CESAG

CENTRE AFRICAIN D'ETUDES SUPERIEURES EN GESTION

INSTITUT SUPERIEUR DE COMPTABILITE
I. S. C.

DESS AUDIT ET CONTROLE DE GESTION
15ème promotion 2003 - 2004

MEMOIRE DE FIN D'ETUDES

THEME :

Incidence de la sécurité informatique sur la démarche d'audit financier de la Société Africaine des Jeux (SAJE)

Présenté par :

Françoise Palamwé ABOULEKA

Sous la direction de :

M. Moussa YAZI

Responsable du programme Audit et Contrôle de gestion au CESAG

SIGLES ET ABREVIATIONS

AICPA : American Institute of Certified Public Accountants

ATH : Association Technique d'Harmonisation

BIR : Bordereau Individuel de Recettes

CAC : Chiffre d'Affaires calculé

CAV : Chiffre d'Affaires Versé

CEFRIO : Centre Francophone d'Informatisation des Organisations

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

CNCC : Compagnie Nationale des Commissaires aux Comptes (en France)

CNIL : Commission Nationale de l'Informatique et des Libertés (en France)

CSI : Computer Security Institute

DA : Direction Administrative

DAT : Digital Audio Tape

DCF : Direction Comptable et Financière

DE : Direction de l'Exploitation

DM : Direction du Marketing

DRH : Direction des Ressources Humaines

ED : Etat de Distribution

FBI : Federal Bureau of Investigation

IFAC : International Federation of Accountants

IFACI : Institut Français de l'Audit et du Contrôle Internes

ISA : International Standards on Auditing

LAN : Local Area Network

LI : Loterie informatisée

LS : Loterie sportive

MARION : Méthode d'Analyse des Risques Informatiques Orientée par Niveaux

MEHARI : Méthode Harmonisée d'Analyse des Risques Informatiques

OCDE : Organisation de Coopération et de Développement Economiques

OR : Ordre de recettes

PC : Personal Computer

PMU : Pari Mutuel Urbain

RTC : Réseau Téléphonique Commuté

SAJE : Société Africaine des Jeux

SYSCOA. : Système Comptables Ouest Africain

UEMOA : Union Economique et Monétaire Ouest Africaine

VPN : Virtual Private Network

LISTE DES TABLEAUX ET FIGURES

I. Liste des tableaux

Pages

II. Liste des figures

Pages

TABLE DES MATIERES

Pages

INTRODUCTION GENERALE

Le monde actuel est massivement géré par des ordinateurs, qui, face à une quantité de plus en plus importante de données à traiter, se sont révélés incontournables. Initialement l'ordinateur était uniquement utilisé dans les grandes organisations qui avaient les moyens de s'en procurer. Par la suite, l'apparition des micro ordinateurs et la chute rapide et généralisée du prix du matériel informatique ont permis aux organisations de taille moyenne de tirer également profit de cette nouvelle technologie.

De nos jours, le développement des activités et l'augmentation des échanges poussent de nombreuses entreprises à déployer des systèmes informatisés sophistiqués pour le traitement et le stockage de toutes leurs données ainsi que pour la production de l'information financière.

Contrairement à ce qui se passait au début de l'informatisation de la gestion, il existe aujourd'hui des mesures permettant de réguler et de contrôler l'utilisation des systèmes informatisés dans les entreprises. Ainsi au niveau de la comptabilité, des textes réglementaires ont été mis en place afin de préciser les obligations des systèmes informatiques, notamment en matière de sécurité. Il s'agit notamment du Nouveau Plan Comptable de 1982 en France et du Règlement relatif au Droit Comptable SYSCOA dans les pays de l'UEMOA.

Dans le domaine de l'audit, l'utilisation de l'ordinateur au sein de l'entreprise est restée pendant longtemps à l'écart des préoccupations des professionnels. C'est seulement à partir des années 1970, que l'environnement informatique a été intégré dans la démarche de l'auditeur. Ce changement a lieu après le scandale provoqué par la société d'assurance Equity Funding Corporation of California. Cette entreprise californienne a fait faillite en 1973 à la suite de la découverte dans le système informatique d'opérations frauduleuses estimées à près de deux (2) milliards de dollars *(traduction libre de l'auteur)* (WEBER, 1999).

Après cette affaire, on assiste à la modification des normes professionnelles d'audit et à la naissance de l'audit informatique. Cette discipline nouvelle s'intéresse aux principales facettes du système d'information de l'entreprise. DERRIEN (1992) précise ainsi que l'audit informatique peut être orienté vers les trois (3) domaines suivants :

- la fiabilité de l'environnement informatique (organisation générale du service, procédures de développement et de maintenance des applications, fonctions techniques, procédures de saisie de données, gestion des sauvegardes, procédures de reprise d'exploitation, sécurité, assurances…) ;
- l'efficacité et les performances de l'activité informatique (performances et dimensionnements des machines adéquation des logiciels systèmes aux besoins…) ;
- la fiabilité des applications informatisées (contrôle de leur utilisation, de leur adéquation aux spécifications fonctionnelles, de leur pérennité, recherche de fraudes…).

Malgré cette évolution « technologique » de l'audit, force est de reconnaître que dans la pratique actuelle de l'audit financier, les professionnels tiennent rarement compte du paramètre informatique dans l'exécution de leurs missions. En effet, la démarche d'audit utilisée pour l'examen de comptes produits par l'informatique est souvent la même que celle utilisée lors de la vérification des comptes établis manuellement.

Face à cet état de fait, on serait tenté de croire, à tort, que l'informatique n'a aucune incidence sur l'opinion que formulent les auditeurs à l'issue de leurs missions.

L'utilisation de l'ordinateur dans le traitement d'informations financières d'importance significative pour l'audit présente des risques spécifiques que l'on peut appeler « risques inhérents à l'informatique ». D'après la Compagnie Nationale des Commissaires aux comptes de France, CNCC (2003 : 7), ces risques « peuvent résulter de défaillances dans les activités informatiques générales, telles que :

- Le développement et la maintenance des programmes ;
- L'exploitation du système ;
- Les traitements particuliers ;
- La sécurité physique ;
- Les contrôles d'accès pour les utilisateurs privilégiés. »

A travers cette analyse de la CNCC, on constate que la sécurité informatique occupe une place non négligeable. En effet, s'il est vrai que la mise en place de systèmes informatisés nécessite généralement des moyens financiers et matériels importants, les données stockées

ou traitées par l'ordinateur sont encore plus précieuses pour les raisons suivantes : (IFACI, 1993) :

- Importance stratégique des données ;
- Dépendance de la prise de décision par rapport aux données ;
- Confidentialité des données ;
- Exigences formulées par des tiers ;
- Impératifs externes.

La sécurité de l'information est donc d'une importance capitale au sein des organisations informatisées.

Par ailleurs, quelque soit la performance d'un matériel, s'il n'est pas entouré d'un maximum de sécurité, sa possession est vaine. La qualité de fonctionnement d'un système informatique suppose donc au préalable une prévention et une protection suffisante vis-à-vis des risques encourus (SARR, 2004).

De manière générale, en négligeant l'environnement informatique de l'entreprise, l'auditeur n'intègre pas le risque informatique dans sa démarche. Dès lors, il est confronté à des difficultés de mise en œuvre en termes d'approche, de nature des contrôles à réaliser et d'exploitation des résultats obtenus à l'issue de ces contrôles.

Par ailleurs, il est, d'une certaine manière, tributaire du client car toutes les informations qu'il examine lui sont fournies par ses interlocuteurs dans l'entreprise auditée.

Il faut aussi noter qu'une mauvaise évaluation de la sécurité du système d'information de l'entité auditée traduit une insuffisance dans l'appréciation du contrôle interne, par conséquent, une mauvaise évaluation des travaux à effectuer et, à terme, des conclusions erronées.

La sécurité informatique doit constituer un objectif prioritaire pour l'auditeur lors de l'évaluation de la qualité du système d'information. Ceci pour les raisons suivantes :

1. Les systèmes informatisés sont sans cesse influencés par des facteurs technologiques tels que : le développement de nouvelles applications de l'informatique, l'ouverture des systèmes d'information à Internet, la généralisation des accès distants, l'explosion des

attaques par Internet, la mise en place d'architectures informatiques complexes, l'arrivée des technologies sans fil, le développement des services de télémaintenance, etc.

2. L'intégrité, la confidentialité ou la disponibilité des données et des ressources des systèmes d'information peuvent être mises en danger par différents types de risques :
   - erreurs humaines ;
   - malhonnêteté, mécontentement des employés ;
   - personnes étrangères à l'organisation ;
   - fluctuations des pannes électriques ;
   - catastrophes naturelles ;
   - introduction d'un code illicite… (IFACI, 1993 : 8-3).

3. Le système d'information est à la base de toute l'activité de l'entreprise et de tous les états financiers produits par celle-ci. Une protection insuffisante ou, plus particulièrement, l'inexistence d'un système de secours en lieu sûr constituerait une menace pour la continuité de l'exploitation de l'organisation.

De manière pratique, l'appréciation de la sécurité informatique lors d'un audit financier peut être effectuée :

1) Par un expert spécialisé en audit informatique ;
2) Ou par les auditeurs financiers eux-mêmes.

Aujourd'hui, grâce à leur maîtrise assez avancée de l'outil informatique, les auditeurs financiers arrivent à intégrer à leurs diligences des travaux s'apparentant à l'audit informatique dans des milieux où le système comptable est informatisé. Par ailleurs, les organisations professionnelles comme l'IFAC ou la CNCC mettent en place des normes et une documentation pertinentes afin d'aider les auditeurs à mieux appréhender les aspects opérationnels de l'audit financier dans un environnement informatique. Ils sont donc parfaitement outillés pour procéder à l'évaluation de la sécurité informatique lors de l'audit financier d'entreprises comme la Société Africaine des Jeux (SAJE).

A partir de là, nous pouvons nous poser la question de recherche suivante : dans quelle mesure la sécurité informatique influe-t-elle la démarche de l'auditeur financier ?
Plus précisément, nous nous efforcerons de répondre aux questions suivantes :

- Quelle est la démarche générale en matière d'audit financier ?
- Quelles sont les mesures de sécurité qui doivent être mises en place dans une organisation utilisant un système d'information basé sur l'ordinateur ?
- Quels sont les risques liés à la sécurité informatique ?
- Comment se traduit, de manière pratique, la prise en compte de ces risques lors d'une mission d'audit financier ?

L'objectif principal de cette étude est de montrer que la prise en compte de la sécurité informatique permet de rendre les travaux de l'auditeur financier plus efficaces principalement lors de la phase de l'évaluation des risques où il est appelé à apprécier les risques inhérent et lié au contrôle.

Les objectifs spécifiques poursuivis se situent à plusieurs niveaux :

- Décrire le système informatique mis en place au sein de la SAJE ;
- Faire ressortir les forces et faiblesses de la politique de sécurité informatique en vigueur dans la société et analyser ces dernières afin de déterminer leur incidence sur le risque d'audit ;
- Formuler des recommandations qui permettront de renforcer le système de sécurité étudié.

Devant le constat de l'émergence des nouvelles technologies de l'information au sein des entreprises de notre sous région, une telle étude présente des intérêts multiples :

- Pour les auditeurs financiers : ce travail de recherche pourra servir de guide pratique pour la prise en compte de la sécurité informatique dans leur démarche lors de missions en milieu informatisé ;
- Pour le lecteur : l'exploitation de ce mémoire permettra d'appréhender l'importance de la sécurité dans un système informatique et d'avoir une vision plus concrète de son influence sur la démarche de l'auditeur financier ;
- Pour nous-même : la rédaction de ce document nous permettra de mettre en pratique les outils pédagogiques acquis lors de notre formation.

Notre travail sera subdivisé en deux grandes parties. La première sera consacrée tout d'abord à la présentation du cadre théorique de l'audit financier (chapitre 1). Ensuite nous décrirons, de manière détaillée, les dispositions de sécurité qui doivent être mises en place dans une

entreprise utilisant un système informatique (chapitre 2) Enfin, nous proposerons une méthodologie de détermination de l'incidence de la sécurité informatique sur la démarche d'audit financier d'une organisation (chapitre 3).

Dans la deuxième partie, nous mettrons notre méthodologie en pratique à travers l'audit financier de la SAJE. Nous commencerons ainsi par présenter la société (chapitre 1). Puis suivra la description des travaux effectués et des résultats obtenus sur le terrain (chapitre 2). Le dernier chapitre de cette partie (chapitre 3) sera consacré à l'analyse des résultats et la présentation des recommandations que nous formulerons à l'endroit des dirigeants de la SAJE.

PREMIERE PARTIE :

CADRE THEORIQUE

CHAPITRE 1 : AUDIT FINANCIER

Introduction

L'entreprise est le lieu de rencontre de toute une série d'intervenants intéressés par sa performance. Il s'agit notamment des dirigeants, des actionnaires et des tiers (institutions de crédit, autorités publiques, clients et fournisseurs, salariés, etc.) regroupés sous le vocable anglais de *« stakeholders »*. Tous ces intervenants ont besoin d'avoir, à un moment ou à un autre, des informations précises sur l'entité. Mais, généralement, seuls les dirigeants ont un accès direct réel à l'activité de l'entreprise. Ce qui leur confère une liberté d'action et un avantage informationnel important.

L'établissement de comptes annuels est un des moyens mis en place pour contrôler les dirigeants et orienter leur comportement. Les états financiers annuels constituent également une synthèse de l'activité de l'entreprise exploitable par l'extérieur. Ils servent aux différents acteurs dans une optique d'évaluation, de prise de décision ou de diagnostic (RAFFEGEAU & al., 1993).

Toutefois, l'établissement et la diffusion des états financiers par la direction pose un problème de fiabilité (fidélité aux normes comptables de constitution et de présentation) car les dirigeants sont justement les personnes que l'on cherche à contrôler. La latitude dont ils disposent peut laisser planer un doute sur la sincérité de l'information qu'ils diffusent.
Cela explique l'apparition de moyens pour vérifier les états financiers produits par les dirigeants à destination de l'extérieur. Ces moyens se sont progressivement développés pour prendre leur forme actuelle : **l'audit financier** (HERRBACH, 2000 :3).

Aujourd'hui, l'audit est une obligation légale dans de nombreux pays pour les sociétés par actions, ainsi que pour certaines autres entreprises ou organisations en fonction de leur taille ou de leur statut.

Ce chapitre s'articulera autour de deux sections principales :

1. **Caractéristiques et objectif ;**
2. **L'approche d'audit financier.**

1.1. Caractéristiques et objectif de l'audit financier

L'audit financier a été défini par de nombreux organismes et auteurs, notamment l'IFAC, la CNCC, le groupement ATH. L'objectif de ce chapitre étant de rappeler la démarche générale d'audit financier, nous ne donnerons pas ici les définitions institutionnelles. Nous mettrons plutôt l'accent sur les principales caractéristiques qui en ressortent ainsi que sur l'objectif poursuivi lors d'une mission d'audit financier.

1.1.1. Caractéristiques

En analysant les différentes définitions de l'audit financier, MERCIER & al. (2002) font ressortir cinq caractéristiques communes relatives au contenu de l'audit financier et à l'auditeur lui-même :

- L'indépendance de l'auditeur financier ;
- La validation des comptes ;
- Le référentiel de travail ;
- L'expression d'une opinion ;
- La délivrance d'une assurance positive.

1.1.1.1. L'indépendance de l'auditeur financier

L'auditeur financier n'appartient pas à l'entité dont les comptes sont examinés : il doit être par essence indépendant de l'entreprise contrôlée. En particulier, la personne qui participe à l'établissement des comptes ne peut prétendre mettre en œuvre l'audit financier car cela la conduirait à être à la fois juge et partie.

1.1.1.2. La validation des comptes

L'audit financier a pour objet la validation de comptes ou d'états financiers établis par l'entité qui en fait l'objet. Les termes utilisés par l'auditeur qui opère cette validation ont pu varier au fil des ans : le commissaire aux comptes statuait, il n'y a pas si longtemps, sur la « régularité et la sincérité » des comptes. Il s'exprime aujourd'hui sur l'image fidèle que donnent, ou ne

donnent pas, les comptes qui ont fait l'objet de son examen. Dans un cas, comme dans l'autre, pourtant, la même idée ressort : les états comptables sont la traduction chiffrée de la situation d'une entreprise à un moment donné, et de la vie qu'elle a menée durant les mois qui ont précédé leur établissement. Le travail de l'auditeur consiste à examiner ces états pour s'assurer qu'ils ne trahissent pas la réalité.

1.1.1.3. Le référentiel de travail

L'auditeur apprécie la qualité des comptes par rapport à un référentiel déterminé. Les comptes sont la traduction d'une réalité et en tant que tels, ils impliquent l'utilisation d'un certain nombre de conventions, d'un langage, qui est constitué en pratique par l'ensemble de normes et principes comptables que l'auditeur prend comme référence pour en apprécier la validité.

1.1.1.4. L'expression d'une opinion

L'auditeur financier fait connaître son opinion dans un rapport écrit. L'opinion exprimée doit être motivée, étayée. L'auditeur ne livre pas une impression, un sentiment plus ou moins fugace pouvant dépendre de son humeur du moment : il doit exprimer l'intime conviction acquise, au terme d'une démarche structurée, par un professionnel compétent.

1.1.1.5. La délivrance d'une assurance positive

Enfin, l'auditeur financier porte un jugement sur les états financiers en délivrant une assurance positive. L'auditeur formule son opinion en utilisant la formule « donne une image fidèle » ou « présente sincèrement sous tous les aspects significatifs », ce qui l'engage bien davantage qu'un simple constat d'absence d'anomalies, qui donnerait une assurance négative sur la fiabilité des comptes…

1.1.2. Objectif

D'après MIKOL (1999), l'objectif attendu du processus d'audit est la *« certification »* des comptes annuels de l'entreprise, c'est-à-dire – si l'on se place dans le contexte terminologique français – la reconnaissance de leur *« régularité »* et de leur *« sincérité »* afin de fournir une

« *image fidèle* » des opérations de l'exercice écoulé et de la situation financière à la fin de cet exercice :

- la régularité est la conformité des comptes à la réglementation et aux principes comptables généralement admis ;
- la sincérité est l'application de bonne foi des règles et des procédures comptables en fonction de la connaissance que les responsables des comptes ont de la réalité ;
- le respect de l'image fidèle consiste à choisir, parmi les méthodes de présentation ou de calcul envisageables, les mieux adaptées à la réalité de l'entreprise et à fournir les informations nécessaires à leur compréhension, en particulier dans le cadre de l'annexe.

Pour MERCIER & al. (2002 : 386), l'audit financier a pour vocation de donner à l'information financière la crédibilité indispensable à un fonctionnement régulier de l'économie.

En effet, le droit à l'information financière n'est plus considéré aujourd'hui comme réservé aux dirigeants ou aux associés des entreprises. Les salariés, les tiers qui travaillent avec l'entreprise (banque, clients, fournisseurs…), les administrations publiques (fisc, sécurité sociale), les investisseurs potentiels, les autorités de régulation, les agences de cotation, etc., attendent également, des entreprises, la production d'une information pouvant servir de base à leurs décisions. Il est donc essentiel, sous peine d'occasionner des préjudices majeurs, que l'information publiée soit fiable.

Les états financiers des entreprises sont établis sous la responsabilité des dirigeants. Ceux-ci, compte tenu de leur position, sont soumis à des contraintes et pressions (implication totale dans la vie de l'entreprise, optimisation fiscale aux dépens de l'image fidèle, prestations jugées par les actionnaires à travers les états financiers). Cette situation paraît difficilement compatible avec l'indépendance requise pour donner une crédibilité suffisante à l'information financière.

L'audit financier confère donc une utilité réelle aux états financiers en donnant à ceux qui l'utilisent une sécurité suffisante dans la prise de leurs décisions.

Par ailleurs, l'audit financier est un des éléments essentiels du bon fonctionnement de l'économie de marché. L'importance attachée aux conclusions des auditeurs légaux par les marchés de capitaux a pu être démontrée au vu des résultats de plusieurs études empiriques réalisées dans des pays anglo-saxons et en France.
Les cours de bourse des actions autour des dates auxquelles les auditeurs légaux émettent des rapports comportant des réserves réagissent de manière négative, et significative, aux informations contenues dans le rapport d'audit. Cette réaction témoigne du crédit accordé par les investisseurs aux réserves formulées dans les rapports (SOLTANI, 1996).

