Centre Africain d'Etudes Supérieures en Gestion

CESAG BF-CCA
Banque, Finance, Comptabilité, Contrôle & Audit

Master Professionnel en Audit et Contrôle de Gestion (MPACG)

Promotion 8
(2013-2015)

Mémoire de fin d'étude

THEME :

CONTRIBUTION DE L'AUDIT INTERNE A LA MAITRISE DES RISQUES LIES AU SYSTEME D'INFORMATION : CAS DE LA BANQUE ATLANTIQUE DU SENEGAL (BAS).

Présenté par :

NGUEMKAP Edwige

Dirigé par :

OUSMANE SY Pape Alpha
Directeur d'Audit Interne à la Banque Atlantique du Sénégal et Enseignant associé au CESAG

Octobre 2015

DEDICACE

Je dédie ce travail à :

- mes parents Monsieur et Madame NOUKOUPOUE ;
- mon frère ainé NJOMGANG Rostand.

REMERCIEMENTS

Je rends grâce à DIEU le tout-puissant, pour tout ce qu'il opère dans ma vie et par lui je puis tout, parce qu'il me fortifie.

Mes remerciements vont également à :

- M. BAIDARI, Directeur Général du CESAG ;
- M. YAZI Moussa, Directeur du Département Banque, Finance, Comptabilité, Contrôle et Audit du CESAG pour ses conseils ;
- M. Alpha OUSMANE SY, mon Directeur de mémoire pour ses conseils et le temps consacré pour l'accomplissement de ce travail malgré sa charge de travail ;
- M. NDIAYE Serigne, mon maître de stage pour ses conseils et à tous les auditeurs internes de la Banque Atlantique du Sénégal ;
- l'ensemble du personnel du contrôle permanent et du service informatique de la Banque Atlantique du Sénégal ;
- toute la famille NOUKOUPOUE ;
- M. GUEYE Ibrahima, pour ses conseils et son soutien moral ;
- mes camarades de la 8ème promotion et particulièrement à AMEDJOKPO Jésus-Damien pour tous ses conseils, le temps consacré et son soutien indéfectible, à Aldelon BIVIHOU et à mon groupe de travail les Phoenix ;
- tous ceux dont j'ai préféré taire le nom et qui ont contribué de près ou de loin à ce travail.

SIGLES ET ABREVIATIONS

ABI	Atlantic Bank International
ACP	Autorité de Contrôle Prudentiel
AFG	Atlantic Financial Group
AFAI	Association Française de l'Audit et du conseil Informatique
AMF	Autorité des Marchés Financiers
AMRAE	Association pour le Management des Risques et des Assurances en Entreprise
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
APSAD	Assemblée Plénière des Sociétés d'Assurance Dommage
BAS	Banque Atlantique du Sénégal
BCEAO	Banque Centrale des Etats de l'Afrique de l'Ouest
BCP	Banque Centrale Populaire
CA	Conseil d'Administration
CIGREF	Club Informatique des Grandes Entreprises Françaises
CLUSIF	Club de la Sécurité de l'Information Français.
COBIT	Control Objectives for Information and related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DAI	Direction de l'Audit Interne
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DRH	Direction des Ressources Humaines
DS	Domaine Stratégique
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
EMEA	Europe, Moyen-Orient et Afrique
ERM	Enterprise Risk Management
FSE	Fonds de Soutien à l'Energie
GTAG	Global Technologies Audit Guide
IFACI	Institut Français de l'Audit et du Contrôle Internes
IIA	Institute of Internal Auditors

ISACA	Information Systems Audit and Control Association
IT	Information Technology
KGI	Key Goal Indicators
KPI	Key Performance Indicators
MEHARI	Méthode Harmonisée d'Analyse de Risques
PGI	Progiciel de Gestion Intégré
RM	Risque Manager
RSSI	Responsable de la Sécurité des Systèmes d'Information
SENELEC	Société Nationale d'Electricité du Sénégal
SI	Système d'Information
UMOA	Union Monétaire Ouest Africaine

LISTE DES TABLEAUX ET FIGURES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ANNEXES

TABLE DES MATIERES

INTRODUCTION GENERALE

La banque est l'un des éléments centraux de la vie économique d'un pays. Elle joue le rôle d'intermédiaire entre les agents qui ont un excédent de capacité de financement et ceux qui ont un besoin de financement.

A l'origine, les services bancaires se limitaient à une simple collecte de dépôt et d'octroi de crédits ; désormais, avec la croissance exponentielle de l'environnement économique, cette considération a évolué. D'autres objectifs leur sont assignés et, les banques sont confrontées aux effets de la mondialisation. Elles ont par ailleurs des exigences de qualité, de sécurité, de normalisation et souhaitent améliorer leurs efficacités internes dans le but d'acquérir et de conserver une position concurrentielle.

Par ailleurs, l'évolution de l'environnement technologique des banques avec l'émergence des Progiciels de Gestion Intégrés (PGI) en leur sein, implique désormais l'adoption de nouvelles démarches et la prise en compte de nouveaux risques liés à l'informatisation des systèmes de l'organisation. En effet, la plupart des processus métiers de l'entreprise à l'instar des processus de vente, d'achat et comptable, reposent maintenant sur des systèmes d'information informatisés.

Les systèmes d'information sont devenus l'outil incontournable dans les banques et ceux-ci suivent des cycles technologiques extrêmement rapides. De plus, les risques liés à l'utilisation de ces derniers sont devenus plus nombreux, significatifs et complexes. Par conséquent, une attention particulière doit leur être portée surtout en ce qui concerne l'évaluation, le contrôle et la surveillance de leurs dispositifs de gestion et de maîtrise des risques mis en place afin d'aider la banque à atteindre ses objectifs ; d'où la nécessité de l'audit interne.

L'audit interne est une fonction indépendante dans la banque. Sa valeur ajoutée n'est plus à prouver car elle aide non seulement l'entreprise à atteindre ses objectifs mais contribue aussi à l'accroissement de sa performance financière et économique. Au niveau international, d'après la norme 2120 de l'IIA [1](in IFACI[2], 2011 : 50), « l'audit interne doit évaluer l'efficacité des processus de management des risques et contribuer à leur amélioration ». C'est dire donc que l'audit interne occupe une position primordiale dans le système de management des risques d'une banque.

[1] The Institute of Internal Auditors
[2] Institut Français de l'Audit et du Contrôle Internes

Au niveau sous régional, l'article 2-d de la circulaire 003-2011/CB/UMOA[3] relative à l'organisation du système de contrôle interne des établissements de crédit de l'UMOA stipule que « l'audit interne a pour rôle la surveillance périodique du système de contrôle interne et du dispositif de gestion des risques, avec une évaluation indépendante du respect des politiques et procédures établies et de la conformité aux lois et règlements ». La fonction d'audit interne au sein des banques devrait donc toujours suivre l'évolution de l'environnement économique. En effet, l'émergence des PGI bancaires et l'automatisation poussée des processus de gestion bancaire (back-office et front-office) induisent des changements incessants dans l'univers des risques et ont un impact considérable sur la fonction et les responsabilités de l'auditeur interne. La compréhension des enjeux de l'automatisation et de son impact sur le processus d'audit sont devenus essentiels pour l'efficacité du département d'audit interne.

Toutes les contraintes évoquées plus haut s'appliquent à la Banque Atlantique du Sénégal (BAS), institution financière d'accueil créée en 2006. Filiale du Groupe Atlantique, la banque dispose d'un large réseau d'agences installées sur l'ensemble du territoire sénégalais. De ce fait, elle gère un grand volume d'informations venant de ses multiples agences (VDN, KM 18, etc.) et dont l'intégrité ne doit être altérée au moment de leur compilation. Par conséquent, la nécessité de disposer d'un système d'information fiable et sécurisé reste une préoccupation centrale pour la Banque Atlantique du Sénégal et l'une des difficultés majeures généralement rencontrées est la maîtrise des risques liés à son système d'information, malgré l'utilisation de certains standards de sécurité.

