CESAG

CENTRE AFRICAIN D'ETUDES SUPERIEURES EN GESTION

INSTITUT SUPERIEUR DE COMPTABILITE
(ISC)

DESS AUDIT INTERNATIONAL ET CONTROLE

MEMOIRE DE FIN DE CYCLE

13ème promotion

Thème :

LA MAITRISE DES RISQUES LIES AU SYSTEME INFORMATIQUE DES BANQUES : LE CAS DE ECOBANK-COTE D'IVOIRE

Mémoire de3ème cycle

Présenté et soutenu par :
N'GUETTA Andju Roland

Directeur de mémoire :

M. Abdourahmane DIOP
Enseignant Vacataire au CESAG

Maître de stage :

Mlle MERCEDES MAIGA
Directeur Département Audit et Contrôle Interne à ECOBANK-COTE D'IVOIRE

Février 2003

DEDICACES

Je dédie ce mémoire à :

Dieu, le Tout-Puissant, qui m'a soutenu et béni au cours de cette formation ;

Mon bien-aimé père, feu **FIAN N'GUETTA**, qui n'a pas pu voir le dénouement de cette formation, Papa, que ton âme repose éternellement en paix !

Ma mère, **AKA ANDIWA**, qui m'a encouragé et m'a appris la persévérance ;

Mon frère aîné, **EBAH BASILE**, pour son soutien financier et pour tous les efforts qu'il a déployés pour que cette formation voit le jour ;

Mes frères et sœurs, pour votre soutien et vos prières quotidiennes ;

Ma petite amie, **SERY LAURE**, pour son soutien moral.

REMERCIEMENTS

A l'issue de cette formation, nous tenons à remercier toutes les personnes qui, par leur soutien moral, intellectuel et financier nous ont permis de réaliser ce travail.

Nous remercions plus particulièrement :

Monsieur **LOUKOU DIA**, DRH du Ministère de la Santé, pour m'avoir facilité le départ sur Dakar ;

Le corps professoral du CESAG notamment MM **ABDOURHAMANE DIOP** et **MOUSSA YAZI**, pour leur disponibilité à nous encadrer ;

Mes neveux et nièces **Michel, Nadia, Annick, Renée, Cyrielle, Aaron,**

Mes frères de la maison blanche **SIDIBE, NAZERI, MOHAMED** pour leurs précieux conseils ;

Mes familles d'accueil à Dakar, les familles **KOFFI** et **MOUSSA** ;

Mes amis de la BCEAO et du point E ;

La 13ème promotion du Cycle Audit International et Contrôle du CESAG.

Nous ne saurions terminer nos propos sans adresser nos remerciements à :

Monsieur **FOGAN SOSSAH**, DG de ECOBANK COTE D'IVOIRE, pour avoir accepté spontanément de nous accueillir au sein de l'institution qu'in dirige ;

Toute l'équipe du Département Contrôle Interne de ECOBANK SENEGAL et ECOBANK COTE D'IVOIRE particulièrement Mlle **MERCEDES MAIGA**, Directeur du Département et son Assistant **PATRICK D'ALMEIDA** ;

Monsieur **AZIZ FAYE**, Directeur de l'Informatique et Technologie de ECOBANK SENEGAL.

ABREVIATIONS ET SIGLES

AFAI	:	Association Française de l'Audit et du Conseil Informatiques
BCEAO	:	Banque Centrale des Etats de l'Afrique de l'Ouest
CEAO	:	Communauté des Etats de l'Afrique de l'Ouest
CLUSIF	:	Club de la Sécurité Informatique Français
DRH	:	Direction des Ressources Humaines
DG	:	Directeur Général
ECI	:	Ecobank Côte d'Ivoire
ICU	:	Internal Control Unit
IFACI	:	Institut Français des Auditeurs Consultants Internes
IIA	:	Institute of Internal Auditors
ISACA	:	Information Systems Audit and Control Association
MARION	:	Méthode d'Analyse des Risques Informatiques et d'Optimisation par Niveau
ONG	:	Organisation Non Gouvernementale
RMT	:	Risque Maximal Tolérable
SI	:	Système Informatique
TIC	:	Technologie de l'Information et de la Communication
UEMOA	:	Union Economique et Monétaire Ouest Africaine

LISTE DES FIGURES ET TABLEAUX

LISTE DES FIGURES

LISTE DES TABLEAUX

SOMMAIRE

INTRODUCTION GENERALE

CONTEXTE DE L'ETUDE

L'importance du système informatique pour l'entreprise, l'aspect stratégique de certaines de ses composantes et la complexité du problème de sa sécurité ne sont plus à démontrer. En 1991, le Secrétariat Général de la Commission Bancaire de la Banque de France a mené une réflexion sur la prise en compte du «risque systémique dans la surveillance prudentielle des établissements de crédit » qui comportait quatre volets dont l'un portait sur les risques informatiques dans le monde bancaire. Les conclusions de cette étude ont montré que la sûreté des systèmes d'information fait partie intégrante de la sécurité des établissements de crédit. Et ces derniers ont un devoir de sécurité vis-à-vis de leurs clients, d'eux-mêmes et de l'ensemble du système bancaire.

C'est pourquoi, dans un contexte marqué par la concurrence accrue, les établissements de crédit devraient porter une attention particulière sur une mesure efficiente des risques qu'ils encourent.

Le règlement du comité de la réglementation bancaire 91-04 relatif à l'organisation du système comptable et au dispositif du traitement de l'information donne les grands principes qui doivent présider à la sûreté des systèmes d'information.

En effet, selon l'article 3 dudit règlement, le contrôle des systèmes d'information s'étend à la documentation relative aux analyses, à la programmation et à l'exécution des traitements. Ce dispositif de contrôle concourt à garantir l'intégrité et la disponibilité de l'information traitée, mieux à assurer la pérennité de l'organisation. C'est pourquoi dans les établissements de crédits, une attention particulière doit être portée sur la sécurité du système informatique.

PROBLEMATIQUE

Les banques et établissements financiers assurent une mission essentielle dans la vie économique, en rapport avec leur pouvoir de création monétaire. Leur rôle primordial réside dans la mobilisation de l'épargne : ils collectent les fonds aux agents économiques disposant d'excédents (épargnants) et les prêtent aux agents à besoin de financement (emprunteurs). Cette fonction d'intermédiation traduit le transfert des risques de la clientèle vers l'établissement financier.

Cependant, avec le développement de l'économie des années 1980, les systèmes bancaires ont connu de profonds bouleversements : la déréglementation, la désintermédiation et le décloisonnement des marchés. Ces mutations ont eu pour corollaire de modifier les statuts, les interventions et le contrôle des différents acteurs du paysage bancaire.

Ainsi, l'exercice de la profession bancaire a-t-il été régi par des dispositions relevant aussi bien des législations nationales, du droit d'essence communautaire que des conventions internationales notamment les recommandations du Comité de Bâle. Cette réglementation spécifique vise essentiellement à garantir la solvabilité et la liquidité des banques, la protection des déposants et de manière générale, la sécurité du système bancaire dans son ensemble.

Les banques, compte tenu du développement et de la complexité croissante des opérations et transactions traitées, sont enclines à reconsidérer leurs méthodes de travail et à se doter d'un système informatique performant. L'émergence des nouvelles technologies de l'information et de la communication (NTIC) constitue une solution pour rationaliser leur structure de fonctionnement et d'être davantage plus compétitif.

En effet, pour affronter un contexte marqué par la globalisation financière, les établissements de crédits sont de plus en plus amenés à consacrer des investissements significatifs dans les systèmes d'information. Ce système repose en particulier sur

l'organisation de la comptabilité, de la fonction informatique, les matériels de traitement et les logiciels mis en œuvre. Il importe que la banque fonctionne dans un environnement sécurisé et que sa capacité corresponde aux besoins de l'établissement.

Cependant, au cours de ces dernières années, avec l'utilisation accrue des réseaux, de la prolifération des micro-ordinateurs et du développement de la culture informatique, les risques d'intrusion dans les systèmes informatiques sont devenus très fréquents (détournement de virements automatiques, divulgations de données confidentielles, attaque de virus...). Alors que les banques ont un devoir de sécurité vis-à-vis d'elles-mêmes, de leurs clients et du système bancaire dans son ensemble. La menace informatique constitue un danger réel pour les établissements de crédit. L'enquête menée en 1992 par le Secrétariat Général de la Commission Bancaire (SGCB) de la Banque de France montre que le niveau de sécurité des systèmes informatiques est encore perfectible.

Pour les établissements de crédit, les nouvelles technologies de l'information et de la communication sont devenues un outil de production principal et incontournable : les valeurs monétaires dématérialisées sont contenues, stockées, transportées et valorisées grâce à elles. Ainsi, les risques induits par les défaillances informatiques sont plus élevés dans les banques et établissements financiers que dans les autres secteurs d'activités parce qu'ils peuvent engendrer des conséquences néfastes pour les autres organisations en relation avec eux ; voire avoir des répercussions sur l'ensemble de l'économie si l'incident était prolongé. L'impact que rencontrerait une banque lorsque la sécurité de son système informatique n'est pas assurée, est important et rapide. En effet, la non disponibilité de l'information n'assurerait pas la continuité du service encore moins les objectifs de performance et temps de réponse et des heures limites de traitement des opérations. Cette situation amènerait les autres agents économiques et financiers à rompre les relations commerciales qu'elles entretiennent avec cette banque en difficulté. Or, tout établissement de crédit ne peut travailler en autarcie. Il a

besoin d'être refinancé par ses confrères et par les dépôts des clients. En outre, les risques encourus par la banque peuvent être dus à l'intégrité de l'information c'est-à-dire des pertes d'information découlant de la destruction totale ou partielle de ses fichiers stratégiques.

Les conséquences de ces risques entraînent des pertes de valeurs (coûts économiques des détournements) et des coûts indirects (pertes d'exploitation, temps perdu de réinstallation du système d'informatique). Ainsi, il convient de mettre en place un ensemble de « verrous » pour limiter les risques de fraudes et de défaillances.

Les raisons qui président à l'élaboration de ce dispositif de sécurité sont dues à l'importance stratégique de l'informatique et de l'information au sein de la banque. En effet, l'informatique occupe aujourd'hui une place prépondérante dans tout système d'information et elle est devenue en conséquence le point de passage obligatoire de tous les flux d'information. L'outil informatique assure aux prestations fournies, plus de rapidité, de souplesse et d'efficacité. La nécessité de protection de l'information et des données réside non seulement dans le maintien de la compétitivité des entreprises mais aussi dans le droit de protection de la liberté des personnes et des entreprises.

C'est pourquoi, notre question de recherche est de savoir :

Comment la banque qui est une activité très risquée, parvient-elle à maîtriser les risques liés à son système informatique ?

De façon spécifique, quelles sont les mesures de sécurité mise en œuvre pour garantir la fiabilité des informations et la continuité de l'exploitation ?

Comment apprécier le niveau de maîtrise des risques qui pèsent sur le système informatique ?

Ces interrogations justifient le choix du thème : « **LA MAITRISE DES RISQUES LIES AU SYSTEME INFORMATIQUE DES BANQUES : LE CAS D'ECOBANK – COTE D'IVOIRE** ».

OBJECTIFS DE L'ETUDE

L'objectif de cette étude est d'évaluer le niveau de sécurité informatique de ECOBANK COTE D'IVOIRE.

De façon spécifique, il s'agira de :

1. Identifier les scenari de menaces informatiques sur l'activité de la banque ;
2. Analyser la pertinence des outils du contrôle interne pour assurer la protection du système ;
3. Faire des propositions d'amélioration.

INTERET DE L'ETUDE

Cette étude dont le thème est « **LA MAITRISE DES RISQUES LIES AU SYSTEME INFORMATIQUE DES BANQUES : LE CAS D'ECOBANK – COTE D'IVOIRE »** s'inscrit dans le cadre des directives des autorités bancaires pour se prémunir contre les menaces qui pèsent sur les établissements de crédit.

En effet, le contrôle des systèmes d'information qui s'étend à la conservation des informations et à la documentation relatives aux analyses, à la programmation et à l'exécution des traitements, doit faire l'objet d'une attention particulière des organes dirigeants en vue de s'assurer que :

- le niveau de sécurité des systèmes d'information est périodiquement apprécié et que, le cas échéant, les actions correctives sont entreprises ;
- les procédures de secours informatique sont disponibles afin d'assurer la continuité de l'exploitation en cas de difficultés graves dans le fonctionnement des systèmes informatiques.

Toutes ces dispositions concourent à fixer des objectifs de sécurité informatique jugés souhaitables par rapport aux exigences du métier.

◆ Cette étude permettra à ECI d'apprécier les zones de vulnérabilité de son système informatique et de mener des actions correctives.

◆ Pour nous-mêmes, l'intérêt que nous portons à cette étude est double.

Lors de notre premier stage à Ecobank – Sénégal, nous avions constaté que le système applicatif était régulièrement en « panne » portant non seulement préjudice aux clients car ne pouvant effectuer des opérations bancaires mais aussi sur la crédibilité (l'image) de l'institution. Cette même situation se reproduit à Abidjan et il nous est donc apparu nécessaire de mener une réflexion dans ce sens afin de déterminer les mesures de sécurité à mettre en œuvre en vue d'assurer la continuité de l'exploitation et de garantir la fiabilité de l'information. En outre, dans le souci d'approfondir nos connaissances théoriques acquises en matière d'audit informatique, nous avons voulu explorer la nécessité d'une réelle maîtrise du risque informatique dans les organisations.

◆ Pour le CESAG, cette étude servira de base à la prise en compte des risques qui pèsent sur son système informatique.

Pour tenter de répondre à ces objectifs, nous avons organisé notre mémoire en deux parties :

- La première partie rassemble les fondements théoriques indispensables. Nous avons regroupé dans trois chapitres :
  - Le premier chapitre traite des principaux concepts nécessaires notamment ceux relatifs au système informatique et les risques qui lui sont liés ;
  - Un deuxième chapitre aborde le dispositif de maîtrise des risques informatiques ;
  - Un troisième chapitre présente l'approche méthodologique de notre étude.
- La deuxième partie est consacrée au cadre pratique. En décrivant les caractéristiques essentielles du système d'information d'ECOBANK, nous souhaitons fournir au lecteur des

éléments de réponse sur les questions de sécurité et de contrôle pour minimiser les risques qui agissent sur le système informatique. Ainsi, nous avons reparti également cette partie en trois chapitres :

- Le premier chapitre concerne la présentation de ECOBANK – COTE D'IVOIRE ;
- Le second chapitre fait le diagnostic du dispositif de maîtrise des risques qui pèsent sur le système informatique de ECOBANK- COTE D'IVOIRE ;
- Le dernier chapitre rassemble les différentes recommandations pour améliorer l'existant.

DELIMITATION DU SUJET

Aux fins de ce mémoire, nous allons nous intéresser principalement à la sécurité de base qui garantit et réduit l'exposition au risque voire son élimination. Le volet sécurité des applications ne sera pas abordé compte tenu du cahier de charges soumis à la présente étude.

PREMIERE PARTIE :
CADRE THEORIQUE

Introduction

La première partie qui constitue le cadre théorique de notre étude, permettra d'éclairer certains concepts, définitions ou points de vue pour la compréhension du sujet et surtout de constituer le cadre de référence pour la bonne conduite de la partie pratique. Nous rappellerons les différents risques existants avant d'aborder les solutions à la disposition des entreprises pour lutter et réduire ces risques

CHAPITRE I : GENERALITES SUR LE SYSTEME INFORMATIQUE ET DE SES RISQUES

Introduction

Les systèmes d'information reposent sur les technologies actuelles de l'information et offrent des services sous forme de fonctionnalités de traitement, de calcul, de communication. Ceci est réalisé par la combinaison d'outils matériels et logiciels. Ainsi le recours étendu aux technologies de l'information a fortement amélioré les performances des systèmes d'information mais sans doute aussi leur vulnérabilité. Les problèmes de sécurité des systèmes d'information, sont très complexes. Tout d'abord, du fait de la multiplicité des formes sous lesquelles ils peuvent apparaître (de la catastrophe naturelle à l'acte malveillant de contamination du système par des virus, en passant par le vol de matériels). Ces problèmes dépassent rapidement le cadre de la seule informatique puisqu'il faut par exemple garantir la sécurité des locaux (contrôle des accès, système de lutte contre les incendies,...) afin de cerner l'ensemble des risques, qu'il soit d'origine informatique ou non. Il existe des méthodes d'évaluation des risques, permettant une approche globale des risques et une analyse précise de l'état de la sécurité au sein de l'entreprise.

Ce chapitre de notre étude est consacré à la présentation du système informatique et des risques qui lui sont associés. Après avoir défini le concept de système informatique, nous allons passer en revue les différents risques qui agissent sur le système informatique.

1. Concept de système informatique

Avant d'aborder le concept de système informatique, il n'est pas superflu de donner la définition de l'informatique.

Qu'est-ce que l'informatique ?

L'Académie Française (1966) définit l'informatique comme étant la science du traitement rationnel, notamment par machines automatiques, de l'information considérée comme le support des connaissances humaines et des communications dans les domaines techniques, économiques et sociaux. Aujourd'hui, le concept d'informatique recouvre d'autres réalités. Il ne désigne pas seulement une discipline scientifique mais c'est aussi le terme qui s'applique pour identifier, d'une part, le secteur d'activité économique qui produit et commercialise les ordinateurs, leurs composantes électroniques (microprocesseurs…), les moyens périphériques (disques, imprimantes, claviers…) et les programmes. Et d'autre part, c'est une technologie de traitement de l'information. Cette approche conceptuelle évoque l'aspect dynamique de l'informatique.

1.1 Définition du système informatique

Les phénomènes économiques contemporains sont caractérisés par une complexité croissante et des interactions multiples. L'approche systémique permet de définir et de caractériser ces phénomènes, quels que soient leur nature et leur degré de complexité. Elle permet en outre de mettre en évidence l'importance de la notion de flux (internes et externes). Au nombre de tous les flux qui traversent l'entreprise, les flux d'information jouent un rôle majeur. En effet , ils assurent la cohésion économique et sociale de l'entreprise en véhiculant une ressource essentielle : l'information (MOINE, 2000 :24).

L'information transite par le système informatique aux finalités et aux fonctions bien précises. Qu'entend – t- on par système informatique? Plusieurs conceptions du système

informatique existent. Mais aujourd'hui, quand on parle de système informatique, on se réfère systématiquement à un support informatique, du fait des progrès technologiques dans ce domaine. En effet, Bruno Fontaine dans son article sur les Nouvelles Technologies (Revue AFAI n° 59 :41) soutient que « l'apparition du concept de système informatique n'est pas sans lien avec les avancées de la technologie en matière de systèmes intégrateurs d'information (les architectures client/ serveur, Intranet, Internet, les bases de données distribuées, ...) ». Ce concept intègre également les éléments extérieurs à l'outil informatique tels les utilisateurs (au niveau connaissance et ergonomie du système), les fournisseurs et les différentes sources d'informations (formats, textes, images, ...), les réseaux et protocoles de communication car sans ces éléments, le système informatique ne serait pas dynamique.

Reix (2000 :75) donne une autre approche du système informatique qui rejoint en partie la 1ère vision. Pour lui, le système informatique est « l'ensemble des moyens et procédures permettant d'identifier, de traiter et d'enregistrer toutes les opérations de l'établissement conformément aux prescriptions en vigueur afin de conduire notamment par le biais d'une architecture informatique cohérente et contrôlable, à l'édition de documents de synthèse fiables et conformes aux exigences légales et réglementaires ».

A partir de ces approches conceptuelles, nous notons que le système informatique utilise les technologies de l'information pour transmettre, stocker, manipuler ou afficher l'information utilisée dans un ou plusieurs processus de gestion. C'est pourquoi à l'heure actuelle, les établissements de crédit mettent beaucoup l'accent sur les systèmes d'information automatisées qui constituent pour eux, un élément vital à son fonctionnement.

Quelles sont les finalités assignées au système informatique ?