HERRBACH (2000 : 18) rappelle que dans d'autres pays, les objectifs assignés à l'audit sont généralement similaires à ceux présentés précédemment. Aux Etats-Unis, par exemple, « l'objectif de l'examen des états financiers par l'auditeur est la formulation d'une opinion sur l'image qu'ils donnent de la situation financière, des résultats des opérations, de l'évolution de la situation financière eu égard aux principes comptables généralement admis » (AICPA : American Institute of Certified Public Accountants).

1.2. L'approche d'audit financier

L'approche d'audit financier renvoie bien souvent aux différentes étapes de la mission. Mais au préalable, il nécessaire de présenter les principes qui régissent l'audit financier.

1.2.1. Principes fondamentaux

Deux (2) principes caractérisent la démarche de l'auditeur financier :

- une méthodologie utilisée fondée sur l'approche par les risques ;
- et l'émission d'une opinion motivée.

1.2.1.1. Approche par les risques

L'approche par les risques suppose que soient distingués les points qui, présentant un risque, doivent faire l'objet d'un contrôle approfondi, de ceux qui, ne soulevant pas de difficultés particulières, peuvent être validés en procédant à des vérifications allégées.

La méthodologie de l'approche par les risques repose sur trois (3) composantes de base :

- La première est la définition de critères de référence servant de support à la recherche et à l'appréciation des risques susceptibles de remettre en cause la certification des comptes : ces critères sont constitués par les assertions d'audit ;
- La deuxième est l'identification des risques propres à remettre en cause ces assertions : dans ce but, l'auditeur détermine les risques qui, d'une part, sont susceptibles de se produire et qui, d'autre part, présente un caractère significatif ;
- Enfin, la troisième et dernière composante de cette approche est la gestion par l'auditeur des risques affectant les états financiers : celui-ci adapte ses diligences en vue de réduire au minimum son propre risque d'audit, qui est d'émettre une opinion erronée sur les états financiers.

1.2.1.1.1. Les assertions d'audit

Les assertions sous-tendant l'établissement des comptes sont définies par la CNCC comme « un ensemble de critères, explicites ou non, retenus par la direction dans la préparation des comptes » (Normes CNCC 0-200, Lexique). Ces assertions, dont le contenu est défini par référence aux actifs et aux passifs détenus par l'entreprise, aux opérations mises en œuvre et aux informations données par l'entité concernée, sont au nombre de sept (7) :

- **Existence** : actif ou passif existant à une date donnée ;
- **Droits et obligations** : actif ou passif se rapportant à l'entité à une date donnée ;
- **Rattachement** : ensemble des actifs, des passifs, des opérations ou des évènements enregistrés de façon complète et tous faits importants correctement décrits ;
- **Exhaustivité** : ensemble des actifs, des passifs, des opérations ou des évènements enregistrés de façon complète et tous faits importants correctement décrits ;
- **Evaluation** : valorisation d'un actif ou d'un passif à sa valeur d'inventaire ;
- **Mesure** : correcte imputation comptable suivant les règles en vigueur et pertinence de l'information financière ;
- **Présentation et informations données** : informations présentées, classées et décrites selon le référentiel comptable applicable.

1.2.1.1.2. Identification des risques pesant sur les assertions

La démarche d'identification des risques retenue par l'auditeur financier comprend généralement :

- *Une identification des erreurs potentielles* : l'erreur potentielle est l'erreur qui pourrait théoriquement survenir si aucun contrôle n'était mis en place pour l'empêcher ou la détecter. Elle est usuellement associée à la notion de risque inhérent. La CNCC (2003 : 8) définit le risque inhérent comme étant « la possibilité que le solde d'un compte ou qu'une catégorie d'opérations comporte des anomalies significatives isolées ou cumulées avec des anomalies dans d'autres soldes ou catégories d'opérations, nonobstant les contrôles internes existants » ;
- *Une identification des erreurs possibles* : l'erreur possible est l'erreur qui peut effectivement se produire compte tenu de l'absence de contrôle dans l'entreprise pour l'empêcher, la détecter et ensuite la corriger. Elle est généralement associée au risque lié ou risque de non maîtrise. Le risque de non maîtrise peut être défini comme le risque qu'une anomalie dans un solde de compte ou dans une catégorie d'opérations, prise isolément ou cumulée avec des anomalies dans d'autres soldes de comptes ou d'autres catégories d'opérations, soit significative et ne soit ni prévenue, ni détectée par les systèmes comptables et de contrôle interne et donc non corrigée en temps voulu (CNCC, 2003) ;
- *La détermination du caractère significatif des erreurs possibles* : l'auditeur est ainsi amené à définir non seulement l'importance relative des systèmes et domaines sur lesquels il est appelé à intervenir, mais également un seuil de signification, à partir duquel il ne peut délivrer sa certification.

1.2.1.1.3. Gestion du risque d'audit

Pour expliciter la notion de risque d'audit, nous retiendrons la définition donnée par l'IFAC dans la Norme internationale d'audit ISA 400 (CHARRON, 1998). Pour cette institution, le risque d'audit est « le risque que l'auditeur financier exprime une opinion incorrecte sur les états financiers soumis à son contrôle du fait d'erreurs significatives contenues dans ces états ».

L'IFAC et la CNCC subdivisent le risque d'audit en trois composantes :

- risque inhérent ;
- risque lié au contrôle ou risque de non maîtrise ;
- risque de non détection.

L'objectif de l'auditeur à ce niveau est de ramener le risque d'audit à un niveau suffisamment faible pour être acceptable. Il applique pour y parvenir un modèle de gestion du risque d'audit qui se présente comme suit :

Risque d'audit	=	Risque inhérent	×	Risque lié au contrôle	×	Risque de non détection

Comme le montre le tableau ci-dessous, la gestion du risque d'audit consiste à définir la nature et l'étendue des contrôles à mettre en œuvre (programme de travail) en fonction du risque d'erreur attaché aux états financiers, c'est-à-dire de l'importance du risque des erreurs possibles.

***Tableau N° 1** : Nature et étendue des travaux d'audit suivant le niveau de risque relevé*

Evaluation par l'auditeur du risque lié au contrôle / **Evaluation par l'auditeur du risque inhérent**	*Elevé*	*Moyen*	*Faible*
Elevé	**Maximum**	**Elevé**	**Moyen**
Moyen	**Elevé**	**Moyen**	**Faible**
Faible	**Moyen**	**Faible**	**Minimum**

Les zones grisées correspondent au niveau des diligences à mettre en œuvre.

Source : MERCIER & al. (2002)

Le modèle de gestion du risque d'audit global doit être mis en œuvre tout au long de la mission. Cependant, en pratique, la fixation du niveau de diligence intervient à deux (2) moments privilégiés dans la démarche d'audit : lors de l'élaboration du plan de mission et à l'issue des travaux sur le risque inhérent et le risque lié.

1.2.1.2. Emission d'une opinion motivée

L'émission d'une opinion motivée repose fondamentalement sur la collecte par l'auditeur d'éléments probants de nature à justifier son opinion. Celle-ci doit donner lieu à une documentation des travaux qui se traduit par l'établissement d'un dossier de travail. Enfin, l'opinion, peut s'appuyer, dans certaines conditions, sur les travaux mis en œuvre par d'autres professionnels.

1.2.1.2.1. Collecte d'éléments probants

Les éléments probants sont obtenus à partir d'une combinaison appropriée :

- des tests de procédures (tests permettant de collecter des éléments probants sur l'efficience de la conception des systèmes comptables et de contrôle interne ainsi que sur l'efficacité du fonctionnement des contrôles internes pendant toute la période considérée) ;
- et des contrôles substantifs (procédures visant à collecter des éléments probants permettant de détecter des anomalies significatives dans les comptes).

Les techniques de collecte d'éléments probants sont généralement les suivantes (CNCC, 1995) :

- ✓ *inspection* (examen des livres comptables, de documents ou d'actifs physiques) ;
- ✓ *observation physique* (examen des procédures et de la façon dont elles sont exécutées) ;
- ✓ *demandes d'informations ou d'explications et demandes de confirmation* (circularisation auprès des tiers, demande d'information dans l'entreprise auditée) ;
- ✓ *mise en œuvre de calculs sur les pièces justificatives et documents comptables* ;
- ✓ *accomplissement de procédures analytiques* (comparaisons, analyses de variations et tendances…).

1.2.1.2.2. Documentation des travaux

L'auditeur doit constituer, pour chaque entreprise, un dossier de travail à conserver pendant dix (10) ans. Les dossiers de travail sont couverts par le secret professionnel et ne peuvent être communiqués qu'aux seules personnes auxquelles le secret professionnel ne peut être opposé (acteurs de l'entreprise, confrères, collaborateurs et experts, organes de contrôle de l'environnement institutionnel, autorités du monde judiciaire).
On distingue :

1.2.1.2.3. Utilisation des travaux d'autres professionnels

L'auditeur financier peut s'appuyer sur les travaux mis en œuvre par les autres professionnels pour justifier son opinion. Ainsi, il peut utiliser des travaux :

- réalisés par un expert : « personne ou cabinet qui possède des compétences, des connaissances et une expérience spécifiques dans un domaine particulier autre que la comptabilité et l'audit » (Norme ISA 620) ;
- mis en œuvre par l'expert-comptable ;
- mis en œuvre par l'auditeur interne.

1.2.2. Déroulement de l'audit financier

La démarche de l'audit financier est une démarche intellectuelle qui suit une progression logique en vue d'atteindre le niveau d'assurance requis pour l'accomplissement de la mission confiée à l'auditeur financier. La mission d'audit se déroule selon une approche composée des quatre (4) phases suivantes :

- la prise de connaissance de l'entité contrôlée ;
- l'évaluation du contrôle interne ;
- la révision des comptes ;
- la finalisation et l'émission des rapports.

1.2.2.1. Phase de prise de connaissance

Cette phase permet à l'auditeur financier de comprendre l'entreprise et l'environnement dans lequel elle évolue, d'évaluer les risques inhérents au secteur d'activité et aux caractéristiques générales de l'entreprise et d'identifier les cycles significatifs. Elle comporte, en association avec l'évaluation du risque inhérent, une évaluation préliminaire du risque lié au contrôle pour déterminer le risque de non détection acceptable. Cette démarche permet à l'auditeur d'établir un plan de mission qui contient notamment la description des risques identifiés, les cycles concernés et l'approche d'ensemble envisagée pour l'audit.

L'auditeur peut utiliser les outils et techniques suivants : base de données sectorielles, entretien avec les principaux responsables de l'entreprise, visite des locaux, connaissance spécifique de l'environnement informatique, examen analytique des comptes, examen des principaux documents juridiques, entretien avec les précédents commissaires aux comptes, questionnaire de prise de connaissance.

A l'issue de cette phase, l'auditeur établit la lettre de mission, adressée à l'entreprise auditée, dans laquelle il expose les travaux qu'il a décidé de mettre en œuvre pour accomplir sa mission.

1.2.2.2. Evaluation du contrôle interne

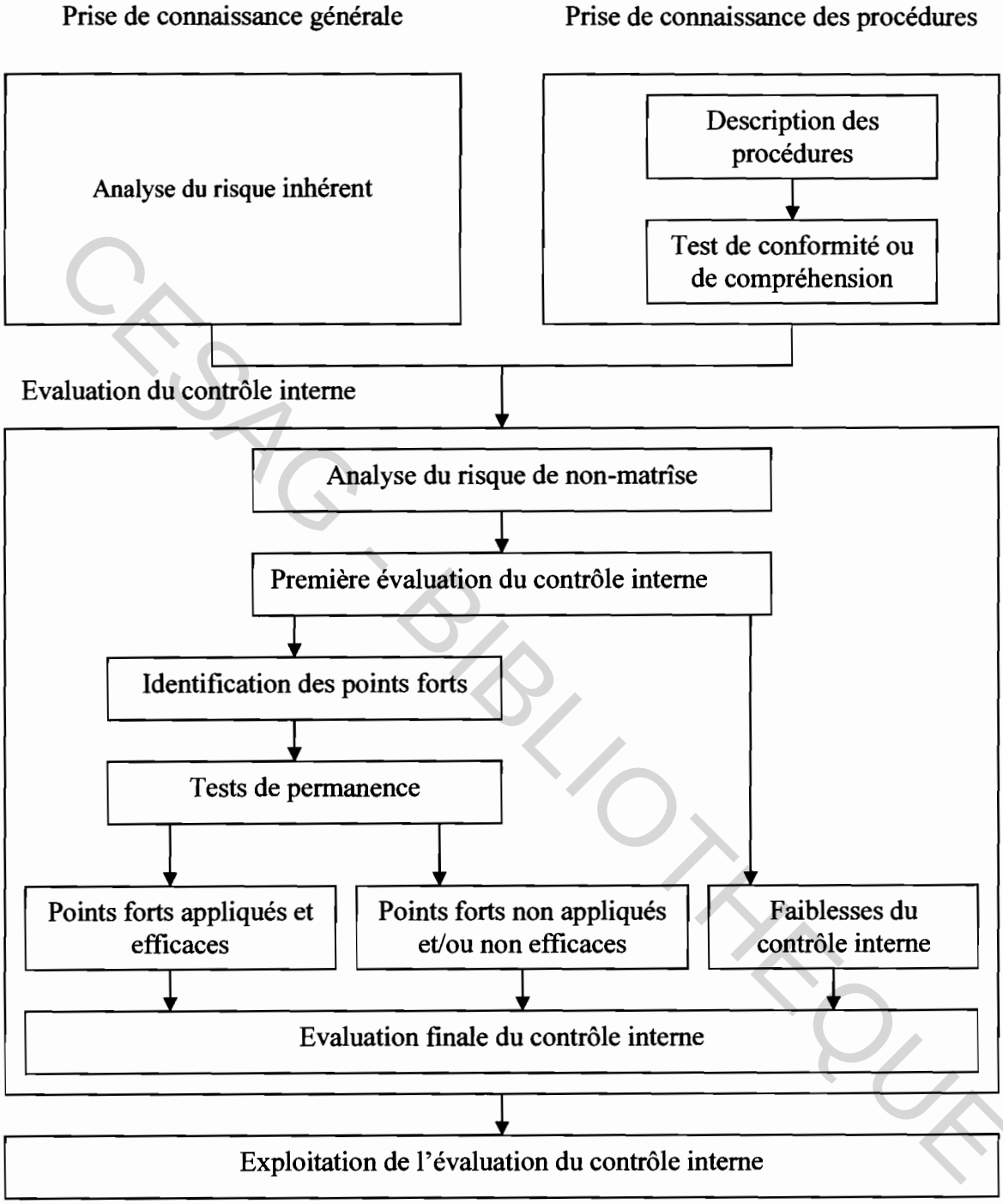
D'après la définition donnée par la Commission Treadway (1992), le contrôle interne peut être considéré comme « un processus mis en œuvre par le conseil d'administration, les dirigeants et le personnel d'une organisation, destiné à fournir une assurance raisonnable quant à la réalisation des objectifs suivants :

- la réalisation et l'optimisation des opérations ;
- la fiabilité des informations financières ;
- la conformité aux lois et règlements en vigueur ».

La phase d'évaluation du contrôle interne permet à l'auditeur d'évaluer les procédures et les systèmes, manuels ou informatisés, utilisés par l'entreprise. Durant cette phase, l'auditeur approfondit la première évaluation du contrôle interne qu'il a réalisé lors de la prise de connaissance générale de l'entreprise. Cette démarche lui permet de statuer définitivement sur la capacité des procédures en place à minimiser les risques inhérents identifiés et d'en déduire les risques d'erreurs possibles sur les états financiers audités.
Les grandes étapes de cette évaluation, présentées dans le schéma suivant, sont :

- la prise de connaissance des procédures ;
- l'évaluation du contrôle interne ;
- l'exploitation de l'évaluation du contrôle interne.

***Figure N° 1* : Démarche d'évaluation du contrôle interne**



Source : MERCIER & al. (2002) (adaptée)

A l'issue de cette phase, l'auditeur détermine, conformément au modèle de gestion du risque d'audit global, le niveau des contrôles substantifs nécessaires pour que le risque d'audit soit acceptable.

1.2.2.3. Révision des comptes

Les travaux de révision comptable ont pour objectif de collecter des éléments probants en quantité suffisante pour pouvoir se prononcer sur les assertions d'audit. Les diligences correspondantes doivent être intégrées dans la démarche d'ensemble de l'auditeur financier.

Cette phase comprend essentiellement deux (2) types de contrôles substantifs dont l'ampleur est définie à l'issue de l'évaluation du contrôle interne :

- les procédures analytiques : comparaisons entre montants, vérification de cohérence par rapport à la connaissance générale de l'entité, calcul de ratios usuels ;
- les contrôles portant sur le détail des opérations et les soldes.

A l'issue de la phase de révision, l'auditeur a acquis une opinion sur le respect des assertions d'audit.

1.2.2.4. Finalisation de la mission

La finalisation de la mission se décompose en quatre (4) parties :

- la vérification de la qualité des informations fournies dans l'annexe aux états financiers ;
- l'examen des évènements postérieurs à la clôture afin de s'assurer que ceux-ci ne sont pas susceptibles de mettre en cause l'opinion sur les états financiers ;
- la communication de l'auditeur avec la gouvernance d'entreprise sur les travaux et ses conclusions ;
- l'émission du rapport exprimant son opinion sur les comptes audités.

Les différentes phases exposées plus haut peuvent être récapitulées dans le tableau suivant :

Tableau N° 2 : Tableau récapitulatif de l'approche d'audit financier par phase

	Phases	Etapes clés	Objectifs
1	Connaissance et compréhension de l'entreprise	- Prise de connaissance générale et par cycle - Examen analytique - Première évaluation du risque inhérent et du risque lié	- Plan de mission (définition de l'approche d'audit) - Lettre de mission
2	Evaluation du contrôle interne	- Prise de connaissance des procédures de contrôle interne et test de conformité - Mise en œuvre de tests de procédures (sur les points forts)	- Evaluation du contrôle interne - Adaptation de l'approche d'audit et du programme de révision des comptes
3	Révision des comptes	- Mise en œuvre de contrôles substantifs et de procédures analytiques conformément au programme défini	- Conclusion sur les assertions d'audit - Préparation de l'opinion sur les comptes
4	Finalisation des travaux	- Contrôle de l'annexe - Examen des évènements post-clôture - Communication avec la gouvernance d'entreprise - Emission des rapports	- Opinion sur les états financiers

Source : MERCIER & al. (2002)

Conclusion du chapitre

L'audit financier, dont l'objectif est la certification des comptes financiers des entreprises par un professionnel, selon des normes généralement reconnues, est en définitive une activité menée suivant une méthodologie intellectuelle et logique. Cette méthodologie a été adoptée par les professionnels dans le but d'obtenir une assurance raisonnable que l'information financière qu'ils examinent présente les caractéristiques requises.

La démarche de l'audit financier décrite dans ce chapitre est d'autant plus efficace qu'elle a été à l'origine des méthodologies utilisées dans la plupart des audits opérationnels : achats, immobilisations, marketing, paie, stocks, ventes,etc.

CHAPITRE 2 : SECURITE INFORMATIQUE

Introduction

Devant la dépendance, sans cesse accrue, des entreprises envers l'informatique et la mondialisation des réseaux d'échange, la sécurité devient indispensable à la bonne marche de la plupart des organisations.

L'enquête « Computer Crime and Security Survey » publiée en mars 2000 aux Etats-Unis par le Computer Security Institute (CSI) et le Federal Bureau of Investigation (FBI), sur un échantillon de 643 organisations, confirme ce fait. En effet, selon les résultats obtenus, 90% des entreprises interrogées ont connu un bris de sécurité informatique au cours de l'année 1999. Par ailleurs, trois-quarts de ces organisations reconnaissent avoir subi des pertes financières dues à des bris de sécurité informatique. La valeur de ces pertes, pour les quelques 47% d'organisations étant en mesure de les chiffrer, totalise 266 millions de dollars américains (CEFRIO, 2005).