En général, l'utilisation des standards de gestion des risques liés au SI[4] implique de définir et de déployer, un système et une politique de gestion des risques dans un environnement de contrôle bien défini. Aussi, l'efficacité et l'efficience de ces standards sont à analyser systématiquement puisque ceux-ci font non seulement partie du dispositif de contrôle interne, mais leurs installations sont susceptibles de générer des risques spécifiques.

Malheureusement, dans la pratique, il est constaté que la maîtrise des risques liés au système d'information reste le parent pauvre des activités de la fonction audit interne de la BAS malgré la part de responsabilité qui lui incombe dans cette activité au même titre, d'ailleurs, que la maîtrise des autres types de risques.

[3] Union Monétaire Ouest Africaine
[4] Système d'Information

L'analyse de ce problème nous a conduit à déterminer les causes suivantes :

- l'absence d'une politique et d'un cadre normatif efficaces de gestion des risques ;
- le département d'audit interne n'est pas suffisamment outillé pour identifier et évaluer les risques liés au SI, spécifiquement les risques liés à la sécurité logique des systèmes ;
- la méconnaissance du rôle et de la responsabilité des auditeurs internes dans la maîtrise des risques du système d'information au même titre que les autres risques ;
- le faible niveau de collaboration entre les auditeurs internes et les autres acteurs dédiés à la gestion des risques.

Les conséquences de ce problème sont les suivantes :

- non-maîtrise des risques liés au système d'information susceptibles d'impacter de façon négative les opérations de la banque ;
- cartographie des risques sur laquelle se basent les auditeurs internes pour la programmation de leurs activités incomplète (programmes d'audit, contrôles etc.) ;
- incapacité de contrôler de façon approfondie l'efficacité et l'efficience des plans d'action logiques mis en place par le contrôle permanent pour mitiger les risques liés au SI ;
- difficulté à maîtriser l'environnement de contrôle du service informatique.

Après analyse du problème, nous pensons que les mesures correctrices suivantes peuvent être prises :

- développer ou acquérir des capacités en audit des SI, les intégrer dans la fonction audit interne de la banque et inclure des activités de contrôles spécifiques au SI dans le programme d'audit annuel ;
- identifier, formaliser et implémenter des standards et des procédures de gestion des risques et former tous les acteurs à leur utilisation ;
- intégrer la dimension culture du risque lié aux SI dans l'élaboration de la cartographie des risques et sensibiliser la direction, le personnel et les auditeurs internes de façon à favoriser l'émergence de cette culture et d'un cadre normatif de gestion de risque au sein de la banque ;
- mettre en place un environnement adéquat (au sein des structures de gouvernance des SI) afin de contribuer au dialogue entre le service informatique, les directions métiers et le département d'audit interne sur les aspects liés aux risques IT ;

- analyser le niveau de contribution actuel de l'audit interne dans la maîtrise des risques liés au SI afin de proposer des axes d'amélioration.

La dernière solution nous semble être la meilleure pour résoudre le problème soulevé car, elle permettra d'accroître l'implication des auditeurs internes de la banque dans le processus de maîtrise des risques liés au système d'information et, par conséquent renforcera le dispositif de maîtrise des risques de la banque.

Au regard de tout ce qui précède, il nous vient à l'esprit de nous poser la question de savoir ce que l'audit interne pourrait apporter au processus de maîtrise des risques liés au système d'information ?

Cette interrogation principale nous conduit à ces sous questionnements :

- qu'est-ce que l'audit interne ?
- qu'est-ce qu'un système d'information ?
- quels sont les principaux risques liés au système d'information ?
- quels sont les outils de gestion des risques utilisés à la Banque Atlantique du Sénégal ?
- quelle est la relation entre l'audit interne et le service informatique à la Banque Atlantique du Sénégal ?
- quelles sont les forces et les faiblesses de l'implication de l'audit interne dans le processus de maîtrise des risques des systèmes d'information ?

Afin de répondre à toutes ces interrogations et points d'éclaircissement, nous avons formulé notre étude autour du thème suivant : « **Contribution de l'audit interne à la maîtrise des risques liés au système d'information** ».

L'objectif principal de ce travail est d'analyser l'apport de l'audit interne dans le processus de maîtrise des risques liés au système d'information. Ce principal objectif est accompagné par des objectifs spécifiques que sont :

- appréhender la fonction audit interne et sa mission dans l'organisation ;
- présenter le concept de système d'information et ses composantes ;
- présenter les principaux risques liés au système d'information et leurs outils de gestion à la banque atlantique du Sénégal ;

- ressortir les forces et faiblesses de l'implication de l'audit interne dans le processus de maîtrise des risques liés au système d'information ;
- formuler des recommandations au regard des faiblesses relevées.

Compte tenu du champ très vaste du système d'information, nous ne traiterons que les risques liés à la partie informatisée du système d'information à savoir les risques informatiques.

Cette étude revêt un double intérêt. Premièrement, elle permettra d'une part, aux dirigeants de la banque de mieux connaître les responsabilités de l'audit interne dans la maîtrise des risques liés au système d'information, et les actions qu'ils peuvent entreprendre pour aider ceux-ci dans cette tâche; d'autre part, elle permettra aux auditeurs internes d'être plus outillés dans le processus de maîtrise des risques liés au SI.

Deuxièmement, ce travail nous permettra non seulement de mieux approfondir nos connaissances jusque-là théoriques en matière de maîtrise des risques liés au système d'information, mais aussi de découvrir la façon dont les risques sont gérés en pratique.

Notre travail s'articulera autour de deux parties :

- la première partie, consacrée à la revue de la littérature consistera à présenter la gestion des risques liés au système d'information (chapitre 1), l'audit interne et la maîtrise des risques informatiques (chapitre 2) et la méthodologie de recherche (chapitre 3) ;
- la seconde partie portera sur la présentation de la Banque Atlantique du Sénégal (chapitre 4), la description du dispositif de maîtrise des risques informatiques de la Banque Atlantique du Sénégal (chapitre 5) et enfin la présentation et l'analyse de la contribution de l'audit interne à la maîtrise des risques informatiques (chapitre 6).

PREMIERE PARTIE : CADRE THEORIQUE DE LA CONTRIBUTION DE L'AUDIT INTERNE A LA MAITRISE DES RISQUES LIES AU SYSTEME D'INFORMATION

INTRODUCTION DE LA PREMIERE PARTIE

Pendant plusieurs années, dans le milieu bancaire, en matière de gestion et de maîtrise des risques, les auditeurs internes ne se sont intéressés principalement qu'à tout ce qui était risque de crédit, risque de contrepartie ou encore risque de change. De plus, les dispositifs de maîtrise des risques étaient rarement la priorité des décideurs qui, la plupart du temps, attendaient souvent d'être confrontés aux conséquences néfastes d'un incident pour remettre à plat les moyens de protection et débloquer les ressources nécessaires. La gestion des risques liés au système d'information dans les établissements financiers était généralement confiée à des cabinets externes spécialisés en la matière.

De nos jours, cette conception a évolué et les auditeurs internes s'intéressent de plus en plus aux risques informatiques, qu'il s'agisse de leur gestion ou bien de leur maîtrise. De plus, la quasi-totalité des processus d'affaires des banques reposent maintenant sur des systèmes d'information de plus en plus complexes et généralement automatisés.

Dans cette première partie réservée à la revue de la littérature de notre étude, nous présenterons la notion de système d'information, ses composantes, sa fonction, les référentiels de gestion des risques du SI et un aperçu de la méthodologie de gestion des risques du SI. Par la suite, nous présenterons la notion d'audit interne, les éléments constitutifs d'un bon dispositif de maîtrise des risques et l'apport de l'audit interne à la maîtrise des risques informatiques. Nous terminerons par la présentation de notre modèle d'analyse ainsi que les outils de collecte et d'analyse des données retenus.