1.2 Les finalités du système informatique

J.L PEAUCELLE (in MOINE, 2000 :25) recense trois finalités du système informatique :

a. Le système informatique aide à la prise de décision

Le système informatique met à la disposition des décideurs les informations nécessaires à la prise de décision et permet d'étudier les conséquences prévisibles des décisions et d'automatiser certaines décisions. Cette finalité joue un rôle majeur dans la gestion de l'établissement car permettant d'anticiper les éventuels dérapages et erreurs potentielles.

b. Le système informatique permet de contrôler l'évolution de l'organisation

Le système informatique permet de détecter les dysfonctionnements internes et les situations anormales. Pour atteindre cet objectif, le système informatique doit être la «mémoire collective » de l'organisation en gardant une trace des informations portant sur le passé.

c. *Le système informatique permet enfin de coordonner l'activité des différentes* composantes de l'entreprise.

Ainsi, ces trois finalités du système informatique permettent de mieux piloter l'entreprise et d'anticiper sur les changements. Pour atteindre ces finalités, des fonctions sont attribuées au système informatique.

1.3 Les fonctions du système informatique

Pour Alter (1996 :2), un système d'informatique est « un système qui utilise des technologies de l'information pour saisir ou recueillir, stocker, exploiter et diffuser l'information utilisée dans un ou plusieurs processus de gestion ». Cette approche conceptuelle du système informatique proposée par Alter permet d'attribuer quatre (4) fonctions : recueillir, mémoriser, exploiter et diffuser l'information.

- ***Recueillir l'information***

Le système informatique dispose de deux grandes sources d'alimentation en informations : les sources internes et les sources externes. Les sources internes sont toutes les composantes de l'entreprise générant de l'information. Le travail du SI consiste à capter tous les flux d'information internes circulant dans l'entreprise (documents comptables, notes d'information, mémorandums). Tandis que les sources externes peuvent être internationales, nationales, régionales ou locales. Ces sources émanent des partenaires, de concurrents ou d'organismes publics (les statistiques produites par la BCEAO ou par l'Institut National de la Statistique, etc.).

Face à ces diverses sources d'information, le système informatique remplit des tâches d'écoute, d'analyse et de saisie. L'information a de la valeur pour l'entreprise mais elle a aussi un coût, surtout quand elle est d'origine externe. La tâche d'écoute se double généralement d'une tâche d'analyse critique de la masse d'informations accessibles, afin d'éliminer toute source d'information et toute information peu pertinente ou de qualité insuffisante.

La phase d'écoute identifie les informations jugées pertinentes pour l'entreprise. Il faut ensuite saisir ces informations, c'est-à-dire les faire entrer dans le SI. L'objectif est de structurer des informations d'origines et de formes diverses. Des moyens humains et techniques sont utilisés mais aussi des méthodes, notamment des méthodes de contrôle et de codification de l'information afin de disposer d'informations fiables et facilement exploitables.

- ***Mémoriser l'information***

Une fois saisie, l'information doit être stockée de manière durable et stable. Le SI met en œuvre des moyens techniques et organisationnels (méthodes archivages, de protection

contre le piratage ou la destruction). Aujourd'hui, la mémorisation des informations se fait au moyen des fichiers et des bases de données.

- ***Exploiter l'information***

Une fois mémorisée, on peut appliquer à l'information une série d'opérations. Ces opérations de traitement consistent à :

- consulter les informations : les rechercher, les sélectionner……
- organiser les informations : les trier, les fusionner, les partitionner,….
- mettre à jour les informations : les modifier, les supprimer…..
- produire de nouvelles informations : informations calculées, cumuls….

- ***Diffuser l'information***

La diffusion consiste à mettre à la disposition des utilisateurs ou de manière générale de ceux qui en ont besoin, au moment où ils en ont besoin et sous une forme directement exploitable, l'ensemble des informations qui leur permettront d'assurer leurs activités. Les supports de cette diffusion sont multiples :

- le support oral utilisé particulièrement pour la communication interne
- le support papier utilisé tant pour la communication interne qu'externe
- le support électronique ou magnétique : aujourd'hui le plus utilisé tant en interne qu'en externe. Ce support est côté dans les services informatisés de l'entreprise ou entre les filiales via un réseau téléinformatique privé.

De ce qui précède, nous constatons que tous les systèmes d'information remplissent les mêmes fonctions à savoir recueillir, mémoriser, exploiter et diffuser l'information. Pour assurer ces différentes fonctions, des moyens sont mis en œuvre : les ressources.

1.4 Les composantes du système informatique

Les composantes ou ressources du système informatique sont tous les moyens qui assurent ou qui participent à la saisie, au traitement, au stockage, à la diffusion et à la transmission des informations au sein de l'entreprise. Elles sont la cible des menaces potentielles. L'AFAI retient les ressources du système informatique en 4 types dont les ressources humaines, le matériel, les logiciels et procédures et les données et leurs supports.

1.4.1 Le personnel

L'homme est une source potentielle de risques directs ou indirects ; les risques qu'il fait encourir à l'entreprise de façon volontaire ou involontaire, sont souvent influencés par le contexte et l'environnement. La motivation, les réactions face au risque ou sinistre, la conscience professionnelle, dépendent du contexte socio-économique de l'entreprise. On peut qualifier et mesurer ces risques, mais les solutions à apporter pour y remédier restent difficile à valider. La qualité des ressources humaines, l'information et la formation peuvent parfois contribuer à atténuer ces risques.

Le personnel comprend les informaticiens et les utilisateurs. Les informaticiens sont des spécialistes de l'activité informatique (programmeurs, analystes, administrateurs réseaux, développeurs…). Ils animent la fonction informatique au sein de l'organisation. Les utilisateurs sont composés de tous les autres membres de l'organisation qui, dans le cadre de leur activité quotidienne, utilisent l'outil informatique.

1.4.2 Les biens matériels

Les biens matériels sont composés des bâtiments et locaux informatiques ainsi que les équipements informatiques mais aussi plus généralement de toutes les ressources matérielles

nécessaires au fonctionnement du système informatique. On peut citer comme biens matériels :

- les bâtiments et locaux abritant les équipements informatiques ;

- les équipements informatiques et leurs périphériques ;

- la climatisation et les dispositifs annexes associés ;

- l'alimentation en énergie électrique avec son câblage et les équipements associés, transformateurs, disjoncteurs, onduleurs, etc... ;

- l'infrastructure des télécommunications, qui comprend les autocommutateurs, les têtes des lignes P.T.T, les armoires et boîtes de raccordement, les commutateurs et routeurs, les modems et enfin les supports de transmissions, câbles et équipements.

1.4.3 Les processus et programmes

Les processus et programmes sont tous les processus de traitement de l'information, qu'ils soient automatisés ou non. Ils seront souvent des cibles primaires à contribution par des agresseurs humains dans le but d'attaquer une autre cible, en général des données (Jouas, 1999 : 33). Ils comprennent :

- Les logiciels et progiciels d'application tant en phase de développement qu'en phase d'exploitation
- Les logiciels de sécurité des systèmes centraux et des stations de travail dont les fonctions sont l'authentification, la certification, le contrôle d'accès, l'administration des droits, la gestion d'alarme.

1.4.4 Les données et les supports

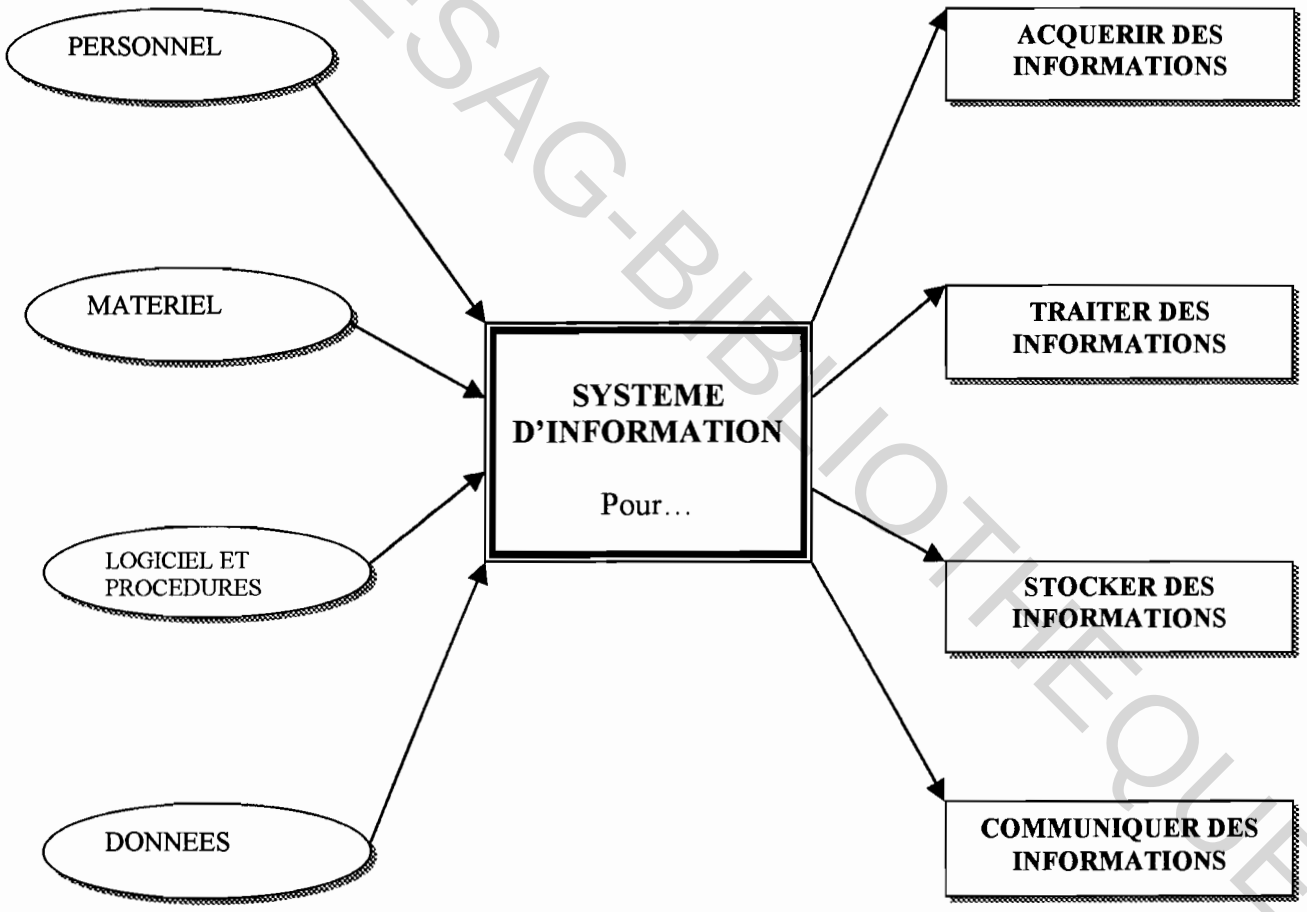
Les données sont le plus souvent représentées par des valeurs chiffrées. Elles décrivent, à un niveau élevé, les entités de gestion d'une entreprise, leurs regroupements logiques ou domaines d'activité ainsi que leurs rapports avec les autres entités de gestion.

Les supports de données ou de programmes peuvent être des supports permanents ou temporaires. On distingue :

- Les supports papier : listings, formulaires de saisie, correspondance
- La documentation : documentation des logiciels, documentation d'exploitation
- Les supports amovibles : bandes magnétiques, disquettes, disques amovibles, CD-ROM, disques optiques numériques.

De façon synthétique, voici les composantes d'un système informatique :

Figure 1 : Composantes du système informatique



Source :(R. Reix, 2000 :76)

Le système informatique comporte plusieurs ressources (personnes, matériel, logiciels et procédures, données) qui sont articulés, combinés pour répondre à des exigences précises d'acquisition, de traitement, de stockage ou de communication d'informations. En effet, ce sont les utilisateurs qui, pour l'exécution de leurs tâches, consomment l'information produite par le système ou contribuent à l'acquisition, au stockage, au traitement ou à la communication d'informations grâce aux supports mis à leur disposition notamment les machines, logiciels, les données.

Conclusion partielle : Cette section nous a permis de définir les concepts fondamentaux notamment le système informatique et ses ressources au sein des organisations. Quels sont les risques qui pèsent sur le système informatique ? C'est à cette question que nous tenterons de répondre dans la section qui suit : le risque informatique.

2. Le risque informatique

Le recours étendu aux technologies de l'information a fortement amélioré les performances des systèmes informatiques mais sans doute aussi leur vulnérabilité. Qu'arriverait-il à une banque si sa base de données « clients » était détruite ? Comment pourrait-elle fonctionner si son système informatique était en panne ?

2.1. Définition du risque informatique

L'activité bancaire est une activité à risque (MADERS, 1994 :1). Avant d'évoquer le risque informatique, il est intéressant de définir la notion de risque.

Le risque peut être défini comme étant « la menace qu'un événement ou une action ait un impact défavorable sur la capacité de l'entreprise à réaliser ses objectifs avec succès » (Bouaniche, 1999 :25). Tel que défini, le risque fait référence à un danger plus ou moins prévisible, à une situation où il y a une possibilité de pertes ou de dommages.

Pour pérenniser son activité, le banquier doit faire face à une multitude de risques. Au nombre de ces risques, figure le risque informatique. Mais qu'entend – t – on par risque informatique ?

Selon S. RAO (2000 :86), le risque informatique peut être défini comme étant « la probabilité qu'une menace se concrétise, à la suite d'un sinistre portant atteinte à l'un des composants du système informatique ou de son environnement, avec un impact que l'on mesure, soit quantitativement par le montant des pertes, soit de façon qualitative ». Ainsi, chaque risque identifié se compose en deux facteurs : son impact, respectivement l'ampleur du dommage si le risque se produit, et la probabilité qu'il se déclenche . La banque gérera différemment un risque dont l'impact est important et la probabilité faible, qu'un risque dont l'impact est faible et la probabilité importante.

Pour mieux maîtriser les différents risques, il est important d'élucider les différentes formes d'agressions et menaces qui agissent sur le système informatique.

2.2. Identification et analyse des menaces sur le système informatique

L'informatique est un moyen comme un autre de commettre une infraction. Certains l'utilisent pour détourner des fonds, d'autres pour se venger personnellement d'une entreprise. Dans un cadre plus organisé, il s'agit même parfois d'espionnage économique.

Une bonne identification des contraintes et des risques permet de recommander des solutions et des méthodes de contrôle adaptées en vue d'assurer l'intégrité et la sécurité de l'information. L'analyse des risques consiste à faire ressortir les forces et les faiblesses de la structure.

La menace peut être assimilée à « toute action d'une personne ou tout événement susceptible de conduire à un changement non souhaité d'une ressource du système informatique » (Jouas, 1999 :24). Tandis qu'une agression est toute action effectivement entreprise par une personne ou tout événement réel, dont l'aboutissement, en l'absence de mesures de sécurité, sera un changement non souhaité d'une ressource du système informatique.

Dans la suite, nous retiendrons comme agression la phase du phénomène naturel, de l'accident, de l'erreur, de la faute ou de la malveillance qui s'étend depuis son déclenchement jusqu'à son aboutissement sous la forme d'un sinistre. Par exemple, une agression peut être constituée d'un événement initial la « chute de la foudre » qui entraîne un incendie se propageant au centre de calcul, le résultat étant la destruction par le feu des équipements informatiques.

L'agression peut comporter deux phases :

- une 1ère phase où la source de l'agression, l'auteur humain ou non pénètre dans la ressource sans dégradation ni détérioration. Il peut s'agir d'un intrus pénétrant dans l'entreprise ou dans les bâtiments où sont situées les ressources informatiques ou d'un pirate pénétrant dans le système informatique par les réseaux de télécommunication ou d'un virus implanté dans une station de travail mais qui n'a pas encore agi.

- la 2nde phase où il y a effectivement changement, détérioration dans la constitution ou l'état d'une ressource du système informatique. Les changements ou détériorations peuvent se poursuivre et s'étendre soit naturellement, soit par une intervention extérieure.

Les agressions sur le système informatique peuvent être de divers types, elles peuvent être physiques ou logiques, accidentelles ou malveillantes, et leur auteur peut être humain ou non humain. D'après l'I.F.A.C.I (module 8), il est nécessaire de distinguer cinq niveaux d'agressions :

- l'environnement physique ;
- les accidents ;
- les erreurs ;
- les malveillances ;
- enfin, les agressions dues à l'environnement social et aux crises correspondantes.

2.2.1 L'environnement physique

L'environnement physique peut être source de deux types d'agressions, les agressions d'origine naturelle et celles d'origine industrielle .

- **Agressions physiques dues à des origines naturelles**

Le sujet d'une telle agression est la nature, et peut appartenir à l'une des deux catégories suivantes :

- Catastrophes et calamités à caractère exceptionnel typiques de zones géographiques et régions particulières : les agressions ou événements possibles sont les séismes, les cyclones et raz de marée, les grandes crues, les glissements de terrain, les avalanches et les feux de brousse. La crue de la Saône dans la région lyonnaise en 1982, le tremblement de terre de San Francisco d'octobre 1989 en sont des illustrations.

- Evénements à caractère météorologique tels les orages, les vents : les événements sont la foudre, les précipitations, les débordements des rivières consécutives à des pluies.

- **Agressions physiques dues à l'environnement industriel**

L'implantation de systèmes informatiques dans une zone industrielle peut les exposer aux origines suivantes de sinistres :

- Corrosion des circuits électroniques et des surfaces magnétiques, pollution

- Travaux et chantiers, voies à grande circulation à proximité : poussière, secousses, câbles sectionnés.

- Emissions radioélectriques parasites :faisceaux hertziens, voisinage de radars

2.2.2 Agressions d'origine accidentelle

A ce niveau, nous pouvons énoncer deux types d'agressions : les agressions physiques d'origine accidentelle et les agressions logiques d'origine accidentelle.

- **Les agressions physiques d'origine accidentelle**

Les sujets de tels accidents peuvent être humains ou non humains. Ces accidents sont généralement le fait du hasard, des négligences, d'une mauvaise conception, d'une mauvaise réalisation ou d'une mauvaise qualité des infrastructures ou des procédures. Ils peuvent être aussi être dus à l'incompétence, à la fatigue ou au stress. Quelques illustrations typiques sont :

- un court-circuit ;

- une fuite d'eau à un étage supérieur ;

- une inattention lors de la modification de l'alimentation électrique, de la climatisation ou des télécommunications ;

- des perturbations électroniques ou électrostatiques au voisinage des équipements informatiques.

- **Les agressions logiques d'origine accidentelle**

Les agressions logiques d'origine accidentelle sont les erreurs au niveau de la conception, de la réalisation, de l'exploitation ou de l'utilisation de systèmes et applications informatiques. Certains accidents physiques peuvent être à l'origine de tels accidents notamment les pannes de la mémoire centrale ou les incidents sur les disques magnétiques qui peuvent entraîner des altérations des programmes et des données.

2.2.3 Les crises ou conflits, origines de sinistres

Il s'agit essentiellement des situations susceptibles de bloquer l'activité informationnelle, ou d'incapacité à assurer le travail, dues :

- à des grèves, en particulier au niveau du service informatique, à des émeutes ou des mouvements populaires ;
- au départ ou à l'absence pour cause de maladie, accident ou démission, de personnels occupants des fonctions stratégiques
- à la malhonnêteté et au mécontentement de certains employés qui sont animés d'un esprit de vengeance.

2.2.4 Les erreurs

Les études statistiques sur la sinistralité informatique de l'A.F.A.I montrent que les erreurs, causes des sinistres, peuvent être regroupées en trois classes :

- **Erreurs de saisie, de transmission et d'utilisation des informations**

Les erreurs de saisie sont les plus fréquentes car il s'agit d'une opération manuelle nécessitant une attention soutenue. L'illustration suivante montre la perte que subirait la banque si un employé faisait une erreur : pour un transfert d'un montant de 5 000 000 FCFA émis par un client, l'agent des opérations en charge saisit 50 000 000 FCFA soit une perte de 45 000 000 FCFA.

La mauvaise qualité des logiciels d'application dotés de contrôles insuffisants en est la cause principale. Les erreurs de transmission sont relativement faibles : il peut y avoir pertes de données ou altérations des données transmises; la qualité des réseaux et des protocoles de transmission en est la cause essentielle.

- **Erreurs d'exploitation**

Les erreurs d'exploitation sont généralement dues à la mauvaise manipulation des utilisateurs du système applicatif.