D'après l'IFACI (1993 : 8-1), la nécessité d'une protection adéquate du système informatique se justifie par « l'importance du matériel et des données pour l'organisation ». Ces données sont d'une importance stratégique du fait qu'elles constituent la base de la prise de décision au sein de l'entreprise. Par conséquent, garantir leur sécurité revient à :

- Protéger la réputation de l'entreprise ;
- Eviter des pertes financières ;
- Satisfaire aux exigences légales… (GODART, 2002).

Il faut également souligner que la sécurité du système d'information au sein d'une entreprise concerne tous les intervenants de l'entité, à savoir, l'ensemble du personnel (utilisateurs), les responsables informatiques (administrateurs réseaux et systèmes) et la direction générale.

L'objectif de ce chapitre est d'apporter de plus amples précisions sur les trois points cités précédemment. Il sera divisé en deux grandes sections :

1. **La gestion de la sécurité;**
2. **La sécurité physique et la sécurité logique.**

2.1. La gestion de la sécurité

La gestion de la sécurité informatique d'une entité implique tout d'abord une identification claire des besoins. En effet l'entreprise doit déterminer les différents aspects de son système d'information qui nécessitent une protection.
Ces besoins permettront par la suite de recenser les risques auxquels sont exposées l'entité et les moyens de protection à mettre en œuvre.

2.1.1. Les besoins de sécurité

Toute entreprise se doit de mettre en place un système de protection dès l'instant où elle décide de baser son activité sur l'informatique (matériel et/ou logiciels). En effet, l'informatisation implique un investissement financier important en matériel et une accessibilité accrue aux données sensibles de la structure.

L'importance du matériel est aisément perceptible mais celle des données stockées ou traitées est plus subtile. L'information contenue dans le système informatique d'une entreprise revêt un caractère « précieux » pour les raisons suivantes : (IFACI, 1993)

2.1.1.1. Importance stratégique

Il peut s'agir de listes de clients ou de prix, de secrets industriels (ex : formules des produits), d'annonces de produits, d'informations sur les prix de revient de certains produits ou services.

2.1.1.2. Aide à la décision

En mettant en place un système informatique de gestion, l'un des objectifs principaux visés par la direction générale est de faciliter la prise de décisions financières et opérationnelles. Le système doit donc contenir et traiter les données nécessaires à cela.

2.1.1.3. Confidentialité

Le caractère confidentiel de certaines données informatiques peut être déterminé par :

- Un impératif légal (ex : données concernant les ressources humaines) ;
- Une requête provenant d'un tiers (ex : données liées à des contrats avec le gouvernement) ;
- Etc.

2.1.1.4. *Respect de la législation*

La protection des données informatiques peut être exigée par la législation. Les systèmes d'information sont généralement soumis aux trois catégories de lois suivantes :

- Le droit pénal ;
- Les responsabilités des sociétés ;
- La confidentialité des données privées.

En ce qui concerne la sécurité informatique en particulier, on peut citer la délibération N° 81-94 du 21 juillet 1981 de la Commission Nationale de l'Informatique et des Libertés (CNIL française) qui recommande « qu'un soin tout particulier soit apporté à définir les dispositions destinées à assurer la sécurité et la confidentialité des traitements et des informations… ».

Les différentes raisons exposées précédemment sont autant de paramètres qui rendent nécessaire la mise en place d'un bon système sécuritaire afin d'assurer la protection du matériel et des données informatiques. Cette tâche relève de la responsabilité de la direction générale de l'entreprise qui doit :

- évaluer les risques auxquels est exposé ou peut être exposé le système d'information ;
- établir la politique de sécurité ;
- et veiller à la mise en œuvre d'une structure organisationnelle permettant d'attendre les objectifs sécuritaires.

2.1.2. La gestion des risques liés à la sécurité des systèmes d'information

La sécurité informatique vise à protéger l'entreprise contre les risques liés à l'informatique, pouvant être fonction de plusieurs éléments :

- les menaces qui pèsent sur les actifs à protéger ;
- la vulnérabilité de ces actifs ;

- la sensibilité de ceux-ci.

Si l'un des éléments est nul, le risque n'existe pas. C'est pourquoi, l'équation est généralement représentée par :

Risque = Menaces × Vulnérabilités × Sensibilité

Les principales menaces effectives auxquelles l'on peut être confronté sont :

- *l'utilisateur* : la majorité des problèmes liés à la sécurité d'un système d'information (70% en 2003 selon le Ministère français de l'Economie et des Finances) est due aux utilisateurs internes (par insouciance ou malveillance) ;
- *les programmes malveillants* : un logiciel destiné à nuire ou à abuser des ressources du système est installé (par mégarde ou par malveillance) sur le système, ouvrant la porte à des intrusions ou modifiant les données (**Cf. Annexe 1, page 93**) ;
- *l'intrusion* : une personne parvient à accéder à des données ou à des programmes auxquels elle n'est pas censée avoir accès ;
- *un sinistre (vol, incendie, dégât des eaux)* : une mauvaise manipulation ou une malveillance entraînant une perte de matériel et/ou de données.

Face à toutes ces menaces, toute organisation doit mettre en place un processus continu de gestion des risques liés au système d'information. En effet, pour être efficace, ce processus doit être régulièrement revu afin de prendre en compte l'évolution du système d'information et de son environnement. Il consiste à :

- Evaluer les risques ;
- Traiter les risques ;
- Et établir une communication relative aux risques (GRALL et GALLET, 2003).

2.1.2.1. *Evaluation des risques*

Comme le souligne L'Organisation de Coopération et de Développement Economiques - OCDE (2002 :7), « Du fait de leur connectivité croissante, les systèmes et réseaux d'information sont désormais exposés à un nombre croissant et à un éventail plus large de

menaces et vulnérabilités, ce qui pose de nouveaux problèmes de sécurité ». Cette organisation a adopté, en 2002, des lignes directives régissant la sécurité des systèmes et réseaux d'information s'adressant à « l'ensemble des parties prenantes à la nouvelle société de l'information… ».

Ces lignes directives font apparaître neuf (9) principes relatifs à la sécurité informatique parmi lesquels l'évaluation des risques. Ce principe rappelle qu'il convient d'analyser les risques en termes d'importance des informations à protéger, de menaces, de vulnérabilités et de préjudices possibles. Cela permet de déterminer un niveau acceptable de risque et des mesures de sécurité appropriées.

L'évaluation des risques doit considérer non seulement la technologie, mais aussi les aspects physiques, humains et organisationnels tels que « les politiques et services de tierces parties ayant des implications sur la sécurité », ainsi que « les préjudices des intérêts d'autrui ou causés par autrui rendus possibles par l'interconnexion croissante des systèmes d'information » (OCDE, 2002).

Par ailleurs, l'IFACI (1993 : 8-3) précise qu'« en cas de modification importante au sein de l'organisation, il convient de réévaluer les facteurs de risques afin de déterminer leur impact sur la structure de sécurité ».

2.1.2.2. *Traitement des risques*

L'évaluation de l'importance des risques informatiques permet de procéder à leur traitement, c'est-à-dire :

- Soit réduire ces risques à l'aide de mesures de sécurité ;
- Soit les transférer (par exemple en sous-traitant des activités) ;
- Ou les accepter consciemment (GRALL et GALLET, 2003).

Dans l'hypothèse d'une conception et mise en œuvre de la sécurité, l'OCDE préconise la mise en place « de mesures de protection et solutions qui doivent être à la fois techniques et non techniques et être proportionnées à la valeur de l'information dans les systèmes et réseaux d'information de l'organisation ».

Il est alors nécessaire de définir, dans un premier temps, **une politique de sécurité**, c'est-à-dire :

- élaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation ;
- définir les actions à entreprendre et les personnes à contacter en cas de détection d'une intrusion ;
- sensibiliser les utilisateurs aux problèmes liés à la sécurité des systèmes d'information.

La politique de sécurité est donc l'ensemble des orientations suivies par une entité en terme de sécurité. A ce titre, elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système (WIKIPEDIA, 2005).

Par ailleurs, l'utilisation de l'outil informatique entraîne également la nécessité absolue d'**un plan de continuité** de l'informatique. Ce plan a pour principaux objectifs :

- *La garantie de la continuité du fonctionnement de l'organisation* en cas de panne prolongée afin d'éviter ou de limiter les pertes de biens physiques et de données ;
- *La réduction de la durée d'indisponibilité des données* afin de diminuer le risque de discontinuité des opérations, d'incapacité à satisfaire les clients, de pertes d'opportunités commerciales et techniques ;
- *Le respect des obligations légales :* notamment les obligations commerciales, (contractuelles ou non), les obligations envers les actionnaires, employés ou commettants, les conditions statutaires et réglementaires (IFACI, 1993).

2.1.2.3. *Communication relative aux risques*

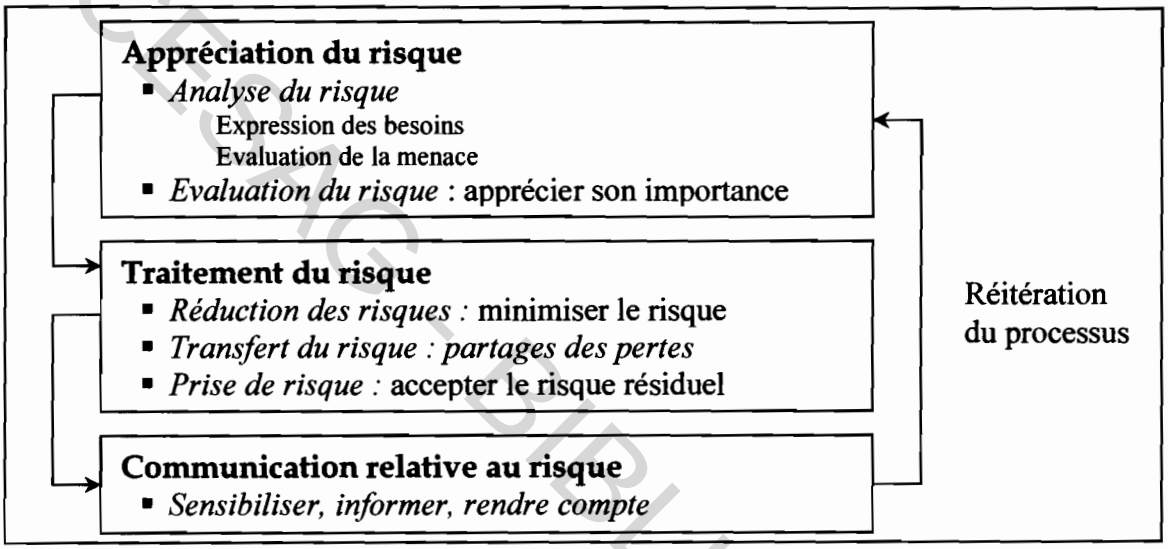
Un bon système de gestion des risques informatiques doit comprendre un volet « Communication » à l'endroit des décideurs, des membres du personnel et des partenaires afin de sensibiliser, d'informer et de rendre compte.

En effet, d'après l'OCDE (2002), toutes les parties prenantes du système d'information doivent « comprendre que les défaillances de sécurité peuvent gravement porter atteinte aux systèmes et réseaux sous leur contrôle mais aussi, du fait de l'inter connectivité et de l'interdépendance, à ceux d'autrui ». Elles doivent également réfléchir à la configuration de

leur système, aux mises à jour disponibles pour ce dernier, à la place qu'il occupe dans les réseaux, aux bonnes pratiques qu'elles peuvent mettre en œuvre pour renforcer la sécurité.

Par ailleurs, il convient d'établir des procédures de compte-rendu en cas d'incident de sécurité. Ces comptes-rendus doivent être régulièrement adressés aux propriétaires de données (IFACI, 1993).

Figure N° 2 : Processus de gestion des risques de sécurité de systèmes d'information



Source : GRALL et GALLET (2003)

En définitive, la mise en place d'une structure de contrôle de la sécurité informatique doit concourir à atteindre les objectifs de sécurité suivants :

- *La confidentialité* : l'information détenue ou conservée ne doit pas être accessible ou divulguée aux personnes non autorisées ou à des fins non prévues ;
- *Authentification :* la personne ou tout autre entité est bien celle qu'elle prétend être ;
- *Non - répudiation :* il est impossible de nier qu'une transaction a eu lieu, puisqu'il existe suffisamment de preuves que la transaction a été effectuée ;
- *Disponibilité :* une information ou un système doit être accessible et utilisable en temps voulu ;
- *L'intégrité :* l'information doit être complète et autorisée. Elle doit être non modifiable et non altérable (VEZINA, 2001).

2.2. La sécurité physique et la sécurité logique

Les mesures de sécurité permettant d'assurer ces caractéristiques peuvent être regroupées en deux (2) catégories principales : la sécurité physique des systèmes et réseaux et la sécurité logique des données et des ressources.

2.2.1. La sécurité physique

La sécurité physique est la première garante de l'intégrité des systèmes informatiques (DELSOL, 1999). Les zones sensibles nécessitant un contrôle physique ne sont pas seulement les zones de travail et d'exploitation informatiques, mais également celles qui abritent l'équipement logistique.

La sécurité physique doit prendre en compte les points suivants :

- Accès physique ;
- Dangers liés à l'environnement ;
- Incendies et inondations.

2.2.1.1. *Accès physique*

De manière générale, la plupart des organisations recherchent avant tout à contrôler l'accès des zones informatiques. Mais elles n'envisagent pas toujours de se pencher sur l'accès aux zones pourvues de lignes téléphoniques, d'alimentations électriques ou des commandes de chauffage et de refroidissement. En effet, ces zones peuvent permettre à des personnes non autorisées d'accéder au système de l'entreprise ou au matériel informatique.

Il convient donc d'installer de systèmes de surveillance pour les visiteurs comme pour les employés (y compris le personnel de sécurité et maintenance), qui peuvent demander une autorisation d'accès aux zones réservées. Les dispositifs physiques de contrôle d'accès qui peuvent être mis en place sont les suivants :

- badges d'identification avec photo ;
- badges optiques ;
- reconnaissance physique par la voix, l'iris ou les empreintes ;

- cartes électroniques.

Par ailleurs, tous les points d'entrée et de sortie potentiels des zones sensibles doivent être dotés d'alarmes. Toutes les alarmes et les autres dispositifs de sécurité électroniques doivent être connectés à une alimentation de secours qui leur permet de fonctionner en cas de coupure de courant (IFACI, 1993).

2.2.1.2. *Dangers liés à l'environnement*

Ces dangers peuvent être d'origine humaine ou naturelle. Il est donc nécessaire de sécuriser aussi bien l'environnement physique que l'environnement d'exploitation spécifique.

Les dispositions suivantes devront, par conséquent, être prises :

- L'organisation ne doit pas être située :
  - ✓ à proximité d'autres entreprises qui représentent une menace potentielle (raffineries, usines chimiques…) ;
  - ✓ dans les zones sujettes à des catastrophes naturelles telles que les tremblements de terre, les tornades… ;
- L'alimentation électrique des équipements informatiques doit être stable et continu. Une source de courant de secours fiable doit être également disponible ;
- Au niveau des zones du système d'information, la concentration en poussière, le taux d'humidité, la chaleur, la lumière doivent faire l'objet d'une surveillance continue. En effet, un taux d'humidité élevé peut endommager le matériel électronique. Il faudra également veiller au bon fonctionnement des systèmes de climatisation et de régulation de température ;
- Des procédures doivent être mises en place pour éviter la réalisation d'attaques terroristes ou gérer leurs conséquences, le cas échéant.

2.2.1.3. *Incendies et inondations*

Les incendies et les inondations, ainsi que les dommages occasionnés par les méthodes de lutte contre l'incendie (eau et fumée), représentent les deux causes les plus fréquentes de dommages subis par les matériels et les données informatiques. Dans la majorité des cas, les

dégâts liés au feu sont causés par la défaillance du dispositif anti-incendie tandis que les inondations ont pour origine une rupture des canalisations d'évacuation ou de refroidissement qui passent dans les plafonds , les murs ou les sols de la salle informatique.

Afin d'assurer la protection du système informatique contre les incendies et les inondations, les dispositions suivantes doivent être prises :

- Les canalisations d'eau et d'évacuation ainsi que les réservoirs d'eau doivent être éloignés des zones d'exploitation du système d'information ;
- Les vannes d'arrêts et le matériel de détection d'humidité doivent être fréquemment contrôlés afin d'en assurer le bon fonctionnement ;
- L'organisation doit se doter d'un certain nombre d'extincteurs manuels ;
- Le matériel de détection de fumée et d'extinction automatique d'incendie doit être régulièrement vérifié, et testé (ces tests devront toujours être documentés) ;
- Les issues de secours doivent être faciles à détecter ;
- Prévoir des cloisons pare-feu dans les locaux pour limiter la propagation d'incendies éventuels dans les zones et les bâtiments adjacents.

2.2.2. La sécurité logique

La propagation de l'utilisation des réseaux de télécommunication a vite montré que les dispositifs de contrôle physique ne suffisent pas à assurer une protection optimale des systèmes d'information. L'interconnexion sans cesse grandissante des installations informatiques ont amené les organisations à mettre en place d'autres types de contrôles, basés ceux-ci sur les logiciels, dans le but d'assurer leur sécurité logique.

« La sécurité logique permet à l'entreprise d'identifier l'utilisation des données et des ressources et de produire des pistes d'audit de l'activité du système et des utilisateurs » (JENKINS & al., 1984). De cette définition découlent les trois tâches principales que doit remplir un bon dispositif de sécurité logique :

- Identifier individuellement et authentifier les utilisateurs des données et des ressources ;
- Limiter l'accès à des données ou des ressources spécifiques ;
- Produire des pistes d'audit de l'activité du système et des utilisateurs.

2.2.2.1. *Identification et authentification des utilisateurs*

L'IFACI (1993) souligne qu'une bonne sécurité logique doit comprendre des dispositifs qui permettent de distinguer un quelconque utilisateur des autres (identification) et de s'assurer que cet utilisateur est bien celui qu'il prétend être (authentification). Ces deux vérifications peuvent se faire à partir de :

- *Ce que l'utilisateur connaît (mots de passe, codes...) :* les mots de passe doivent rester secrets et être fréquemment changés. La protection des mots de passe peut être assurer par la fixation de leur longueur minimale, l'interdiction d'utiliser certains mots ou chaînes de caractères, l'imposition d'une durée de validité ;
- *Ce que l'utilisateur possède (badge, cartes magnétiques etc.) :* ces badges et cartes comportent des caractéristiques compréhensibles par un ordinateur. Pour éviter toute falsification, ils doivent être recouverts d'un cache codé disponible uniquement auprès de la source d'habilitation ;
- *Une caractéristique de l'utilisateur (empreintes voix, iris, géométrie de la main, dynamique de frappe,...) :* il s'agit de technologies biométriques fondées sur les caractéristiques biologiques ou comportementales des utilisateurs.

2.2.2.2. *Contrôles d'accès*

Le poste de travail, en réseau ou en mode autonome, permet à tout utilisateur en possession des connaissances suffisantes d'accéder aux données, aux applications, aux programmes et aux fichiers (CLUSIF, 2005). De plus, l'utilisation très répandue de réseaux de télécommunications et l'interconnexion avec des systèmes externes rendent nécessaire le contrôle systématique de l'accès aux données et ressources des entreprises.

Les accès directs, c'est-à-dire, de l'intérieur, de l'entreprise peuvent être contrôlés avec le système d'identification et d'authentification que nous avons décrit précédemment. Mais lorsqu'il s'agit d'un accès à partir de l'extérieur, principalement d'Internet, la société doit mettre en place d'autres moyens de contrôle qui sont :

- L'installation d'un pare-feu ;
- L'installation d'un Réseau Virtuel privé ;
- Ou l'utilisation d'un proxy.

2.2.2.2.1. L'installation d'un pare-feu

Le pare-feu est un système par lequel transite tout le trafic entre Internet et le réseau local. Il a l'avantage de concentrer les aspects de sécurité en un seul point, de permettre la génération d'alarmes et le suivi (*monitoring*). En cas de panne, un seul point est touché (pas d'influence sur le réseau interne). Le pare-feu est basé sur l'un des principes suivants : « tout ce qui n'est pas autorisé est interdit » ou « tout ce qui n'est pas interdit est autorisé ». Les paquets interdits sont soit rejetés ou refusés (mis de côté sans avertir l'expéditeur) .