CHAPITRE 1 : GESTION DES RISQUES LIES AU SYSTEME D'INFORMATION

Les systèmes d'information évoluent rapidement et sont au cœur de toutes les activités de l'organisation. En effet, selon GRAEVE & al. (2001 : 3), « le système d'information peut être considéré comme la moelle épinière de l'entreprise, de même que le système de pilotage en est le cerveau et que le système opérant en est les membres ». Par ailleurs, DEYRIEUX (2003 : 10) rajoute que le système d'information peut être considéré comme la colonne vertébrale de l'organisation.

De nos jours, on observe une grande dépendance entre les organisations et leur système d'information. Ainsi, la quasi-totalité des processus de l'entreprise reposant sur les SI, une attention particulière doit leurs être portée et encore plus en ce qui concerne les risques susceptibles d'enfreindre leur bon fonctionnement.

La suite de ce travail reposera sur la présentation de la notion de système d'information, les principaux risques informatiques, les référentiels de gestion des risques du SI, un aperçu des méthodologies de gestion des risques du SI ainsi que ses principaux acteurs.

1.1. Notion de système d'information

Dans cette section, nous allons définir la notion de système d'information, présenter sa fonction et ses composantes, faire une classification des types de système d'information et terminer par la distinction entre système d'information et système informatique.

1.1.1. Définition d'un système d'information

Plusieurs définitions ont été données au système d'information :

Selon LAUDON & al. (2011 : 18), « un SI se définit comme un ensemble de composantes interreliées qui recueillent (ou récupèrent) de l'information, la traitent, la stockent et la diffusent afin d'aider à la prise de décision, à la coordination et au contrôle au sein d'une organisation ».

Toutefois, précisons que la diffusion de l'information produite ne se limite pas exclusivement à de l'organisation. En effet, elle peut également être faite à l'extérieur de celle-ci dans le cadre de l'entreprise étendue selon PILLOU & al. (2011 : 81).

Complétons alors cette définition avec REIX & al. (2011 : 4) pour qui le SI « est un ensemble organisé de ressources : matériel, logiciel, personnel, données, procédures… permettant d'acquérir, de traiter, de stocker des informations (sous forme de données, textes, images, sons…) dans et entre des organisations ».

Au regard de ces définitions données, force est de constater qu'un SI occupe une place de choix dans l'organisation. Présentons à présent ses fonctions.

1.1.2. La fonction du système d'information dans l'organisation

La production de l'information peut être considérée comme le rôle principal du SI. Pour LAUDON & al. (2011 : 19) et MONACO (2014 : 17), cette production tourne autour de quatre (04) activités principales :

- **l'entrée ou l'acquisition** : cette activité consiste à collecter et à entrer les données brutes dans le système. Ces données peuvent être d'origine externe (fournisseur, client, Etat, marché boursier, etc.), ou interne (Directeur Général, différents chefs de département, etc.) ;
- **le traitement** : il s'agit de la transformation (calcul, comparaison, etc.) des données brutes en informations. Il peut se faire manuellement, c'est-à-dire traité par l'homme lui-même ou automatiquement, c'est-à-dire effectué par des ordinateurs (forme la plus courante) ;
- **le stockage** : le stockage peut être fait sur divers supports. Aujourd'hui, l'information est stockée dans des disques durs, des serveurs, des CD Room, clés USB, etc. ;
- **la sortie ou la diffusion** : c'est la restitution de l'information aux personnes concernées. Elle peut se faire par voie orale, sur support papier ou par support numérique (plus efficace que les autres en termes de rapidité).

1.1.3. Les composantes du système d'information

Le SI est composé de données, matériels, personnes, logiciels et des procédures selon DELMOND & al. (2008 : 112). Le management du système d'information se construit autour de ces éléments. Ainsi, distinguons :

- **les données** : ce sont « des valeurs à l'état brut représentant des événements qui ont lieu dans ou en dehors des organisations » selon LAUDON & al. (2011 : 19). Nous pouvons

donc affirmer qu'une donnée est la matière première du SI. Elle constitue un véritable actif, indispensable au fonctionnement de l'organisation car tout part d'elle ;

- **les personnes** : il ne peut avoir de système d'information sans les personnes d'après REIX & al. (2011 : 4). On peut distinguer deux (02) catégories de personnes à savoir les utilisateurs du système (employés, cadres) et les spécialistes de sa construction (analyste, programmateur, etc.). En allant dans le même sens, pour O'BRIEN (1995 : 19), les personnes peuvent être soient des utilisateurs finaux, soient des informaticiens. Les utilisateurs finaux ou maîtres d'ouvrage sont des personnes qui utilisent le SI ou l'information produite et les informaticiens ou maitres d'œuvres sont quant à eux chargés du déploiement de l'infrastructure technologique en adéquation avec les besoins des utilisateurs ;
- **les matériels** : sont considérés comme matériels, les dispositifs physiques (photocopieurs, scanners, ordinateurs, moyens de communication) plus ou moins techniques qui permettent de recevoir, d'émettre, de manipuler les informations. Par ailleurs, les supports de l'information tels que les papiers, les magnétiques et les optiques sont également inclus selon MONACO (2014 : 18) ;
- **les logiciels et les procédures** : généralement, le SI repose sur l'utilisation des ordinateurs. Pour fonctionner, ces ordinateurs ont besoin de logiciels, c'est-à-dire des programmes enregistrés qui commandent le fonctionnement automatisé des machines. La définition des rôles respectifs de la machine et de l'homme est décrite par des procédures qui constituent la partie dynamique du SI et assurent la coordination entre les différents acteurs dans l'organisation selon REIX & al. (2011 : 5).

1.1.4. Les types de système d'information

Les systèmes d'information varient considérablement d'une organisation à l'autre. Il en résulte que la présentation de la typologie des systèmes d'information diffère selon les auteurs.
Pour SATZINGER & al. (2003 : 8), les organisations réalisent différents types d'activités. Il existe donc beaucoup de types de système d'information dont les plus courants sont :

- le système de traitement transactionnel ;
- le système d'information de gestion ;
- le système d'information pour les cadres ;
- le système d'aide à la décision ;
- le système auxiliaire de communication et de soutien bureautique.

Par contre, l'approche adoptée par DELMOND & al. (2008 : 113) est de présenter les types de systèmes d'information en fonction des usages qui en sont faits. Elle distingue trois (03) types de SI :

- le système d'information opérationnel ;
- le système d'information d'aide à la décision ;
- le système d'information de communication.

De nos jours, les systèmes d'information sont pratiquement tous basés sur du matériel informatique, les logiciels, et bien sûr les nouvelles technologies de l'information et de la communication pour transformer les données en informations et en divers produits informatifs. Cependant, l'étroitesse de la relation entre le SI et le système informatique est source de confusion. La distinction de ces deux (02) concepts fera l'objet du point suivant.

1.1.5. Distinction entre système d'information et système informatique

Ces deux (02) concepts étroitement liés prêtent très souvent à confusion. La définition de l'un est parfois attribuée à l'autre.

Pour DAYAN & al (2004 : 1075) et DEYRIEUX (2003 : 11), le système informatique est le support technique du SI et sa partie croissante. Il comprend : les technologies de l'information, les ordinateurs, les applications, les réseaux et les autres systèmes qui permettent à tous d'accéder à l'information, de l'analyser, de la créer, de l'échanger et de l'utiliser.

En allant dans le même sens, VOLLE (2004 : 11) énonce que le système informatique est « l'ensemble des moyens matériels et logiciels assurant le stockage, le traitement et le transport des données sous forme électronique ». Il est ressort donc que le système informatique est la partie informatisée du SI.

Distinction faite, demandons-nous alors quels sont les risques de cette partie du SI? La réponse à cette question constituera l'objet de la section suivante.

1.2. Risques informatiques

Avant de présenter un essai de panorama de risques informatiques, il est nécessaire de comprendre au préalable ce que l'on entend par risque.