2.2.5 Les malveillances

Les malveillances sont des actes volontaires, provoqués par des êtres humains qui peuvent ou non faire partie du personnel de l'entreprise. Robert Longeon sur la page web www.cnrs.fr donne la définition suivante : «la malveillance informatique consiste en l'utilisation de, ou l'accès à, un ordinateur sans autorisation, et dans un but contraire aux désirs du propriétaire de cet ordinateur ou des données qu'il contient. » Cette description

s'applique à des actions telles que l'accès non autorisé à des systèmes informatiques, la modification des programmes, la manipulation ou l'interception de données. On peut citer :

- le sabotage matériel qui est l'endommagement ou la destruction d'une ressource physique (équipement ou support de données) ;

- le sabotage immatériel qui est une agression perpétrée par voie logique dans le but de détruire ou d'altérer des données ou des programmes ;

- les détournements de fonds par l'intermédiaire du système informatique, ces détournements pouvant découler de modifications de certaines données ou programmes ou résulter d'un chantage, après introduction d'un sabotage immatériel caché appelé bombe logique (programme qui se déclenche sur ordre ou à une date programmée et qui altère le fonctionnent d'autres programmes);

- les agressions physiques ou détournements de biens physiques rendus possibles ou facilités par l'altération de données ou de programmes ;

- les détournements de logiciels qui sont surtout importants dans les entreprises produisant des logiciels ;

- les détournements d'information par vol ou copie ;

- le vol de ressources physiques essentiellement du petit matériel et en particulier vol des terminaux, PC ;

- l'utilisation frauduleuse de ressources en particulier des réseaux de télécommunication.

Toutes ces différentes menaces identifiées exposent le système informatique à diverses voies d'accès aux ressources qu'il convient d'aborder : les vulnérabilités.

2.3 Étude des vulnérabilités

Une agression est caractérisée par un certain nombre de voies d'accès jusqu'à l'atteinte des ressources cibles de l'agression (Angot, 1994 :45). Chacune de ces voies d'accès possibles à une ressource constitue pour l'entreprise une « vulnérabilité ». Les vulnérabilités exploitées par les pirates sont regroupées en deux grandes catégories, les voies d'accès logiques et les voies d'accès physiques .

2.3.1 Les voies d'accès logiques

Les voies d'accès logiques et les vulnérabilités associées représentent toutes les manières d'accéder aux données ou aux informations par voie logique, c'est-à-dire par l'intermédiaire du système sans avoir accès physiquement à un support d'information . Il s'agit donc d'accès empruntés par des personnes de l'entreprise ou non. Ces vulnérabilités peuvent être représentatives de la manière dont l'accès peut être obtenu.

L'accès autorisé : c'est la vulnérabilité liée au fait que des individus autorisés à accéder à une information peuvent délibérément ou par erreur la divulguer, l'altérer voire la détruire.

L'acquisition illicite de droits d'accès : il s'agit des cas où pour obtenir des droits d'accès qu'il n'a pas, un « pirate » va agir de manière illicite, en forçant le système de gestion des droits, au niveau des tables système par exemple ;

L'usurpation d'identité qui consiste à se présenter sous le nom d'une autre personne pour obtenir ses droits. En effet, posséder un mot de passe constitue le moyen le plus simple d'accéder à une machine mais aucun mot de passe n'est infaillible. Le pirate utilise un programme nécessitant un fichier de mots qui va essayer chacun de ces termes jusqu'à obtenir une autorisation d'accès sur la machine visée. Il peut aussi utiliser des programmes espions qui vont capter les entrées claviers et ainsi permettre de récupérer des mots de passe de manière indirecte.

L'abus de droits : il s'agit de tous les cas où des voies dérobées et non documentées en général, permettent d'obtenir avec un niveau d'habilitation donné, plus de droits réels que prévus. Par exemple, certains ingénieurs de développement peuvent prévoir des « portes dérobées d'accès » ou « chevaux de Troie » dans les logiciels pour intervenir plus facilement en phase d'exploitation, en cas de problème.

Le forçage de l'accès : il s'agit de la violation des systèmes de sécurité pour acquérir l'accès aux données ou aux programmes en l'absence de droits.

2.3.2 Les voies d'accès physiques

Les voies d'accès physiques sont toutes les manières d'accéder physiquement à une ressource du système informatique. Il s'agit donc soit de ressources physiques, soit de supports de données. Ces voies d'accès peuvent être empruntées aussi bien par des êtres humains que par des éléments naturels comme le l'air, le feu ou l'eau. Parmi ces voies d'accès qui sont autant de vulnérabilités, on distingue :

- Les accès aux locaux qui peuvent se faire de différentes manières :

On peut accéder les locaux par les issues normales (portes et fenêtres) qui peuvent se situer à la périphérie du site, des bâtiments ou du local ;

Par les faux planchers ou faux plafonds ;

Par les murs et les cloisons.

- Les accès aux ressources situées dans les locaux de l'entreprise :

Accès au contenu des supports de données ;

Accès aux stations de travail ;

Accès aux équipements en particulier de télécommunication ou de servitudes comme la climatisation ou l'énergie.

En définitive, il faut retenir que les bâtiments et locaux de l'entreprise doivent faire l'objet d'une attention particulière en matière de sécurité. En commençant par l'étude de

l'environnement naturel (rivières, climat, terrains) et artificiel (pollution, nuisances sonores, thermiques, ...), et installations électriques, on peut éviter quelques catastrophes naturelles.

Conclusion partielle : Les agressions et vulnérabilités auxquelles s'expose le système informatique sont réelles et menacent la survie de l'entreprise. Quel est l'impact de ces différentes menaces sur l'activité de la banque ?

2.4. Evaluation de l'impact des différents menaces

Les menaces qui pèsent sur le SI ont des conséquences sur les données et sur les ressources informatiques de l'organisation voire sur sa pérennité. L'impact peut être élevé, moyen ou faible selon le préjudice causé à l'institution. D'une manière générale, Magnier (1995 :65) , reconnaît que l'impact d'un scénario de sinistre est double : il faudra restaurer les ressources de l'entreprise détériorées et il faudra, en attendant cette restauration, subir les conséquences des dysfonctionnements engendrés par les détériorations. Evaluer l'impact des détériorations revient à estimer le coût des restaurations.

Evaluer l'impact des dysfonctionnements de l'entreprise, revient à déterminer la gravité de l'ensemble des conséquences d'une atteinte à la confidentialité, à l'intégrité ou à la disponibilité d'une des ressources constituant le système informatique.

Nous pouvons citer la détérioration des ressources, la compromission d'informations sensibles, les informations altérées et les pertes (Jouas, 1999 :59).

2.4.1 La détérioration des ressources

Elle peut porter sur la confidentialité des données, l'intégrité et la disponibilité des ressources ou la disponibilité des services. Les différentes détériorations rendent inutilisables le matériel informatique dont dispose l'établissement.

2.4.2 La compromission des données ou informations sensibles

Selon l'encyclopédie informatique (2001), compromettre les données ou les informations, c'est altérer ou détourner tout ou partie de ces informations. La compromission des données peut être due à l'ignorance, à une erreur, une négligence, un accident ou à la malveillance et porter ainsi une atteinte à l'image de l'entreprise et à sa crédibilité en ce sens qu'elle porte sur des données techniques, commerciales, que des données nominatives ou stratégiques de l'entreprise. Elle peut se faire au profit de la presse, de l'administration fiscale, du personnel de l'entreprise, des compagnies d'assurances, des concurrents, des clients ou des fournisseurs.

2.4.3 Les informations altérées ou fausses

Il s'agit des données qui ont subi une perte d'intégrité. Ces altérations font suite à des ajouts ou à des manques d'informations sur des fichiers ou programmes de l'entité. Ce qui induit la non fiabilité des informations traitées.

2.4.4 Les pertes

Il s'agit des frais supportés par l'entreprise pour remédier aux détériorations subies par ses ressources. L'objectif est de réparer ou de reconstruire les ressources matérielles, de reconstituer les bases de données, les fichiers de données ou de corriger les programmes. On distingue différents types de pertes :

- Pertes de valeurs (encaisse, réserves, fonds)
- Perte de valeur liée à des valeurs immobilisées : bâtiments et locaux, matériels informatiques, armoires et câbles, télécommunications, etc.
- Perte de valeur liée aux petits matériels, micros et équipements de bureau et fournitures diverses
- Frais de ressaisie ou reconstitution d'informations perdues, détruites ou dégradées

Outre les pertes financières, s'ajoutent :

- la perte de confiance des clients, fournisseurs, employés, actionnaires
- la perte de productivité qui se produit quand le personnel ne peut pas exécuter les travaux qui lui sont assignés
- Perte de disponibilité du service : L'indisponibilité du service peut être de courte, moyenne ou longue durée. Il peut s'agir d'une baisse de performances, de taux d'attente à la connexion, de taux d'erreurs important ralentissant les échanges ou d'une interruption totale du système informatique résultant d'un sinistre ayant atteint les ressources du système informatique.

Au regard de ces conséquences, quel est le niveau d'impact sur l'activité ?

2.4.5 Mesure du niveau d'impact

Le niveau d'impact peut être évalué par rapport à la capacité de l'entreprise à pérenniser son activité (Jouas, 1999: 72). Ainsi, nous avons selon l'ampleur de la conséquence sur l'activité.

- *Un impact extrêmement grave* : ce niveau est réservé à des sinistres qui peuvent compromettre l'avenir de la société. Il est rare de trouver des systèmes d'informations à ce niveau tant en ce qui concerne la confidentialité que l'intégrité. C'est le cas des sinistres majeurs de salles machines pour lesquelles aucun plan de secours (machine back-up) n'avait pas été prévu et qui conduit à des dépôts de bilan.
- *Un impact très grave* : c'est le cas des sinistres ayant un impact très sérieux sur le fonctionnement de l'organisation sans toutefois que son avenir soit menacé. En termes financiers, cela peut aller jusqu'à l'annulation du résultat de l'exercice. En termes d'image, c'est une perte d'image dommageable qu'il faudra plusieurs mois pour remonter.

- *Un impact moyennement grave* :c'est un niveau d'impact qui relève de tous les sinistres dont les conséquences sur l'entreprise sont notables au plan des résultats, de son climat social ou de son image mais non durables.
- *Un impact faible* : ce niveau d'impact n'a pas d'effet significatif sur l'entreprise. Il peut être caractérisé par un sinistre de courte durée de perturbation.

Conclusion partielle : Les risques évoqués ci-dessus mettent en jeu soit la protection du patrimoine voire l'activité de l'établissement, soit la mise en cause de sa responsabilité à l'égard de tiers, et notamment des clients. Sous la pression de la concurrence et des attentes des clients, une indisponibilité prolongée, outre le risque financier immédiat qu'elle peut comporter, peut être fortement dommageable pour l'établissement en termes d'image et de crédibilité. C'est pour ces raisons que les dirigeants doivent démontrer qu'ils maîtrisent tous les aspects du système informatique utilisé en mettant en place un dispositif de sécurité et de contrôle conforme aux exigences du métier.

CHAPITRE II : MAITRISE DU RISQUE INFORMATIQUE

Maîtriser ses activités, atteindre ses objectifs, c'est avant tout gérer ses risques. La maîtrise des risques se définit par son corollaire la sécurité. Ainsi, toute organisation a intérêt à identifier et à gérer les risques liés à l'implantation et à l'exploitation de son système informatique.

Ce chapitre aborde donc dans un premier temps les objectifs de sécurité puis les mesures de sécurité à mettre en œuvre pour minimiser les risques.

1. Objectifs de sécurité

Tout le monde parle de sécurité des systèmes d'information (SSI), mais que renferme ce concept ? La sécurité est-elle un état objectif, observable par des effets mesurables, ou simplement un sentiment de bien-être ?

Le dictionnaire Larousse nous donne du mot « sécurité » la définition suivante : « confiance, absence d'inquiétude, sûreté ». Tel que définie, la sécurité garantirait la fiabilité du dispositif mis en place à 100%. Cependant, avec l'évolution technologique, aucun système ne peut avoir la prétention d'être en sécurité à 100%. Cette idée rejoint avec celle soutenue par Thomas Martin (Revue AFAI n°61 de 2000), expert en système d'information, lors de la conférence sur la sécurité des systèmes informatiques organisée par l'AFAI. Pour lui, « si un système peut être piraté, il le sera. Construisez un système à l'épreuve des idiots, la nature créera un idiot plus efficace ».

En effet, la sécurité d'un système d'information est « sa non – vulnérabilité à des accidents ou à des attaques volontaires, c'est – à – dire l'impossibilité que ces agressions produisent des conséquences graves sur l'état du système ou son fonctionnement. »

(MAGNIER, 1995 :10). Cette définition nous amène à nous assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le domaine qu'il est prévu qu'elles le soient.

On s'accorde à retenir trois objectifs principaux à la sécurité informatique :l'intégrité, la confidentialité, la disponibilité. En plus de ces 3 critères garantissant la sécurité informatique, BRUGUIER (1996 :23) a ajouté un 4ème objectif (contrôle et preuve) qui vise à assurer la traçabilité des opérations et traitements.

Dans la suite de notre étude, nous retiendrons ces quatre objectifs de sécurité. Pour mieux cerner ces objectifs, il convient de les définir.

1.1 Disponibilité

C'est l'aptitude des systèmes à remplir une fonction dans des conditions prédéfinies d'horaires, de délais et de performance. Ce critère vise à garantir la continuité du service, de respecter les dates et heures limites des traitements. Il y a indisponibilité si l'utilisateur ne peut pas avoir connaissance de l'information ou exécuter des opérations.

1.2 Intégrité

C'est la propriété qui assure que des informations sont identiques en deux points, dans le temps et dans l'espace. Ce facteur garantit l'exhaustivité, l'exactitude et la validité de l'information. Il permet d'éviter la modification par erreur de l'information.

1.3 Confidentialité

C'est la propriété qui assure la tenue secrète des informations avec accès aux seules entités autorisées. Ce critère garantit le secret des données échangées par deux correspondants sous forme de message ou de fichiers.

1.4 Contrôle et Preuve

C'est la faculté de vérifier le bon déroulement d'une fonction. Ce facteur garantit la possibilité de reconstituer un traitement à tous les niveaux (logique de programmation, déroulement du traitement, forme des résultats) à des fins de contrôle ou de preuve. La traçabilité des opérations facilite la vérification du bon fonctionnement du système et permet en cas de sinistre, de remonter aux causes. En effet, selon l'article 2 du règlement N°90-08 du 25 juillet 1990 de l'UEMOA, le système de contrôle interne doit garantir l'existence d'un ensemble de procédures appelé **piste d'audit** qui permet :

- de reconstituer dans un ordre chronologique les opérations ;
- de justifier toute information par une pièce d'origine à partir de laquelle il doit être possible de remonter par un cheminement ininterrompu au document de synthèse et réciproquement ;
- d'expliquer l'évolution des soldes d'un arrêté à un autre par la conservation des mouvements ayant affecté les postes comptables.

Pour répondre efficacement aux objectifs de sécurité cités plus haut, il faut mettre en place des mesures techniques de sécurité mais aussi un dispositif de contrôle interne des moyens mis en œuvre.

2. Les mesures de sécurité

Le CLUSIF et l'AFAI classent en trois domaines principaux les mesures destinées à réduire les risques : la sécurité physique, la sécurité organisationnelle et la sécurité logique. Cette décomposition classique des mesures de sécurité est insuffisante pour comprendre ce qu'il convient de faire à chaque phase du scénario de sinistre. C'est pourquoi, Jouas (1999 :70) propose une autre typologie des mesures de sécurité se basant sur les scénarios de

Cette nouvelle cartographie des mesures de sécurité nous permet de disposer de six grandes familles qui sont : les mesures structurelles, les mesures dissuasives, les mesures préventives, les mesures de protection, les mesures palliatives et les mesures de récupération.

2.1 Les mesures structurelles

Les mesures structurelles ont un impact sur la structure du système informatique, de son architecture et permettent d'éviter certaines agressions. Ces mesures permettent de protéger les biens de l'entreprise. Dans cette section, on a la fragmentation de l'information, l'occultation des ressources, la réduction de la valeur des ressources et les mesures structurelles d'organisation .

- La fragmentation de l'information consiste à découper l'information en fragments afin qu'une agression ne puisse affecter qu'un fragment isolé.
- L'occultation des ressources consiste à cacher l'existence d'une cible potentielle afin de ne pas attirer l'attention d'éventuels agresseurs. Il s'agit entre autres de ne faire ni publicité sur son informatique ni révéler les informations traitées.
- La réduction de la valeur des ressources
- Les mesures structurelles d'organisation : ce sont des mesures prises pour éviter les mécontentements, pour sensibiliser et motiver le personnel. Il s'agit des politiques de sensibilisation et de formation du personnel sérieuses et actualisées en permanence, des conditions de travail ergonomiques et agréables pour éviter la fatigue et le stress, de la sensibilisation du personnel aux problèmes de sécurité, de la bonne adaptation de chaque salarié à son travail aussi bien du point de vue de sa formation que du point de vue de ses goûts personnels.

2.2 Les mesures dissuasives

Elles permettent dans le cas d'une agression humaine d'éviter qu'ils mettent à exécution la menace potentielle. Ainsi donc, ces différentes mesures empêchent le passage à l'acte d'un agresseur humain et la concrétisation de la menace. Généralement, ces mesures sont prises par l'entreprise pour réduire voire éliminer les causes ou motivations qui sont à l'origine d'un accident, d'une erreur, ou d'une agression dus à des êtres humains. La mise en place de moyens de détection et de trace suffisamment complets et précis pour pouvoir identifier l'agresseur sans ambiguïté en est un exemple.

2.3 Les mesures préventives

Ces mesures sont mises en place lorsque les mesures dissuasives n'ont pas pu empêcher la concrétisation de la menace.

Ces mesures visent à empêcher l'agression d'aboutir à des détériorations soit par des mesures prises de manière permanente, soit par la détection de l'agression et intervention pour la stopper avant détérioration. On distingue les barrages, la détection - interception, le masquage de l'information, les contrôles d'accès.

2.3.1 Les barrages

Le barrage permet d'obstruer les voies d'accès aux ressources sans distinction de personnes ni de circonstances. Par exemple, une cage de Faraday fera un obstacle contre les perturbations électromagnétiques de l'environnement industriel ou contre la compromission électromagnétiques.