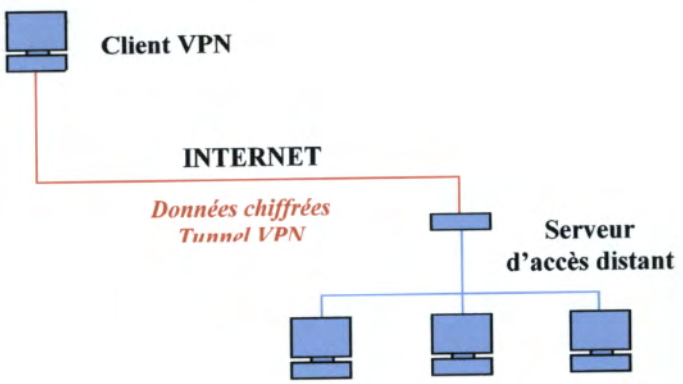
2.2.2.2.2. L'installation d'un Réseau Virtuel Privé (VPN en anglais)

Les données transmises sur Internet sont beaucoup plus vulnérables que lorsqu'elles circulent sur un réseau interne à une organisation car elles empruntent une infrastructure réseau publique appartenant à différents opérateurs. Ainsi il n'est pas impossible que sur le chemin parcouru, le réseau soit écouté par un utilisateur indiscret ou même détourné.

L'installation des liaisons spécialisées n'étant pas à la portée de la plupart des entreprises, il est parfois nécessaire d'utiliser Internet comme support de transmission. Un bon compromis consiste à utiliser Internet comme support de transmission en utilisant un protocole d'"encapsulation" (en anglais « tunneling »), c'est-à-dire encapsuler les données à transmettre de façon chiffrée. On parle alors de réseau privé virtuel (noté RPV ou VPN, acronyme de Virtual Private Network) pour désigner le réseau ainsi artificiellement créé. Ce réseau est dit virtuel car il relie deux réseaux "physiques" (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent "voir" les données.

Le protocole de tunneling permet aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie (PILLOU, 2005).

Figure N° 3 : Représentation d'un Réseau Virtuel Privé



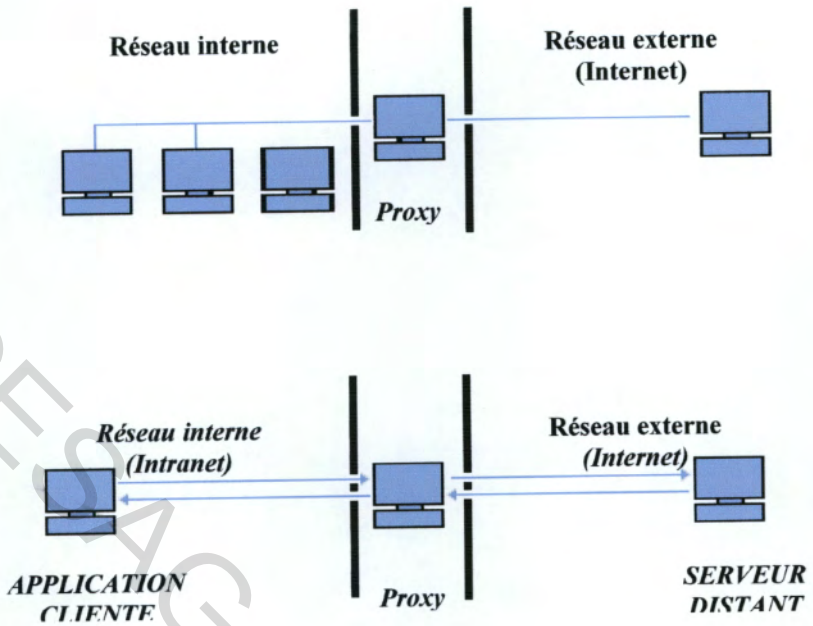
Source : PILLOU (2005)

2.2.2.2.3. L'utilisation d'un serveur proxy

Un serveur proxy, appelé aussi «serveur mandataire» est à l'origine, une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et internet. Le principe de fonctionnement basique d'un serveur proxy est assez simple : il s'agit d'un serveur "mandaté" par une application pour effectuer une requête sur Internet à sa place. Ainsi, lorsqu'un utilisateur se connecte à Internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête. Le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.

La plupart des proxys assurent une fonction de cache (serveurs proxys - cache), c'est-à-dire qu'ils ont la capacité à garder en mémoire (en "cache") les pages les plus souvent visitées par les utilisateurs du réseau local afin de pouvoir les leur fournir le plus rapidement possible. Cette fonctionnalité permet d'une part de réduire l'utilisation de la bande passante vers Internet et de réduire le temps d'accès aux documents pour les utilisateurs.
D'autre part, grâce à l'utilisation d'un proxy, il est possible d'assurer un suivi des connexions (en anglais *logging* ou *tracking*) via la constitution de journaux d'activité en enregistrant systématiquement les requêtes des utilisateurs lors de leurs demandes de connexion à Internet. Il est ainsi possible de filtrer les connexions à Internet en analysant d'une part les requêtes des clients, d'autre part les réponses des serveurs. Lorsque le filtrage est réalisé en comparant la requête du client à une liste de requêtes autorisées, on parle de **liste blanche** ; lorsqu'il s'agit d'une liste de sites interdits, on parle de **liste noire**. Enfin l'analyse des réponses des serveurs conformément à une liste de critères (mots-clés, ...) est appelé **filtrage de contenu**.
Dans la mesure où le proxy est l'intermédiaire indispensable des utilisateurs du réseau interne pour accéder à des ressources externes, il est parfois possible de l'utiliser pour authentifier les utilisateurs, c'est-à-dire de leur demander de s'identifier à l'aide d'un nom d'utilisateur et d'un mot de passe par exemple. Il est ainsi aisé de donner l'accès aux ressources externes aux seules personnes autorisées à le faire et de pouvoir enregistrer dans les fichiers journaux des accès identifiés (PILLOU, 2005).

Figure N° 4 : Représentation et fonctionnement d'un serveur proxy



Source : PILLOU (2005)

2.2.2.3. *Pistes d'audit*

Les pistes d'audit permettent de surveiller les accès autorisés et refusés. Chaque logiciel installé par l'entreprise doit générer une piste d'audit concernant les fonctions qu'il exécute, notamment si ces fonctions modifient ou actualisent des données. La piste d'audit peut être maintenue dans un fichier séparé, transmise au journal d'activité du système ou conservée en tant que partie d'un autre enregistrement.

En principe, les pistes d'audit de toute activité liée aux données et aux programmes relatifs au logiciel sont générées par le logiciel de contrôle d'accès ou le système d'exploitation. Elles peuvent contenir un enregistrement des modifications apportées au niveau du fichier et/ou du programme. Il appartient à l'équipe d'installation de déterminer si la piste d'audit devra enregistrer la totalité des activités.

Les pistes d'audit revêtent une importance particulière pour l'analyse du processus de contrôle car elles fournissent un enregistrement des modifications mises en œuvre (IFACI, 1993).

Conclusion du chapitre

La sécurité informatique se révèle être une caractéristique importante dans le système d'information des entreprises. En effet, le matériel physique et les logiciels constituent le premier élément sur lequel repose l'informatique d'une organisation. De même, les données traitées et stockées sont indispensables à l'activité de l'entreprise. Il est donc nécessaire de mettre en place une politique de sécurité qui assurent la protection du matériel, des logiciels et des données.

L'auditeur financier, dont le rôle est de s'assurer de la régularité et de la sincérité de l'information financière produite par l'entreprise, ne peut donc pas ignorer la sécurité informatique dans les différentes entités où il doit intervenir.
En effet, avant de se prononcer sur les comptes qu'il examine, l'auditeur se doit d'abord, d'évaluer le système qui a contribué à l'établissement de l'information financière. Il doit donc se prononcer sur la fiabilité du système d'information lorsque l'activité de l'entreprise auditée est basée sur l'informatique. Se faisant, le contrôle de la sécurité informatique devient incontournable.

CHAPITRE 3 : SECURITE INFORMATIQUE ET AUDIT FINANCIER

Introduction

La pratique actuelle de l'audit financier souligne le double aspect de sa démarche : il s'agit à la fois d'un contrôle sur les comptes de l'entreprise tels qu'ils sont présentés, mais aussi d'un contrôle sur la manière dont les comptes sont établis. Les procédures de leur constitution, c'est-à-dire l'organisation et le fonctionnement du système d'information comptable et financière de l'entreprise, sont partie intégrante de la confiance que l'on va accorder aux états financiers. Ceci donne une vision plus large de l'audit financier que l'on peut présenter comme « un examen critique qui permet de vérifier les informations données par l'entreprise et d'apprécier les opérations et les systèmes mis en place pour les traduire » (RAFFEGEAU & al., 1993).

Par ailleurs, l'importance de l'informatique dans le système d'information des entreprises modernes a pour conséquence sa prépondérance dans la production de l'information financière. Dès lors, la démarche de l'auditeur, lorsque l'environnement est informatisé, doit être adaptée à cette donne. Plus particulièrement, la sécurité informatique, qui est la première garante de l'intégrité du système d'information, doit faire l'objet d'un examen minutieux de la part des auditeurs financiers.

La CNCC (1995 : 3) précise que « l'existence de systèmes informatiques ne modifie pas le schéma général de la méthodologie d'audit, elle implique des risques et des techniques nouvelles de contrôle qui peuvent modifier sensiblement le déroulement des missions ». Cela permet donc de rassurer les auditeurs traditionnels qui, très souvent, relèguent à un second plan, la fonction informatique des entités dans lesquelles ils interviennent et ne se consacrent qu'aux comptes.

L'objectif de ce chapitre est de présenter, dans le cadre d'un audit financier, les risques inhérents liés à la sécurité du système d'information **(section 1)**.
Nous exposerons, par la suite, les différentes méthodes et techniques dont disposent les auditeurs financiers pour s'assurer de la parfaite sécurisation du système d'information de

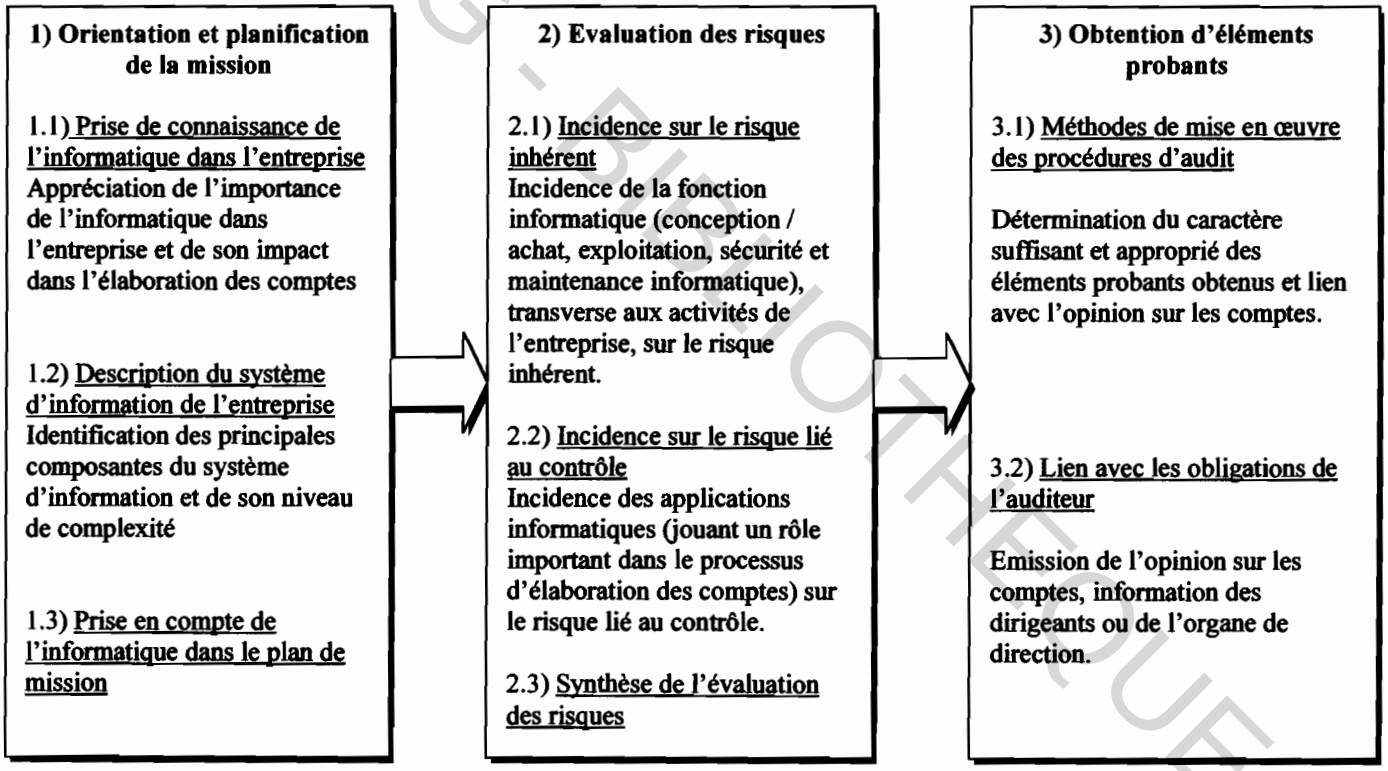
l'entreprise auditée ainsi que le modèle d'analyse et les méthodes de collectes de données retenues dans le cadre de l'audit de la SAJE **(section 2).**

3.1. Risques liés à la sécurité informatique

Dans un environnement informatique, la méthodologie de l'auditeur financier ne diffère pas de celle adoptée en milieu non informatisé. En effet, il conduit ses travaux en respectant les principales étapes suivantes :

- Orientation et planification de la mission ;
- Evaluation des risques ;
- Obtention d'éléments probants.

Figure N 5 : Méthodologie d'audit en environnement informatique



Source : CNCC (2003) (adaptée)

Comme le montre la figure ci-dessus, la prise en compte de la sécurité informatique dans la démarche d'audit financier se matérialise principalement lors de la phase de l'évaluation des risques. L'objectif de l'auditeur est alors d'apprécier l'influence du système informatique sur le risque inhérent.

L'appréciation de l'incidence de l'informatique s'effectue sur la base des éléments suivants :

- Pour le risque inhérent :
  - ✓ la conception et l'acquisition des solutions informatiques ;
  - ✓ la distribution et le support informatique ;
  - ✓ la gestion de la sécurité ;
  - ✓ la gestion des projets informatiques.
- Pour le risque lié au contrôle : l'étude des processus et des applications jouant un rôle significatif direct ou indirect dans la production des comptes de l'entité.

Ainsi donc, la politique de sécurité mise en place par l'entreprise a une incidence sur le risque inhérent qu'identifie l'auditeur financier. Cette incidence se manifeste au niveau des trois aspects suivant du système informatique :

1. La sécurité physique ;
2. La sécurité logique
3. Les sauvegardes et le plan de secours

3.1.1. Le risque inhérent lié à la sécurité physique

Un niveau de sécurité physique insuffisant peut entraîner, en cas de sinistre, une indisponibilité plus ou moins importante des systèmes d'information (mise en péril du bon fonctionnement de l'entreprise). Une sécurité physique non satisfaisante peut également être source de fraudes de la part de personnes non autorisées qui ont accès au système.

L'auditeur cherchera donc à identifier s'il existe :

- Un risque qu'une personne extérieure non autorisée puisse s'introduire dans les locaux de la société afin d'accéder au système d'information (accès aux locaux) ;
- Un risque de destruction physique des outils informatiques notamment par les incendies et les pannes électriques.

L'incidence de la gestion de la sécurité physique sur le risque inhérent peut être schématisée de la manière suivante, en fonction des circonstances :

Tableau N° 3 : Incidence de la sécurité physique sur le risque inhérent

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
Moyens d'accès aux locaux	Les locaux sont surveillés, un badge est nécessaire pour y accéder, les visiteurs doivent passer à l'accueil et sont accompagnés pendant la durée de leur présence dans les locaux de l'entreprise, les salles machines sont sécurisées et interdites aux personnes extérieures à la société.	L'entreprise ne dispose pas de sas ou de portillon de sécurité pour accéder à ses locaux. Les visiteurs ne sont pas systématiquement raccompagnés jusqu'à la sortie et aucune pièce ne leur est demandée à leur entrée, mais les salles machines disposent de digicodes. *Risque que des personnes extérieures à l'entreprise puissent accéder dans les locaux librement.*	Toute personne peut accéder aux locaux de l'entreprise sans se présenter à l'accueil et y circuler librement. Les locaux des salles machines ne sont pas fermés et ne sont pas surveillés. En dehors des heures de travail, les locaux ne présentent pas de dispositifs antivol. *Risque que des personnes puissent accéder librement aux salles machines de l'entreprise.*
Protection incendie	L'entreprise dispose de détecteurs de fumée, d'armoires ignifugées et d'extincteurs. Les salles machines n'abritent pas les consommables et les fournitures.	L'entreprise respecte les réglementations de protection incendie en vigueur, mais ne dispose pas de dispositifs supplémentaires. *Risque de dégâts importants en cas d'incendie.*	L'entreprise ne respecte pas la réglementation en terme de protection incendie. *Risque de pénalités en cas de vérification et risque de dégâts importants en cas d'incendie.*
Protection électrique	L'entreprise dispose d'onduleurs permettant d'éviter des dégâts suite à des coupures de courants ou des variations de tension.	L'entreprise dispose d'onduleurs sur les serveurs les plus critiques. En revanche, les postes de travail n'en sont pas dotés. *Risque de perte de données en cas de coupure de courant.*	L'entreprise ne dispose d'aucune protection contre les variations de tension électrique. *Risque de pertes de données et de matériel en cas d'incidents électriques.*

Source : CNCC (2003)

3.1.2. Le risque inhérent lié à la sécurité logique

L'inexistence ou l'insuffisance de sécurité logique peut être source de fraudes au niveau de l'information financière ou remettre en cause la continuité de l'exploitation.

L'étude de la sécurité logique de l'entreprise permet à l'auditeur d'évaluer les risques suivants :

- Les risques d'accès aux données de l'entreprise par des personnes non autorisées (internes ou externes) qui sont liés à la définition des profils utilisateurs,à la surveillance de l'accès aux données sensibles, à l'utilisation d'Internet … ;
- Ainsi que les risques d'altération des données causée par des virus, des attaques externes et des manipulations accidentelles ou frauduleuses des utilisateurs.