1.2.1. Définition du risque

D'après le document ISO guide 73, le risque est défini comme « l'effet de l'incertitude sur l'atteinte des objectifs ». Cet effet correspond soit à un écart négatif, soit à un écart positif par rapport à l'objectif initialement fixé (CLAUDE, 2012 : 39). En général, l'écart positif correspond à une opportunité.

Par contre, pour l'IFACI (in Renard, 2010 : 155), un risque est défini comme « un ensemble d'aléas susceptibles d'avoir des conséquences négatives sur une entité et dont le contrôle interne et l'audit ont notamment pour mission d'assurer autant que faire se peut la maîtrise ».

Le risque informatique devrait donc être considéré comme le risque dû à l'utilisation, la possession, l'exploitation, l'influence et l'adoption de l'informatique dans une organisation.

Pour que l'on puisse parler de risque, la combinaison de deux (02) éléments est préalablement nécessaire. En effet, il faut d'une part, qu'il y'ait une menace et d'autre part, que l'on soit vulnérable à cette menace.

RISQUE = MENACE * VULNÉRABILITÉ

D'après la norme ISO/CEI 27002 : 2005, la menace est définie comme « la cause potentielle d'un incident indésirable pouvant entraîner des dommages au sein d'un système ou d'un organisme ». La vulnérabilité (encore faille ou brèche) quant à elle est définie comme « la faiblesse d'un bien ou d'un groupe de biens pouvant faire l'objet d'une menace » (CLAUDE, 2012 : 41-42). En effet, le bien dont il est question ici est en fait un actif informationnel.

1.2.2. Les types de risques informatiques

Les risques informatiques peuvent être présentés selon diverses approches (fonctionnelle, par nature, synthétique, etc.). L'approche synthétique ayant l'avantage d'identifier les principaux risques informatiques est à considérer prioritairement dans l'entreprise (DARSA, 2013 : 218), c'est elle que nous adopterons pour la présentation des types de risques informatiques (annexe 1, page 100).

Les risques informatiques peuvent avoir divers sources ou facteurs. Selon la nature de la source du risque, nous distinguons les risques humains, environnementaux et technologiques.

1.2.2.1. Risques humains

Les risques humains sont ceux causés par les hommes. BARTHELEMY (2004 : 87) dans son discours sur les atteintes sur un actif matériel affirme que : l'intrusion, la fraude et la malveillance sont les risques dont la source est une personne ayant la volonté de nuire et dont l'objet du risque est généralement un matériel (endommagement ou vols de bien). Plus précisément, il distingue :

- l'intrusion : il s'agit de l'accès des personnes non autorisées dans locaux ;
- la malveillance : il peut s'agir d'un détournement de mot de passe (un informaticien peut détourner le mot de passe d'un utilisateur à son insu afin de bénéficier de tous les privilèges qui lui sont accordés) ;
- la fraude : la fraude concerne tous les salariés de l'entreprise, seuls ou en collusion avec des complices externes à l'entreprise ;
- vols : il s'agit des détournements d'actifs informatiques ;
- endommagement : il s'agit de la destruction du matériel informatique. Il peut être volontaire (sabotage) en raison de la mauvaise foi ou involontaire (maladresse ou erreur de manipulation).

Complétons ces sources de risques avec CALE & al. (2007 : 57) qui considèrent comme risques de source humaine, les erreurs humaines (erreur de conception, erreur de programmation, erreur de configuration et erreur par négligence).
Rajoutons à cette catégorie, le social engineering (les pirates, hacker, cracker) et le phishing (technique utilisée par les pirates pour se faire passer pour un organisme connu auprès de leur victime).

1.2.2.2. Risques environnementaux

Nous distinguons dans cette catégorie, l'hygrométrie, les changements brusques de température (DELEUZE, 2013 : 299).

Les sinistres et l'électricité sont également des sources de risques dus à l'environnement. En effet, pour BARTHELEMY (2004 : 72), les sources naturelles de risque sont assez diversifiées. Il considère comme étant un sinistre, les inondations, les mouvements de terrains, les raz de marrées, les éruptions volcaniques, les tremblements de terre, les explosions pour ne citer que

ceux-là. En ce qui concerne les risques dus à l'électricité, ils proviennent généralement des surtensions, des sous-tensions et des coupures de courant.

Les concepteurs de matériaux électroniques devraient prendre en compte la menace que peut constituer l'électricité mais aussi la poussière pour les matériaux informatiques lors de leurs conceptions. En général, les appareils électroniques situés à proximité de la mer se détériorent plus rapidement du fait de la brise.

1.2.2.3. Risques technologiques

Ce sont les risques causés par tout ce qui est lié à l'aspect technologie de l'entreprise. Ils peuvent affecter les données, les logiciels mais aussi les informations stockées par l'entreprise. Nous distinguerons dans cette rubrique les malwares, les spams, les atteintes à la disponibilité des services.

1.2.2.3.1. Les malwares

Pour CALE & al. (2007 : 43), « malware » est utilisé pour désigner l'ensemble des programmes malveillants qui peuvent être utilisés par les pirates afin de commettre leurs méfaits. Les principaux malwares sont :

- le virus informatique : similaire à un virus biologique qui se fixe à l'intérieur d'une cellule, le virus informatique est un logiciel qui s'introduit dans les programmes des utilisateurs, se reproduit et contamine le plus grand nombre de leurs fichiers. Les cinq (05) catégories de virus existant sont les virus du secteur d'amorçage ou boot sector, les virus d'application, les virus furtifs, les virus flibustiers et les virus polymorphes ou mutants ;

- vers informatique : contrairement au virus, un vers est un programme autonome qui n'utilise pas de support (vecteur) pour se propager car il se déplace dans les réseaux informatiques grâce à sa capacité de duplication ;

- cheval de Troie : c'est un logiciel qui se présente sous une forme bénigne en apparence (jeux, utilitaire, etc.) mais qui recèle en lui un grand péril pour l'utilisateur qui l'installera sur ma machine. Dès lors que l'utilisateur se servira du logiciel, le logiciel effectuera avec toute la discrétion possible des vols ou destructions de données par exemple et ceci à l'insu de l'utilisateur du logiciel. Il est généralement employé dans les cas de chantage, d'espionnage commercial/industriel, détournement de fond, et de prise

de contrôle à distance, relais spam etc. La bombe logique est un type particulier du cheval de Troie qui s'active à un moment précis et cause par la suite un maximum de dégâts (formatage du disque dur, corruptions des données, etc.) au sein du système dans lequel il a réussi à s'introduire ;

- back door : il s'agit d'une fonctionnalité insérée dans un logiciel ou système d'exploitation par un développeur ou autre logiciel dans le but d'accéder à certaines fonctions sans devoir s'authentifier au préalable ;

- logiciels espions : il s'agit des logiciels utilisés pour voler des données. On distingue les spywares (petits logiciels s'installant à l'insu des utilisateurs), les keylogger (petit programme qui enregistre secrètement les informations tapées au clavier des ordinateurs par les utilisateurs) et l'adware (collecteur d'informations personnelles pour transmettre aux sociétés faisant le marketing en ligne) selon CALE & al. (2007 : 44).

1.2.2.3.2. Les spams

Le spam ou pourriel désigne l'envoi massif de courriers publicitaires dans les boîtes aux lettres électroniques des personnes sans leurs approbations d'après CALE & al. (2007 : 55).

1.2.2.3.3. Les atteintes à la disponibilité des services (déni de service)

Le déni de service est un type d'attaque ayant pour but de rendre indisponible un service ou bien d'en détériorer la qualité afin de l'empêcher de répondre aux demandes légitimes d'après CALE & al. (2007 : 66).

1.3. Gestion des risques informatiques

Afin de mieux cerner cette partie, il convient de présenter au préalable ce que l'on entend par gestion des risques.