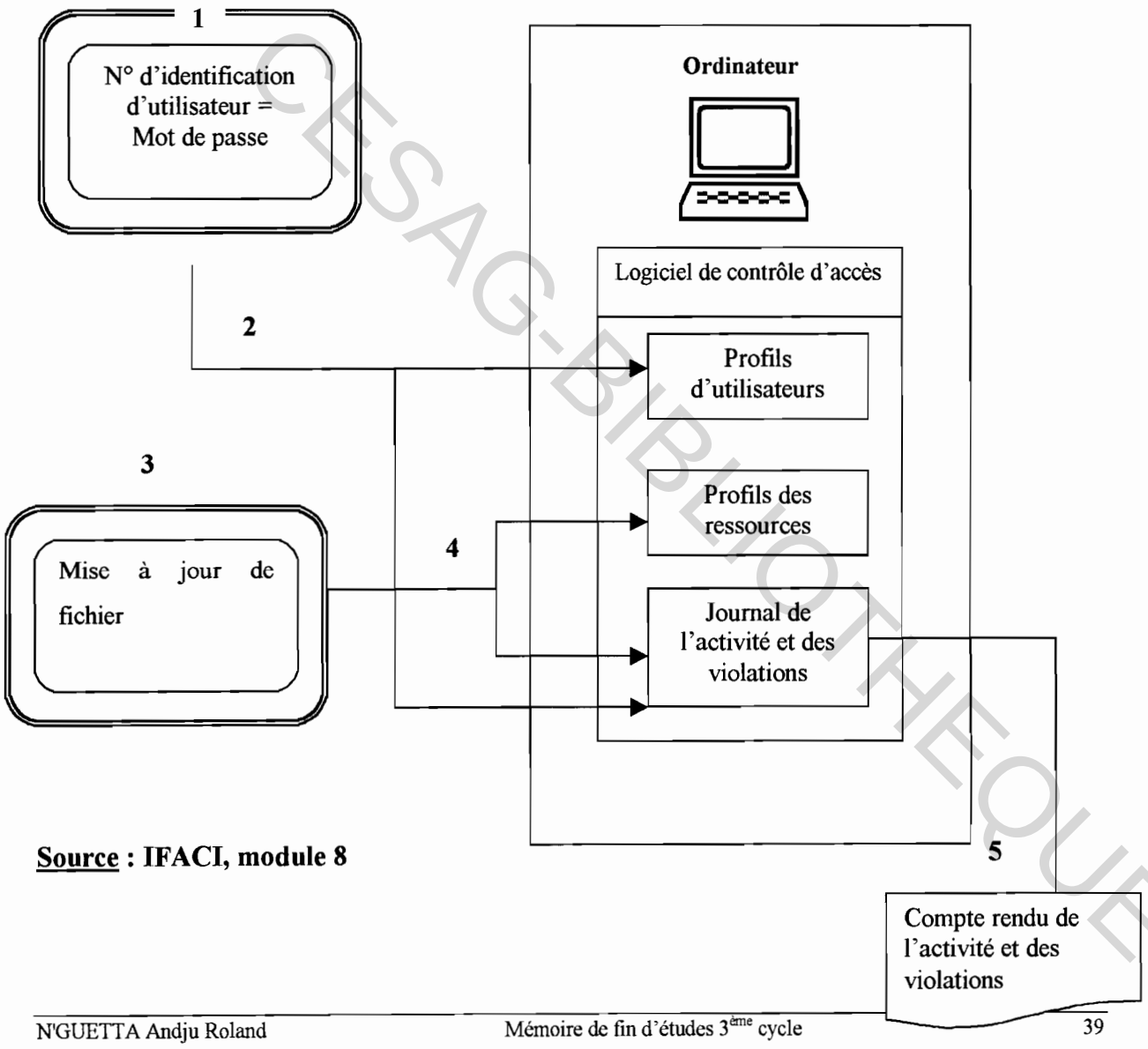
2.3.2 Les contrôles d'accès

Il s'agit des mesures permettant l'accès sélectif à une ressource à un nombre limité de personnes habilitées (Bruguier, 2000 :135). Toute tentative d'accès est ainsi filtrée et celles

non autorisées rejetées. Ces mesures sont aussi bien physiques que logiques. Au niveau physique, nous avons des dispositifs de contrôle à l'entrée d'un centre de calcul notamment les serrures à combinaison (miniclavier à touches) qui autorisent l'accès aux personnes qui détiennent la bonne combinaison, les systèmes de badges, les systèmes biométriques qui reposent sur l'identification de caractéristiques physiques (empreintes digitales, voix, vascularisation de la rétine).

De même au niveau logique, l'accès à une application ou à un fichier peut être réglementé par des droits d'accès notamment les mots de passe ou codes d'accès comme illustre le schéma suivant.

Figure 2 : Logiciel de contrôle d'accès logique



Source : IFACI, module 8

1 : Demande de connexion de l'utilisateur
2 : vérification du n° d'identification d'utilisateur / mot de passe et consignation de la demande de connexion
3 : Demande de connexion de l'utilisateur
4 : Vérification de l'autorisation d'accès de l'utilisateur et consignation de l'activité
5 : Génération et examen des rapports d'activité et de violation (suivi et compte rendu)

2.3.3 La détection – interception

L'agression de la ressource est en cours mais il faut un certain temps pour qu'elle produise un début de détérioration et on profite de ce laps de temps pour intercepter la progression de l'agresseur.

Un incendie peut être détecté avant qu'il n'atteigne les équipements informatiques et l'intervention des pompiers pour le circonscrire avant toute détérioration de ressources du système informatique.

2.3.4 Le masquage des informations

Le masquage de l'information est une technique permettant d'assurer la confidentialité des données. Un exemple de masquage est le brouillage d'un message à l'émission par chiffrement. Le message, même intercepté ne sera pas compris par le pirate. Seul le destinataire légitime pourra le déchiffrer car étant en possession de la clef du chiffre. Notons que le masquage des informations n'empêche pas l'altération ou la destruction des données masquées.

2.4 Les mesures de protection

Les mesures de protection sont celles qui permettent de limiter l'ampleur des détériorations. On trouve aujourd'hui sur le marché des outils de sécurité comme des firewall (pare-feu) personnels ou des détecteurs d'intrusion. Elles sont orientées vers les ressources.

On distingue la détection – réaction, les mesures anti – propagation et la certification des données.

2.4.1 La détection – réaction

La mesure de détection – réaction consiste à réagir immédiatement dès que le système a détecté une intrusion. Le dispositif mis en place permet de surveiller le fonctionnement du système et de faire contrôle de cohérence.

2.4.2 Les mesures anti – propagation

Les mesures anti – propagation permettent d'empêcher la propagation d'un sinistre dans tout le système informatique. Il s'agit de portes coupe-feu ou de fermeture automatique des clapets de ventilation dans le cas d'un incendie. Ces mesures permettent également d'isoler certaines parties du système ou certaines données sensibles.

2.5 Les mesures palliatives

Ce sont des mesures prises une fois que les détériorations ont été accomplies et visent d'une part à en minimiser les conséquences au niveau de l'organisation, d'autre part à restaurer les ressources détériorer pour retrouver l'état initial. Dans cette section, nous étudierons successivement les mesures de restauration des ressources détériorées et les mesures atténuant les dysfonctionnements.

2.5.1 Les mesures de restauration des ressources détériorées

Ces mesures visent à rétablir l'état normal du système. On distingue la réparation, la correction et la reconstruction.

La réparation concerne les éléments matériels tels que les machines et les bâtiments. Elle peut être accélérée par la disponibilité en stock de pièces de rechange, de documentation et de personnels compétents. Elle s'appuie également sur des ressources externes et sur la maintenance corrective.

Par contre, la correction touche les éléments immatériels (les données et programmes). Lorsqu'on détecte une altération des données ou des programmes, il faut rétablir la version d'origine.

La reconstruction s'applique aussi bien aux ressources matérielles qu'aux bases de données ou aux programmes et consiste à rebâtir à nouveau ce qui a été détruit.

2.5.2 Les mesures atténuant les dysfonctionnements

Ces mesures permettent de pallier la perte de disponibilité des ressources par une reconfiguration. En effet, la reconfiguration est une technique générique utilisée dans les cas liés aux pertes d'intégrité ou de disponibilité.

Les reconfigurations seront de trois types :

- la « *reconfiguration dynamique* » qui agit par les redondances intégrées en différents points du cycle de traitement : les redondances ici permettent la continuation du service, mais on ne peut affirmer à tous les coups qu'il sera totalement conforme, à cause des délais ou retards possibles induits par certains types de détériorations.
- la reconfiguration semi-automatique : ce type de reconfiguration s'appuie sur des redondances non-intégrées. Les délais et retards ici sont plus conséquents, de par la nécessaire élimination des résidus des détériorations (s'il y en a), et l'activation des redondances ; les délais induits peuvent être techniques ou organisationnels, et souvent les deux.
- la reconfiguration statique ou secours : dans ce cas, les dégâts ont rendu indisponibles tout ou partie des ressources. Si les dégâts sont partiels, on peut réaffecter les ressources restantes, pour favoriser les activités prioritaires, dans ce que nous avons appelé un « *fonctionnement*

dégradé ». Si le système est inutilisable, ou si le mode dégradé est, en tout état de cause, insuffisant, on bascule alors en secours total ou partiel, sur un système externe de délestage (back-up). On s'appuie ainsi sur des redondances externes. Ce qui est primordial dans ces deux cas de figures, c'est le travail de préparation et de planification préalable nécessaire pour être prêt à toute éventualité, travail qui peut être considérable : c'est le *« plan de secours »* (contingency plan) qui doit être réglé dans ses moindres détails et être constamment à jour, si on veut être secouru correctement et surtout dans des délais raisonnables.

2.6 Les mesures de récupération

Il s'agit ici des mesures prises pour restaurer et annuler tous les dégâts ou dysfonctionnements.

En effet, pour diminuer le préjudice subi et les pertes induites, les systèmes informatiques doivent être assurés. Même s'il est coutume de dire : « mieux vaut investir dans les systèmes informatiques que dans les primes d'assurance », il faut noter que l'assurance est une garantie complémentaire qui se traduit par des compensations d'ordre financier. L'assurance apparaît ainsi comme indispensable voire obligatoire au niveau des dégâts matériels. De nos jours, on peut s'assurer non seulement contre le vol et les dégâts physiques mais aussi contre les pertes d'exploitation.

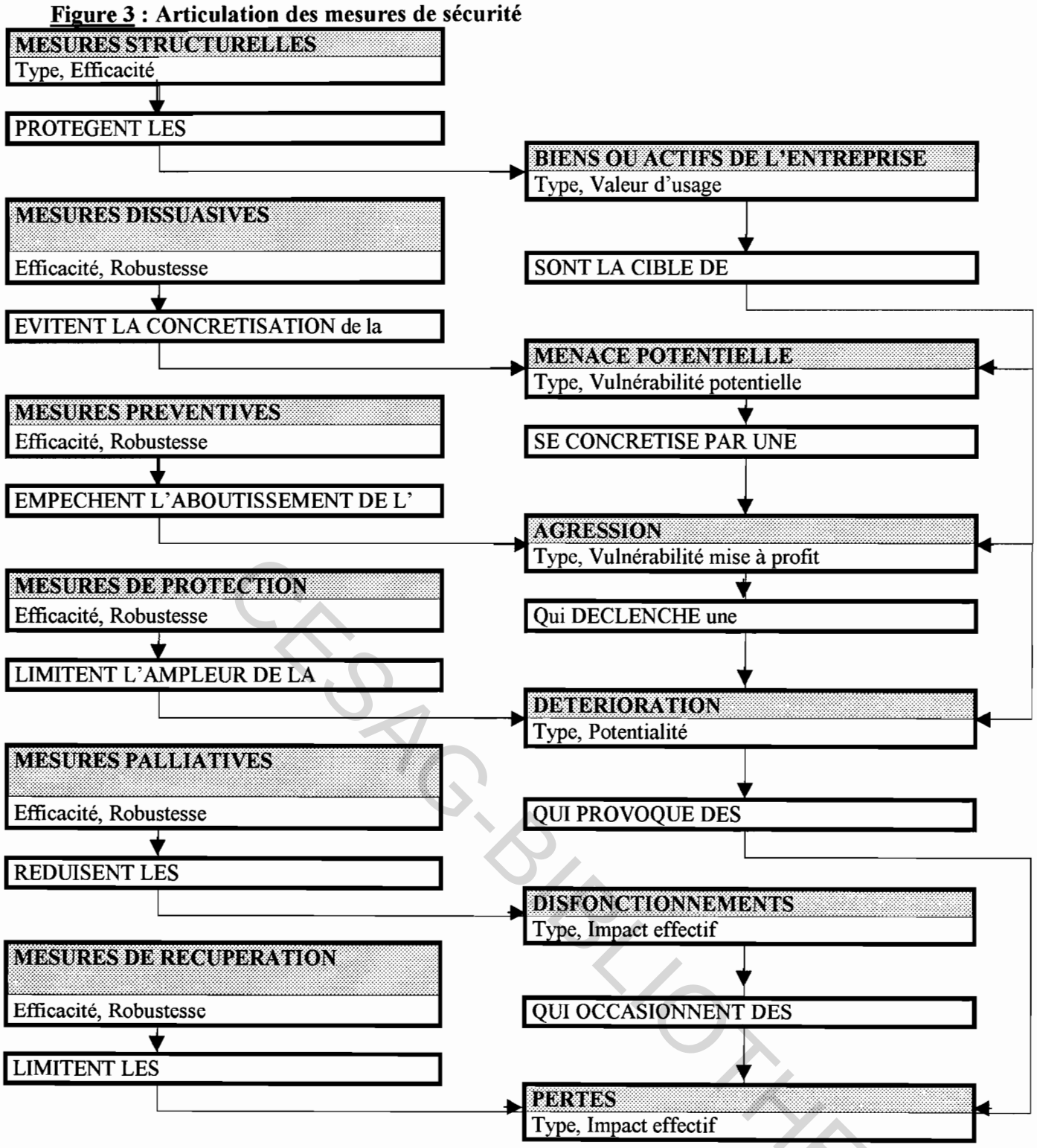
Des exemples de contrats garantissant les dommages peuvent être envisagés :

- Tous risques informatiques (TRI) : ce contrat vise à couvrir en risque direct (incendie, explosion, chocs, bris de machines, événements naturels, vol, attentat, sabotage)
- Fraude et détournement : ce contrat couvre les pertes pécuniaires dues à une fraude, escroquerie, détournement.
- Pertes d'exploitation : ce contrat couvre les équipements purement informatiques et les équipements d'environnement (alimentation, climatisation).

Cependant, avant de s'assurer, il faut évaluer correctement les risques à couvrir, estimer les conséquences s'ils se réalisent et enfin prévoir ce que l'entreprise pourra supporter en termes de dommages et intérêts sans remettre en cause la pérennité de l'établissement.

Pour bien comprendre l'articulation de ces mesures, nous avons fait un schéma.

Figure 3 : Articulation des mesures de sécurité



Source : (Jouas, 1999 : 36)

Les mesures structurelles caractérisées par leur efficacité protègent les biens de l'entreprise qui sont la cible de menaces potentielles, d'agressions et de détériorations. Ainsi

pour éviter la concrétisation de ces différentes menaces et agressions, des mesures dissuasives robustes sont mises en œuvre. Dans le même temps, des mesures de prévention empêchent l'aboutissement de ces agressions. Elles agissent donc sur la probabilité d'atteindre les ressources informatiques. L'agression déclenche une détérioration des ressources du système informatique. Pour limiter l'ampleur de ces détériorations, des mesures de protection efficaces sont mises en place et ces mesures permettent d'agir sur l'impact que causeraient ces détériorations. Les détériorations ont pour conséquence la provocation de dysfonctionnements qui occasionnent des pertes. D'une part, pour réduire ces dysfonctionnements, des mesures palliatives sont mises en œuvre. D'autre part, des mesures de récupération vont limiter les pertes.

Conclusion partielle : Même si le risque informatique correspond à l'occurrence d'un fait imprévisible, les différentes mesures de sécurité mises en place concourent à éviter les « surprises désagréables ». Cependant, en plus de moyens techniques de sécurité mis en place, un système de contrôle interne efficace doit y être associé. Ce dispositif de contrôle garantira l'opportunité de mettre en œuvre ces mesures de sécurité et en évaluera la performance.

3. Appréciation du niveau de maîtrise des risques informatiques

Tout établissement au cours de son évolution doit faire face à des problèmes de gestion pour garantir son bon fonctionnement. La multiplicité et la complexité de ces problèmes rendent le suivi des activités difficiles. Ainsi, pour remédier à ces difficultés, la mise en place au sein de l'organisation de dispositif de sécurités permanentes s'avère nécessaire et incontournable : le contrôle interne.

En effet, selon Coopers & Lybrand (2000 :24), « le contrôle interne est 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 aux réglementations en vigueur. »

Cette définition du contrôle interne renvoie aux objectifs de sécurité de l'organisation, d'efficacité et qualité des services, de conformité aux dispositions légales et réglementaires.

Le système de contrôle interne d'une organisation doit mettre les moyens permettant à atteindre ces objectifs d'une manière efficace, appropriée et économique dans une marge de probabilité raisonnable. Il peut être comparé à un filtre faisant obstacle à certains actes ou événements susceptibles d'entraîner des problèmes dans l'organisation. Ainsi, un environnement de contrôle sain garantirait le bon fonctionnement des systèmes et des contrôles et contribue à leur fiabilité. Dans le cadre de la maîtrise des risques informatiques, quels sont les différents contrôles à mettre en œuvre ?

Pour atteindre ses objectifs et réduire au minimum les risques inhérents à l'utilisation de l'informatique, la fonction Audit doit mettre en place des contrôles appropriés. L'activité de contrôle consistera à vérifier l'application des règles de gestion et d'exploitation de

l'entreprise et, en cas de manquement, à faire prendre immédiatement les mesures correctives. Bien que les évolutions technologiques font apparaître de nouveaux risques et nécessitent des techniques de contrôle différentes, les principaux contrôles à mettre en œuvre devront permettre d'assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des données et informations.

L'auditeur devra apprécier l'efficacité des moyens techniques mises en place (audit des performances techniques et de l'efficacité fonctionnelle), de respect des procédures internes (audit de conformité). Son évaluation doit porter sur les conditions générales de sécurité du système informatique, la sécurité organisationnelle , la sécurité physique, la continuité, l'organisation informatique, la sécurité logique, le suivi de l'exploitation, la sécurité des applications.

De part le caractère multiforme et complexe de la sécurité informatique, il est parfois difficile d'évaluer les risques qui pèsent sur le système informatique d'une entreprise. Il n'est pas toujours évident de définir précisément à quels types de risques le système d'information est encore vulnérable, et pour quels autres il est correctement sécurisé. Pour simplifier cette évaluation, de nombreuses méthodes d'analyse des risques sont à la disposition des Responsables de la Sécurité des Systèmes d'Information (RSSI) et des auditeurs: les méthodes BUDDY, CRAMM, MARION, MELISA ,... concourent à l'élaboration du plan de sécurité (in SARR, 2002 :34). Dans le cadre de cette étude, nous allons présenter la méthode MARION. La présente présentation est tirée du site de la société TEAMLOG (www.securite.teamlog.com).

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

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

L'ensemble des indicateurs est évalué par le biais de plusieurs centaines de questions dont les réponses sont pondérées (ces pondérations évoluent suivant les mises à jour de la méthode). Cette méthode attribue à chaque facteur étudié une valeur variant entre 1 et 4, avec comme objectif minimal la valeur 3. Tout résultat inférieur à 2 est mauvais et doit être rapidement étudié et amélioré. (1=mauvais ; 2=médiocre ; 3=assez bon ; 4=bon)

Pour employer cette méthode, l'outil utilisé est le questionnaire de contrôle interne. Des procédés de preuve peuvent être également y être associés afin de garantir la fiabilité des informations recueillies.

Déroulement de la méthode

La méthode se déroule en 4 phases distinctes :

Phase 0 : Préparation

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

Phase 1 : Audit des vulnérabilités

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

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

Cette rosace permet de juger facilement et rapidement des domaines vulnérables de l'entreprise, la cohérence et l'homogénéité des niveaux de sécurité des différents indicateurs, et donc d'identifier également rapidement les points à améliorer.

Phase 2 : Analyse des risques

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

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

Phase 3 : Plan d'action

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

Conclusion partielle

Ce chapitre nous a permis de voir les mesures de sécurité à mettre en œuvre pour minimiser les risques qui agissent sur le système informatique. Ces différentes mesures conjuguées au dispositif au dispositif de contrôle interne mis en place au sein de la structure, visent à garantir la sécurité du système informatique.

CHAPITRE III : APPROCHE METHODOLOGIQUE DE L'ETUDE

La méthodologie consiste à décrire la façon dont les données seront collectées et les outils de collecte. Notre démarche consistera à élaborer dans un 1er temps notre modèle d'analyse qui servira de guide. Après avoir présenté le modèle d'analyse, nous allons définir les différentes variables avec des indicateurs et leurs mesures. Nous allons enfin exposer les procédures de collecte des informations que nous recueillies et comment nous les avons analysées.

1. MODELE D'ANALYSE

Le modèle d'analyse est un modèle de synthèse réduit mettant en relation des variables qui influent sur le phénomène étudié (dans notre cas, c'est le dispositif de maîtrise des risques sur le système informatique).