L'incidence des modalités de mise en œuvre de la sécurité logique sur le risque inhérent peut être récapitulée de la manière suivante, en fonction des circonstances :

Tableau N° 4 : Incidence de la sécurité logique sur le risque inhérent

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
Gestion des habilitations / profils utilisateurs	Chaque utilisateur dispose d'un compte avec des droits d'accès nécessaires à sa fonction. Les habilitations sont créées lors de l'entrée du salarié selon sa fonction et désactivées lors de sa sortie. Elles sont régulièrement revues afin qu'aucun compte non utilisé ne soit actif.	Des identifiants communs existent au sein de l'entreprise. Seuls deux profils : administrateur et utilisateur. *L'identification de l'utilisateur ayant effectué des opérations sous un compte commun est impossible.* *Certains utilisateurs auront des droits trop étendus par rapport à la fonction occupée.* Les entrées / sorties de personnel ne sont pas communiquées à l'administrateur. *Risque que les comptes d'utilisateurs ayant quitté l'entreprise soient encore actifs et représentent des points d'accès possibles au réseau pour des attaques logiques provenant de l'extérieur.*	L'entreprise ne gère pas de profils différents et ne dispose pas d'une politique de mot de passe. *Risque que des utilisateurs aient des droits illimités alors qu'ils ne doivent pas en avoir l'usage dans le cadre de leur fonction.* Des identifiants communs sont utilisés par plusieurs utilisateurs et aucun profil différent n'a été créé. *Risque que l'identification de la personne ayant effectué des opérations sous un autre compte commun soit impossible.*
Gestion des mots de passe	Des notes de sensibilisation sont	Les mots de passe ne comportent pas de	Des mots de passe génériques ou mots de

	envoyées régulièrement au personnel concernant la gestion des mots de passe. Le système impose un nombre minimum de caractères pour les mots de passe, ainsi qu'un changement régulier aux utilisateurs.	blocage de longueur lors de leur création et ne sont pas changés régulièrement. *Risque que les mots de passe puissent être découverts facilement et que des personnes non autorisées puissent avoir accès au réseau de l'entreprise.*	passe facile à deviner ou identique à l'identifiant existent pour des comptes utilisateurs ayant des droits étendus. *Risque que les mots de passe puissent être découverts facilement et que des personnes non autorisées aient des droits administrateurs sur le réseau de l'entreprise.*
Utilisation d'Internet / messagerie	L'accès à Internet est contrôlé par un pare-feu (firewall) et limité à quelques postes dans l'entreprise. Le pare-feu a fait l'objet d'un paramétrage. Une charte décrit les modalités d'utilisation de ces outils dans le cadre professionnel.	Aucune sensibilisation à l'utilisation d'Internet et de la messagerie n'a été menée auprès du personnel, mais ces outils ne sont accessibles que de quelques postes spécifiques. *Risque limité d'importation de virus, de visites de sites non autorisés, d'utilisation des outils à des fins personnelles.*	Tous les postes disposent d'une connexion Internet et d'une messagerie mais aucune sensibilisation à leur utilisation n'a été menée auprès du personnel. *Risque élevé d'importation de virus, de visites de sites non autorisés, d'utilisation des outils à des fins personnelles.*
Antivirus	L'entreprise dispose d'un antivirus mis à jour en ligne quotidiennement, installé sur tous les postes et ne pouvant être désactivé par l'utilisateur.	L'antivirus dont dispose l'entreprise n'est mis à jour qu'une seule fois par mois. *Risque de contamination du réseau par des virus nouveaux.*	Des postes de travail avec lecteurs de disquettes ou CD-ROM et accès à Internet ne disposent d'aucun antivirus. *Risque élevé d'importation de virus et de contamination du réseau.*
Protection du réseau	Le réseau est protégé de l'extérieur par un pare-feu (firewall) et les accès utilisateurs font l'objet d'un suivi.	Le réseau est relié à Internet, les flux entrants et sortants sont répertoriés, mais aucun pare-feu n'en assure la protection. *Risque d'attaques logiques provenant d'Internet.*	L'entreprise détient des données sensibles et aucun flux entrant ou sortant du réseau n'est répertorié : les éventuelles attaques dont l'entreprise pourrait être la cible ne peuvent pas être détectées. *Risques d'attaques logiques provenant d'Internet ne pouvant être identifiées.*
Sensibilisation des utilisateurs	Une charte de bonne utilisation du système	Une charte de bonne utilisation du système	Aucune opération de sensibilisation aux

	d'information est distribuée à l'ensemble des utilisateurs et doit être signée par chacun. Des courriels de sensibilisation sont régulièrement envoyés à tous sur la gestion des mots de passe, la sécurité logique. L'encadrement intermédiaire s'assure du relais de l'information.	d'information existe et est remise au personnel à son entrée dans la société : toutefois, elle n'est pas à retournée signée à la direction. De même, il n'existe pas de preuve que les courriels ou notes internes de sensibilisation ont été lus par les destinataires. *Risques que les utilisateurs n'aient pas lu la charte et ne se sentent pas impliqués dans ce processus.*	problématiques de sécurité logique et / ou aucune formation n'est dispensée aux utilisateurs. *Risque que le personnel effectue des opérations pouvant poser des problèmes de sécurité (échanges de mots de passe, antivirus non mis à jour...)*

Source : CNCC (2003)

3.1.3. Le risque inhérent lié aux sauvegardes et au plan de secours

L'inexistence de procédures de sauvegarde efficaces et d'un plan de secours remet sérieusement en cause la continuité de l'exploitation de l'entreprise. En effet, en cas de défaillance du système d'information, les données ne pourront être récupérées en l'absence de sauvegardes. Par ailleurs, dans certains secteurs d'activité, les entreprises doivent prévoir une solution capable de se substituer au système d'information courant pour pouvoir faire face à un sinistre majeur.

L'incidence des modalités de la gestion des sauvegardes sur le risque inhérent peut être récapitulée de la manière suivante, selon des circonstances :

Tableau N° 5 : Incidence des sauvegardes et du plan de secours sur le risque inhérent

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
Procédures de sauvegarde	Une procédure de sauvegarde est rédigée et mise à jour. Elle détaille les supports utilisés, le rythme des sauvegardes, les acteurs impliqués dans le processus.	Une procédure est appliquée mais n'a pas été formalisée. *Risque que la procédure ne soit pas correctement appliquée et que la sauvegarde ne soit pas exhaustive.*	Aucune procédure de sauvegarde n'est appliquée dans l'entreprise. *Risque de pertes de données en cas d'incident dans le système d'information.*
Modalités de sauvegarde	Une sauvegarde quotidienne des données sensibles est effectuée.	Une sauvegarde quotidienne est effectuée, des tests de reprise de données sont	Les sauvegardes ne sont pas effectuées régulièrement et les supports ne sont pas

	Les supports sont conservés à l'extérieur de la société dans un coffre ignifugé, les états d'exécution sont revus après chaque opération de sauvegarde.	menés par sondage mais les états d'exécution ne sont pas analysés. *Risque que la sauvegarde ne soit pas exhaustive et que des anomalies survenant lors de la sauvegarde ne soient pas décelées.*	testés. *Risque que la sauvegarde ne soit pas exhaustive et que les données sauvegardées ne soient pas toutes récupérables.*
Plan de secours	Un contrat a été passé avec une société spécialisée dans les plans de secours pour une prestation de site de secours ou détention de matériel en double en cas de panne. Un plan de reprise d'activité est formalisé avec les rôles des différents acteurs et les matériels à remettre en marche en priorité. Le plan est régulièrement testé et est opérationnel.	Une réflexion a été menée pour identifier les données les plus sensibles et les parties du système d'information sans lesquelles l'entreprise ne peut plus exercer son activité. Toutefois, aucun plan formalisé de reprise d'activité en cas d'incident n'a été rédigé. *Risque que la mise en place du plan de secours soit désordonnée et que les différents acteurs ne soient pas prévenus de leur rôle en cas d'incident.*	Aucune réflexion n'a été menée au niveau du plan de secours. *Risque d'indisponibilité longue du système en cas d'incident : d'où des difficultés à assurer la poursuite des activités de l'entreprise et un risque de pertes financières et de pertes de données.*

Source : CNCC (2003)

Pour évaluer les différents risques présentés précédemment, l'auditeur dispose d'une méthodologie cohérente et d'outils techniques. Cette méthodologie est à la base du modèle d'analyse que nous avons adopté dans le cadre de l'audit de la SAJE.

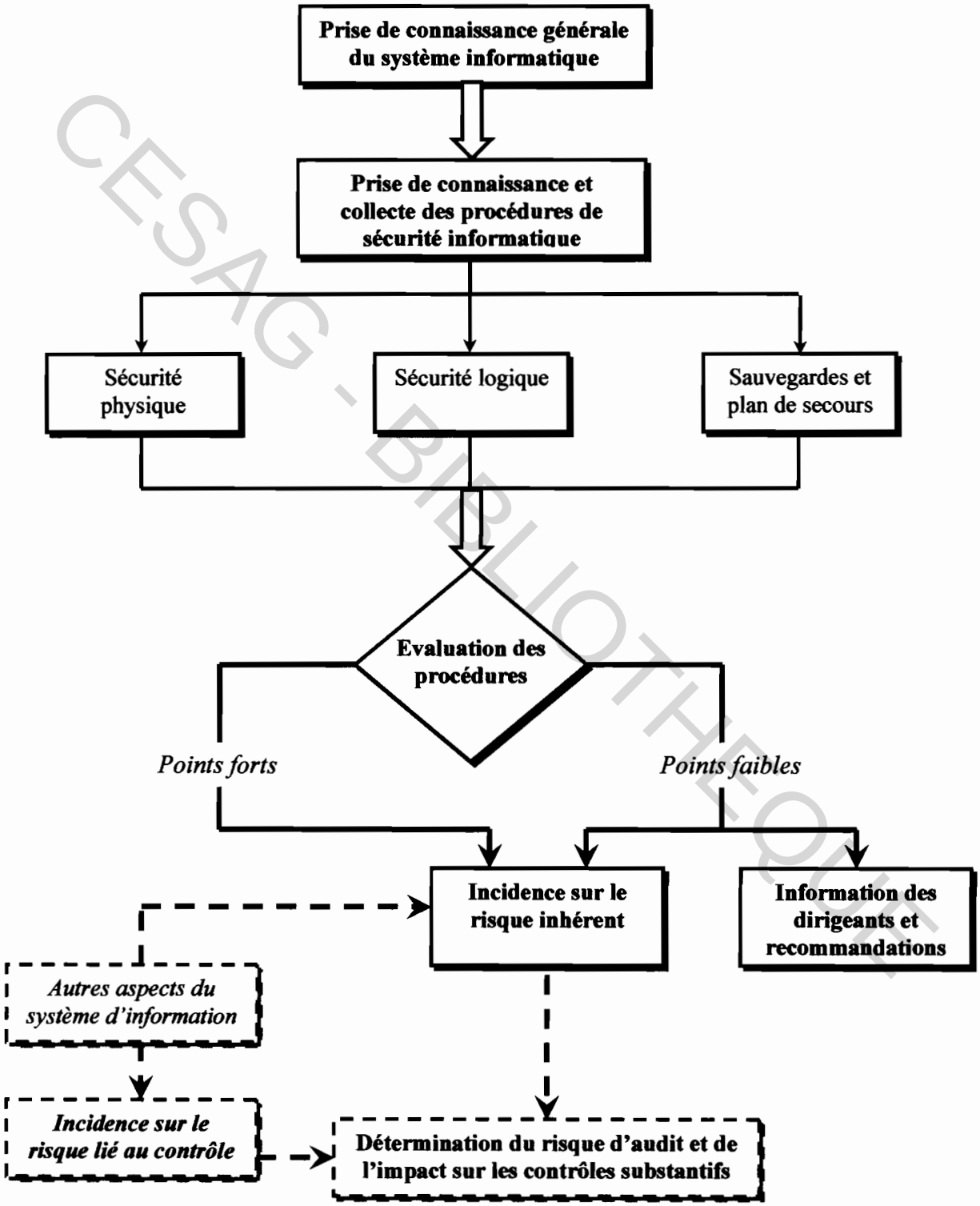
3.2. Modèle d'analyse et méthodes de collecte de données

Dans un contexte d'audit financier, l'étude de la sécurité informatique se réalise suivant une méthodologie cohérente et logique. De même, pour recueillir les informations nécessaires à l'évaluation de l'incidence de la sécurité du système d'information, l'auditeur dispose de plusieurs méthodes.

3.2.1. Modèle d'analyse

Dans le cadre de l'examen financier de la SAJE, l'incidence de la sécurité informatique sur la méthodologie d'audit a été déterminée suivant le modèle d'analyse schématisé ci-après :

Figure N° 6 : Modèle d'analyse



Source : Nous-même

3.2.2. Méthodes de collecte de données

Lorsqu'il intervient dans un environnement informatisé, l'auditeur financier dispose de plusieurs méthodes de collecte de données pour procéder à l'évaluation de la politique de sécurité informatique de l'entreprise.

Dans le cadre de notre étude, nous avons choisi d'utiliser les méthodes de collecte de données suivantes :

- La revue documentaire ;
- L'entretien ;
- Et l'observation physique.

3.2.2.1. La revue documentaire

La revue documentaire intervient principalement dans la phase de prise de connaissance de l'entreprise. Elle consiste à accumuler des connaissances qui permettront ultérieurement à l'auditeur de collecter des éléments probants adéquats (MERCIER & al., 2002).

Dans le cas particulier de la sécurité informatique, la majorité de la documentation est fournie par le service informatique. Nous devrons ainsi réclamer :

- Les manuels des procédures ;
- Le schéma directeur et le budget informatique : une description de la politique informatique (actuelle et future) de la société ;
- Les organigrammes et les descriptions des fonctions du personnel (job descriptions) ;
- Les contrats d'acquisition de services et de matériel informatique ;
- Les contrats de maintenance des applications acquises et du matériel ;
- Le document définissant la politique de sécurité de la société ;
- Les procédures qui définissent les processus d'exploitation de la société.

La revue documentaire nous permettra de mieux comprendre le fonctionnement général de la SAJE et d'avoir une première idée de la politique de sécurité existante. Elle nous permettra également de préparer des entrevues plus ciblées

3.2.2.2. *L'entretien*

Après la revue documentaire, nous comptons mener des entretiens avec les personnes ressources de l'entreprise. Dans un premier temps, nous rencontrerons le personnel de la direction informatique afin d'accumuler les informations sur lesquelles nous allons nous appuyer pour la compréhension du système informatique et surtout pour l'identification des failles et des faiblesses du système.
D'autres entretiens seront par la suite menés avec le personnel de la direction générale et des autres directions, pour en arriver aux simples utilisateurs du système.

Lors de ces entrevues, nous tenterons de prendre connaissance de la structure informatique de la SAJE, notamment du rôle des hommes qui la gèrent. Il s'agira :

- De s'informer sur l'historique de l'informatisation de la société, les pratiques réelles, les difficultés mal résolues ;
- De dresser l'inventaire des différents systèmes utilisés en se faisant préciser les matériels et les techniques informatiques retenus ;
- De se faire décrire les principales mesures prévues en matière de sécurité physique et logique ;
- De recueillir enfin le degré de satisfaction des utilisateurs, souvent révélateur des risques réels.

Nous prendrons également connaissance des opérations traitées et nous tenterons de recueillir des renseignements sur les domaines couverts, le volume des opérations, leur fréquence et leur impact sur la marche de l'entreprise. Ces éléments seront fondamentaux pour établir le programme de travail détaillé (LAMY, 1996 : 38).

3.2.2.3. *L'observation physique*

D'après MERCIER & al. (2002 : 414), « l'observation physique est une technique consistant à examiner un processus, ou la façon dont une procédure est exécutée par d'autres personnes. L'auditeur utilise cette technique pour apprécier la qualité d'un contrôle qu'il estime efficace, mais qui ne donne pas lieu à une matérialisation particulière ».

Après s'être entretenus avec les principaux responsables de la SAJE et les différents intervenants des procédures de sécurité, nous procèderons à l'observation physique de ces procédures. Par la suite, nous effectuerons des tests de permanence par sondage afin de nous assurer de la correcte application des procédures. Nous serons alors amenés à procéder à la visite des différents locaux informatiques afin de rechercher les différentes manifestations qui prouvent le respect des procédures décrites.

Au terme de la revue de la sécurité informatique, un rapport est systématiquement établi. Lorsque les auditeurs constatent que l'un des aspects passés en revue ne donne pas satisfaction, ils décrivent le point relevé, expliquent les risques encourus et émettent une recommandation destinée à apporter la correction nécessaire (LAMY, 1996 : 52).

Conclusion du chapitre

La revue de la sécurité informatique lors d'une mission d'audit financier se révèle être d'une importance primordiale. En effet, dans les entreprises dont l'activité est basée sur un système d'information, les procédures de sécurité doivent faire l'objet d'une attention particulière de la part des auditeurs. Comme nous l'avons souligné précédemment, l'auditeur financier doit tenir compte des paramètres sécuritaires du système d'information lors de l'appréciation du risque inhérent.

Ses travaux sont conduits suivant une méthodologie calquée sur celle de l'évaluation du contrôle interne. Il dispose également de techniques de travail qui lui permettent de distinguer de manière efficace les points forts et les points faibles du système de sécurité informatique.

L'objectif de sa mission étant d'apporter une valeur ajoutée à l'entreprise, l'auditeur doit, au terme de la revue de la sécurité porter à la connaissance de la direction tous les points faibles relevés tout en faisant des recommandations pertinentes dans le but d'améliorer le système en place.

CONCLUSION DE LA PARTIE THEORIQUE

L'introduction de l'informatique dans la gestion des activités des entreprises a permis à celles–ci de réaliser des économies de temps et d'argent considérables. Cela a également entraîné la réorientation de la démarche traditionnelle des auditeurs financiers qui doivent maintenant prendre en compte l'aspect technologique lors de leurs interventions.

Avec la mondialisation des échanges économiques et l'interconnexion des systèmes d'information, la sécurité informatique est devenue une des premières préoccupations des chefs d'entreprises qui souhaitent protéger au mieux le patrimoine de leur organisation. Face à ces besoins de sécurité, plusieurs mesures de sécurité peuvent être prises. Ces mesures concernent notamment la sécurité physique du matériel informatique, la sécurité logique de système d'information et des données ainsi que les procédures de sauvegarde qui permettent d'assurer la continuité de l'exploitation de l'organisation.

Dans le cadre de sa mission, l'auditeur financier doit prêter une attention particulière au système de sécurité informatique de l'entité auditée car la politique sécuritaire en vigueur peut influer sur le s contrôles à mettre en œuvre, à travers le risque inhérent. L'étude de la sécurité informatique de la SAJE nous permettra d'illustrer cette incidence.

D E U X I E M E P A R T I E :

CADRE PRATIQUE

INTRODUCTION

Notre étude pratique s'est déroulée lors d'une mission d'audit contractuel commanditée par la nouvelle direction de la Société Africaine des Jeux (SAJE). Il s'agissait de procéder à l'audit financier des comptes de la SAJE pour l'exercice clos au 31 décembre 2003.

Une grande partie des activités de la société reposant sur un système informatique, cette mission ne pouvait se dérouler sans que le système d'information ne fasse l'objet d'une étude particulière de la part de l'équipe d'audit. L'examen des comptes de la SAJE constitue donc un contexte opportun pour la mise en pratique du modèle d'analyse proposé pour l'étude de l'incidence de la sécurité informatique sur la démarche d'audit financier d'une organisation.

Cette partie pratique sera consacrée, dans un premier temps, à la présentation de la Société Africaine des Jeux (**chapitre 1**). Puis nous décrirons les travaux et investigations menés sur le terrain ainsi que les résultats obtenus (**chapitre 2**). Enfin, nous analyserons ces résultats afin de déterminer leur incidence sur la démarche adoptée pour l'audit de la SAJE et nous présenterons les recommandations qui ont été adressées à la direction générale de la société, à l'issue de la mission, concernant le système de sécurité informatique (**chapitre 3**).

CHAPITRE 1 : PRESENTATION DE LA SOCIETE AFRICAINE DES JEUX (SAJE)

Introduction

Les progrès technologiques observés dans l'informatique ont conduit plusieurs sociétés africaines anciennes à développer des systèmes d'information afin de soutenir leur activité. Ainsi depuis une vingtaine d'années, plusieurs sociétés de la sous région ont procédé à l'informatisation de leur comptabilité, dans un premier temps, et, par la suite, du reste de leur activité.

C'est le cas de la Société Africaine des Jeux qui a d'abord automatisé le traitement de quelques tâches isolées et évolue maintenant vers une informatisation de toute son activité.

Ce chapitre consacré à la présentation de la société étudiée sera divisé en deux (2) sections.

La première section présentera les missions, les perspectives et l'organisation détaillée de la SAJE ainsi que la description de l'activité de l'organisation.

Dans la seconde section, nous nous intéresserons plus précisément au système informatique de la société.

1.1. Présentation générale de la Société Africaine des Jeux

Cette présentation consistera, dans un premier temps, à rappeler les missions et perspectives de la société. Par la suite nous décrirons de manière détaillée l'organisation ainsi que les activités de la SAJE.

1.1.1. Missions et perspectives

La Société Africaine des Jeux (SAJE) est une société nationale au capital de cinquante millions de francs CFA (50 000 000 F CFA) réparti en 5 000 actions d'une valeur nominale de 10 000 francs CFA.

Elle a pour objet l'exploitation de toutes les formes de loteries, de jeux de hasard, de pronostics et assimilés. Elle participe également, sous quelque forme que ce soit, à toutes entreprises et à toutes sociétés créées ou à créer, tant dans le pays qu'à l'étranger, dont l'activité serait susceptible de concourir à la réalisation de son objet social.