1.3.1. Définition de la gestion des risques

La gestion des risques est définie comme un ensemble de moyens, de comportements, de procédures et d'actions adaptés aux caractéristiques de chaque société qui permet aux dirigeants de maintenir les risques à un niveau acceptable pour la société. Cette gestion poursuit principalement quatre (04) objectifs :

- créer et préserver la valeur, les actifs et la réputation de la société ;

- sécuriser la prise de décision et les processus de la société pour favoriser l'atteinte des objectifs ;
- favoriser la cohérence des actions avec les valeurs de la société ;
- mobiliser les collaborateurs de la société autour d'une vision commune des principaux risques et les sensibiliser aux risques inhérents à leur activité selon l'AMF [5](2010 : 6).

Toutefois, l'efficacité de tout dispositif nécessite au préalable la définition d'une bonne politique de gestion des risques car c'est elle qui donne l'impulsion à cette activité et définit les responsabilités des principaux acteurs.

1.3.2. La politique de gestion des risques informatiques

La politique de gestion des risques informatiques est généralement incluse dans la politique de sécurité informatique. Il s'agit d'un document qui présente les buts et les orientations du management.

Une politique de sécurité informatique contient quatre (04) thématiques clés que sont :

- la gestion des risques fondée sur l'évaluation et la réduction des risques ;
- la qualification de l'information fondée sur une classification de l'information destinée à adapter le niveau de protection de celle-ci ;
- la conformité des systèmes avec les politiques et standards de sécurité en vigueur ;
- la sensibilisation à la politique de sécurité SI fondée sur une communication adéquate auprès de chaque employé (en modes « push et pull ») selon le CIGREF (2009 : 120).

La politique de gestion des risques informatiques formule les objectifs du dispositif de gestion des risques en cohérence avec la culture de l'entreprise, le langage commun utilisé, la démarche d'identification, d'analyse et de traitement des risques et le cas échéant, le seuil de tolérance (HERVE, 2014 : 6).

1.3.3. Les stratégies de mitigation des risques informatiques

Les risques informatiques peuvent avoir d'importantes répercussions sur la réalisation, le bon fonctionnement et la rentabilité de l'entreprise. Une fois le risque identifié, il convient de choisir

[5] Autorité des Marchés Financiers

la position ou l'option face à ce risque. En effet, il s'agit des différentes parades ou postures qu'il est possible d'adopter vis-à-vis du risque par rapport au seuil de tolérance fixé par le CA.

L'atténuation (mitigation) des risques est une méthode systématique utilisée par la haute direction pour réduire le risque. L'atténuation des risques peut être atteinte par l'une des options suivantes :

- **acceptation du risque** : il consiste à accepter le risque potentiel et de continuer l'exploitation du système informatique ;
- **évitement** : il s'agit d'éviter le risque informatique en éliminant la cause et/ou la conséquence des risques (par exemple, renoncer à certaines fonctions du système ou arrêter le système lorsque les risques sont identifiés) ;
- **mitigation du risque** : il s'agit de limiter le risque par la mise en œuvre des contrôles qui minimiseront l'impact négatif d'une menace et l'exercice d'une vulnérabilité (par exemple, l'utilisation de soutien, de prévention, de contrôle de détection). Dans certains cas, il s'agira simplement de mettre en œuvre des contrôles pour réduire le risque à un niveau acceptable ;

- **transfert de risque** : il consiste à transférer le risque en utilisant d'autres options pour compenser la perte, tels que l'achat d'assurance, la sous-traitance. Dans la pratique, on observe souvent chez certaines entreprises que pour atténuer le risque de perte de données, elles préfèrent faire appel aux sociétés spécialisées dans le stockage des données. D'autres sociétés font parfois appel aux structures spécialisées dans la production de service internet afin de limiter le risque d'indisponibilité de connexion internet selon NIST (2002 : 27).

Une fois l'option choisie, le gestionnaire du risque informatique procède à son application en gardant de vue le niveau de risque fixé par l'entreprise. Généralement, la mise en application de l'option choisie est suivie de monitoring (contrôle et suivi des contrôles) de la part des instances de contrôle. La présentation des principaux risques informatiques et leurs différentes stratégies de mitigation ayant été faite, présentons les principaux référentiels qui gouvernent cette gestion des risques liés au SI.

1.3.4. Référentiels de gestion des risques du SI

Plusieurs référentiels existent et gouvernent les systèmes d'information.

De façon générale, « un référentiel est une collection de bonnes pratiques sur un sujet donné. Lorsque celui-ci fait l'objet d'une large diffusion et qu'il est reconnu sur le marché on parle alors de standard » (CIGREF, 2009 : 9).

Dans le domaine du SI, un référentiel est un ensemble cohérent et outillé de données du système d'information de l'entreprise, partagé par une communauté d'acteurs et qui possède les cinq (05) caractéristiques suivantes :

- centralité : il doit être reconnu comme la référence sur le sujet qu'il traite ;
- stabilité : ses données ne changent pas beaucoup avec le temps ;
- qualité : les processus associés à un référentiel assure une certaine maîtrise de la fiabilité des données ;
- unité de sens : le sens sémantique de ses données ont une certaine homogénéité ;
- interopérabilité : il est techniquement coordonné avec le système d'information et lui procure un certain nombre de services selon BIZINGRE & al. (2013 : 13).

C'est dire donc que le référentiel joue un rôle centralisateur et octroie à celui qui s'y conforme, une validité reconnue. Il est généralement élaboré par une organisation regroupant un ensemble d'experts. Dans le cadre de notre travail, nous ne présenterons que ceux qui ont une importance particulière dans le processus de gestion/maîtrise des risques informatiques.

1.3.4.1. COSO (Committee of Sponsoring Organizations of the Treadway Commission)

Le COSO publie en 1992 une définition standard du contrôle interne et crée un cadre pour évaluer et améliorer le dispositif de contrôle interne.

Pour atteindre ses objectifs, le COSO 1 a présenté cinq (05) composantes sur lesquelles une organisation peut s'appuyer. Il s'agit :

- de l'environnement de contrôle ;
- d'évaluation des risques ;
- d'activités de contrôle ;
- d'information et communication ;
- du pilotage (PWC & IFACI, 2014 : 38).

En 2004, le COSO 2 ERM (Enterprise Risk Management) a repris les composantes du COSO 1 en les complétant avec le concept de management des risques (définition des objectifs, identification des évènements et réponse aux risques) et ramenant ainsi les composantes à huit (08).

1.3.4.2. COBIT (Control Objectives for Information and related Technology)

Publié en 1996 par l'IT Gouvernance Institute et l'ISACA, le COBIT est une méthodologie d'évaluation des services informatiques au sein de l'organisation. Il propose un ensemble de bonnes pratiques de gouvernance IT.

Le COBIT propose au management un cadre de référence des pratiques de contrôle et de maîtrise de l'informatique, applicable pour évaluer un environnement informatique existant ou en phase d'implémentation. Ses processus concernent les domaines fonctionnels que sont : planification et organisation (domaine 1), acquisition et mise en place (domaine 2), distribution et support (domaine 3), et surveillance et évaluation (domaine 5). Dans son guide de mise en œuvre, le COBIT propose également des outils d'analyse et d'évaluation de risques des environnements informatisés selon DESROCHES & al. (2007 : 219-220).

De plus, cette démarche s'appuie sur un référentiel de processus et sur des indicateurs d'objectifs KGI (Key Goal Indicators) et de performance KPI (Key Performance Indicators) permettant de mettre le processus sous contrôle afin de disposer des données permettant à l'entreprise d'atteindre ses objectifs. Les trente-quatre (34) processus du COBIT permettent de couvrir trois cent dix-huit (318) objectifs selon PILLOU & al. (2011 : 79).

L'utilisation du COBIT permet aux systèmes d'information de l'entreprise :

- de s'aligner sur le métier de l'entreprise ;
- d'apporter un plus aux métiers ;
- de gérer au mieux ses ressources ;
- de gérer les risques de façon efficace (CIGREF, 2009 : 44).