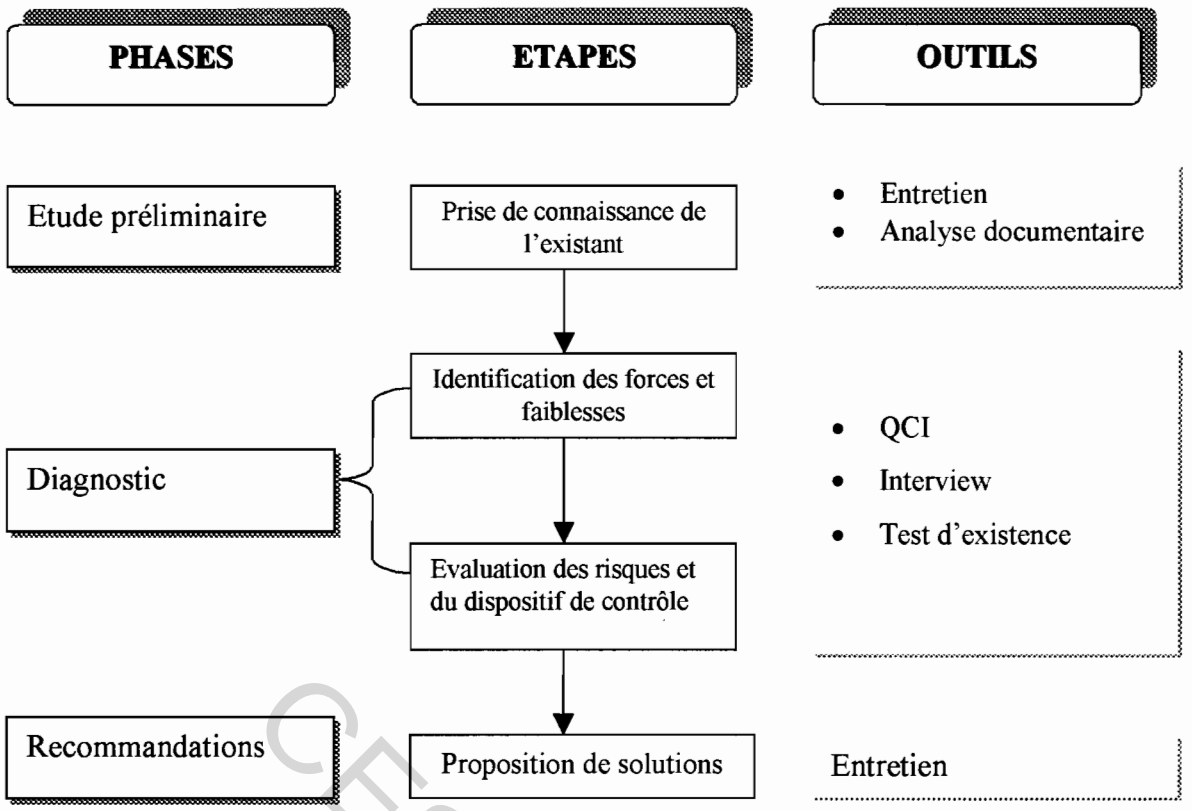
1.1 Description du modèle

La démarche que nous avons retenue pour traiter le sujet est la suivante :

- une phase d'étude préliminaire ;
- une phase de diagnostic ;
- une phase de recommandations.

De façon schématique, le cadre d'analyse de notre étude se présente comme suit :

Figure 4: le modèle d'analyse



Source : Nous-mêmes

a. La phase préliminaire

Cette première phase nous a permis de prendre connaissance des activités et du fonctionnement général de ECOBANK-COTE D'IVOIRE, plus spécifiquement des départements Audit & Contrôle Interne et Informatique & Technologie. Cette étape a été menée grâce aux outils de collecte d'informations suivants : l'entretien et l'analyse documentaire.

b. Phase de diagnostic

Cette étape nous a permis d'identifier les forces et les faiblesses du système et d'évaluer les risques et leurs conséquences sur le système. Nous avons fait ce diagnostic selon trois dimensions : organisationnelle, physique et logique. Cette évaluation des risques a abouti à l'appréciation du degré de maîtrise des risques qui pèsent sur la banque. Ainsi, nous avons, à partir du questionnaire de contrôle interne élaboré, tracé la rosace MARION qui fait

ressortir les zones à risques donc non maîtrisables du système informatique. Pour motiver notre opinion, des tests de conformité et d'existence ont été faits pour vérifier la véracité et l'objectivité des réponses.

c. Phase de recommandations

Cette phase nous a permis d'élaborer des recommandations à l'issue des faiblesses constatées. Pour les modalités pratiques, nous avons fait des entretiens avec le responsable de l'audit interne.

Le développement qui va suivre, s'intéresse aux différents indicateurs qui vont nous permettre d'apprécier la maîtrise du risque qui pèse sur le système informatique.

1.2 Indicateurs et leurs mesures

Les indicateurs et mesures retenus seront présentés sous forme de tableau pour une meilleure lecture.

Tableau 1 : Indicateurs et leurs mesures

Dimensions	Indicateurs	Mesures
Sécurité physique	Contrôle accès	- Existence et suivi du registre - Existence d'une vidéo - surveillance ou de détecteurs d'intrusion
	Gestion du parc informatique	• Existence d'un tableau de bord de suivi • Adéquation du personnel aux ressources informatiques

Sécurité logique	• Journalisation des accès	• Existence et suivi des journaux d'accès
	• Mots de passe	• Existence • Confidentialité
	• Sauvegardes des données et programmes	• Effectivité
	• Protection antivirale	• Existence d'antivirus à jour
Sécurité organisationnelle	• Organigramme	• Existence
	• Comité de sécurité	• Existence
	• Séparation des fonctions	• Effectivité
	• Politique de sécurité	• Existence d'une procédure et mise à jour
	• Satisfaction des utilisateurs	• Durée d'indisponibilité par mois • Taux de fiabilité (moyenne des temps de bon fonctionnement du système)

Source : nous-même

2. Méthode de collecte et d'analyse des données

Nous allons décrire tous les procédés utilisés pour recueillir les informations nécessaires à la bonne conduite de cette étude. Une analyse des informations sera faite pour en ressortir les plus pertinentes.

2.1. La procédure d'échantillonnage et de collecte de données

Le plan du mémoire a été conçu de manière à solliciter le point de vue des différents acteurs intéressés par le contrôle interne dont notamment les dirigeants de la banque, le personnel, les auditeurs internes et les informaticiens. Au départ, compte tenu de la pertinence du sujet, nous avions voulu interroger tout le personnel du siège. Mais au regard de la

situation socio-politique qui prévalait au moment de l'étude (temps de travail réduit, indisponibilité du personnel, instabilité politique), la collecte des données a finalement été effectuée auprès du responsable du Département Informatique et Technologie, du responsable du Département Contrôle Interne, 5 auditeurs internes ayant une bonne connaissance de l'entreprise ainsi qu'auprès des informaticiens. Nous avons également interrogé 20 employés des départements des opérations, de la trésorerie, du risque et de la clientèle privée avec qui nous avons fait notre « stage d'imprégnation » pendant 45 jours.

Cet échantillon est représentatif de la population du personnel étant donné que les personnes ciblées ont une bonne connaissance de l'informatique et de l'audit.

Notre « stage d'imprégnation » nous a permis d'avoir une appréciation globale du fonctionnement de la banque, des produits et services offerts par la banque et des problèmes liés au système informatique. En accord avec le Directeur de l'Audit Interne, notre champ d'intervention a été limité à l'évaluation de la sécurité de base eu égard à la confidentialité de certaines données et informations stratégiques de la banque. C'est pourquoi, dans le présent mémoire, aucun chiffre n'y sera incorporé.

Dans le cadre de la collecte des données, nous avons d'abord recueilli la documentation sur la maîtrise des risques dans les entreprises plus précisément dans les banques.

Nous avons étudié la documentation existante afin d'identifier les différents concepts, points de vue et interprétations sur les questions de menaces sur le système informatique des établissements de crédit. Nous avons également exploré le manuel de procédures pour avoir une idée des différents contrôles nécessaires à la maîtrise du risque informatique.

2.2 Les outils de collecte des informations

Pour compléter nos informations, nous avons élaboré un questionnaire de contrôle interne et effectué des interviews.

❶ Le questionnaire

Nous avons élaboré un questionnaire afin de compléter et d'approfondir les informations obtenues précédemment. Le questionnaire a été soumis au Directeur de l'Audit et administré au Directeur du Département Informatique et Technologies. Certaines questions techniques ont été posées aux informaticiens en charge à l'initiative du Directeur du Département. Etant donné que la sécurité de la banque relève du Directeur de l'audit, certaines questions lui ont été directement posées. Les questions portent essentiellement sur :

- la sécurité physique et logique,
- les procédures de secours,
- l'environnement de travail ;
- Les procédures mises en place et leur application
- L'organisation du département

L'administration du questionnaire s'est faite en accord avec le responsable du Département ICU et sur rendez-vous avec les personnes concernées car le contexte socio-politique dans lequel le pays vit, a conduit la direction générale a réduire les horaires de travail. Nous avons recoupé les informations recueillies pour nous assurer de leur exactitude. En cas de divergence de points de vue sur des questions, nous en faisons part à notre responsable de Département et une solution est trouvée.

❷ Les interviews

Nous avons fait des entretiens individuels afin de recueillir le point de vue du personnel cité plus haut sur le sujet. Ces interviews nous ont permis de savoir si les dispositions

minimales de la sécurité du personnel face au risque informatique étaient connues et pratiquées.

❹ **L'observation physique**

Elle a consisté à valider les procédures de sécurité décrites notamment les accès physiques, l'existence physique des registres et de la vidéo - surveillance. Nous avons visité tous les compartiments de la banque pour nous assurer de l'existence des consignes de sécurité. Concernant le système de détection d'incendie dans la salle d'ordinateurs, nous n'avons pas fait le test de fonctionnement car il nous fallait mettre le feu pour que le système se déclenche.

2.3 Le traitement et l'analyse des données

Sur la base des informations recueillies, nous avons pris connaissance de l'environnement de maîtrise des risques qui pèsent sur le système informatique de la banque. Cela nous a conduit mettre en lumière les forces et les faiblesses et d'apprécier par la suite le niveau de sécurité atteint par la banque grâce à la méthode MARION. Le traitement des données s'est fait grâce au logiciel ETHNOS 2 qui est un logiciel statistique d'analyse des questionnaires. Pour utiliser MARION, les facteurs utilisés doivent être pondérés en fonction de leur impact sur l'activité. La littérature nous a fourni un tableau indicatif de pondération relatif au secteur bancaire et de concert avec mon maître de stage, nous avons réajusté les pondérations des facteurs concernés par l'étude. Les pondérations retenues sont présentées en annexe.

Conclusion partielle :

La méthodologie proposée n'est pas différente de la démarche d'évaluation du contrôle interne. Elle nous conduit à répondre aux objectifs assignés à cette étude.

DEUXIEME PARTIE :
CADRE PRATIQUE

Introduction

Cette deuxième partie est le cadre pratique de notre étude. Elle vise à étudier les mesures et dispositifs de sécurité mis en œuvre par notre structure d'accueil pour maîtriser ses risques informatiques. Nous allons dans un premier temps présenter Ecobank - Côte d'Ivoire puis faire le diagnostic de son dispositif de maîtrise des risques informatiques et enfin terminer par les recommandations et les perspectives de mise en œuvre.

CHAPITRE I : PRESENTATION GENERALE DE ECOBANK COTE D'IVOIRE

Introduction

ECOBANK-CI est la banque qui nous a accueilli pour mettre en pratique les aspects théoriques abordés au cours de notre formation. Comment a-t-elle été créée ? Comment est elle organisée ? Comment fonctionne-t-elle ? Ce sont à ces différentes questions que ce chapitre de notre étude tente d'apporter des éléments de réponses.

1. Historique de ECOBANK

Le groupe ECOBANK est une institution bancaire régionale présente dans 11 pays de l'Afrique de l'Ouest dont la création remonte au début des années 1980. C'est à l'initiative de la Fédération des Chambres de Commerce de l'Afrique de l'Ouest dans son projet de création d'une banque régionale du secteur privé en Afrique de l'Ouest que les bases de cette institution ont été formulées. Il a fallu attendre en Août 1984 pour que les actionnaires fondateurs aient apporté le capital initial devant servir au financement des études de faisabilité, du travail d'évaluation et des activités de promotion en vue de la création du groupe ECOBANK.

En 1985, Ecobank Transnational Incorporated (ETI) fut créée avec l'accord des Etats membres de la Communauté Economique des Etats de l'Afrique de l'Ouest (CEAO) comme une société de holding de banque. 1200 actionnaires originaires de 14 pays ont souscrit à son capital. ETI a démarré ses activités effectivement avec sa première filiale au Togo en mars 1988.

Un an plus tard (1989), Ecobank Côte d'Ivoire voit le jour. Sa mission est de fournir des produits bancaires et des services financiers aux personnes physiques, entreprises,

institutions et aux gouvernements en Afrique de l'Ouest et Centrale. Sa clientèle est composée d'institutions étatiques, d'organisations non gouvernementales (ONG), d'institutions multilatérales, bilatérales et régionales, de sociétés multinationales, nationales et de particuliers.

Elle offre une gamme complète de produits et services de banque commerciale et d'investissement dont :

- les comptes courants ;
- les comptes de dépôts ;
- le change ;
- les comptes d'épargne ;
- les prêts et découverts ;
- le financement du commerce ;
- la gestion de portefeuille ;
- la gestion de trésorerie ;
- les marchés monétaires ;
- les marchés de capitaux.

ECI dispose d'un capital social de FCFA 3 226 000 000.

Après avoir passé en revue l'historique de ECI, nous allons étudier son organisation et son fonctionnement.

2. Organisation générale et fonctionnement de la banque

La structure organisationnelle de ECOBANK fait apparaître outre le Conseil d'Administration et la Direction Générale, les départements suivants (cf. annexe 1 pour l'organigramme):

1. le Département de la Clientèle Privée (Consumer Banking)
2. le Département du Commercial Banking (CBG)
3. le Département des Clients Institutionnels (Institutional Banking)
4. le Département des Opérations
5. le Département du Risque
6. le Département de la Trésorerie
7. le Département des Ressources Humaines (Human Resources)
8. le Département du Contrôle Financier (Financial Control)
9. le Département Audit & Contrôle Interne (Internal Control Unit)
10. le Département Juridique
11. le Département Informatique et Technologie (I.T)

Cette organisation est basée sur une décentralisation des responsabilités et des pouvoirs. Les missions et attributions assignées à chaque département se présentent comme suit :

a. Le Département de la Clientèle Privée (Consumer)

Ce département est chargé du marketing de la banque. Il joue le rôle d'interface entre les clients et les services opérationnels. Il s'occupe des ouvertures et fermetures de comptes, d'informer les clients sur leur position et des produits offerts par la banque. Le département a en charge les cinq (**5**)agences (agence principal du Plateau et les agences de Treichville, Adjamé, II Plateaux et Bouaké).

b. Le Département Commercial Banking ou CBG

Le CBG est chargé de gérer les comptes des entreprises privées (PME). Il a pour mission de suivre le portefeuille de ses clients et d'inspecter le marché pour attirer de nouveaux clients. Le CBG est également chargé de proposer de nouveaux produits et services aux clients afin de les fidéliser.

c. Le Département Institutionnal Banking ou IBG

L'IBG a les mêmes attributions que le CBG. Mais la différence réside dans le portefeuille de clients gérés. En effet, l'IBG gère la clientèle institutionnelle (ambassades, BAD, ONG, grandes entreprises).

d. Le Département du Contrôle Financier (Financial Control)

Le département du contrôle financier se charge d'établir le budget de la banque, les états financiers, les rapports d'activité destinés à la Direction Générale et autres organismes utilisateurs. Il réalise l'étude des gros investissements, fait le suivi des immobilisations et est responsable de la comptabilisation des écritures d'opérations diverses et de régularisations.

e. Le Département des Ressources Humaines (Human Resources)

Le département des ressources humaines est le département chargé du recrutement, de la formation, de la paie et de la gestion prévisionnelle des ressources humaines.

f. Le Département Juridique

Le Département Juridique gère tous les dossiers litigieux et contentieux de la banque.

g. Le Département du Risque

Le département du risque s'occupe de l'ensemble des moyens mis en œuvre pour gérer les risques pris par la banque particulièrement le risque de contrepartie (la gestion des prêts et découverts).

h. Le Département des Opérations

Le Département des Opérations se charge de toutes les opérations de la banque notamment :

- Les opérations de transfert :le transfert est un envoi de fonds d'une banque à une autre en faveur d'un bénéficiaire à l'initiative d'un client ou d'une banque.

- Les opérations du commerce extérieur (TRADE) : elles concernent les remises documentaires à l'importation et à l'exportation, les « bills negociated », les lettres de crédit à l'importation et à l'exportation, les cautions et garanties, les crédits documentaires
- Les opérations du portefeuille local : elles concernent l'encaissement et le paiement des valeurs sur place par l'intermédiaire de la " Chambre de Compensation " de la BCEAO.
- Les opérations du money market : il s'agit des dépôts à terme, des chèques et effets à l'encaissement, des effets à l'escompte

En plus, le Département des Opérations se charge de l'approvisionnement et de la tenue de stocks de fourniture de bureau.

i. Le Département Informatique et Technologie (I.T)

Il joue un rôle de premier plan dans la banque. Il étudie et propose des solutions aux problèmes que rencontre la banque en vue d'améliorer la qualité de ses services. Il comprend deux services : le service réseau et le service développement.

j. Le Département de la Trésorerie

Ce département se compose deux services : le service marché monétaire et le service des opérations de change.

Le service marché monétaire est chargé de :

- Déterminer les taux du jour à appliquer pour toutes les opérations à partir du Reuters
- Renseigner la situation des réserves obligatoires
- Etablir l'état du solde des comptes des filiales afin d'éviter que la banque ne payent des pénalités
- Faire le point des avoirs en caisse et en coffre des agences

Tandis que le service des opérations de change se charge de :

- la vente et l'achat des devises
- la fixation les taux à appliquer au client et aux correspondants pour toutes les opérations de transfert.

k. Le Département Audit et Contrôle Interne

Le département Audit & Contrôle Interne ou Internal Control Unit (I.C.U) est un département rattaché hiérarchiquement à la direction générale. De façon fonctionnelle, le département est rattaché à l'inspection générale du groupe E.T.I. Il est chargé d'assurer la mise en œuvre du contrôle interne au sein de la banque.

CHAPITRE II : DIAGNOSTIC DU DISPOSITIF DE MAITRISE DES RISQUES LIES AU SYSTEME INFORMATIQUE DE ECOBANK COTE D'IVOIRE.

Introduction

Ce chapitre nous permet de voir les dispositions prises par l'entreprise pour se protéger contre les risques éventuels liés à son informatique. Ainsi, nous pourrons juger du niveau de sécurité de atteint. Pour mieux comprendre les actions entreprises par ECI dans le cadre de la réduction des risques liés à son système d'information, il convient d'identifier les ressources de l'établissement pour savoir ce qu'il faut protéger et à quel niveau.

1 Description des ressources informatiques

Les ressources informatiques comprennent les biens matériels, le personnel, les processus et programmes, les données et les supports.

1.1 Les biens matériels

L'institution dispose de bâtiments loués (le siège et les 4 agences) qui abritent toutes ses activités. En plus de ces locaux, un autre bâtiment loué loge les archives de la banque. Ses équipements informatiques comprennent des ordinateurs (serveurs et postes de travail), les imprimantes (laser, jet d'encre et matricielles), le Minitel, le Modem. Pour des questions de confidentialités, la spécification du parc en nombre et en fonctionnalités ne sera pas mentionnée dans le présent mémoire.

En plus de l'alimentation électrique avec son câblage connecté à la société de distribution de l'énergie, Ecobank dispose d'un groupe électrogène et d'onduleurs qui assurent la continuité de l'alimentation en cas de coupure. Il existe également un réseau téléphonique qui permet au personnel de communiquer entre eux et avec l'extérieur.

L'établissement dispose également d'une machine qui sert à trier les chèques qu'on appelle la trieuse et d'une autre servant à la mise sous pli des relevés des clients.

1.2 Les programmes informatiques

Au niveau des programmes informatiques, ECI utilise principalement l'applicatif bancaire GLOBUS de la société TEMENOS. Cette application a son serveur de production (LIVE) situé dans une agence et son serveur de secours (BACKUP) situé dans une autre. Ce progiciel bancaire fonctionne sur un système de base de données relationnelles développé sous UNIX.

ECI utilise le logiciel de transferts bancaires (SWIFT), SAARI pour la paie, le Reuters pour les opérations de Trésorerie. En outre, la banque dispose des logiciels de bureautique (MS Office 97& 2000 : Word, Excel, Powerpoint, Access).

Des applications internes ont également été développées par le Département Informatique et Technologie : TRAITE 2000 pour la gestion des effets à l'encaissement et escomptés, ECOCHEQ pour la gestion de la commande des chéquiers, le REFER Management qui gère le traitement des chèques à insuffisance ou défaut de provision.