L'activité de la SAJE est constituée par la commercialisation des carnets de jeux du PMU (Pari Mutuel Urbain), de la loterie sportive (LS) et des tickets de loteries instantanées ainsi que l'organisation de la loterie informatisée (LI).

Dans le souci de mieux satisfaire les parieurs, de réduire les risques liés à l'exploitation des jeux et d'améliorer les performances globales, la SAJE envisage la mise en œuvre et le développement d'un processus automatisé pour le PMU qui représente près de 75% du chiffre d'affaires global de la société.

Cette automatisation permettra de remédier aux inconvénients du système d'exploitation manuel tels que :

- L'importance des charges liées à l'exploitation manuelle ;
- La lenteur du traitement manuel qui prolonge les délais de paiement et empêche la société d'organiser des jeux tous les jours de la semaine ;
- Les erreurs au niveau du calcul de la recette réelle réalisée par chaque vendeur et de l'enregistrement des numéros des tickets gagnants ;
- les omissions de tickets gagnants dont la régularisation entame le solde concessionnaire de la SAJE ;
- La multiplicité des tentatives de fraude enregistrées au niveau des salles de traitement des jeux ;

Depuis deux ans, des études sont menées dans ce sens et la société a déjà acquis un système informatique global de gestion et d'exploitation du PMU. Les bons résultats enregistrés au niveau de la loterie informatisée ont conforté la SAJE dans ce projet d'informatisation.

1.1.2. Organisation détaillée de la société

La SAJE est une organisation ayant à sa tête un directeur général qui tient ses pouvoirs d'un conseil d'administration. L'activité de la société est organisée autour des cinq (5) directions présentées dans le tableau ci-après.

Il faut par ailleurs noter que le directeur général est assisté de plusieurs conseillers dont le responsable informatique. Celui-ci est à la tête du service informatique.

Tableau N° 6 : Présentation des différentes directions de la SAJE

Direction	Département	Service	Missions
Direction Administrative (DA)	**1) Achats et approvisionnements**	*a) Gestion des stocks*	- Gestion des stocks de produits destinés à la vente (carnets de jeux, tickets de loteries instantanées) - Gestion des fournitures de bureau
		b) Achats	- Préparation des offres - Passation des commandes
	2) Administration générale	*a) Equipement et logistique*	- Gestion des immobilisations - Suivi des travaux exécutés par les tiers pour le compte de la société - Gestion des missions
		b) Documentation, Archives et gestion des contrats	- Gestion de tous les contrats signés avec les tiers (fournisseurs, avocats, entretien…).
Direction des Ressources Humaines (DRH)	**1) Personnel**	*a) Administration du personnel*	- Recrutement du personnel - Suivi des congés, des affectations - Gestion des dossiers du personnel
		b) Paie	- Préparation des salaires des employés permanents - versements des retenues fiscales et sociales
		c) Gestion prévisionnelle du personnel	- Tenue des statistiques sur les mouvements de personnel - Propositions d'affectation du personnel - Suivi des retraites
	2) Affaires sociales et sanitaires	*a) Médecine d'entreprise*	- Traitement des employés et de leur famille - Orientation des malades vers les spécialistes agréés
		b) Social	- Organisation de l'arbre de noël, des colonies de vacances

Direction	Département	Service	Missions
Direction du Marketing (DM)	**1) Ventes**	*Gestion du réseau commercial*	- Gère toutes les agences - Tient les statistiques de vente pour tous les produits - Organise le réseau commercial, encadre et forme la force de vente - Centralise les rapports d'activités des agences.
	2) Etudes stratégies et développement des produits	*a) Etudes*	- Etude de la faisabilité (technique) des nouveaux produits - Conception et élaboration des cahiers de charges
		b) Stratégies et Développement des produits	- Gestion de la vie des produits
	3) Communication	*a) Promotion et Publicité*	- Lancement des nouveaux produits - Remise de chèques aux gagnants
		b) Relations publiques	- Mêmes missions que le service Promotion et Publicité - Remise des lots en nature
		c) Bureau de presse	- Confection du programme du PMU et de la loterie sportive, en relation avec les imprimeurs et agences de presse
Direction de l'Exploitation (DE)	**1) PMU**	-	- Contrôle des carnets vendus - Calcul des recettes par vendeur - Détermination de la recette globale - Contrôle de la régularité des opérations - Tri des tickets pour déterminer les gagnants - Répartition du chiffre d'affaires entre les gagnants, l'Etat et la SAJE - Calcul de la commission des vendeurs - Gestion des prestataires qui font le dépouillement - Traitement des réclamations des parieurs, envoyées par les agences
	2) Loterie sportive et Loteries instantanées	-	- Mêmes missions que le département PMU - Pour les loteries instantanées, rapprochement entre les recettes versées et états de distribution des tickets - Vérification des gagnants à partir du listing de contrôle
Direction Comptable et Financière (DCF)	**1) Finance**	*a) Fiscalité*	- Vérification de l'aspect fiscal des factures et des contrats avant comptabilisation
		b) Trésorerie	- Suivi des comptes bancaires à partir du Minitel.
		c) Caisses	- Réception et vérification des recettes provenant des agences et reversement en banque - Gestion des caisses
	2) Comptabilité	*a) Achats, Frais généraux*	- Comptabilisation des dépenses d'achats après vérification des pièces justificatives
		b) Charges conventionnelles & Recettes	- Comptabilisation des produits à partir des états de recettes contrôlées établis par la DE - Comptabilisation des lots payés
		c) Caisses & Banques	- Comptabilisation des encaissements à partir des feuilles d'imputation envoyées par les agences - Comptabilisation des opérations de banque
		d) Valeurs inactives	- Contrôle de tous les tickets gagnants a posteriori pour assurer la fiabilité des lots payés

Source : Nous-même

1.1.3. Description de l'activité de la société

Cette description concernera la vente des supports de jeux (PMU, LS, loteries instantanées et LI), l'encaissement des resettes et le paiement des commissions vendeurs et des lots.

1.1.3.1. Vente des supports de jeux

Pour la commercialisation de ses produits, (carnets de jeux du PMU et de la LS, tickets de loteries instantanées et LI), la SAJE s'appuie sur un réseau commercial composé d'une vingtaine d'agences et bureaux installés sur l'ensemble du territoire national et près de 2 000 vendeurs rattachés à ces agences et bureaux.

L'approvisionnement des agences en supports de jeux se fait au service Gestion des stocks de la Direction Administrative. Les vendeurs s'approvisionnent quotidiennement en tickets et en carnets de jeux auprès des agents commerciaux des agences auxquelles ils sont rattachés. Les agents commerciaux mentionnent sur des états de distribution (ED) les dotations des vendeurs.
Les carnets et tickets de jeux sont vendus au niveau des points de vente.
En fin de matinée, les vendeurs retournent les carnets de jeux contenant les souches des tickets vendus ainsi que les carnets non entamés aux agences. Ils y reversent la recette réalisée. Les carnets sont ensuite acheminés à la Direction de l'Exploitation où ils sont dépouillés manuellement.

- **Dépouillement du PMU**

Les carnets sont d'abord contrôlés par rapport aux états de distribution. Les dépouilleurs procèdent ensuite au calcul de la recette de chaque vendeur qu'ils reportent sur les bordereaux individuels de recettes (BIR). Ces BIR sont centralisés au service informatique de la Direction de l'Exploitation afin de déterminer la recette globale. Cette recette calculée est comparée, agence par agence et vendeur par vendeur, à la recette déclarée (déterminée à partir des ordres de recettes (OR) envoyés par les agences).
En cas d'écart, les recettes correspondantes sont recalculées par les dépouilleurs.
Les écarts définitivement relevés entre les recettes réelles et les reversements sont imputés sur les commissions des vendeurs.

Les recettes calculées sont ensuite récapitulées et envoyées à la Direction Comptable et Financière pour comptabilisation.

Les dépouilleurs procèdent par la suite au dépouillement des tickets pour déterminer les gagnants. La récapitulation des gagnants est faite à l'issue de deux dépouillements (le 2ème est contradictoire). Après contrôle par le chef de centre, les états récapitulatifs des gagnants sont envoyés au service informatique pour le partage de la recette (entre les parieurs, l'Etat, la SAJE et les vendeurs).

- **Loteries instantanées**

Les états de distribution et les ordres de recettes relatifs à la vente des tickets de grattage sont traités au niveau de la Direction de l'Exploitation. Ces documents sont contrôlés afin de s'assurer de leur conformité et de la correspondance entre les séquences numériques des tickets vendus et celles des tickets reçus. En cas d'incohérence entre les séquences numériques, le nombre ou la valeur des tickets, les recettes sont réajustées au niveau des états de distribution.

Les agents de la Direction de l'Exploitation établissent ensuite des états de contrôle du chiffre d'affaires en dégageant le chiffre d'affaires calculé par vendeur (CAC), le montant de la recette versée (CAV), l'écart entre le CAC et le CAV, s'il y a lieu, et le nombre de tickets vendus. Ces états sont centralisés pour déterminer la recette globale par agence.

Les opérateurs de saisie procèdent ensuite à la saisie des ordres de recettes et des états de distribution et éditent un état de contrôle des ventes soumis au chef du service Loteries instantanées. Celui-ci établit un compte-rendu de remontée en dressant un tableau de détermination du chiffre d'affaires global qui fait ressortir les CAC, les CAV et les écarts relevés. Il vise tous les documents et les transmet à son chef de département.

Après visa du chef du département Loterie sportive et loteries instantanées, le compte-rendu de remontée et l'état de centralisation du chiffre d'affaires sont transmis à la Direction Comptable et Financière pour comptabilisation.

Au niveau de la DCF, les documents sont contrôlés et comptabilisés par le chef du service recettes et charges conventionnelles.

1.1.3.2. Encaissement des recettes

Le reversement de la recette réalisée au niveau des agences se fait chaque soir à la Caisse Centrale, sur la base des états récapitulatifs des ordres de recettes établis par les caissiers principaux des agences et visés par le chef des caisses (du siège). Après recomptage des espèces, le caissier central établit un reçu de versement.

Le chef des caisses établit également un état récapitulatif des recettes sur la base des ordres de recettes envoyés par les agences. Cet état est ensuite comparé aux sommes réellement encaissées.

La comptabilisation des reversements se fait à la DCF sur la base du reçu établi par le caissier central.

Les versements à la banque se font tous les lendemains de jeux, sur instruction du directeur comptable et financier et. Les recettes réalisées les vendredis, samedis et dimanches ne sont reversées en banque que les lundis.

1.1.3.3. Paiement des commissions vendeurs et des lots

Les commissions des vendeurs ainsi que les indemnités des stagiaires et prestataires sont payées chaque quinzaine sur la base des états de paiements établis par la Direction de l'Exploitation et signés par le directeur général ou le directeur comptable et financier.

Les lots dont le montant est inférieur à FCFA 500 000 sont payés au niveau des agences. Au-delà de ce montant, le paiement est effectué par la Direction Comptable et Financière.

Ce paiement se fait dans les conditions suivantes :

- le gagnant doit se présenter muni de son ticket au niveau de l'agence dont dépend le vendeur qui a enregistré sa mise, dans un délai d'une semaine ;
- un contrôle préalable est fait au niveau de l'agence ;
- le gagnant doit se présenter muni de son ticket, visé par le chef d'agence, au niveau de la Direction Comptable et Financière ;
- le ticket doit figurer sur l'état des tickets gagnants établi par la Direction de l'Exploitation ou par le responsable informatique ;

- la souche de contrôle (pour le PMU et la loterie sportive) ou une copie du ticket déduit du système (en ce qui concerne la loterie informatisée) est bien reçue à la DCF.

Le chèque (accompagné de l'avis de règlement) est remis au parieur sur présentation d'une pièce d'identité, d'une attestation de dépôt de valeur signée par le chef du département finances et contre décharge sur le cahier de transmission.
La comptabilisation du règlement est faite par le comptable du service Banques et Caisses sur la base de l'avis de règlement.

1.2. L'organisation informatique de la société

Pendant longtemps, l'informatique de la SAJE n'était pas réellement organisée. En effet, plusieurs départements disposaient de leurs « propres informatiques » sans aucune liaison ou intégration entre elles. C'est seulement avec l'introduction de la loterie informatisée qu'un système informatique structuré a été mis en place au sein de l'organisation.

Ce système est géré par le service informatique dirigé par le responsable informatique et dépendant directement de la direction générale.

1.2.1. Présentation du service informatique

Le service informatique de la SAJE est chargé de :

- La gestion de la loterie informatisée à partir du centre de suivi ;
- La gestion du matériel (terminaux) installé dans les espaces de la loterie informatisée ;
- La gestion de l'informatique interne, principalement de l'informatique de gestion (au niveau de la DCF) ;
- Le développement d'applications utilisées en interne.

Le personnel du service informatique comprend deux (2) techniciens supérieurs, quatre (4) agents d'exploitation et de maintenance, cinq (5) analystes-programmeurs, deux (2) programmeurs et un (1) administrateur réseau.

1.2.2. Description du système informatique

Le système informatique de la SAJE peut être présenté sous deux aspects :

1) Les matériels, les plateformes et les logiciels utilisés ;
2) Les câblages et réseaux installés.

1.2.2.1. Matériels, plateformes et logiciels

Le parc informatique de la Société Africaine des Jeux comprend :

- 90 postes de travail (PC) ;
- 90 onduleurs ;
- 75 imprimantes et
- 4 serveurs (deux serveurs d'applicatif, un serveur vocal et un serveur de messagerie et WEB).

Les plateformes utilisées sont les suivantes :

- **Plateforme Windows** : pour les postes de travail (Windows 98, 2000 ou NT), le serveur d'applicatif pour les applications de gestion et le serveur vocal ;
- **Plateforme LINUX** : pour le serveur de messagerie et WEB ;
- **Plateforme UNIX** : pour le serveur d'applicatif utilisé pour l'exploitation de la loterie informatisée.

La société utilise également plusieurs logiciels :

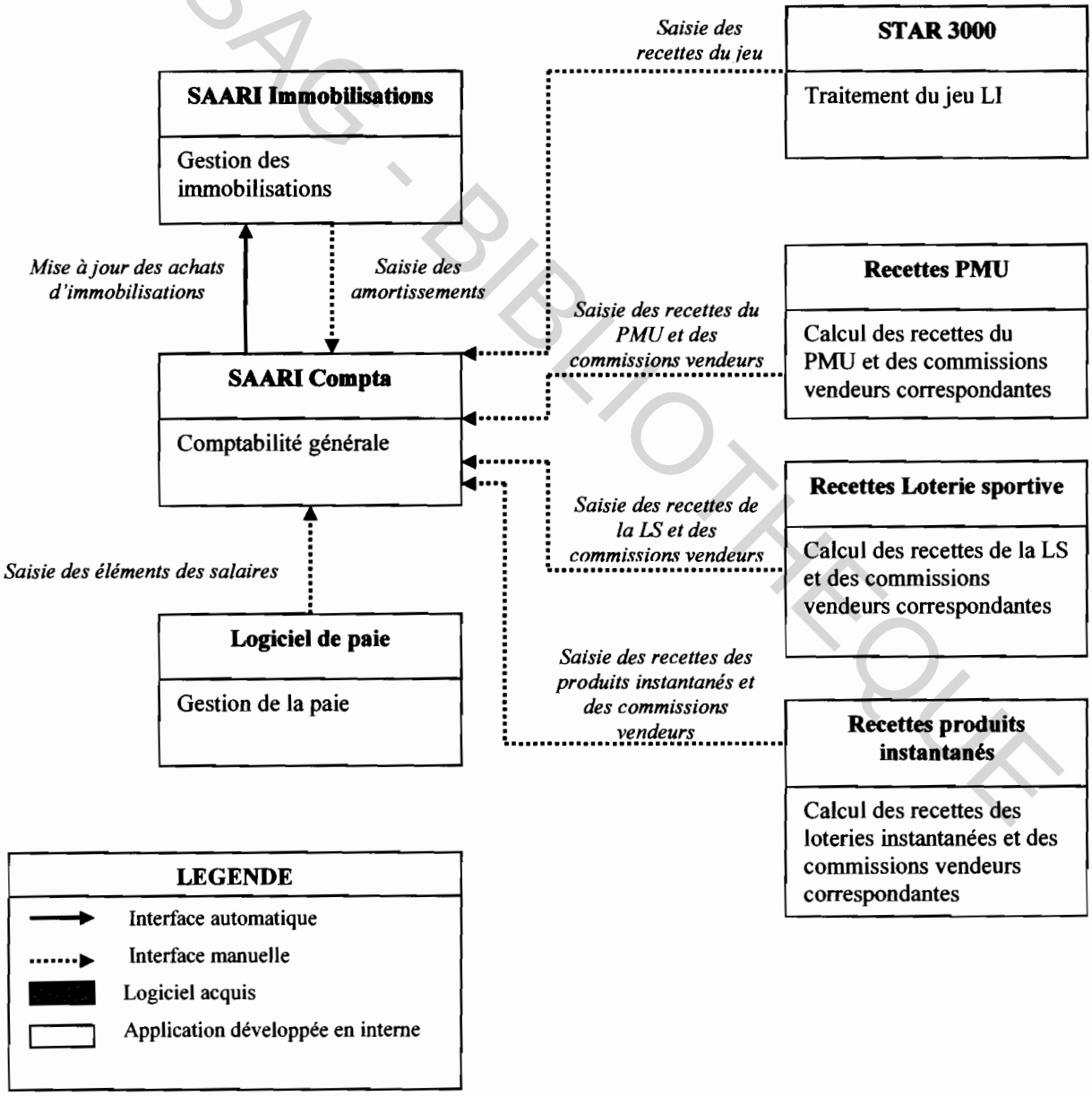
- **Logiciel SAGE SAARI 500** pour la comptabilité avec les modules comptabilité générale, immobilisations et états financiers au niveau de la Direction Comptable et Financière.
- **Logiciel de paie** développé sous Visual Basic (VB). 6 en interne, utilisé par le service paie pour le traitement des salaires ;
- **Logiciel STAR 3000** utilisé pour le traitement de la loterie informatisée ;
- **Logiciel de gestion des recettes et commissions du PMU** développé sous D Base en interne ;
- **Logiciel de gestion des recettes et commissions de la Loterie sportive** développé sous Cobol en interne ;

- **Logiciel de gestion des recettes et commissions des produits instantanés** développé sous ACCESS en interne.

Ces trois derniers logiciels, développés avant la mise en place du service informatique, sont utilisés au niveau de la Direction de l'Exploitation pour le calcul des recettes réalisées et les commissions à payer aux vendeurs.

La figure ci-dessus présente la cartographie de ces logiciels et applications.

Figure N° 7 : Cartographie générale des applications de la SAJE



Source : Nous-même

1.2.2.2. Câblages et réseaux

Les principaux sites informatiques de la société sont :

- **Le siège :** le LAN (Local Area Network) regroupe la direction générale, la Direction Comptable et Financière, la Direction Administrative et la Direction des Ressources Humaines. Le câblage y est réalisé à 100%.
  Un réseau comprenant dix (10) postes (PC) sous Windows 2000, dont un dédié serveur sous Windows NT Server 4.0, est installé au niveau de la DCF
  Un autre mini – réseau indépendant du LAN du siège (directement par HUB) est installé au niveau de la DRH. Il comprend deux (2) postes et un serveur pour la gestion de la paie.
  Par ailleurs tous les postes, exceptés ceux de la Direction Comptable et Financière, ont accès à Internet.

- **Le Site 1** (situé à environ cinq (5) kilomètre du siège) : il regroupe la Direction de l'Exploitation (DE) et la Direction du Marketing, (DM). Le câblage y est effectué à 45%. Aucun poste n'est mis en réseau. Pour l'accès à Internet, plusieurs postes disposent de comptes individuels par Réseau Téléphonique Commuté (RTC).

- **Site 2** : (à un kilomètre du siège) : il regroupe le centre de suivi du système de la loterie informatisé (LI) et l'espace de LI 1. Ce site est câblé à 100% et est doté d'un réseau composé de 2 serveurs, 4 postes de travail, 2 imprimantes laser et une imprimante matricielle. L'accès Internet n'est disponible que sur un seul poste, non connecté au réseau du système de loterie informatisée.