Le COBIT est l'élément de base pour une bonne gouvernance d'activité et institutionnelle de l'entreprise. La mise en œuvre de ses bonnes pratiques crée de la valeur ajoutée.

1.3.5. Aperçu des méthodologies de gestion des risques liés au système d'information

Les instances professionnelles CLUSIF[6], AMRAE[7], APSAD[8] ont développé depuis plusieurs années des méthodes de gestion des risques (reposant sur l'analyse de scénario de type « conséquences-causes-origines ») et qui ont pour but de permettre une planification des besoins et des actions de sécurité. Le tableau ci-dessous présente les différentes méthodes qu'on peut avoir :

Tableau 1: Différentes méthodes de gestion des risques informatiques

Méthode de type « Analyse des risques »	Méthode de type « Approche par les processus »
MARION MELISA MEHARI EBIOS	Norme BS7799 Approche du DSIS Approche de COBIT

Source : DESROCHES & al. (2007 : 209).

Dans le cadre de ce travail, nous ne présenterons que les outils les plus utilisés à savoir MEHARI et EBIOS.

1.3.5.1. MEHARI

MEHARI (Méthode Harmonisée d'Analyse des Risques) est une méthode complète d'évaluation et de management des risques liés à l'information, ses traitements et les ressources mises en œuvre. Elle est conforme aux exigences de la norme ISO/IEC 27005 pour gérer les risques. MEHARI consiste à :

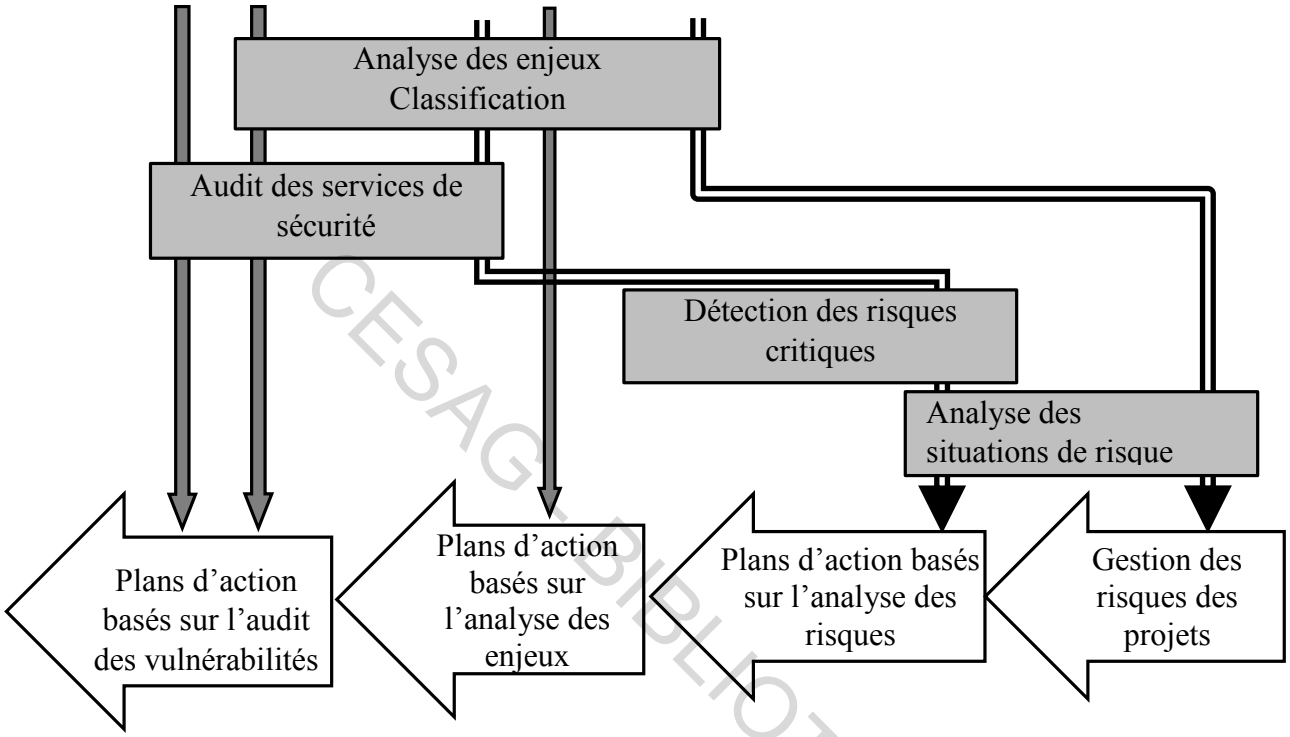
- identifier et évaluer les risques dans le cadre d'une politique de sécurité (Planification) ;
- faire des revues des points de contrôle des vulnérabilités (Contrôle) ;
- fournir des indications précises sur les plans à bâtir à partir des revues effectuées (Déploiement) ;

[6] Club de la Sécurité de l'Information Français
[7] Association pour le Management des Risques et des Assurances en Entreprise
[8] Assemblée Plénière des Sociétés d'Assurance Dommage

- piloter ces plans d'action dans une approche cyclique (Amélioration) (CLUSIF, 2010).

MEHARI apporte une aide efficace pour manager et sécuriser l'information dans toutes sortes d'organisations. Cette méthode se résume à travers la figure ci-dessous.

Figure 1: Etapes de la méthode MEHARI et ses objectifs



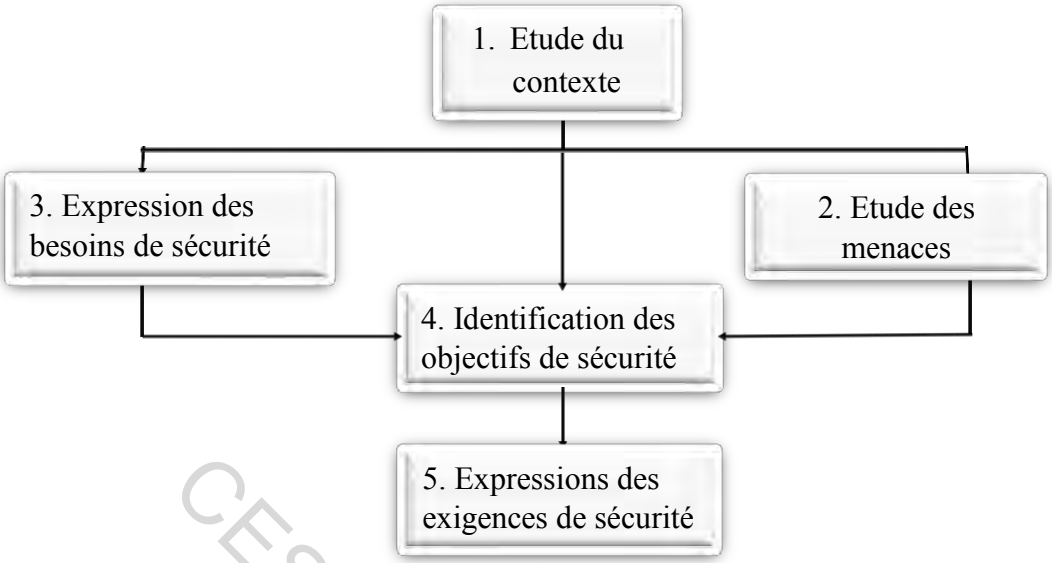
Source : Nous-mêmes à partir de CLUSIF (2010).

1.3.5.2. EBIOS

La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est également une méthode de gestion des risques de la sécurité du SI développée par l'ANSSI et conforme aux normes ISO 27001, 27005 et 31000. Elle permet d'apprécier, de traiter les risques relatifs à la sécurité des SI et de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires, constituant ainsi un outil complet de gestion des risques. C'est une approche plus simple, plus claire. Elle contient des exemples et des conseils offrant la possibilité d'élaborer et d'assurer le suivi d'un plan d'actions relevant de la sécurité des systèmes d'information (ANSSI, 2010).

