel. Il importe de définir la nature des évalués et des évaluateurs et le type d'évaluation (subjective, statistique ou analyse comparative).

L'assurance qualité des systèmes d'information a pour objectifs de positionner la qualité dans les systèmes d'information, dans le développement du logiciel et dans le produit ou les activités informatiques. Il est question pour la DG de cibler tous les aspects qualité, de prendre en compte les étapes d'une démarche de certification et d'élaborer une cartographie des normes assurance qualité de produits, de développement de logiciels et d'une inspection d'audit. La qualité doit être définie, mesurée et reliée aux objectifs.

3.2.2 Au niveau de la Direction Informatique (DI)

- **Rédiger des procédures d'exploitation et de développement**

D'une manière générale, nous avons constaté des lacunes concernant les procédures d'exploitation. La Direction Informatique se doit donc de rédiger l'ensemble des procédures d'exploitation indispensable au bon fonctionnement du SI de la CNCAS. Avec l'aide de la

Direction de l'Audit Générale, certaines procédures qui nous semblent nécessaires doivent être prises en compte. Ces procédures sont présentées à titre indicatif dans le tableau 9 suivant avec une description de leur contenu.

Tableau 9 : Quelques procédures d'exploitation

PROCEDURES	DESCRIPTION DE LA PROCEDURE
Politique de sécurité	Elaborer une politique de sécurité de façon à couvrir l'ensemble des sujets pertinents et intégrer les éléments relatifs à l'architecture des systèmes et aux procédures rédigées
Séparation des fonctions	Définir les principes de séparation de fonction. Ce document établira les rôles et responsabilités de chacun des membres de l'équipe ainsi que les droits particuliers affectés à chaque fonction.
Procédure d'habilitation des personnels	Définir la procédure d'habilitation des personnels pour les différentes composantes du système d'information
Plan de secours	Elaborer un plan de secours et des procédures de gestion de la continuité de l'activité Ce plan identifiera de façon détaillée les différents scénarios susceptibles d'interrompre l'activité de tout ou partie de la CNCAS et listera les actions à mener pour rétablir la situation dans les meilleurs délais.
Journalisation des événements	Définir les procédures de journalisation des informations. Ce document fixera les objectifs de journalisation des évènements de l'ensemble du système d'information
Protection de l'information	Définir les règles de protection physique et logique de l'information véhiculée ou hébergée par les systèmes de la CNCAS.
Gestion des fichiers et des documents sensibles	Définir les règles et modalités de gestion des documents sensibles
Règles de sécurité liées aux nouvelles technologies	Définir les règles de sécurités spécifiques aux contextes nouvelles technologies au sein de la CNCAS. Ce document mettra en avant les objectifs à retenir en matière de règles de sécurité
Sécurité physique	Formaliser les sécurités physiques pour le siège et les agences

Sécurité logique informatique	Définir les règles générales de sécurité logique pour les systèmes informatiques Cette procédure traitera aussi de la disponibilité.
Plan qualité	Définir les normes de qualité que la CNCAS souhaite instaurer et préciser la façon dont elles sont atteintes. Ce document n'est pas en aucun cas un plan qualité complet, amis définira les normes et standards applicables par la CNCAS.

Source : CNCAS

Concernant les procédures de développement, la majorité des applications a été développée en interne essentiellement en visual basic. Ces applications ne répondraient pas tous aux exigences qui pourraient être exercées sur des prestataires en matière de gestion et de documentation que doivent prendre en compte les développeurs de la CNCAS. Pour palier à cela, la Direction Informatique devrait :

- ✓ Accroître le nombre de personnes capables de maintenir chaque application (3 ou 5 au lieu de 1 ou 2) ;
- ✓ Accroître la documentation informatique de sorte à mettre en place une maintenance efficace des applications en cas de départ du programmeur qui l'a développée ;
- ✓ Spécifier le niveau de détail souhaité concernant les commentaires effectués dans le code des applications ;
- ✓ Spécifier le degré de documentation utilisateur et administrateur.

- **Améliorer les applications du progiciel DELTA BANK**

Le progiciel DELTA BANK est le plus utilisé au sein de la CNCAS et assure presque toute la gestion des principales prestations bancaires. Aussi la DI se doit de veiller à la mise à jour des applications du progiciel :

- ✓ Mettre en place une vraie politique de gestion des habilitations de DELTA ;
- ✓ Faire un développement spécifique sur DELTA ;
- ✓ Un bon mappage des utilisateurs de DELTA et leurs pendants sur UNIX.

3.2.3 Au niveau de la Direction de l'Audit Général (DAG)

Au niveau de la Direction de l'audit Général, en matière de sécurité du système d'information, l'accent sera mis surtout sur la formation et sur la mise en place des audits sécurité.