- **Espaces LI** : ils sont au nombre de cinq (5). Chaque espace est câblé à 100% et dispose de 4 à 5 terminaux de prise de pari. Les espaces LI sont connectés au centre de suivi par des liaisons point à point.

Conclusion du chapitre

Ce premier chapitre consacré à la présentation de la SAJE nous a permis d'avoir une meilleure compréhension de son organisation générale et de son activité.

Par ailleurs, la description de l'organisation informatique de la société a servi de prise de connaissance générale du système d'information et nous permet d'entamer l'étude de la sécurité informatique qui est l'objet du chapitre suivant.

CHAPITRE 2 : LA SECURITE INFORMATIQUE AU SEIN DE LA SAJE

Introduction

Du fait de l'utilisation importante de l'informatique dans les activités de la Société Africaine des Jeux, le système d'information a fait l'objet d'une attention particulière lors de la mission d'audit financier de la société. C'est ainsi qu'une revue de la sécurité a été effectuée afin de déterminer l'incidence de la sécurité informatique de la société sur le risque inhérent.

Ce deuxième chapitre comportera deux (2) principales sections. La première sera consacrée à la présentation les travaux effectués dans le cadre de la revue de la sécurité informatique de la SAJE. Dans la seconde, nous présenterons les résultats obtenus lors de nos travaux.

2.1. Travaux effectués

Les travaux que nous avons effectués lors de la revue de la sécurité de la SAJE sont essentiellement constitués de la revue de la documentation informatique, d'entretiens avec les principaux acteurs du service informatique et avec quelques utilisateurs, ainsi que de la visite des différents sites informatiques.

2.1.1. Revue de la documentation informatique

Nous avons adressé un mémorandum au responsable informatique afin d'obtenir la documentation suivante :

- Le manuel de procédures informatiques ;
- Le plan de sécurité ;
- La charte de sécurité destinée au personnel ;
- La liste des profils et des habilitations par application ;

Nous n'avons obtenu que la liste des profils et des habilitations pour le logiciel SAARI et celui de la loterie informatisée. Le responsable informatique nous a expliqué que la société n'avait établi aucune documentation formelle concernant la sécurité informatique.
Notre revue documentaire ne s'est donc limitée qu'à l'étude des listes de profils et habilitations qui nous ont été fournies.

2.1.2. Entretiens

Nous nous sommes entretenus avec les personnes suivantes :

- Le responsable informatique ;
- L'administrateur réseau ;
- Le chef des opérations techniques ;
- Le chef du service de suivi du système ;
- Le directeur de l'exploitation ;
- Le chef du service paie ;
- Les utilisateurs de la DFC et de la DE.

2.1.2.1 *Entretien avec le responsable informatique*

Lors de cette entrevue, le responsable informatique nous a expliqué qu'aucune politique de sécurité particulière n'avait été mise en place par la société. Il a rappelé que la service informatique n'avait été mise en place qu'en 2003 et qu'aux yeux de la direction générale, celui-ci avait pour principale mission, la maintenance du parc informatique, la gestion du système de la loterie informatisée et la conduite du projet d'automatisation du PMU. Mais vu le manque de compétences informatiques poussées au sein du personnel de la Direction Comptable et Financière, il a assigné à l'administrateur réseau la responsabilité de la gestion des accès et des sauvegardes au niveau du logiciel SAARI. Il nous a également précisé que le service informatique ne gérait ni le logiciel de paie, ni les logiciels de calcul des recettes et des commissions des vendeurs.

2.1.2.2 *Entretien avec l'administrateur réseau*

L'administrateur réseau est responsable de la gestion de la sécurité du réseau du siège. Il est également chargé de la gestion des accès et des sauvegardes au niveau du logiciel de comptabilité. Cet entretien nous a permis d'obtenir des informations sur la politique de sécurité réseau appliquée au sein de l'entreprise et le système de gestion des sauvegardes des données comptables et des accès au SAARI.

2.1.2.3 *Entretien avec le chef des opérations techniques et le chef du service de suivi du système*

Compte tenu de l'importance que revêt le projet d'informatisation complète du PMU, le système de gestion de la loterie informatisée fait office de test. En effet, la réalisation du projet dépend des résultats que produira le système de la loterie informatisée.
Les entrevues avec les différents responsables de ce système nous ont permis de prendre connaissance des mesures de sécurité physique et logique mises en place au niveau du centre de suivi de la loterie informatisée et des différents espaces LI.

2.1.2.4 *Entretien avec le directeur de l'exploitation*

Les logiciels de calcul des recettes et des commissions des vendeurs étant placés sous la responsabilité de la Direction de Exploitation, l'entretien avec le responsable de cette direction nous a permis d'obtenir des informations sur le système de sécurité physique et logique ainsi que les mesures de sauvegarde appliquées à ce niveau.

2.1.2.5 *Entretien avec le chef du service paie*

Le chef de service paie est l'un des concepteurs du logiciel de paie. Il en est également le principal utilisateur. Il constitue donc une personne ressource en ce qui concerne les mesures de sécurité appliquées au niveau de l'informatique de la paie.

2.1.2.6 *Entretien avec les utilisateurs de la DCF et de la DE*

Enfin, pour mesurer le degré de vulgarisation de la sécurité au niveau du personnel et son niveau d'implication dans la politique de sécurité informatique de la SAJE, nous nous sommes également entretenus avec quelques utilisateurs. Nous nous sommes principalement intéressés à ceux du logiciel SAARI au niveau de la Direction Comptable et Financière et ceux des logiciels de calcul des recettes et des commissions vendeurs de la Direction de l'Exploitation.

Ces différents entretiens nous ont permis d'obtenir une description détaillée des mesures de sécurité informatique en vigueur au sein de la SAJE. Pour obtenir l'assurance de leur correcte application, nous avons procédé à leur observation physique. Cette observation s'est essentiellement traduite par des visites que nous avons effectuées au niveau des principaux sites informatiques de l'entreprise.

2.1.3. Visites des sites informatiques

Dans le but de confirmer l'application effective des procédures de sécurité informatique qui nous ont été décrites lors des entretiens, nous avons effectué des visites des différents locaux informatiques de la SAJE. Certaines de ces visites se sont déroulées en présence des différents responsables rencontrées. D'autres phases de l'observation physique ont été effectuées à

l'insu des acteurs de la société, notamment des utilisateurs mais toujours avec l'autorisation des responsables de l'informatique.

Nous avons ainsi eu l'occasion de visiter certains locaux informatiques du siège, principalement :

- L'entrée principale du siège ;
- Les locaux de la Direction Comptable et Financière ;
- La salle des serveurs du siège ;
- Les locaux du service paie ;
- L'entrée du Site 1 ;
- Les locaux informatiques de la Direction de l'Exploitation ;
- Le centre de suivi de la loterie informatisée ;
- L'espace LI 1.

La revue de la sécurité informatique effectuée à travers les travaux décrits précédemment nous a permis de faire ressortir les caractéristiques du système de sécurité existant au sein de la SAJE. Les résultats obtenus à l'issu de cette revue sont présentés dans la section suivante.

2.1. Présentation des résultats obtenus

A l'issue des travaux que nous avons effectués, les procédures de sécurité informatique mises en place et appliquées par la SAJE se présentent comme suit :

2.1.1. Sécurité physique de la société

Les procédures de sécurité physique appliquées au sein de la SAJE peuvent se subdiviser en trois niveaux :

- Les moyens d'accès aux locaux ;
- La protection contre les incendies ;
- Et la protection électrique.

2.1.1.1. Moyens d'accès aux locaux

Les procédures d'accès aux locaux de la SAJE se présentent comme suit :

- Les locaux (siège Site1 et Site 2) sont surveillés par des vigiles d'une société de sécurité de la place ;
- L'accès des locaux n'est pas règlementé par le port du badge ;
- L'identité des visiteurs n'est pas systématiquement vérifiée à l'entrée des locaux ;
- Les visiteurs ne sont pas accompagnés pendant leur présence dans les locaux de l'entreprise ;
- L'accès au centre de suivi de la loterie informatisée est strictement surveillé et chaque visiteur est y est accompagné durant toute la durée de sa présence ;
- Les salles serveurs du siège et du centre de suivi sont toujours fermées à clé et seul le personnel autorisé y a accès ;
- Le service paie ne dispose pas de salle informatique particulière. Les postes de travail ainsi que le serveur sont installés dans le bureau du responsable du service. L'accès de ce bureau n'est pas règlementé.

2.1.1.2. Protection incendie

Les procédures anti-incendies de la SAJE présentent les principales caractéristiques suivantes :

- Les locaux de la société ne disposent pas de détecteur de fumée ;
- Seul le centre de suivi de la loterie informatisée dispose d'une sirène et d'un gyrophare qui se déclenchent en cas d'incendie ;
- Des extincteurs sont installés dans tous les locaux de la société ;
- Les armoires de la société ne sont pas ignifugées ;
- Les salles serveurs du siège et du centre de suivi n'abritent ni les consommables, ni les fournitures.

2.1.1.3. *Protection électrique*

Afin d'éviter les dégâts dus à l'électricité, la SAJE a pris toutes les dispositions pour que chaque ordinateur de la société soit relié à un onduleur.

2.1.2. Sécurité logique de la société

Nos travaux nous ont permis d'établir un état des lieux de la sécurité logique en vigueur dans la SAJE. Cet état des lieux concerne essentiellement les points suivants :

- La gestion des habilitations et des profils utilisateurs ;
- La gestion des mots de passe ;
- L'utilisation d'Internet et de la messagerie ;
- Les antivirus ;
- La protection du réseau ;
- La sensibilisation des utilisateurs.

2.1.2.1. *Gestion des habilitations et des profils utilisateurs*

Les utilisateurs du réseau du siège, ceux du logiciel comptable et du système de la loterie informatisée disposent chacun d'un compte avec des droits d'accès correspondants à leur fonction.

Mais aucune gestion des profils n'est assurée pour le logiciel de paie et ceux de calcul des recettes et des commissions vendeurs.

2.1.2.2. *Gestion des mots de passe*

- Les mots de passe pour l'accès au SAARI ont été créés lors de l'installation du logiciel et n'ont pas été changés depuis ;
- Il n'y a aucun mot de passe pour l'accès au logiciel de paie ;
- Au niveau du système de la loterie informatisée, les mots de passe sont régulièrement changés et un nombre minimum de caractères est requis à leur création ;
- Les mots de passe pour l'accès aux logiciels de calcul des recettes et des commissions ne sont pas changés, les utilisateurs actuels ont conservé les mots de passe créés par les concepteurs.

2.1.2.3. *Utilisation d'Internet et de la messagerie*

- La société ne dispose pas de messagerie interne ;
- L'accès à Internet au sein de l'entreprise est protégé par des pare-feux (firewall) ;
- Aucune action de sensibilisation à l'utilisation d'Internet et de la messagerie n'a été menée auprès du personnel ;
- Au siège comme au Site 2, la connexion Internet n'est pas disponible sur les postes accédant aux logiciels de gestion (SAARI, LI, paie, calcul des recettes et des commissions) ;
- Les postes du siège disposant de la connexion Internet y ont accès à travers des comptes individuels et des modems individuels.

2.1.2.4. *Antivirus*

La société dispose d'un antivirus installé sur tous les postes de la société. La mise à jour est effectuée par l'Administrateur réseau une fois par semaine.

2.1.2.5. *Protection réseau*

- Le réseau du siège est protégé de l'extérieur par un pare-feu mais les accès utilisateurs ne font l'objet d'aucun suivi ;
- Les accès au système de la loterie informatisée font l'objet d'un suivi quotidien ;
- Au niveau des autres logiciels de la société, aucun suivi des accès n'est effectué.

2.1.2.6. *Sensibilisation des utilisateurs*

- La société n'a pas établi de charte de bonne utilisation du système informatique pour les utilisateurs ;
- Aucune action de sensibilisation aux problèmes de sécurité logique n'a été menée auprès du personnel ;
- Au niveau du logiciel SAARI, aucune séance de formation n'a été dispensée aux utilisateurs après celle organisée par le fournisseur ;

- En ce qui concerne les autres logiciels de gestion, aucune séance de formation n'est organisée, les nouveaux utilisateurs apprennent l'utilisation des différents logiciels avec l'aide de leurs collègues ;
- Pour le système de la loterie informatisée, les guichetiers des différents espaces (utilisateurs des terminaux) sont formés à leur entrée dans la société

2.1.3. Procédures de sauvegardes et plan de secours

Les résultats obtenus lors de nos travaux sur les procédures de sauvegarde et le plan de secours se présentent comme suit :

2.1.3.1. Procédures de sauvegarde

- Les procédures de sauvegarde ne sont pas formalisées ;
- Il existe cependant des procédures de sauvegarde appliquées pour le logiciel comptable, le logiciel de paie et le système de gestion de la loterie informatisée ;
- Aucune procédure de sauvegarde n'est appliquée au niveau des logiciels de calcul des recettes et des commissions des vendeurs.

2.1.3.2. Modalités de sauvegardes

- Au niveau du logiciel comptable SAARI, les sauvegardes sont effectuées quotidiennement par l'administrateur réseau sur des CD qu'il conserve ;
- Les sauvegardes du logiciel de paie sont effectuées chaque mois sur le disque dur du serveur du service paie ;
- Pour le système de gestion de la loterie informatisée, les sauvegardes des données sont effectuées quotidiennement sur disquettes DAT (Digital Audio Tape). Les sauvegardes du logiciel et des références sont effectuées mensuellement. Les supports sont conservés au niveau du centre de suivi, dans de simples armoires.

2.1.3.3. Plan de secours

La société ne dispose pas de plan de secours et aucune réflexion n'a été menée à ce niveau

Conclusion du chapitre

La revue de la sécurité informatique menée au cours de la mission d'audit financier de la Société Africaine des Jeux a permis d'obtenir une description détaillée des mesures de sécurité physique, logique et des procédures de sauvegarde mises en place et appliquées dans l'entreprise.

Les résultats présentés dans ce chapitre ont fait l'objet d'une analyse afin de déterminer l'incidence de la politique de sécurité informatique de la société sur le risque inhérent et donc sur le risque d'audit que présente cette mission.

CHAPITRE 3 : ANALYSE DES RESULTATS ET RECOMMANDATIONS

Introduction

Dans le cadre de l'étude de l'incidence de la sécurité informatique sur la démarche d'audit financier de la Société Africaine des Jeux, nous avons effectué une revue qui a révélé des résultats présentés dans le chapitre précédent. Ces résultats ont fait l'objet d'une analyse afin de déterminer leur effet sur les diligences à mettre en œuvre lors de la mission.

Par ailleurs les points faibles relevés au niveau de la sécurité informatique de la SAJE ont fait l'objet d'un rapport adressé aux dirigeants de la société. Ce rapport avait pour principal objectif d'apporter des recommandations constructives aux différents problèmes soulevés et de proposer un plan de mise en œuvre des solutions suggérées.

Le présent chapitre sera divisé en deux principales sections :

1. **Analyse des résultats obtenus ;**
2. **Recommandations et plan de mise en oeuvre.**

3.1. Analyse des résultats

L'incidence des procédures de sécurité informatique sur la démarche d'audit de la SAJE a été déterminée après analyse des différents résultats obtenus au cours de nos travaux.
Cette analyse qui est en fait une évaluation des procédures décrites consistait essentiellement à identifier les points forts et les points faibles du système ainsi que les risques liés à ces derniers.

Notre évaluation a été effectuée sur les trois plans suivants :

- La sécurité physique ;
- La sécurité logique ;
- Les sauvegardes et le plan de secours.

3.1.1. Analyse de la sécurité physique de la société

L'évaluation des procédures de sécurité physique de la SAJE a relevé les forces suivantes :

- ✓ Surveillance de l'accès aux locaux de la société ;
- ✓ Correcte sécurisation de l'accès au centre de suivi de la loterie informatisée et de ces locaux informatiques ;
- ✓ Présence d'extincteurs au niveau de tous les locaux de la société ;
- ✓ Lieux de stockage des fournitures et des consommables (différents des salles serveurs) ;
- ✓ Bonne protection des ordinateurs contre les dégâts électriques.

Les points faibles relevés au niveau de la sécurité physique de la société se résument dans le tableau suivant :

Tableau N° 7 : Faiblesses relevées au niveau de la sécurité physique de la SAGE

	Points faibles	Incidence sur le risque inhérent
Accès aux locaux	- Absence de vérification de l'identité des visiteurs et de surveillance de ces derniers pendant leur présence au siège, (principalement au service paie) et au Site 1	Risque de fraudes ou d'accès non autorisés aux biens de la société et à des données confidentielles par des personnes mal intentionnées
Protection incendie	- Absence de détecteurs de fumée dans les locaux de la société - Armoires non ignifugées	Des dégâts importants peuvent être causés par des incendies, ce qui rendrait le système indisponible Risque de pertes de données importantes pouvant entraîner l'arrêt des activités de la société

Source : Nous-même

Les failles exposées ci-dessus peuvent être l'origine d'éventuels vols de biens de la société, ce qui remettrait en cause l'existence des actifs comptabilisés. Elles peuvent également mettre en cause la continuité des activités de la société.

3.1.2. Analyse de la sécurité logique de la société

Les points forts relevés à ce niveau sont les suivants :

- ✓ Les comptes et les droits d'accès du logiciel comptable et du système de gestion de la LI correspondent aux fonctions des utilisateurs ;
- ✓ Il existe des mots de passe au niveau le logiciel SAARI, du système de la loterie informatisée et des logiciels de calcul des recettes ;

- ✓ Au niveau du système de gestion de la loterie informatisée, une longueur minimum est requise à la création des mots de passe et ceux-ci sont régulièrement changés ;
- ✓ Des pare-feux ont été installés sur le réseau et pour l'accès à Internet ;
- ✓ La connexion Internet n'est pas disponible sur les postes reliés au système de traitement des données (loterie informatisée, comptabilité, paie, calcul des recettes) ;
- ✓ Mise à jour régulière de l'anti-virus ;

L'évaluation des procédures de sécurité logique de la société a également révélé des faiblesses qui se présentent comme suit :

Tableau N° 8 : Faiblesses relevées au niveau de la sécurité logique

	Points faibles	**Incidence sur le risque inhérent**
Gestion des habilitations/ profils utilisateurs	- Les profils pour l'accès aux logiciels de paie et de calcul des recettes et des commissions vendeurs ne sont pas gérés	Risque que les utilisateurs de ces logiciels aient accès à des informations sensibles ou aient des droits illimités qu'ils ne devraient pas avoir du fait de leur fonction
Gestion des mots de passe	- Le logiciel de paie de la société ne comporte pas de mot de passe - Les mots de passe du SAARI et des logiciels de calcul des recettes et des commissions vendus ne sont pas régulièrement changés	Risque que des personnes non autorisées, notamment les employés, aient accès aux informations concernant le personnel et que certaines données concernant les salaires soient modifiées ou supprimées Risque que les mots de passe soient connus par des personnes non autorisées qui peuvent avoir accès aux données de la comptabilité et de

	Points faibles	**Incidence sur le risque inhérent**
		la Direction de l'Exploitation afin de les modifier, de les subtiliser, de les modifier ou de les altérer
Utilisation d'Internet / messagerie	- Le personnel de la société n'a pas été sensibilisé aux modalités d'utilisation d'Internet dans le cadre professionnel - Il existe des accès individuels multiples pour la connexion à Internet	Risque que les utilisateurs visitent des sites non autorisés et importent des virus qui peuvent altérer les données de l'entreprise ou détruire son système. Risque plus élevé d'attaques externes mettant en danger le réseau car la société disposent de plusieurs ouvertures, ce qui la rend plus vulnérable
Antivirus	- La mise à jour de l'antivirus se fait de manière manuelle	Risque que certains postes soient oubliés lors des mises à jour
Protection réseau	- Les accès au réseau du siège et aux logiciels de gestion (SAARI, paie, calcul des recettes) ne font l'objet d'aucun suivi	Risque de non détection des attaques et impossibilité de situer les responsabilités en cas d'incidents au niveau du réseau ou en cas de fraudes informatiques au niveau des logiciels de gestion
Sensibilisation des utilisateurs	- La société ne dispose pas de charte de bonne utilisation du système informatique et le personnel n'a pas été sensibilisé aux problèmes de sécurité - Les utilisateurs ne bénéficient	Risque de non respect des consignes de sécurité informatique par les utilisateurs, pouvant entraîner de sérieux problèmes de sécurité Risque d'erreurs dans le système de

	Points faibles	Incidence sur le risque inhérent
	pas d'une formation continue sur l'utilisation des différents outils informatiques	la société et d'altération des données causées par une mauvaise utilisation des outils informatiques.