La démarche générale d'EBIOS comprend cinq (05) étapes résumées à travers le schéma ci-dessous :

Figure 2 : Démarche globale d'EBIOS



Source : ANSSI (2010).

La gestion et la maîtrise des risques informatiques concernent un ensemble d'acteurs dans l'entreprise dont la présentation fera l'objet du point suivant.

1.3.6. Les acteurs de la gestion des risques informatiques

Les principaux acteurs de la gestion des risques informatiques sont : la Direction Générale, le Risk Manager, le RSSI et l'Audit Interne.

1.3.6.1. La Direction Générale

Selon GREUNING & al. (2004 : 33), il est de la responsabilité de l'équipe dirigeante, et de la Direction Exécutive de définir les orientations stratégiques et de les suivre en ce qui concerne la gestion des risques au sein de l'entreprise.

En effet, la Direction Générale fait partager à toute l'entreprise la vision d'une gestion rigoureuse et efficace du risque, donne l'impulsion de celle-ci et crée les conditions de mise en œuvre du processus de management des risques. Il est également de sa responsabilité d'instaurer une bonne culture de gestion des risques au sein de l'entreprise sur le giron de la gouvernance des risques avec pour objectif principal, la maîtrise des risques.

1.3.6.2. Le Risk Manager (RM)

Selon le CLUSIF- AMRAE (2006 : 4), le RM est chargé de concevoir les méthodes et les outils

de gestion des risques (cartographie des risques, etc.), d'élaborer et de mettre en œuvre la politique et le plan d'assurance de l'entreprise, de conseiller les métiers sur les mesures de prévention, de protection, de détection et de réaction face au risque.

1.3.6.3. Le RSSI

Le RSSI est chargé de prévenir les risques dès leur phase de développement, de proposer des plans d'action de réduction et de contrôle des risques, de suivre la mise en place des actions décidées, de rendre compte à la Direction Générale et de communiquer sur la sécurité du SI avec le ou les Directeurs en charge des SI (CLUSIF-AMRAE, 2006 : 4).

1.3.6.4. L'audit interne

Selon GREUNING & al. (2004 : 53), les auditeurs internes ont une contribution très importante à apporter en ce qui concerne le processus de gestion des risques liés au système d'information.

En effet, d'après la norme 2120.A1 de l'IIA (in IFACI, 2013 : 51), « l'audit interne doit évaluer les risques afférents au gouvernement d'entreprise, aux opérations et aux systèmes d'information de l'organisation au regard de :

- l'atteinte des objectifs stratégiques de l'organisation ;
- la fiabilité et l'intégrité des informations financières et opérationnelles ;
- l'efficacité et l'efficience des opérations et des programmes ;
- la protection des actifs ;
- le respect des lois, règlements, règles, procédures et contrats ».

Par ailleurs, une fois le processus de gestion des risques installé au sein de l'entreprise, la fonction d'audit interne est considérée comme un prolongement de la gestion des risques selon GREUNING & al. (2004 : 7).

Ce prolongement du processus de gestion des risques étant la maîtrise des risques, c'est dire donc que l'audit interne joue un rôle dans la maîtrise des risques du système d'information.

CONCLUSION DU PREMIER CHAPITRE

Parvenu au terme de ce chapitre, nous avons présenté la notion de système d'information, ainsi que la différence existant entre celui-ci et le système informatique. Ayant délimité notre travail aux risques informatiques, nous avons présenté les types de risques informatiques, les stratégies de mitigation, et les méthodologies de gestion des risques telles que MEHARI, EBIOS. Le chapitre suivant consistera à présenter l'apport de l'audit interne dans la maîtrise des risques informatiques compte tenu de sa fonction de prolongement du processus de gestion des risques informatiques.

CHAPITRE 2 : AUDIT INTERNE ET MAITRISE DES RISQUES INFORMATIQUES

Pour un manager, la maîtrise des risques vise à être « maître des situations à risques », de telle sorte que les moyens proportionnés aux enjeux, produisent de façon efficace les effets souhaités. De plus, cette maîtrise de risques contribue de façon rationnelle à ce que l'organisation atteigne ses objectifs (DELEUZE, 2013 : 200).

Dans cet ordre d'idées, les actionnaires, les dirigeants et les autorités attendent des auditeurs internes qu'ils contribuent à une bonne maîtrise des risques au sein de leurs entreprises, constituant ainsi la cheville ouvrière du dispositif de maîtrise des risques (HERVE, 2014 : 3).

Avant de présenter l'apport de l'audit interne dans la maîtrise des risques informatiques, il importe au préalable de présenter la notion audit interne.

2.1. Audit interne

Le mot audit vient du latin « audire », c'est-à-dire « écouter ». Le 29 juin 1999, l'IIA a donné une définition officielle de l'audit interne qui, plus tard fut traduite par l'IFACI.

2.1.1. Définition de l'audit interne

D'après la définition faite par l'IIA et traduite en français par l'IFACI, « l'audit interne est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systémique et méthodique, ses processus de management des risques, de contrôle et de gouvernement d'entreprise et en faisant des propositions pour renforcer son efficacité » (BERTIN, 2007 : 20).

De cette définition, il ressort que la pratique de l'audit interne requiert une certaine indépendance de l'auditeur interne vis-à-vis des autres membres de l'entreprise. Il améliore le fonctionnement de l'organisation et aide l'entreprise à atteindre ses objectifs. Afin de mieux comprendre son fonctionnement, présentons son cadre de référence, ses missions et sa démarche.

2.1.2. Cadre de référence pour la pratique professionnelle de l'audit interne

L'audit interne est une fonction normalisée et normée qui se base sur un cadre de référence bien défini afin de fournir à celle-ci un cadre unique d'application. Ce cadre de référence comprend des bonnes pratiques, guides et lignes directrices approuvés par l'IIA. Ainsi, nous distinguons :

2.1.2.1. Normes professionnelles d'audit interne et modalités pratiques d'application

D'après l'IIA (in IFACI, 2013), les normes professionnelles se composent des :

- **normes de qualification** : il s'agit des normes de la série 1000 et relatives aux missions, pouvoirs et responsabilités de l'audit interne ;
- **normes de fonctionnement** : il s'agit des normes de la série 2000 et relatives à la gestion de l'audit interne ;
- **norme de mise en œuvre** : il s'agit des normes de la série 1000 ou 2000, assorties d'une une lettre « A » pour dire assurance « C » pour dire conseil.

Les modalités pratiques d'applications représentent les conseils pratiques visant à faciliter l'application des normes. Contrairement aux normes professionnelles qui ont un caractère obligatoire, celles-ci présentent un caractère facultatif afin de laisser à l'auditeur le soin d'adapter ses pratiques aux réalités de l'organisation et du pays dans lequel il se trouve (Schick 2010 : 29).

2.1.2.2. Déclaration des responsables de l'audit interne

C'est un document écrit et signé par le responsable de l'audit interne et approuvé par la plus haute hiérarchie de l'entreprise. Ce document présente le degré de responsabilité accordé à la structure en charge de l'audit. La déclaration prend aussi en compte l'indépendance de la fonction et des acteurs au sein de l'entreprise.

2.1.2.3. Le code de déontologie

Le code de déontologie de l'IIA comprend les principes applicables à la profession et à la pratique de l'audit interne, ainsi que douze (12) règles de conduite décrivant le comportement attendu des auditeurs internes. Ces principes sont au nombre de quatre (04). En effet, il s'agit de :

- l'intégrité : c'est la base de la confiance accordée aux auditeurs ;
- l'objectivité : il doit exercer en toute impartialité et indépendance ;
- la confidentialité : elle fait référence au respect du secret professionnel ;
- la compétence : il faut disposer de l'expertise suffisante pour l'accomplissement de la mission (IFACI, 2013 : 19).