Toutes les machines sont interconnectées en réseau interne grâce à WINDOWS NT. Le serveur étant lui –même connecté par VSAT au siège et par Internet à un fournisseur d'accès local.

1.3 Les données

En ce qui concerne les données et informations, ECI utilise les notes de service, le courrier électronique. Il existe également un Intranet sur lequel on trouve toutes les informations concernant l'organisation et le fonctionnement de la banque, le numéro des postes téléphoniques de tous les agents, la stratégie de l'entreprise pour l'année en cours, les thèmes de formation interne des employés. Les données et informations traitées sont relatives

à la clientèle, à la planification et aux éléments fondamentaux de la compétitivité de l'entreprise.

Les supports de données sont constitués par les listings (édition du grand livre, etc.), les bandes magnétiques et les disquettes, CD-ROM. Les disquettes et CD-ROM des différents programmes et logiciels sont gardés dans des boîtiers à clés. Egalement toute la documentation et les licences d'exploitation des logiciels existent.

1.4 Le personnel

Au niveau des ressources humaines, ECI a en son sein trois types de personnel : le personnel permanent ou les embauchés qui ont un contrat à durée indéterminée, les agents ayant un contrat à durée déterminée et les stagiaires. Ce sont toutes ces personnes qui animent l'organisation.

Après avoir présenté succinctement les ressources du système informatique de notre structure d'accueil, il convient de décrire le dispositif de maîtrise des risques informatiques qui existent au sein de la banque.

2 Appréciation du dispositif en place

La présente section permettra de mettre en relief les différentes forces et faiblesses du dispositif en place.

2.1 Dispositions générales

Organisation

La structure organisationnelle de ECI met les Départements IT et ICU au même niveau. Le département Audit & Contrôle Interne ne dispose pas de personne ressource

spécialisée en matière d'Audit Informatique alors que c'est le département qui est chargé de veiller à la sécurité de la banque.

La gestion du parc informatique

La gestion du matériel informatique est du ressort du Département Contrôle Financier qui tient une base de données de tous les moyens informatiques dont dispose la banque. Le recensement exhaustif des matériels permet de connaître la valeur globale du parc, la valeur de chaque poste de travail, les caractéristiques techniques du parc et les progiciels achetés, qu'ils soient standards ou applicatifs. Constituant l'un des postes de l'actif du bilan, un suivi rigoureux du parc ne peut être effectué que sur la base d'un recensement. Cependant, les statistiques concernant le parc informatique n'ont pu être établies dans cette étude à cause du non dénouement de l'inventaire initié par le ICU.

Le comité sécurité et technologie

Ce comité composé des responsables de départements suivants (Audit Interne, Contrôle Financier, Opérations et Informatique & Technologie) se réunit une fois par trimestre pour examiner tous les problèmes technologiques susceptibles d'avoir des répercussions sur l'activité de la banque. Ce comité donne son avis sur les choix technologiques et les implications technologiques qui en résultent.

Assurances

L'examen du dossier d'assurances nous a permis de noter que cette police d'assurance couvre les risques d'incendie, les dégâts des eaux, le vol des matériels informatiques de la banque. Il est évident que le contrat d'assurances ne garantit pas la reprise des traitements informatiques mais il permet de garantir une compensation financière en cas d'accident.

Le système d'archivage

En ce qui concerne l'archivage des pièces comptables, c'est la section Archive du Département Audit qui en a la charge. L'archivage répond à un besoin fonctionnel qui vise à conserver des données ou informations de la banque, stratégiques ou non, mais nécessaires sur le plan professionnel, social, fiscal ou juridique. Les informations archivées seront utilisées à des fins de consultation et de recherche ou servir de preuves. Ainsi, après avoir vérifié l'exactitude des pièces transmises par l'agent des opérations ou d'un autre département, l'archiviste les met dans des cartons archives avant de les classer sur les rayons métalliques. La salle des archives est climatisée et est dotée d'extincteurs d'incendie.

2.2 Sécurité physique

L'accès au bâtiment

L'accès aux bâtiments de l'institution est composé d'une chaîne de sécurité constituée d'une vidéosurveillance et d'un gardiennage. La vidéosurveillance qui fonctionne 24h/24, permet de surveiller tous les mouvements au sein de la banque. Conformément aux procédures internes de la banque, la gestion des cassettes vidéo est du ressort du Contrôle Interne. Un test de fiabilité est fait pour s'assurer du contenu de la cassette vidéo. Pour motiver notre opinion, nous avons vérifié l'existence et la fiabilité de la vidéosurveillance grâce à un test de fonctionnement. Dans les autres agences, c'est le chef d'agence qui en est le responsable. Les gardiens contribuent également à renforcer le dispositif de sécurité mis en place.

L'accès à la banque comporte deux entrées : la porte d'entrée du personnel et la porte d'entrée des clients. En ce qui concerne l'ouverture de la porte d'entrée du personnel, les procédures internes prévoient la présence d'un gardien, d'un agent des opérations et d'un auditeur. En plus des clés des portes, l'auditeur doit composer le code secret d'accès. Le

système étant relié à une société de sécurité, toute intrusion non autorisée déclenche l'alarme. Un rapport quotidien est établi par les gardiens et transmis au ICU pour s'assurer du bon déroulement de l'ouverture des accès au sein de la banque.

En outre, un registre indiquant les heures d'entrée et de sortie de chaque employé est ouvert ; ce registre permet de suivre le mouvement du personnel. Pour identifier le personnel au sein de la banque, chaque employé est tenu de porter son badge d'identification. L'ouverture de la porte d'entrée des clients se fait à l'intérieur de la banque.

L'accès à la salle machine

L'ouverture de la salle contenant le matériel informatique (serveurs, dérouleurs de bandes, matériel de télécommunications tel que modems, minitel) se fait à clé par le personnel du département informatique. Malgré l'affiche indiquant la zone interdite à toute personne étrangère, tout agent non habilité peut y entrer et il n'existe pas de dispositifs permettant de canaliser les flux de circulation. Seul un registre déposé à l'entrée à la salle permet de connaître toutes les personnes qui ont pénétré dans cette salle.

Il est à noter que cette salle est protégée par une installation d'extinction automatique d'incendie fonctionnant en permanence. Dès que le système détecte une fumée, il se met en marche en déclenchant l'alarme et en ouvrant les vannes d'extinction.

Les installations électriques

En ce qui concerne les installations électriques, nous avons constaté que le câblage dans certains services comme le Commerce Extérieur (Trade) est visible et ne garantit pas la sécurité aussi bien des biens que des personnes. En effet, les fils de raccordements traînent dans le bureau et les conditions ergonomiques de travail ne sont également pas observées.

En outre, tous les ordinateurs ne sont pas connectés sur des prises ondulées, ce qui fait qu'en cas de coupure, les machines se désactivent. Cette faiblesse constitue un danger pour la banque en ce sens la machine peut être détériorée mais aussi une perte de temps pour l'utilisateur qui est obligé de recommencer le travail exécuté.

Les consignes de sécurité physique

Aucune consigne de sécurité générale (urgences, SAMU, évacuation) ni de consignes de sécurité physique spécifique aux risques liés à l'informatique (incendie, dégâts des eaux) n'est affichée au sein de la banque. Cela ne garantit ni la sécurité du personnel ni des ressources informatiques.

Au niveau de la sécurité des micro-ordinateurs, on note une absence de structure d'accueil et de formation des nouveaux utilisateurs, constituant ainsi une faiblesse d'ordre organisationnel. Cela expose les micro-ordinateurs à une fragilité potentielle. En effet, la méconnaissance des utilisateurs de l'environnement informatique entraîne souvent des manipulations hasardeuses qui ont pour effet de dégrader sensiblement la qualité et la productivité du service voire la détérioration du disque dur, ce qui représente un coût pour la banque.

En plus, les principales consignes en matière de sécurité micro ne sont pas observées. Il s'agit principalement de la protection des postes de travail. Il existe un antivirus Mac Afee installé sur les postes de travail, cependant il n'est pas régulièrement mis à jour afin de tenir compte des nouveaux virus. Si la maintenance des serveurs est régulièrement assurée, celle des postes de travail ne l'est pas. Le Département IT n'intervient sur les postes que si l'utilisateur signale une défaillance et le temps de réponse est souvent long d'où une insatisfaction des utilisateurs.

Aussi, l'utilisation des disquettes par le personnel, même si elle est moins fréquente, expose les machines à des infections de virus. Une note de service du Département IT interdit l'utilisation des disquettes au sein de la banque mais cette mesure n'est pas rigoureusement suivie.

Le serveur

La capacité du serveur ne correspond plus au volume d'activités traitées. Le microprocesseur du serveur ne répond pas aux attentes des utilisateurs, il est lent. En effet, acquis fin 1997, le serveur ne supportait que des transactions pour 5000 clients répartis dans deux agences. A l'heure actuelle, la banque compte plus de 22000 clients et 5 agences.

En plus, des incidents liés à l'exploitation de l'application de GLOBUS surviennent généralement à chaque fin de mois. La durée moyenne d'indisponibilité du système est de 2 heures par mois. Les causes généralement évoquées sont soit le fait que le système n'a pas fini le traitement de la veille à cause de l'arrêté mensuel des comptes, soit le fait d'un problème logiciel. La non disponibilité de l'applicatif induit une perte financière, une qualité de service médiocre, une atteinte à l'image de la banque et un manque de productivité du personnel. Pour gérer ces problèmes, des actions correctives sont mises en œuvre notamment le remplacement du serveur.

De plus, il faut signaler que la licence d'exploitation de l'applicatif autorise un nombre limité d'utilisateurs. Ainsi tous les utilisateurs ne peuvent accéder au système au même moment. La planification des services informatiques n'a pas tenu compte des perspectives d'évolution de l'effectif du personnel de la banque ainsi que des besoins actuels et futurs en matière de prestations de service. Cet état de fait traduit la non satisfaction des utilisateurs qui n'arrivent pas à accéder au système en temps voulu.

Logiciel de base et la documentation

Les logiciels de base (disquettes, CD-ROM) et leurs licences d'exploitation sont gardés dans des armoires ignifuges. Les documentations relatives aux logiciels par contre sont rangées dans des armoires qui ne ferment pas à clé.

2.3 Sécurité logique

La gestion de l'applicatif bancaire GLOBUS

C'est le contrôle interne qui est habilité à introduire tous les nouveaux utilisateurs dans le système, modifier le profil informatique des utilisateurs et enfin soustraire un utilisateur du système informatique.

Il contrôle le droit d'utilisation de Globus : quand l'utilisateur en a le droit, quelle partie du système il doit avoir accès. Il détecte, empêche et enregistre toute tentative d'utilisation non autorisée du système. En fait, il s'agit d'un contrôle programmé intégré au logiciel.

L'accès au système informatique repose sur une démarche en deux phases. Il s'agit pour l'utilisateur dans un premier temps, par le couple (login / password), d'entrer dans l'interface du système. Si l'ordinateur reconnaît ces informations alors la deuxième phase se déclenche. Cette phase comprend un moyen de reconnaissance en deux temps : l'identification et l'authentification qui est basée sur un dialogue entre l'utilisateur et la machine.

L'identification consiste à décliner son identité (SIGN ON NAME) puis à introduire son droit d'accès (PASSWORD). Ces informations ne peuvent être fournies que par la personne ayant un profil dans le système. La vérification de la validité de l'association identifiant et preuve permet à l'utilisateur d'accéder aux ressources qui lui ont été affectées. Ainsi, conformément à la politique de contrôle des systèmes informatisés de l'établissement, l'accès aux données ainsi qu'aux systèmes et aux logiciels réservé aux personnes autorisées,

permettra d'assurer la protection des informations aussi bien de l'institution que des clients car le secret bancaire l'oblige.

Les procédures internes interdisent aux utilisateurs d'imprimer et d'afficher leurs mots de passe (cf. CAP Manual 20.010.2.2.2) et obligent les utilisateurs à changer périodiquement leur mot de passe (période de 1 mois).

Au niveau de la séparation des fonctions, les procédures stipulent que les systèmes en temps réel ne doivent pas permettre l'utilisation du même mot de passe pour :

1. Saisir et autoriser la même transaction
2. Faire des saisies et changer les programmes
3. Faire des changements aux programmes et les approuver ou les autoriser

Toutes ces dispositions sont effectivement suivies et bien gérées par le Département Audit.

Exemple : Grille d'analyse de la création du profil utilisateur

Tâches	**Nature opérations**	**Utilisateur**	**Chef de service ou de département de l'utilisateur**	**Auditeur interne**	**Chef du département ICU**
Remplissage de la fiche et Transmission de la fiche au chef de service	Ex	X			
Approbation et émargement de la demande	C		X		
Transmission de la fiche au I.C.U	Ex	X			
Réception, vérification et approbation du directeur de ICU	C				X
Création de profil	Ex/En			X	
Autorisation de la création	C				X

Ex = tâche d'exécution ; C = contrôle et supervision ; En = Enregistrement

Pour vérifier l'accès au système, il est généré un rapport quotidien indiquant la liste complète de tous les messages d'erreurs dus à une utilisation incorrecte du système : le protocol report.

En effet, le protocol report enregistre non seulement toutes les tentatives de violation de la sécurité dans le fichier Protocol (mot de passe incorrect après trois tentatives, mot de passe terminé, utilisateur déjà connecté à un autre terminal) mais aussi tous les accès autorisés au système.

L'exploitation quotidienne de ce fichier permet de suivre toutes les intrusions dans le système. Egalement, il existe un fichier permettant de lister toutes les personnes ayant eu accès au système

La procédure de journalisation des accès qui permet donc d'établir des pistes d'audit de l'activité du système et des utilisateurs, répond bien aux exigences réglementaires de la commission bancaire de l'UEMOA.

Le dispositif mis en place pour gérer le système informatique est tel que seul le département contrôle interne est habilité à introduire un nouvel utilisateur ou à le soustraire.

Signalons que l'introduction ou la modification d'un utilisateur fait l'objet d'une demande dûment approuvée par son chef de département et par le directeur de l'Audit. Ces différentes procédures effectivement suivies par la banque permettent de centraliser et de surveiller la gestion du système.

Ainsi donc, les données ou informations contenues dans le système ne sont exploitées que par les ayant-droits.

En plus, pour mieux sécuriser l'utilisation de Globus, un système de « time-out » y est paramétré. Au bout de cinq (5) minutes d'inutilisation du système, le système sort automatiquement l'utilisateur.

Sécurité des données et des informations

Au risque de compromettre l'intégrité des données du système, toute modification apportée à GLOBUS est convenablement testée sur la machine BACKUP avant de la transposer dans l'environnement de production LIVE.

La messagerie de Transfert bancaire (SWIFT)

La définition du profil utilisateur SWIFT fait l'objet d'une demande par le Département concerné qui est transmise au Département I.C.U. Après approbation du Directeur de I.C.U, le profil est créé. L'accès au SWIFT se fait en spécifiant son identité et son mot de passe. Le couple authentifiant et identifiant est personnel et confidentiel pour chaque utilisateur habilité. Le risque ici est de se voir usurper son code d'accès. Il faut signaler que, pour envoyer des messages à d'autres correspondants pour exécuter un ordre de virement ou de transfert par cette messagerie, trois personnes habilitées sont nécessaires: un initiateur, un vérificateur et un autoriseur. Le dispositif de contrôle en place est tel que tous les ordres de transferts sont vérifiés à partir de pièces comptables. En effet, au sein du département ICU, un agent est chargé de faire ces vérifications.

Concernant les autres logiciels cités plus haut, la séparation des tâches est également observée. La séparation des fonctions permet de limiter les risques d'erreurs ou d'actions malveillantes. Pour motiver notre opinion sur cette séparation des tâches, nous avons dépouillé 20 fiches de demande et de modification de profil. Nous avons rencontré les utilisateurs concernés et avons fait des simulations pour voir s'il y avait une conformité entre le profil demandé et le profil créé.

Le système de sauvegarde des données et informations

La sauvegarde est un processus préventif géré par les informaticiens et qui consiste à recopier périodiquement les fichiers ou base de données dans le but de reconstruire, en cas de besoin, les informations altérées ou perdues.

Ainsi, pour permettre le redémarrage du système informatique après un sinistre, matériel ou logique, ayant détruit ou altéré de façon importante les supports de données, des copies de celles-ci sont faites et envoyées chez une consœur régulièrement sous forme de bandes magnétiques. Avant de transmettre cette bande, un test de fonctionnalité est fait sur le dérouleur de bandes pour s'assurer de la fiabilité de son contenu.

Il existe également une machine back-up qui doit assurer le relais et poursuivre les activités de la banque dans les meilleures conditions et diminuer le montant des pertes financières liées à la situation de catastrophes. Ce plan de secours doit être formalisé dans un manuel et garder hors de la banque.

A l'heure actuelle, l'établissement ne dispose pas de plan stratégique d'urgence (contingency plan). En effet, le manuel rédigé n'a pas encore été validé par la Direction Générale et le Département Audit.

En ce qui concerne l'archivage des pièces comptables, c'est la section Archive du Département Audit qui en a la charge. L'archivage répond à un besoin fonctionnel qui vise à conserver des données ou informations de la banque, stratégiques ou non, mais nécessaires sur le plan professionnel, social, fiscal ou juridique. Les informations archivées seront utilisées à des fins de consultation et de recherche ou servir de preuves. Ainsi, après avoir vérifié l'exactitude des pièces transmises par l'agent des opérations ou d'un autre département, l'archiviste les met dans des cartons archives avant de les classer sur les rayons métalliques. La salle des archives est climatisée et est dotée d'extincteurs d'incendie.

Sécurité du réseau

Comme nous l'avions souligné plus haut, le serveur est connecté à Internet. La connexion de la banque à Internet représente l'ouverture de son système informatique à l'extérieur, ouvrant ainsi la porte à toutes les formes d'agressions. C'est pourquoi, consciente de ce danger, la banque a mis en place un pare-feu (ou en anglais firewall) sur le réseau pour le protéger contre toutes les tentatives d'intrusion.

En outre, pour réduire les risques de vulnérabilités du serveur, la direction générale a limité l'accès à Internet aux Directeurs de Département et à leur Assistant.

Conclusion partielle:

La description de l'existant fait ressortir les forces et les faiblesses du système que nous allons analyser.

3. Analyse des forces et faiblesses

Cette section de notre étude va s'intéresser à l'analyse des points forts et des points faibles du système informatique. Nous avons choisi de développer cette analyse suivant les trois dimensions : organisationnelle, physique et logique. Nous avons cherché à mettre en relief les risques potentiels et leur impact sur le système.

3.1 Tableau 2: Analyse de la sécurité organisationnelle et générale

FORCES	FAIBLESSES	RISQUES
• Existence d'un comité de sécurité • Existence d'un contrat d'assurance couvrant les risques d'incendie, de dégâts des eaux, de vol des matériels informatiques de la banque. • Les procédures internes de la banque prévoient un plan de reprise de l'activité. Ce plan est formalisé dans un manuel. • Des bandes de sauvegardes sont régulièrement faites, testées et envoyées hors de la banque • Il existe une machine back-up qui assure le relais. • Il existe un registre d'entrée et de sortie du personnel de la banque • Maîtrise du parc informatique en nombre.	• Absence de personne spécialisée en Audit Informatique • Inexistence d'une « hot-line » au sein de la banque • Absence de consignes de sécurité générales : aucune consigne n'est affichée au sein de la banque. • La machine back-up est souvent ramenée au siège • Non respect des conditions ergonomiques de travail • Les procédures ne sont pas régulièrement mis à jour • Non évaluation du risque maximal tolérable lié à l'informatique • Il n'existe pas de structure d'accueil et de formation des utilisateurs.	• Non maîtrise des activités du personnel informatique En effet, l'absence d'auditeur informatique au sein de la banque ne permet pas d'apprécier de façon efficace les activités du personnel informatique. Le personnel informatique peut connaître les faiblesses du contrôle interne et en conséquence modifier les programmes ou les données lors de leur traitement. • Le personnel risque de paniquer en cas d'incendie car les mesures sont à prendre ne sont pas connues. • Le disque dur du serveur peut être endommagé lors du transport • Non prise en compte des risques nouveaux • Non maîtrise des fonds que supporteraient l'entreprise en cas de sinistre.