- **Formation des auditeurs en Sécurité du SI**

La DAG doit faire des plans réguliers de formation des auditeurs en matière d'informatique, de système d'information, de sécurité informatique, etc.
Ces formations pourraient se faire par le biais des informaticiens de la banque (moins coûteux), de séminaires ou de conférences. Les plans de formations doivent être établis par chaque service selon leurs besoins et soumissent à la Direction générale avant le vote du budget annuel.

- **Mise en oeuvre des audits de la sécurité**

Cette étude à révéler l'importance de l'audit de la sécurité du SI pour la CNCAS. La DAG doit veiller à la mise en place d'audit sécurité de manière régulière diriger par les auditeurs sous sa direction. Les différents audits sécurité réalisés précédemment à la CNCAS, notamment l'audit externe fait par le cabinet Deloitte Touche Tohmatsu et notre étude sur l'audit de la SSI, pourraient servir de base de travail.

Cependant la Direction Générale doit sensibiliser les agents de toute la banque (au siège et dans les agences) pour la réalisation des missions d'audits sécurité, de ses objectifs de même que de la politique et le management de la sécurité

CONCLUSION

Ce chapitre nous a permis de faire la synthèse de l'audit sécurité réalisé à la CNCAS, particulièrement les recommandations et leurs perspectives de mise en œuvre.

Il ressort que la CNCAS a une bonne connaissance de la notion de la sécurité du système d'information, mais la pratique et la mise en place d'outils de gestion pour la fonction informatique doivent être prise en compte par la Direction Générale avec l'aide des Directions Informatique (qui doit être séparé de la Direction financière) et de l'Audit Général.

CONCLUSION DE LA DEUXIÈME PARTIE

Dans la perspective de comprendre et d'apprécier la sécurité du SI de la CNCAS, nous avons présenté l'entreprise à savoir :

- la présentation générale de la CNCAS ;
- le système informatique de la CNCAS ;
- la sécurité du SI de la CNCAS.

Par la suite, l'ensemble des investigations et démarches entreprises dans le cadre de notre étude a été exposé :

- les entretiens avec les responsables de la CNCAS ;
- les entretiens avec les responsables de la fonction informatique ;
- le questionnaire de la Méthode d'Analyse des risques Orientée par Niveau (MARION) adressé au responsable informatique ;
- le questionnaire de contrôle interne spécifique aux services informatiques ;
- les questionnaires d'évaluation du SSI adressés à différents utilisateurs de l'ordinateur à la CNCAS ;
- l'observation physique ;
- le follow up.

A la suite de ces investigations, ayant une bonne connaissance de l'entreprise, nous avons réalisés notre étude sur la sécurité du SI à travers un audit sécurité portant sur:

- l'organisation générale de la sécurité ;
- l'architecture technique, applicative et développement ;
- la sécurité physique et logique ;
- la formation sécurité du personnel.

Par la suite une synthèse et des perspectives de mise en œuvre des recommandations nous ont permis d'explorer les voies pour la CNCAS d'améliorer la gestion et le fonctionnement de sa fonction informatique et par delà de toute la banque en générale.

Nous considérons que pour l'amélioration du SI de la CNCAS nos recommandations doivent être prise en compte afin d'assurer à l'entreprise une plus grande garantie pour la continuité de son exploitation, la sauvegarde de son patrimoine et la survie de l'entreprise en cas de survenance d'un sinistre.

CONCLUSION GÉNÉRALE

Les systèmes d'information peuvent entraîner des pertes financières pour les établissements financiers comme la CNCAS dans les cas où ils seraient vulnérables aux attaques, tentatives de fraude et autres menaces.

C'est pourquoi nous avons porté notre choix sur ce sujet « la sécurité du système d'information », qui permet de contribuer à améliorer la sécurité du SI, à garantie la continuité de l'exploitation et la sauvegarde du patrimoine.

Ce mémoire s'articule autour de quatre (4) principaux chapitres regroupés en deux parties :

- la partie théorique qui traite de la notion de la sécurité du SI ; des missions et des démarches à l'audit de la sécurité.
- La seconde partie pratique, qui porte sur la prise de connaissance de l'entité étudiée et de l'expérimentation de l'audit de la sécurité à la CNCAS.

D'une manière générale la question fondamentale à la quelle nous apportons un élément de réponse est de savoir si le système d'information mis en place est intègre, à l'abri des attaques, menaces et autres vulnérabilités pouvant affecter la pérennité de l'entreprise ? Autrement dit « avons-nous pu atteindre un niveau de sécurité du SI acceptable pour l'entreprise ? »

Aussi, le traitement de l'information qui est au cœur de toutes activités composant les métiers de l'organisation, bénéficie de plus en plus de l'automatisation des tâches grâces aux performances sans cesse accrues de l'informatique. L'évolution de la technologie donne aux services, aux agences et aux personnes physiques ou morales en relation avec l'entreprise, des moyens accrus de traitement et d'accès aux informations.