Source : Nous-même

Les faiblesses constatées au niveau des procédures de sécurité logique ont une répercussion sur les comptes de la société en ce sens qu'elles peuvent être la cause d'erreurs, d'omissions ou de destruction de données au niveau de la comptabilité (exhaustivité et rattachement des opérations enregistrées).

3.1.3. Analyse des procédures de sauvegarde et du plan de secours de la société

Au niveau des sauvegardes et du plan de secours, nos travaux n'ont révélé qu'un seul point fort. Il concerne la fréquence des sauvegardes au niveau du système de gestion la loterie informatisée. Les données y sont sauvegardées quotidiennement et les références mensuellement.

Les faiblesses relevées ont fait l'objet d'une analyse qui est résumée dans le tableau ci-dessous.

Tableau N° 9 : Faiblesses relevées au niveau des procédures de sauvegarde et du plan de secours

	Points faibles	Incidence sur le risque inhérent
Procédures de sauvegarde	- Les procédures de sauvegarde appliquées au sein de la société ne sont pas formalisées	Risque que les utilisateurs ne soient pas correctement informés sur ces procédures et que celles-ci ne soient pas correctement appliquées
Modalités de sauvegarde	- Les données traitées au niveau des logiciels de calcul des	En cas d'incident au niveau de ces logiciels, impossibilité de récupérer

	Points faibles	Incidence sur le risque inhérent
	recettes et des commissions des vendeurs ne font l'objet d'aucune sauvegarde	les données. Par ailleurs, cela n'est pas en conformité avec l'obligation légale de conservation des justificatifs de la comptabilité pendant dix (10) ans
	- Les sauvegardes effectuées (SAARI et LI) ne sont pas conservées hors de la société	En cas d'incendie ou d'inondation, la société ne serait pas en mesure de récupérer les données perdues, ce qui mettrait en péril la continuité de l'exploitation
Plan de secours	- La société ne dispose pas de plan de secours et aucune réflexion n'est menée sur ce sujet	En cas de sinistre, (incendie, inondation, indisponibilité longue du système informatique) entraînant une destruction des données et du matériel, la société ne pourrait plus assurer la poursuite de ses activités

Source : **Nous-même**

Les lacunes au niveau des procédures de sauvegarde ne permettent, ni d'assurer la protection du patrimoine de la société, ni de garantir la continuité de l'exploitation de la SAJE.

La multiplicité et l'importance des faiblesses relevées dans le système de sécurité informatique de la Société Africaine des Jeux ont rendu nécessaire la rédaction d'un rapport sur la sécurité informatique que nous avons adressé à la direction générale. Ce rapport avait pour objectif, d'attirer l'attention des dirigeants sur les lacunes des procédures de sécurité informatique en vigueur dans la société, de mettre l'accent sur les conséquences que pourraient avoir ces lacunes sur l'activité de la SAJE et enfin de proposer des recommandations en vue de renforcer la sécurité informatique.

3.1. Recommandations

Les termes de références de la mission d'audit de la SAJE à laquelle nous avons participé précisaient que le consultant devra présenter à la direction générale un rapport sur les procédures comportant des recommandations constructives. Pour être en conformité avec ces exigences, nous avons rédigé, à la fin de nos travaux, un rapport sur les procédures de sécurité informatique afin de faire part à la direction de l'entreprise de nos observations et recommandations. Celles –ci se présentent comme suit :

3.2.1. Recommandations sur la sécurité physique

Les recommandations faites concernant la sécurité physique de la SAJE sont les suivantes :

1. L'identité des visiteurs devrait être systématiquement vérifiée à leur entrée dans les locaux de la société. Pendant toute la durée de leur présence dans la société, ils devraient porter un badge « visiteur » et être accompagnés ;

2. L'accès à toutes les salles informatiques, notamment celles du service paie et de la Direction de l'Exploitation, devrait être règlementé par la présentation de cartes magnétiques ou de badges afin de s'assurer que seules les personnes autorisées accèdent à ces salles ;

3. Des détecteurs de fumée devraient être installés dans tous les locaux de la société pour prévenir d'éventuels incendies ;

4. Toutes les salles informatiques devaient disposer d'armoires ignifugées pour la conservation des sauvegardes pour permettre une récupération des données sauvegardées en cas d'incendie ;

3.2.2. Recommandations sur la sécurité logique

Sur le plan de la sécurité logique, nous avons formulé les recommandations suivantes :

1. Le responsable informatique devrait veiller à la bonne gestion des accès aux logiciels de paie et de calcul des recettes et des commissions afin de s'assurer que les droits attribués correspondent aux fonctions des utilisateurs ;

2. Tous les logiciels et applications utilisés au sein de la société doivent comporter des mots de passe pour en restreindre l'accès ;

3. Tous les mots de passe devraient être changés régulièrement pour qu'ils ne soient pas connus de personnes non autorisées. Pour ce faire, les mots de passe devraient être configurés pour expirer après une certaine durée (ex : 2 mois). A l'approche de la date d'expiration, des rappels devraient être automatiquement envoyés aux utilisateurs ;

4. La société devrait rédiger une charte d'utilisation du système informatique et d'Internet dans le cadre professionnel. Cette charte devra être lue et signée par chaque utilisateur ;
5. La connexion Internet devrait être centralisée au niveau d'un seul modem afin de faciliter la gestion des accès au web et de réduire la possibilité d'attaques externes ;

6. L'antivirus de la société devrait être installé en ligne sur tous les postes et faire l'objet d'une gestion centralisée. Ainsi, les mises à jour se feraient automatiquement ;

7. Les accès aux logiciels de gestion (SAARI, paie, calcul des recettes) devraient faire l'objet d'un suivi afin de situer les responsabilités en cas d'incident informatique ou de fraude ;

8. Des sessions de formation devraient régulièrement être organisées pour les utilisateurs du système de la société afin d'assurer la correcte utilisation des outils informatiques (matériel et logiciels) et réduire ainsi les risques d'erreurs dans les données et les incidents informatiques en général.

3.2.3. Recommandations sur les procédures de sauvegarde et le plan de secours

Les principales recommandations faites concernant les procédures de sauvegarde et le plan de secours sont les suivantes :

1. Le service informatique devrait élaborer un manuel de procédures informatiques qui comprendrait les procédures de sauvegarde et serait mis à la disposition de tous les utilisateurs ;

2. Toutes les données traitées au niveau des différents logiciels de la société (SAARI, paie, système de la loterie informatisée, calcul des recettes) devraient faire l'objet de sauvegardes quotidiennes. Ces sauvegardes devraient être faites en deux copies, une serait conservée par les différents responsables informatiques dans des coffres ignifugés et l'autre hors de la société.

3. La direction générale de la société devrait initier une réflexion en ce qui concerne le plan de secours afin de disposer le plus tôt possible d'un site de secours et d'un plan de reprise et être ainsi en mesure d'assurer la continuité des activités en cas de sinistre grave.

Les recommandations présentées dans notre rapport sur la sécurité informatique de la SAJE ont été acceptées. Nous avons par la suite proposé un plan de mise en œuvre pratique.

3.2.4. Plan de mise œuvre des recommandations

Ce plan a pour objectif de préciser les modalités pratiques de mise en application des recommandations formulées dans notre rapport, tout en respectant le principe de d'indépendance. Il a été établi en tenant compte des capacités économiques et humaines de l'entreprise.

Pour renforcer la sécurité informatique de la Société Africaine des Jeux, la direction générale devrait veiller à :

- la centralisation de toute l'informatique de la société au niveau du service informatique ;
- la nomination d'un responsable de la sécurité informatique ;
- l'élaboration d'une charte de sécurité informatique
- l'établissement par les responsables du service informatique d'un budget informatique annuel ;
- la mise en pratique de chacune des recommandations formulées dans notre rapport ;
- à la réalisation d'un audit des différents logiciels utilisés au sein de la société ;
- la réalisation d'un audit de la sécurité informatique tous les trois (3) ans.

Conclusion du chapitre

Ce dernier chapitre, consacré à la présentation des résultats de nos travaux sur le terrain, permet d'illustrer de manière pratique l'incidence de la sécurité informatique sur la démarche d'audit financier d'une organisation. Le contexte de notre étude étant une mission d'audit financier contractuel, nous nous devions de présenter ces résultats sous la forme d'un rapport en formulant des recommandations afin d'améliorer les procédures en vigueur dans la société. Enfin, le plan de mise en œuvre présenté dans ce chapitre a reçu l'approbation de la direction générale et a déjà commencé à être appliqué.

CONCLUSION DE LA PARTIE PRATIQUE

Comme pour toute société informatisée, l'audit financier de la Société Africaine des Jeux ne pouvait s'effectuer sans une étude du système informatique. La mission d'audit de cette société a donc constitué le cadre idéal pour la mise en pratique de notre modèle d'analyse.

L'objectif de cette partie était de déterminer l'incidence que pouvait avoir la politique de sécurité informatique de la SAJE sur la démarche adoptée lors de la mission d'audit financier à laquelle nous avons pris part.

Pour atteindre cet objectif nous avons effectué différents travaux constitués essentiellement d'une revue documentaire, d'entretiens et d'une observation physique des procédures qui nous ont été décrites. A la suite de ces travaux, nous avons constaté que le système de sécurité informatique de la SAJE présentait de nombreuses lacunes qui, du fait de leur incidence sur le risque inhérent ont influé sur les contrôles substantifs à mettre en œuvre dans la phase de collecte d'élément probants.

L'analyse des failles du système de sécurité a également permis de formuler, conformément aux exigences des commanditaires de la mission, des recommandations permettant d'améliorer les procédures en vigueur et de réduire les risques auxquels était exposée la société. La mise en pratique des recommandations, à travers le plan de mise en œuvre présenté à la direction, permettra à la SAJE de renforcer son système de sécurité informatique et de garantir la continuité de son exploitation et la sauvegarde de son patrimoine.

CONCLUSION GENERALE

Un des signes les plus visibles de l'évolution du monde des affaires est, sans nul doute, l'informatisation grandissante des entreprises. Mais ce développement technologique ne va pas sans son corollaire : la fraude informatique. Ce constat paradoxal est à l'origine de la prise de conscience, dans le milieu de l'audit financier, de l'importance de l'étude du système informatique et plus particulièrement du système de sécurité informatique.

Les travaux menés lors de notre étude nous ont amenés à la conclusion que la politique de sécurité informatique en vigueur dans une organisation a une incidence sur la démarche adoptée pour l'audit financier de celle-ci.
En effet, la démarche finale retenue pour l'audit financier d'une organisation dépend du niveau du risque d'audit déterminé par l'auditeur. Ce risque d'audit est lui-même constitué du risque inhérent et du risque lié au contrôle. Ainsi tout élément influant sur l'un ou l'autre de ces deux composantes aura une incidence sur la démarche d'audit à adopter. La spécificité de la démarche se manifestera à travers les contrôles à mettre en œuvre pendant la phase de collecte d'éléments probants.

Notre revue de littérature avait révélé que l'incidence de la sécurité informatique sur la démarche de l'auditeur financier se manifeste principalement au niveau du risque inhérent. Nos travaux lors de la mission d'audit de la SAJE ont permis de le démontrer.

Cependant il faut noter que le risque inhérent seul ne peut pas permettre de définir la nature et l'étendue des contrôles à mettre en œuvre (**Cf. Tableau N° 1**). Il faudrait également évaluer le risque lié au contrôle.
Or dans la méthodologie d'audit financier en milieu informatisé présenté dans la partie théorique (**Cf. Figure N° 5**), l'évaluation du risque lié au contrôle dans une entreprise informatisée se fait à travers l'étude des applications informatiques jouant un rôle important dans le processus d'élaboration des comptes.
Ainsi donc, un élargissement du cadre de notre mémoire à l'étude des principales applications de la Société Africaine Jeux, aurait permis d'obtenir des résultats plus précis notamment de déterminer l'impact définitif de la sécurité informatique sur les contrôles substantifs mis en œuvre pour l'audit de la société.

Par ailleurs, les sociétés informatisées se montrent de plus en plus concernées par les problèmes de sécurité informatique et font plus souvent appel à des spécialistes (auditeurs informatiques) pour des audits réguliers de leur système de sécurité. Ceux-ci dans le cadre de leurs missions, disposent d'outils sophistiqués comme la méthode MARION (Méthode d'Analyse des Risques Informatiques Orientée par Niveaux) ou la méthode MEHARI (Méthode Harmonisée d'Analyse des Risques Informatiques) qui permettent de déceler, de manière plus efficace, les failles du système de sécurité informatique de l'organisation et de proposer des mesures permettant de pallier au mieux ces failles.

BIBLIOGRAPHIE

Ouvrages

1. BENSOUSSAN Alain (1994), *L'informatique et le droit. Tome 1 : assistance technique, assurance, audit, banques de données, centres de secours, comptabilité, contrats, distribution, EDI, études et conseils, facilities management, financement,* Hermès Paris, 694 pages
2. CHARRON Claude (1998), *Normes internationales d'audit : IFAC handbook 1998 : traduction française,* CNCC Edition Paris, 524 pages
3. CNCC (1995), *La démarche du commissaire aux comptes en milieu informatisé,* CNCC Edition Paris, 142 pages
4. CNCC (Avril 2003), *Prise en compte de l'environnement informatique et incidence sur la démarche d'audit*, CNCC Edition Paris, 227 pages
5. COLLINS Lionel, VALIN Gérard (1992), *Audit et contrôle interne : aspects financiers, opérationnels et stratégiques*, DALLOZ Paris, 373 pages
6. DELSOL Xavier (1999), *Guide d'audit des associations : le diagnostic juridique, social, fiscal, comptable, financier et informatique,* Juris-Service Paris, 319 pages
7. DERRIEN Yann (1992), *Les techniques de l'audit informatique,* DUNOD Paris, 238 pages
8. DUNSMORE Bradley, BROWN Jeffrey, BALLEW Jolli Annette (2002), *Sécurité Internet,* First Interactive Paris, 512 pages
9. GODART Didier (2002), *Sécurité informatique : Risques, Stratégies et Solutions*, Chambre de Commerce et d'Industrie, 334 pages
10. GRAND Bernard, VERDALLE Bernard (1999), Audit comptable et financier, Economica Paris, 112 pages
11. HERRBACH Olivier (2000), *Le comportement au travail des collaborateurs de cabinets d'audit financier : une approche par le contrat psychologique* (Thèse de doctorat - Université des Sciences sociales – Toulouse I), [En ligne]. Adresse : lirhe.univ-tlse1.fr/membres/cv/cv-herrbach.pdf
12. HOUNZANGBE Frédéric (1994), *Audit comptable et financier en milieu informatique* CESAG Dakar, 87 pages

13. IFACI (1993), *Audit et contrôle des systèmes d'information. Module 5 : audit des systèmes applicatifs,* IFACI Paris, 136 pages

14. IFACI (1993), *Audit et contrôle des systèmes d'information. Module 8 : sécurité,* IFACI Paris, 130 pages

15. IFACI (1993), *Audit et contrôle des systèmes d'information. Module 9 : plan de secours,* IFACI Paris, 58 pages

16. JENKINS Brian, PINKNEY Anthony (1984), *Audit des systèmes et des comptes gérés sur informatique*, Publi-Union Paris, 369 pages

17. JORAS Michel (1996), *Les fondamentaux de l'audit,* Préventique Bordeaux, 99 pages

18. LAMY Jean-Paul (1996), *Audit et certification des comptes en milieu informatisé*, Editions d'organisation Paris, 127 pages

19. MAÏDOUDOU Abakar (1992), *Rôle de l'auditeur en matière de système d'information de l'entreprise*, CESAG Dakar, 112 pages

20. MERCIER Antoine, Merle Philippe (2002), *Audit et commissariat aux comptes 2003 – 2004,* Francis Lefebvre

21. MIKOL Alain (1999), *Les audits financiers : comprendre les mécanismes du contrôle légal,* Editions d'organisation Paris, 198 pages

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

23. RAFFEGEAU Jean, RITZ Alain (1993), *Audit et Informatique,* 2ème édition, Presses Universitaires de France Paris, 127 pages

24. SAJE, *Manuel de procédures*

25. SARR Ababacar (2004), *Audit informatique*, CESAG Dakar, 68 pages

26. SOLTANI Bahram (1996), *Le commissaire aux comptes et le marché financier*, Economica, 176 pages

27. THORIN Marc (1991), *L'audit informatique. Méthodes, règles, normes*, 3ème édition, Masson, 176 pages

28. THORIN Marc (2000), *L'audit informatique*, Hermès, 184 pages

29. WEBER Ron (1999), *Information systems control and audit,* Prentice Hall Upper Saddle River, 1013 pages

Articles

30. CEFRIO (2003, octobre), « Sécurité informatique votre entreprise est-elle vraiment à l'abri », *Info CEFRIO,* [En ligne]. Adresse par FTP : cefrio.qc.ca **Répertoire :** InfoCEFRIO **Fichier :** info_vatis.cfm

31. FOUR Ludovic (2004, juin), « Sécurité informatique et besoins des utilisateurs : un compromis difficile », *Sécurité informatique,* [En ligne] (49) : pp 1 - 4. Adresse par FTP : sg.cnrs.fr **Répertoire :** FSD/securite-systemes/revues-pdf **Fichier :** num49.pdf

32. GRALL Matthieu, GALLET Alain (2003, décembre), « EBIOS, une méthode de gestion des risques », *Sécurité informatique,* [En ligne] (47) : pp 1 - 4. Adresse par FTP : sg.cnrs.fr **Répertoire :** FSD/securite-systemes/revues-pdf **Fichier :** num47.pdf

Site Internet

33. CEFRIO, *Infomètre Répertoire d'études statistiques sur les technologies de l'information,* [En ligne]. http://www.infometre.cefrio.qc.ca/ (Page consultée le 10 septembre 2005)

34. CLUSIF, *Ouvrages CLUSIF en libre téléchargement - Dossiers techniques,* [En ligne]. http://www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=DOSSIERS%20TECHNIQUES (Page consulté le 09 octobre 2005)

35. Comité réseau des Universités, *Pourquoi la sécurité,* [En ligne]. http://www.cru.fr/securite/Generalites/pourquoi.html (Page consultée le 23 novembre 2005)

36. Comment Ca Marche Encyclopédie informatique, *Introduction à la sécurité informatique,* [En ligne]. http://www.commentcamarche.net/secu (Page consultée le 23 novembre 2005)

37. HOFFMANN Michel, *Sécurité informatique: foire aux questions,* [En ligne]. http://users.swing.be/michel.hoffmann/faq.htm (Page consultée le 23 novembre 2005)

38. OCDE, *Recommandation du Conseil concernant les Lignes directrices régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité,* [En ligne]. http://webdomino1.oecd.org/horizontal/oecdacts.nsf/0/9a7ef793aa8a28f3c1257089002b8052?OpenDocument&Click= (Page consultée le 10 octobre 2005)

39. PILLOU Jean-François, *Mise en place d'un réseau privé virtuel,* [En ligne]. http://www.commentcamarche.net/faq/sujet-2639-%5BWindows-XP%5D-Mise-en-place-d'un-r%E9seau-priv%E9-virtuel-VPN (Page consultée le 10 octobre 2005)

40. SAIZ Jérôme, *Protéger ses infrastructures : la sécurité physique requiert des spécialistes,* [En ligne]. http://www.01net.com/article/175234.html (Page consultée le 23 novembre 2005)

41. WIKIPEDIA l'encyclopédie libre, *Sécurité informatique*, [En ligne]. http://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_informatique (Page consultée le 23 novembre 2005)