3.2 Tableau 3 : Analyse de la sécurité physique

Forces	Faiblesses	Risques
• Le système de vidéo – surveillance qui est installé au sein de la banque, est un atout pour surveiller tous les flux de mouvements et constitue une preuve en cas d'actes de vol ou de sabotage matériel. • Les cassettes vidéo sont remplacées chaque trois jours et sont testées pour s'assurer de leur efficacité. • La présence des gardiens renforce le dispositif de sécurité mis en place. • La salle machine contenant les serveurs se ferme à clé et il existe un registre d'accès à cette salle. • Les disquettes, CD-ROM et la documentation sur les logiciels sont conservées dans une armoire ignifuge. • Il existe un système de détection et d'extinction de fumée installée à la salle machine. Ce système permet d'éviter les risques de propagation du feu au sein de toute la banque.	• Le système de détection d'incendie n'est pas installé dans toute la banque • Le câblage dans le service « Trade » n'est pas protégé.	• Les risques de court-circuit et d'incendie sont donc à envisager. • Perte financière due aux dégâts causés par le sinistre.

Forces	Faiblesses	Risques
• L'alimentation physique est suppléée par un groupe électrogène. Ce qui garantit la continuité de l'alimentation du système en cas de coupure de courant. • La présence d'onduleurs permet de stabiliser les variations intempestives de la tension du courant • La salle machine et de façon générale toute la banque sont climatisées. • Le câblage est protégé par une goulotte		

3.3 Tableau 4 : Analyse de la sécurité logique

FORCES	FAIBLESSES	RISQUES
• Le contrôle des accès est réservé au Département ICU. En effet, c'est le seul département habilité à créer le profil des utilisateurs. • L'accès à l'applicatif bancaire GLOBUS se fait grâce à un couple d'identification et d'authentification (mot de passe) qui est personnel. • Les droits d'accès sont invalidés après trois tentatives et sont débloqués par le ICU. La procédure de journalisation des accès au système à travers les fichiers «protocol» et «user activity» permet de lister toutes les personnes qui ont travaillé dans le système. Elle constitue une piste d'audit pour détecter toute intrusion illicite. La mise en place de contrôles programmés, assurant la cohérence et l'intégrité des opérations effectué	• La procédure d'attribution de profil utilisateur n'est pas respectée. En effet, le Département ICU a attribué des profils utilisateurs à certains stagiaires en particulier à tous les stagiaires dudit département. • Tous les utilisateurs ne peuvent accéder au système au même moment. • L'indisponibilité de GLOBUS • La protection antivirale des postes de travail n'est pas mise à jour régulièrement	• L'attribution des profils aux stagiaires ne garantit pas la confidentialité des données et fichiers. • L'impossibilité d'accéder au système à tout instant induit une insatisfaction et une baisse de productivité des utilisateurs. • Perte d'image de la banque • Perte de clientèle • Les ordinateurs risquent d'être infectés de virus • Le disque dur des machines peut être détérioré conduisant à une indisponibilité des postes de travail • Les données et informations stratégiques peuvent être altérées ou être divulguées.

FORCES	FAIBLESSES	RISQUES
• La technique de «time-out» paramétrée au logiciel permet de quitter et de préserver la sécurité du système informatique en cas d'abandon involontaire de son poste de travail. • Le renouvellement des mots de passe est imposé par le système après un délai de 1 mois. • Les mots de passe sont cryptés • La séparation des fonctions est observée. La définition du profil d'utilisation est du ressort du Département ICU qui s'assure de l'opportunité d'attribuer un droit d'accès au personnel	• Certains utilisateurs désactivent directement leur machine par le bouton de mise hors tension • Certains postes de travail ne sont pas connectés aux prises ondulées • Les disquettes sont utilisées sur les postes de travail. • La capacité du serveur ne répond plus au volume d'activité	• Divulgation et/ ou accès à des données confidentielles par des personnes de l'entreprise n'ayant pas à les connaître (données sur la paie par exemple) • Pertes financière dues à l'indisponibilité des postes de travail • Indisponibilité des machines et des données •

Forces	Faiblesses	Risques
• L'accès au SWIFT est autorisé en spécifiant son identité et son mot de passe. • Le parc informatique est maîtrisé en nombre, en configuration matérielle et logicielle • Les incidents matériels et logiciels sont gérés de façon permanente • Un pare-feu existe sur le réseau pour prémunir les données et les serveurs contre les attaques possibles.		

Source : nous-même

A travers cette analyse, nous remarquons que tous les risques qui agissent sur le système informatique de la banque ne sont pas maîtrisés. Pour motiver notre opinion, nous allons évaluer le niveau de sécurité atteint par la banque. Cette appréciation donnera une vision globale des mesures à entreprendre pour limiter les risques de défaillance.

4. Evaluation du niveau de sécurité

Pour apprécier le niveau de sécurité atteint par ECOBANK, nous avons utilisé la méthode d'analyse des risques informatiques et d'optimisation par niveaux (MARION) présentée dans le cadre théorique. L'objectif est d'obtenir une vision de la sécurité de la banque par rapport à un niveau jugé «correct ou acceptable ». Le questionnaire utilisé dans cette étude est une adaptation de l'enquête réalisée en 1994 par la Commission Bancaire de France.

Ainsi, nous avons évalué le niveau de sécurité suivant 15 facteurs répartis en 3 thèmes (sécurité organisationnelle, sécurité logique et sécurité physique), chacun d'eux se voyant attribuer une note de 1 à 4. Par exemple, pour la question :« Les salles d'ordinateurs sont – elles protégées par une installation d'extinction automatique fonctionnant en permanence ?», nous avons défini une règle du type :

4= oui, des tests de fonctionnement sont régulièrement faits et elle fonctionne toujours.

3= oui, des tests de fonctionnement sont régulièrement faits mais elle ne fonctionne pas en permanence

2= oui, mais certaines salles sont dépourvues d'extincteurs

1= absence d'extincteur

Pour chaque facteur de sécurité, une formule de pondération (moyenne arithmétique) permet d'obtenir le niveau.

4.1 Résultats de l'étude

Le résultat des questionnaires permet d'obtenir la " rosace " propre à ECOBANK. Cela permet de juger facilement et rapidement des domaines vulnérables de l'entreprise, la cohérence et l'homogénéité des niveaux de sécurité des différents indicateurs, et donc d'identifier également rapidement les points à améliorer.

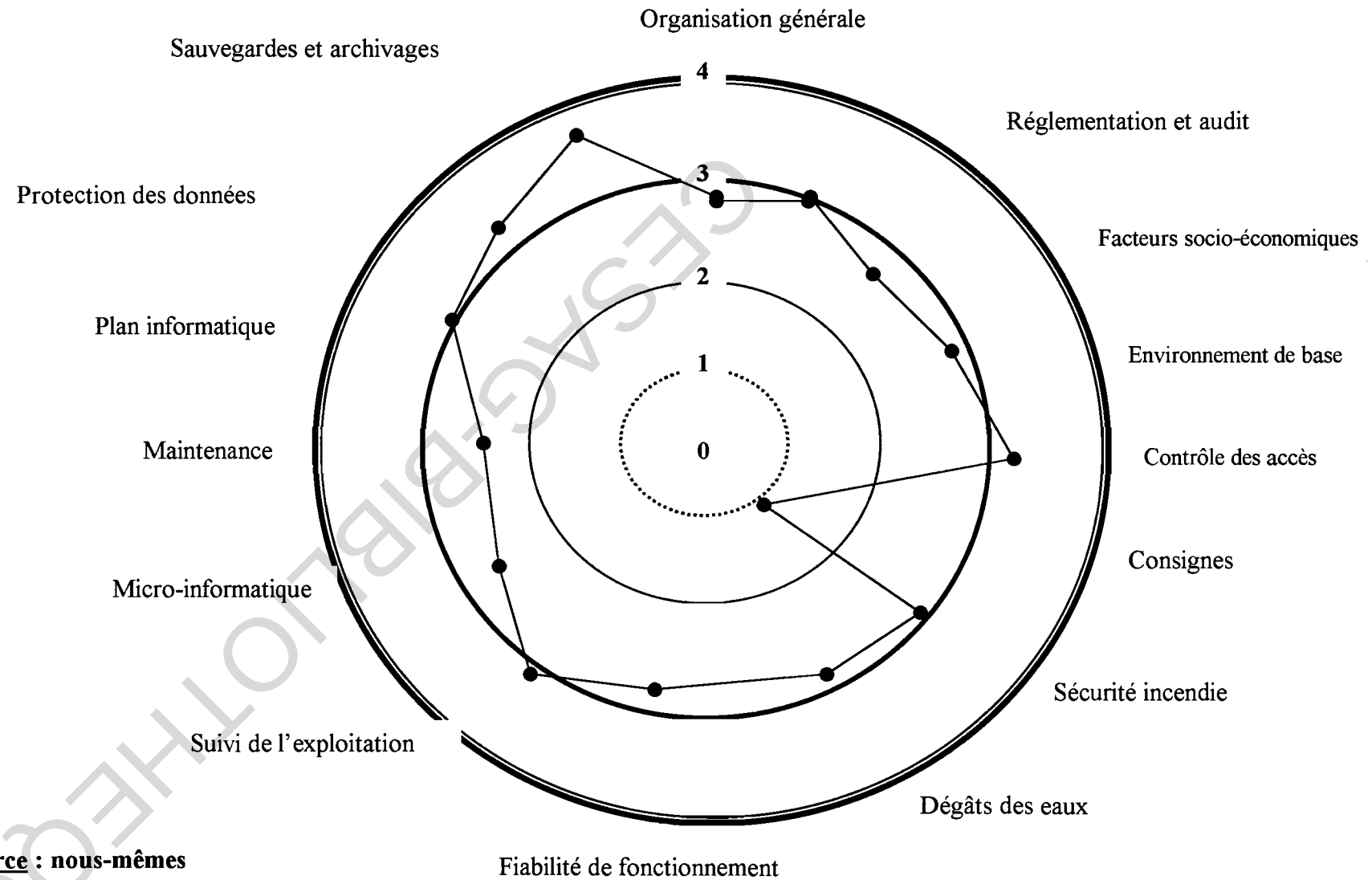
Tableau 5: Valeurs de la rosace

Noms des facteurs	Coefficient	Valeurs trouvées
Organisation générale	3,1	2,5
Réglementation et audit	1,5	2,8
Facteurs socio-économiques	2	2,5
Environnement de base	1	2,7
Contrôle des accès	4,5	3,2
Consignes	**1**	**1,3**
Sécurité incendie	1	3
Dégâts des eaux	1	3
Fiabilité de fonctionnement	2	3
Suivi de l'exploitation	3	3,3
Micro-informatique	1	2,7
Maintenance	1	2,5
Plan informatique	1	3,2
Protection des données	1	3,1
Sauvegardes et archivages	8	3,5

Source : nous-mêmes

Moyenne : 3,01

Figure 5 : Rosace MARION



Source : nous-mêmes

4.2 Analyse des résultats

Les résultats de cette étude font apparaître les forces et les faiblesses du dispositif de maîtrise des risques liés au système informatique. D'une manière générale, le niveau de sécurité moyen de ECI se situe à 3,01, niveau qui est supérieur à la base de référence des établissements de crédits (2,6).

Pour comprendre et suivre l'interprétation des résultats de notre étude, nous allons rappeler la règle de décision proposée par la méthode. En effet, les facteurs de sécurité ayant une valeur supérieure ou égale à 3 traduisent la maîtrise des risques liés à ces facteurs. Cela suppose que le dispositif de contrôle interne mis en place permet à ECI non seulement de se défendre mais aussi de se connaître et de s'adapter en fonction d'un milieu qui évolue.
Par contre, les facteurs dont les niveaux sont inférieurs à 3, indiquent les domaines vulnérables de la banque et les points à améliorer.

Nous allons présenter dans un premier temps les domaines maîtrisés puis dans un second temps les zones vulnérables.

- **Domaines maîtrisés**

A travers cette étude, nous constatons que sur les 15 facteurs de sécurité étudiés, 8 facteurs sont à un niveau acceptable. Il s'agit du contrôle de l'accès, la sécurité incendie, les dégâts des eaux, la fiabilité de fonctionnement, le suivi de l'exploitation, la protection des données, le plan informatique, les sauvegardes.
Le plan de sauvegarde a le niveau de sécurité le plus élevé et tourne autour de 3,5. Cela traduit les mesures prises par la banque pour reconstituer son activité en cas de sinistre informatique. En effet, la possibilité de redémarrer rapidement les applications est une garantie très appréciable et Nous avons ensuite le suivi de l'exploitation et le contrôle de

l'accès (niveau respectivement égal à 3,3 et 3,2) qui garantissent en temps réel, la détection de toutes les intrusions illicites dans le système informatique. La protection des données dont le niveau se situe à 3,1 est également assurée eu égard au caractère stratégique des informations et des données que la banque gère. Ces facteurs mis en place permettent à la banque de se prémunir contre les accidents et malveillance physique, l'attaque logique du réseau et des composants, le détournement de biens.

En outre, nous avons la sécurité incendie tout comme la fiabilité du fonctionnement et les dégâts des eaux qui se trouvent à un niveau de 3. La banque a axé sa sécurité incendie dans la salle contenant le serveur ; cette zone est plus sensible que tous les autres parties de son exploitation. L'assurance contractée en matière de risques d'incendie et de dégâts des eaux renforce le dispositif de sécurité en place. Concernant le fonctionnement du système, son niveau est acceptable dans la mesure où le taux d'indisponibilité tourne autour de 2h par mois.

- **Domaines vulnérables ou à améliorer**

La rosace MARION montre que le niveau de 7 facteurs (l'organisation générale, la réglementation et l'audit, les facteurs socio-économiques, l'environnement de base, les consignes de sécurité physique, la micro - informatique et la maintenance) est inférieur à 3. Parmi ces facteurs énumérés, ce sont les consignes de sécurité qui sont dans une zone critique (1,3). L'absence de consigne de sécurité constitue un risque pour la banque car elle ne respecte pas les dispositions générales de sécurité des personnes au sein d'une entreprise. Chaque employé doit recevoir une formation adéquate et des test doivent avoir lieu au minimum deux fois par an. Ces consignes ont pour objet de garantir en permanence la confidentialité, l'intégrité et la disponibilité du système d'information.

Outre ce facteur, les autres énumérées se trouve à niveau relativement acceptable. Le renforcement des parades mis en œuvre au niveau de ces facteurs permettra d'atteindre le niveau jugé acceptable.

La prévention des risques se fait d'abord par les moyens techniques adaptés (réductions des accidents, détection des erreurs) mais aussi par le maintien de la qualité de l'environnement professionnel, gage de bonne conduite et d'épanouissement. L'instauration de moyens de dissuasion à travers le salaire justifié et la possibilité de promotion permet d'éviter les actes malveillants. La sécurité des micro-ordinateurs conjuguée à leur maintenance (niveau respectivement égal à 2,7 et à 2,5) si elles sont assurées, permettront de répondre efficacement au besoin de productivité de la banque.

Chapitre III : RECOMMANDATIONS ET PERSPECTIVES DE MISE EN ŒUVRE

Ce chapitre a pour objectif de présenter les recommandations consécutives à l'analyse des faiblesses énumérées. En effet, les recommandations faites par l'auditeur sont des propositions d'amélioration du système. La responsabilité de la mise en œuvre relève du management.

1. Les recommandations

1.1 Les facteurs socio-économiques

La nécessité d'aborder le problème de sécurité, de manière globale, nécessite l'implication, et la sensibilisation de tous les niveaux de l'entreprise, de la direction générale au simple employé voir éventuellement du client. La structure des responsabilités de chaque intervenant doit être établi. Les contrôles permanents sont un moyen de prévenir d'éventuels problèmes, et le cas échéant d'avoir une meilleure réactivité. Ces contrôles doivent être réalisés dans des cadres bien définis. Pour cela il est important de disposer d'une bonne réglementation. Les documents réglementaires sont là pour décrire les étapes des contrôles et des procédures effectuées au sein de l'entreprise. Pour vérifier l'application de ces règles, l'entreprise met en place des audits.

1.2 Sécurité logique

Afin de réduire les risques liés au virus informatique à un niveau acceptable, il convient d'instaurer de prudentes politiques et procédures de gestion conjointement aux mesures techniques de protection (logiciel antivirus).

- Sensibiliser le personnel sur les symptômes d'une attaque de virus. Par exemple, les données sont incohérentes ou les messages d'erreurs inhabituels apparaissent fréquemment à l'écran d'ordinateurs.

- Sensibiliser les utilisateurs et les rendre conscients et responsables de la sécurité de leur poste de travail.
- Décourager le partage des disquettes mieux interdire l'utilisation des disquettes. Cette mesure pourra être effective en désactivant les lecteurs de disquettes et en formant davantage le personnel à l'utilisation du « voisinage réseau » ou la messagerie électronique.
- Une gestion permanente des incidents matériels et logiciels permet de situer le niveau de fonctionnement et de satisfaction des utilisateurs.
- La mise à jour des antivirus devra être assurée régulièrement afin d'actualiser la définition des nouveaux virus.
- Le matériel, et les logiciels de base doivent être maintenus régulièrement afin de garantir la fiabilité et l'optimisation du système informatique. surveiller la saisie et le transfert de données, afin de garantir l'intégrité des données.

1.3 Embauche d'un Auditeur Informaticien

Au sein du Département Audit Interne, l'embauche d'un auditeur informaticien est inéluctable. Cette fonction doit être confiée de préférence à un informaticien formé aux techniques de l'audit. En effet, étant donné que tout le système d'exploitation de la banque est informatisé, il est nécessaire de donner l'assurance au management que le système informatique répond aux objectifs de sécurité (confidentialité, intégrité, disponibilité, traçabilité). Ainsi pour atteindre ces objectifs, au-delà des missions d'audit de conformité menées par le département audit, l'auditeur informaticien assurera des missions d'audit d'efficacité du système informatique. L'audit d'efficacité permettra d'apprécier :

- L'adéquation des logiciels aux besoins des utilisateurs
- La performance technique des machines

Il devra également mettre en place des procédures de contrôle de toutes les activités du département informatique.

1.4 Mise en place des consignes de sécurité physique

Les consignes de sécurité doivent impérativement être mis en place afin de répondre aux besoins de sécurité des employés. Elles doivent être affichées, précises, à jour, testées et doivent permettre de mettre en œuvre les premières mesures d'urgences. Toutes ces consignes doivent l'objet de concertation, d'information et de formation des employés.

1.5 **Mise en place d'un système de contrôle d'accès automatique à la salle machine**

Nous pensons qu'il est nécessaire de disposer un système de contrôle d'accès en entrée et sortie par lecteur de badges magnétiques muni de code avec bouton d'ouverture d'urgence. Dans ce système, l'entrée ne sera permise qu'aux personnes autorisées aux heures et endroits choisis. Le système gérera la liste des personnes possédant le droit d'accès au site. De ce fait, le contrôle de « qui a accès ?», «où il a accès ? » et « quand il a accès ? » sera facilement maîtrisé. Ce dispositif permettra de canaliser tous les flux d'entrée dans cette salle.

1.6 Acquisition d'un nouveau serveur

L'acquisition d'un nouveau serveur de capacité plus grande permettra de garantir la rapidité des services offerts aux clients et aux utilisateurs.

1.7 Mise à jour de la politique de sécurité de la banque

La politique de sécurité qui sert à définir des mesures de prévention, de récupération, de détection et de gestion des incidents devrait être mise jour pour tenir compte des risques actuels et futurs auxquels la banque est exposée.

2. Les perspectives de mise en œuvre

2.1 Sécurité logique

La mise en œuvre de cette recommandation passe par la création d'une structure d'accueil, d'assistance et de formation, qui va réaliser un guide d'utilisation des équipements informatiques afin d'éviter les manipulations hasardeuses. Cette structure sera animée par les informaticiens et les auditeurs en collaboration avec le comité de sécurité de la banque. Elle entreprendra des rencontres avec le personnel afin qu'il adhère à la politique de l'entreprise, à l'organisation mise en place et au respect des moyens mis à sa disposition.

Cette structure se chargera également de la mise à jour régulière antivirus. Cette démarche doit être l'émanation de la Direction Générale et reposer sur une réglementation.