Cependant, le recours croissant à des procédés de stockage magnétique ou numérique de l'information, la généralisation progressive de l'usage de terminaux de saisie ou de consultation, l'extension des réseaux de transport de données ouverts sur l'extérieur sont

autant d'accès nouveaux à l'information qui sont à l'origine de nouveaux risques pour l'entreprise.

En effet, les moyens modernes de traitement de l'information ont progressé plus vite que les techniques ou les procédures permettant d'en prévenir le vol, la perte ou la modification non contrôlée.

C'est ainsi qu'une prise en compte insuffisante de la sécurité peut générer avec une ampleur nouvelle, des risques informatiques spécifiques : les erreurs de conception ou d'analyse des projets informatiques, les manipulations défectueuses des matériels et des logiciels, les malveillances de toute nature, le détournement des logiciels ou la divulgation de données confidentielles, enfin l'organisation insuffisante de moyens de sauvegarde et de secours ne mettre pas la banque à l'abri de détournement d'argent de carte bancaire par exemple.

Aucune disposition ne peut garantie en toute certitude l'absence de risques informatiques. De ce fait, l'objet de la sécurité est de contenir ces risques à un niveau acceptable au moyen d'un ensemble de mesures de protection technique et opérationnelle visant à :

- Identifier ou authentifier tout utilisateur des SI ;
- Assurer l'intégrité des informations stockées ou transportées ;
- Respecter la confidentialité des données ;
- Rapporter la preuve de toute utilisation des ressources informationnelle ou d'échanges d'information ;
- Organiser les moyens de secours en cas de défaillance du service rendu par le SI.

Et les mesures de sécurité du SI à mettre en œuvre s'appliquent à l'établissement, aux données et aux programmes enregistrés en mémoire centrale ou sur supports en entrée et en sortie du système. En outre, les règles de sécurité s'appliquent à la Direction Générale, aux services centraux des directions, aux agences, aux prestataires et utilisateurs, à toutes personnes appartenant ou entretenant des relations avec l'entreprise.

Ainsi donc, à travers l'Audit sécurité du SI de la CNCAS, nous avons pu faire l'état des lieux, l'analyse des risques, proposer des recommandations et une possibilité de mise en oeuvre de ces recommandations, afin de répondre à la question fondamentale posée plus haut.

Les nouveaux outils (automatisés) d'analyse et les nouvelles pratiques de gestion des systèmes informatiques (contrôle de gestion de l'informatique, tableaux de bords informatiques, re engineering du SI, performance et assurance qualité des SI), pourraient améliorer la gestion quotidienne de la sécurité informatique.

BIBLIOGRAPHIE

Ouvrages

1. A.T.H (1986), *Audit opérationnel : guide pour l'audit opérationnel et des systèmes d'information*, éd .Clet, 273pages.

2. Banque de France (1996), Livre blanc sur la sécurité des Systèmes d'information, Commission Bancaire, Paris, 339 pages.

3. BOISVERT Jean (1994), *les grands esprits du management,* Québec, 141 pages.

4. CNCAS (2001), *Audit sécurité du Système d'Information à la CNCAS.*

5. CNCAS (2003), *Budget prévisionnel.*

6. CNCAS (2003), *Bussiness plan.*

7. CNCAS (2003), *Manuel de procédures*, Cabinet Mazard & Guérard, classeur n°2.

8. CNCC (Avril 2003), Prise en compte de l'environnement informatique et incidence sur la démarche d'audit, édit. CNCC, CD-ROM.

9. CNCC (Juillet 2003), Référentiel normatif et déontologique de la CNCC, édit. CNCC, CD-ROM.

10. DIAGNE Samba (2004), *Système d'Information*, Codex : Vital Roy 2000, CESAG, Dakar, Pas de pagination.

11. Dictionnaire PETIT ROBERT illustré (1996).

12. DUNSMORE B.; BROWN J.; CUNNIN Ghams S. (2002), *Sécurité Internet*, edit. First interactive, 512 pages.

13. IFACI (1993), *Audit et contrôle des systèmes d'informations. Module 8 : Sécurité*, Institut Française des Auditeurs et consultants, Paris, 130 pages.

14. MAIDOUDOU Abakar (1992), *Rôle de l'auditeur en matière de système d'information de l'entreprise*, Cesag, Dakar, 112 pages.