2.2 La création d'une responsabilité Audit Informatique

L'embauche d'un Auditeur Informatique doit être motivée par le Directeur de l'Audit Interne même si elle relève de la direction générale. Son recrutement devrait être basé sur sa compétence, sa moralité. Etant donné que ECOBANK est dans une phase de renforcement de son personnel, il est nécessaire de le faire actuellement.

2.3 Mise en place des consignes de sécurité physique

La mise en œuvre de cette recommandation doit relever du comité de sécurité en accord avec la direction générale. Elle a d'ailleurs été prise en compte dans le budget 2003.

2.4 Mise en place d'un système de contrôle d'accès automatique à la salle machine

Le Département de l'Audit en accord avec le comité de sécurité a commandité une étude visant à contrôler l'accès de façon automatique dans toute la banque y compris les

agences. Cette disposition prend en compte l'accès à la salle machine. Le début des travaux devrait commencer en mars 2003.

2.5 Acquisition d'un nouveau serveur

L'acquisition du nouveau serveur a été budgétisée. Sa mise en œuvre ne saurait tarder.

2.6 Mise à jour de la politique de sécurité de la banque

La mise à jour a été faite mais la direction de l'informatique attend la validation de la direction générale et du département Audit.

CONCLUSION GENERALE

Au terme de notre étude, il est important de souligner que les risques qui pèsent sur le système informatique des banques plus spécifiquement de ECOBANK-COTE D'IVOIRE sont réels et doivent être en compte dans l'évaluation globale des risques de la profession. L'évaluation du niveau de sécurité globale de ECI montre que le niveau est relativement bon (3,01) même si certains facteurs sont à améliorer (consignes de sécurité, maintenance, sécurité de la micro-informatique).

La maîtrise des risques informatiques passe par sa gestion efficace pour la bonne marche de la banque, en raison :

- de la dépendance croissante de l'information et des systèmes qui la traite ;
- du montant des investissements actuels et futurs, affectés à la mise en place et à l'évolution de la technologie ;
- de la capacité des nouvelles technologies à modifier profondément les organisations et les pratiques professionnelles pour créer de nouvelles opportunités.

Dans un monde où la concurrence est forte et les changements rapides, les dirigeants attendent beaucoup de leur informatique. Ils demandent plus de qualité, plus de fonctionnalités, des délais de réalisation plus courts et des niveaux de services plus élevés. Le système informatique constitue ainsi un facteur essentiel d'accroissement de la compétitivité et est porteur de bénéfices non négligeables, qui vont de l'efficacité des processus à des avantages concurrentiels majeurs.

Cependant, il recèle des dangers qui peuvent affecter la confidentialité, la fiabilité, l'intégrité et la disponibilité des données et informations de la banque voire compromettre la survie de la banque. L'enjeu de ces menaces informatiques est tellement important qu'il

convient de disposer d'outils de sécurité et un dispositif de contrôle pour évaluer régulièrement son efficacité.

De façon générale, la maîtrise des risques qui pèsent sur le système informatique est obtenue grâce à du personnel de qualité, par des protections physiques (contrôle de l'accès), des protections logiques (antivirus installé et mis à jour, pare-feu), par la mise en place d'un plan de secours (contingency plan) et de sécurité qui sera périodiquement mis à jour. Penser que la sécurité est totalement assurée par des dispositifs matériels et logiciels est une utopie dangereuse. Sans réflexion organisationnelle, sans sensibilisation et formation du personnel, elle risque de ne constituer qu'un investissement décevant. Les mesures techniques de sécurité devront être couplées d'un bon dispositif de contrôle interne.

BIBLIOGRAPHIE

1. ALTER S. (1996), « Information Systems : a Management Perspective » Benjamin Cummings Publishing Company, 2ème édition
2. ANAGO Damien (2000), « Adéquation entre le contrôle interne et les exigences de la commission bancaire de l'UEMOA : cas de la banque prospérité »
3. ANGOT Hugues & FISCHER C. (1994) « Audit Comptable- Audit Informatique », 2ème édition
4. BOUDINOT & FRABOT J.C (1984) « Techniques et pratiques bancaires » Ed. Sirey
5. COOPERS - LYBRAND & IFACI (2000), « La nouvelle pratique du contrôle interne » Editions d'organisation
6. BARLEY M. & DIONGUE Y. (1985) «Control & Administration Policies (CAP) Manual» de ECOBANK
7. Encyclopédie informatique, 2001
8. FAIVRE Claude & LOREAU Yvon -Michel (1993), « Audit de la micro-informatique » Ed. Publi-Union
9. IFACI (1993) « Audit et contrôle des systèmes d'informations » module 3 : Gestion des ressources informatiques
10. IFACI (1993) « Audit et contrôle des systèmes d'informations » module 2 : Les outils informatiques de l'audit
11. IFACI (1993) « Audit et contrôle des systèmes d'informations » module 8 : Sécurité
12. JENKINS Brian et PINKNEY Anthony « Audit des systèmes et des comptes gérés sur informatique » Ed. Publi-Union
13. JOUAS J.P ET HARARI Albert (1999) « Le Risque Informatique », Ed. SSI
14. José BOUANICHE (1999), Article sur « COBIT, référentiel de gouvernance de l'informatique », revue de l'AFAI, N°53
15. KOBIANE Marie Paule « La pratique du contrôle interne dans les établissements publics communaux pour le développement : cas de GAMA » ,2001.
16. KONAN KONAN Thomas (2002), « Evaluation du contrôle interne dans le cadre d'un audit légal en milieu informatisé : le cas de la SICOGI »
17. MADERS Henri – Pierre (1994), « Audit opérationnel dans les banques » Editions d'organisation

18. MAGNIER J.P (1995) « Logiciel d'aide à la gestion de la qualité et sécurité des systèmes d'information : les bases théoriques », document de recherche CREGO
19. MOINE Camille (2000), « Informatique appliquée à la gestion 1ère et 2ème année » Editions FOUCHER
20. Patrick BRUGUIER, Alain DEQUIER, J.R FANGET et al, (1996) « Livre blanc sur la sécurité des systèmes d'information » COMMISSION BANCAIRE, 2nde édition
21. REIX Robert (2000) « Systèmes d'information et management des organisations » Editions VUIBERT
22. RENARD Jacques (2000), « Théorie et pratique de l'audit interne » Les éditions d'organisations
23. ROUACH Michel & NAULLEAU Gérard (1998) « Contrôle de gestion bancaire et financier » 3ème édition
24. SARR Ababacar, « cours d'audit informatique », 2002
25. SIRIGUET J.L & KOESSLER Lydia (1998), « Le contrôle comptable bancaire : un dispositif de maîtrise des risques : Normes, Techniques et mise en œuvre »
26. Thomas Martin « Article sur la sécurité des systèmes informatiques », Revue AFAI n°61 de 2000.
27. THORIN Marc (1991), « L'audit informatique : Méthodes, règles, normes » 3ème édition
28. VALLABHANENI Rao S. (2000), « Information Technology and systems auditing », 2ème edition
29. www.bceao.int
30. www.bis.org
31. www.clusif.asso.fr
32. www.cnrs.fr
33. www.commentcamarche.net
34. www.ecobank.com
35. www.ifaci.com
36. www.institut.capgemini.fr
37. www.lynx-technologies.com
38. www.securite.temlog.com

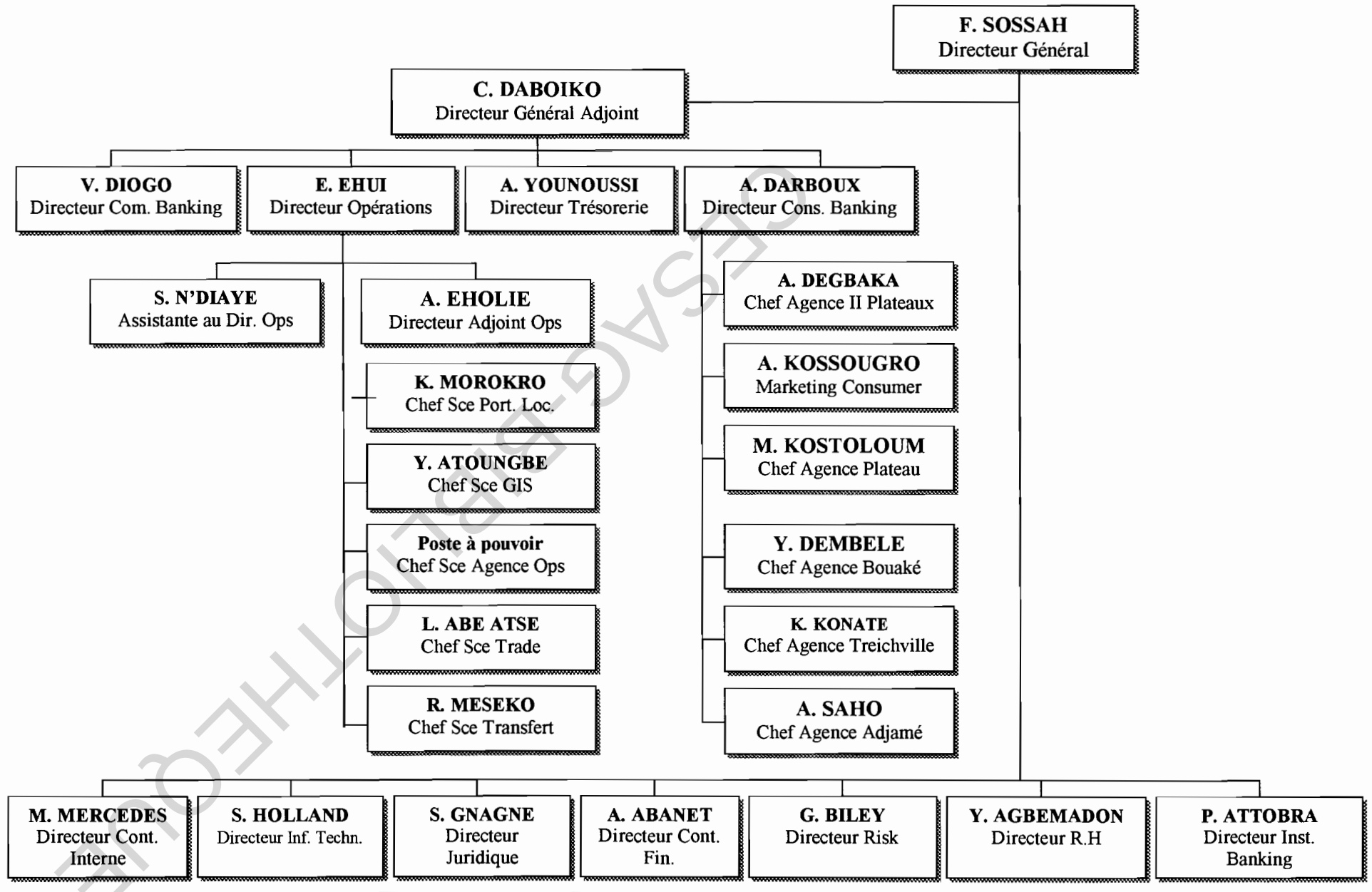
ANNEXES

***Annexe 1**: Organigramme de Ecobank Côte d'Ivoire*

***Annexe 2**: Questionnaire de contrôle interne*

***Annexe 3**: Tableau de pondération*

ORGANIGRAMME DE LA DIRECTION GENERALE AU 10/08/02



Annexe 1

QUESTIONNAIRE DE CONTROLE INTERNE	REPONSES			OBSERVATIONS
	OUI	NON	NA	
Appréciation générale de la sécurité de la banque				
1. Avez – vous souvent des pannes de votre système informatique ?				
2. Si oui, en moyenne combien de fois par mois ?				
3. Des actions correctives ont – elles été prises dans ce sens ?				
4. Avez – vous provisionné un montant pour faire face à un sinistre ?				
5. Connaissez – vous des méthodes d'appréciation et d'évaluation des risques informatiques (MARION, MEHARI,…)?				
6. Quel type d'assurances avez – vous souscrit ?				
7. Avez – vous subi des vols de matériels au cours des trois dernières années ?				
Organisation générale				
8. Existe t-il un organigramme hiérarchique et fonctionnel de l'entreprise, mis à jour régulièrement et proposant une définition des fonctions précisant les attributions – et les restrictions de responsabilité – pour chaque poste ayant une responsabilité décisionnelle ?				
9. Existe t-il un Comité de sécurité permanent chargé d'étudier tous les problèmes liés à la sécurité, se réunissant périodiquement et chaque réunion donnant lieu à un compte rendu écrit ?				
10. Y a-t-il un suivi et contrôle des recommandations prescrites par le rapport précédemment cité ?				
11. Y a-t-il eu une étude sur la vulnérabilité de la banque face à différents types de risques physiques ou non –pas nécessairement informatiques ?				
12. Existe – t – il une fonction sécurité au sein de la banque disposant d'un poste spécifique sur l'organigramme ?				
Contrôles permanents				
13. La mise en place des contrôle utilisateurs fait t-elle l'objet de procédures écrites ?				
14. A-t-on effectué une classification objectives –selon les critères Disponibilité, Intégrité, Confidentialité, Preuve- des informations en fonction des impacts –risque maximum- qu'un sinistre touchant ces informations aurait sur l'entreprise ?				

Annexe 2

QUESTIONNAIRE DE CONTROLE INTERNE	REPONSES			OBSERVATIONS
	OUI	NON	NA	
15. Y a-t-il une analyse des comptes comptables sensibles – distincte de celle des Commissaires aux comptes- au moins deux fois par an, les résultats étant consignés par écrit ?				
La réglementation de l'Audit				
16. Le département Audit a – t – il les compétences requises pour exercer le contrôle du département informatique ?				
17. Existe-t-il un règlement écrit précisant les responsabilités des personnes et la procédure de signature selon le type de document traité ?				
18. Tout document comportant des information stratégiques est-il accompagné à la saisie de pièces justificatives signées par les personnes accrédités ?				
19. Y a-t-il un audit général (externe ou interne) annuel consacré au moins le tiers du temps au contrôle de l'informatique ?				
Les facteurs socio-économiques				
20. A-t-on le sentiment que le climat social est correct et qu'il n'y a pas à redouter d'action bloquante pour l'exploitation informatique ou d'action interne malveillante ?				
21. A-t-on formalisé un code d'éthique ou de déontologie interne et sensibilise –t – on le personnel sur cette base ?				
Les principes généraux de la sécurité				
22. Y a – t – il des études contrôlées périodiquement par un organisme spécialisé, sur les dangers présentés par des facteurs extérieurs sur les locaux informatiques avec un suivi des recommandations prescrites ?				
23. Dispose – t – on d'un système opérationnel, cohérent et complet, de contrôle des accès et de détection des intrusions à la périphérie de tous les bâtiments renfermant des locaux informatiques relié à un poste permanent de surveillance ?				
24. Y a – t – il des études, contrôlées périodiquement par un organisme spécialisé, sur les dangers présentés par des facteurs internes au bâtiment renfermant les locaux informatiques ?				

Annexe 2

QUESTIONNAIRE DE CONTROLE INTERNE	REPONSES			OBSERVATIONS
	OUI	NON	NA	
Les consignes de sécurité physique				
25. Des directives concernant l'usage des codes secrets, codes confidentielles ou mots de passe dans le SI ont – elles été diffusées à l'ensemble du personnel ?				
26. Toutes les consignes de sécurité générale sont-elles correctement affichées et ont-elles fait l'objet de concertation, d'information et de formation ; sont – elles testées périodiquement ?				
Détection automatique salles informatiques				
27. Existe – t – il une installation de détection automatique d'incendie complète pour les salles ordinateurs, composée d'au moins 2 types de détecteurs et ayant fait l'objet d'une déclaration de conformité ?				
28. Existe – t – il des extincteurs installées au sein de la banque ?				
29. Les salles ordinateurs sont – elles protégées par une installation d'extinction automatique d'ambiance fonctionnant en permanence (sans débrayage manuel) ?				
Fiabilité de fonctionnement des matériels informatiques				
30. Y a – t – il une redondance réelle locale des unités centrales des ordinateurs et des organes stratégiques (contrôleurs, frontaux, etc.) qui repose sur un plan de basculement écrit et testé périodiquement ?				
31. Y a – t – il des procédures de contrôles de tous les rapports d'activités ?				
Plan de secours				
32. Existe – t – il un plan de secours reprenant l'exploitation éventuellement en mode dégradé et / ou éclaté ainsi que des documents permettant la mise en œuvre rapide des procédures de sauvetage ?				
33. Le plan de secours est – il remis à jour et sauvegardé périodiquement ?				
34. La solution de secours est – elle complètement testée au moins 2 fois par an ?				
35. Y a – t – il une identification et une authentification pour chaque utilisateur (mot de passe, clé ou carte personnelle) ?				

Annexe 2

QUESTIONNAIRE DE CONTROLE INTERNE	REPONSES			OBSERVATIONS
	OUI	NON	NA	
36. Y a – t – il une journalisation et un suivi quotidien des tentatives infructueuses de connexions ?				
37. Existe – t – il une solution de back-up sur un site de secours en dehors des locaux de la banque ?				
Dégâts des eaux				
38. Y a – t – il des dispositions prises face aux dégâts des eaux ?				
Micro-informatique				
39. La direction de l'informatique dispose – t – elle des moyens de détection d'intrusion de virus dans le système informatique ?				
40. Les stations de travail sont – elles dépourvues de lecteurs de disquettes (ou l'accès en est – il physiquement interdit ?				
41. Dispose – t – on de procédures et de moyens de prévention, de protection et de détection de sabotages immatériels (bombes logiques, virus,…) ?				
42. Existe – t – il une sensibilisation et une information de l'ensemble des utilisateurs aux problèmes de sécurité et en particulier a – t – on réalisé un guide de sécurité micro ?				
43. Existe – t – il un pare-feu installé sur le réseau informatique ?				
44. Existe – t – il un antivirus régulièrement mis à jour sur les postes de travail ?				
Maintenance				
45. Dispose – t – on d'une « hot-line » pour signaler ses problèmes ?				
46. Les interventions sont – elles rapides et efficaces ?				
Sauvegardes et archivages				
47. Existe – t – il une procédure de sauvegarde périodique des données ?				
48. Les disquettes et CD-ROM originales des logiciels ainsi que les contrats de licence et la documentation sont – ils répertoriés et stockés dans une armoire de sécurité ?				

QUESTIONNAIRE DE CONTROLE INTERNE	REPONSES			OBSERVATIONS
	OUI	NON	NA	
Le contrôle d'accès				
49. Y a – t – il un système automatique et complet de contrôle d'accès systématique aux salles contenant les ordinateurs ?				
50. Y a – t – il une analyse et un outil de suivi et de contrôle (tableau de bord, trace d'audit) permettant de mémoriser et de suivre les accès aux ressources ?				
51. le système de contrôle d'accès prend – il en compte tous les accès locaux ou à distance sans aucune exception ?				
52. Y a – t – il une identification et une authentification pour chaque utilisateur (mot de passe, carte professionnelle) ?				
La protection des données				
53. Existe – t – il un administrateur des bases de données responsable de la mise en place, des modifications et la surveillance de la structure des bases ?				
54. Utilise – t – on des techniques de chiffrement pour le stockage des fichiers et des archivages des données stratégiques ?				
55. Toutes les mises – à – jour sont – elles journalisées avec des procédures spécifiques de sécurité pour la conservation des supports et la restauration ?				
Le suivi de l'exploitation				
56. Dispose – t – on de procédures et de moyens de prévention, de protection et de détection de sabotages immatériels (bombes logiques, virus, …) ?				
57. Y a – t – il des procédures de contrôle de tous les rapport d'activités ?				
58. Y a – t – il une journalisation et un suivi quotidien des tentatives infructueuses de connexions ?				
Fiabilité de fonctionnement				
59. Existe – t – il un groupe électrogène et un système de régulation de l'alimentation électrique ?				

Tableau de pondération

Noms des facteurs	Coefficient de pondération
Organisation générale	3,1
Réglementation et audit	1,5
Facteurs socio-économiques	2
Environnement de base	1
Contrôle des accès	4,5
Consignes	1
Sécurité incendie	1
Dégâts des eaux	1
Fiabilité de fonctionnement	2
Suivi de l'exploitation	3
Micro-informatique	1
Maintenance	1
Plan informatique	1
Protection des données	1
Sauvegardes et archivages	8

Annexe 3