15. MATHON Phillipe (2002), *ISA Server 2002 Proxy et Firewall : optimiser l'accès internet et sécuriser son réseau d'entreprise*, édit. Eni, 372 pages.

16. MEILLAN, Eric (1993), *La sécurité des systèmes d'information : les aspects juridiques*, édit. HERMES, Paris, 204 pages.

17. MOUMOUNI Moussa Boubacar (2002), *Audit d'une application informatique de gestion clientèle : cas de la Société Nigérienne d'Electricité (NIGELEC)*, CESAG, Dakar, 164 pages.

18. N'GUESSAN N'DRI Parfait David (2004), *Audit informatique dans une entreprise pétrolière : OXYGAZ Sénégal*, CESAG, Dakar, 136 pages.

19. RENARD Jacques (2004), *Théorie et pratique de l'Audit Interne*, 5ème édition, édit.d'Organisation, Paris, 487 pages.

20. REIX Robert (2002), *Système d'information et management des organisations*, Edit .Vuibert, 443 pages.

21. SARDI Antoine (1993), *Audit et inspection bancaire, Tome 1*, edit. Arfges, 464 pages.

22. SARR Ababacar (2004), *Audit Informatique*, Codex, CESAG, Dakar, 68 pages.

23. SOW Ngary (2004), *Audit interne et procédures*, Codex, CESAG, Dakar, 130 pages

24. TALL Mamadou (2004), *Audit de la sécurité informatique*, Codex DESCOGEF, CESAG, Dakar, 102 pages.

25. THORIN Marc (2000), *l'Audit Informatique*, éd. Hermes, Paris, 184 pages.

26. WATERFIELD, charles ; RAMSING, Nick (1998), *Systèmes d'information de gestion pour les institutions de microfinance : guide pratique* ; CGAP, série « outil et technique », n°1, 22 pages.

27. YAZI Moussa (2004), Méthodologie de la recherche, Codex, CESAG, Dakar, pp. 21-28.

Revues

28. ALTER S (1996)., Information *System : a management prospe ctive, Benjamin cusmings publishing company*, 2ème édit., 2 pages.

29. BONANICHE, José (2002), *COBIT : le guide de management des outils pour developper et maîtriser une vision stratégique*, revue Française de l'audit interne, n° 159, pp 29-31.

30. CUCCHI A. (2004), *complémentarité et substitution des médias : le cas du courrier électronique et du téléphone, Système d'information et management*, revue trimestrielle, volume 9, n°3, PP. 3-27.

31. Dumoulin C. (1986), *Management des systèmes d'information, Editions* d'organisation.

32. HILLIAN Jean Claude (2002), *Interne ou la nécessité renforcée d'une réelle maîtrise de risque, système d'information des établissements de crédits*, bimestrielle Française de l'audit interne,Paris, n°158, pp 22-24.

33. MOHAMED, Naaima (2002), *Les technologies de l'information et de la communication sont entrées dans le champ d'action de l'audit interne (1ère partie)*, bimestrielle Française de l'audit interne, n°158, PP 34-36.

34. Lucas H.C. (1986), *Système d'information pour le management.*

Sites Web

35. ACL, « Présentation de ACL », site consulté le 25 avril 2005, (www.acl.com/products/).

36. AFAI, *Cobit*, page consultée le 14 décembre 2004, (www.idbconsulting.com/francais/increferebtielcobit.cfm).

37. AUD-IT, *Norme ISO/IEC 17799 : 2000*, page consulté le 15 avril 2005, (www.aud-it.ch/bs7799.htm).

38. AUD-IT, *Politique de sécurité informatique, politique de sécurité des systèmes d'information*, pages consultées le 05 juin 2004, (www.audit-it.ch/pol.htm).

39. AUD-IT, *Sécurité et Organisation Informatique*, Evaluer les risques informatiques, pages consultées le 05 juin 2004. (www.audit-it.ch/audit.htm).

40. CLUSIF, *Méhari,* page consultée le 14 décembre 2004, (www.clusif.asso.fr/fr/production/mehari/3.qsp)

41. ERCOM, *Sécurité du système d'information*, page consultée le 23 juillet 2004, (www.ercom.fr).

42. ERNST & YOUNG, *Audit et Sécurité des Systèmes d'Information*, page consulté le 29 juillet 2004, (www.ey.com/global/content.nsf/Francophone_Africa/home_isaas).

43. ERNST & YOUNG, *Résultats de l'enquête sur la performance des systèmes d'information en 2003*, page consultée le 29 juillet 2004, (www.ey.com/global/content.nsf/france/index_etudes_si).

44. NESSUS, « présentation de NESSUS », site consulté le 25 avril 2005, (www.nessus.org/about/).