2.1.3. La charte de l'audit interne

Selon RENARD (2010 : 397), « la charte d'audit interne est le document constitutif de la fonction d'audit interne et destiné à la présenter et à la faire connaitre aux autres acteurs de l'entreprise ». Rajoutons ici que la charte doit être évolutive car l'environnement interne et externe de l'entreprise sont en constante évolution et de nouvelles responsabilités pèsent de plus en plus sur l'auditeur interne.

De plus, une charte d'audit interne doit garantir les conditions d'indépendance des auditeurs vis-à-vis des autres membres de l'entreprise mais aussi protéger les audités contre tout abus de la part des auditeurs internes. Cette charte doit préciser les missions, les objectifs, les responsabilités et les procédures de travail (SCHICK, 2007 : 28).

2.1.4. Les missions et objectifs de l'audit interne

Très souvent, les missions et les objectifs de l'audit interne prêtent à confusion alors qu'il s'agit de deux (02) concepts distincts.

2.1.4.1. Missions de l'audit interne

L'auditeur interne mène principalement deux (02) types de missions : les missions d'assurance et les missions de conseil.

Selon l'IFACI (2013), l'audit interne a pour principales missions de :

- analyser et évaluer les processus de gouvernement d'entreprise, de management d'entreprise et de contrôle ;
- faire des recommandations en vue de leur amélioration ;
- vérifier que les dispositifs mis en place sont en conformité avec les lois et règlements en vigueur ;
- apprécier l'efficacité du processus d'auto-évaluation mis en œuvre par le management ;
- conseiller en matière de management des risques ou d'autres sujets.

Par ailleurs, dans le cadre de sa mission, l'auditeur interne peut être amené à effectuer les audits suivants :

- **audit de conformité** : il consiste à vérifier la bonne application des règles et politiques internes, la conformité aux lois et règlementations en vigueur en faisant une comparaison de ce qui est ou est fait à ce qui devrait être ou devrait être fait ;
- **audit du management** : cet aspect de l'audit s'intéresse au style de gouvernance de la direction ;
- **audit de la stratégie** : il consiste à identifier les risques associés aux objectifs et aux grandes orientations stratégiques définies par l'entreprise et évaluer la cohérence ou la conformité entre ce qui a été décidé et ce qui est ;
- **audit opérationnel** : il s'agit principalement de vérifier le respect des procédures écrites par les opérationnels et est plus tourné vers l'efficacité de l'organisation (RENARD, 2010 : 48-55) et (BERTIN, 2007 : 21).

La fréquence des missions d'audit interne est prévue dans un plan d'audit annuel validé par le Comité d'Audit ou le Conseil d'Administration. Néanmoins, il peut arriver qu'il y ait des missions spéciales non prévues dans le plan d'audit en cas demande expresse du CA, du Comité d'Audit, de la Direction Générale ou en cas de fraude.

L'élaboration d'un plan d'audit sur la base d'une évaluation annuelle de risque serait considérée déficiente si elle ne couvre pas les risques informatiques. En effet, l'audit interne ne devrait pas perdre de vue trois (03) aspects :

- actuellement, la quasi-totalité des dispositifs de contrôle interne clés pour l'organisation repose sur un système informatisé ;
- la compréhension par l'organisation des risques stratégiques induits par les environnements complexes des SI est primordiale ;
- le développement des contrôles généraux des SI et des contrôles applicatifs doit gérer convenablement les risques relatifs aux SI selon le GTAG[9] 11 (IFACI, 2015 : 7-12).

Par ailleurs, la fonction d'audit interne doit :

[9] Global Technologies Audit Guide.

- inclure les systèmes d'information dans son processus de planification annuelle des travaux d'audit ;
- repérer et évaluer les risques SI qu'encourt l'organisation ;
- veiller à disposer d'une expertise suffisante dans les domaines de SI ;
- évaluer les contrôles relatifs à la gouvernance et à la gestion des SI ainsi que les contrôles techniques ;
- affecter les auditeurs présentant un niveau de compétence suffisant dans les SI à chaque mission d'assurance ;
- utiliser à bon escient les techniques d'audit informatisées (IFACI, 2015 : 7-27).

2.1.4.2. Objectifs de l'audit interne

D'après la norme 2120.A1 de l'IIA (in IFACI, 2013 : 51), « l'audit interne doit évaluer les risques afférents au gouvernement d'entreprise, aux opérations et aux systèmes d'information de l'organisation au regard de :

- l'atteinte des objectifs stratégiques de l'organisation ;
- la fiabilité et l'intégrité des informations financières et opérationnelles ;
- l'efficacité et l'efficience des opérations et des programmes ;
- la protection des actifs ;
- le respect des lois, règlements, règles, procédures et contrats ».

Cette norme présente la responsabilité de l'auditeur interne dans l'évaluation des risques des systèmes d'information de l'entreprise. L'audit interne est devenu un acteur capital dans le dispositif de maîtrise des risques, du contrôle interne et de la gouvernance d'entreprise.

2.2. Maîtrise des risques informatiques

La maîtrise des risques informatiques est une nécessité pour atteindre les objectifs de l'entreprise.

Elle s'occupe des aspects humains et organisationnels à mettre en œuvre pour que les activités d'analyse et de gestion des risques fonctionnent correctement. Elle comprend d'une part, une composante « leadership » et mobilisations des équipes et, d'autre part une composante de direction, hiérarchie, reporting, et contrôle. La maîtrise des risques diffère de la gestion des

risques en ce sens que la gestion des risques se préoccupe plus des moyens et des techniques (DELEUZE, 2013 : 199).

Par ailleurs, la mise en place d'un dispositif de maîtrise des risques informatiques se fait au niveau du contrôle interne ; aussi, pour une bonne analyse de celui-ci, présentons d'abord ce que c'est qu'un dispositif de contrôle interne.

2.2.1. Dispositif de contrôle interne

L'aptitude d'une entreprise à atteindre ses objectifs dépend en grande partie de la qualité de son dispositif de contrôle interne.

2.2.1.1. Définition du contrôle interne

Selon le COSO, « 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 l'atteinte des objectifs suivants :

- réalisation et optimisation des opérations ;
- fiabilité des informations financières ;
- conformité aux lois et aux réglementations en vigueur » (BERTIN, 2007 : 57).

D'après cette définition, il est clair que le contrôle interne est un processus et non une fonction. Il couvre l'ensemble des processus de l'entreprise.

2.2.1.2. Les objectifs du contrôle interne

D'après le COSO (in RENARD, 2013 : 126), nous avons quatre (04) objectifs du contrôle interne. Il s'agit de :

- la protection des actifs : elle est relative à la sauvegarde du patrimoine de l'entreprise (actifs de l'entreprise, les hommes et l'image de l'entreprise) ;

- la fiabilité et l'intégrité des informations financières et opérationnelles : la qualité de l'information joue sur l'image de l'entreprise ;

- le respect des lois, règlements et contrats : il concerne les dispositions législatives, règlementaires mais aussi les contrats conclus par l'entreprise ;

- l'efficacité et l'efficience des opérations : ces deux notions rejoignent l'objectif de permanence de l'entreprise.

2.2.2. Dispositif de maîtrise des risques informatiques

Un dispositif de maîtrise des risques pour être et rester efficace doit évoluer au même rythme que les enjeux stratégiques et opérationnels qu'il couvre.

Quelle que soit la nature du risque, un bon dispositif de maîtrise des risques doit contenir un certain nombre d'éléments. Pour DELEUZE (2013 : 200), la maîtrise des risques repose sur trois (03) points :

- la définition des niveaux de risques inacceptables et résiduels ;
- l'organisation, le pilotage, la coordination des parades, des moyens matériels, humains et organisationnels ;
- le contrôle, la mise en œuvre efficace des parades et de leurs évolutions.

Par ailleurs, DARSA (2013 : 249) évoque quatre (04) vecteurs clés pour une bonne maîtrise des risques. En effet, ce sont :

- **Vecteur 1 : la formation et la sensibilisation des équipes**

Chaque salarié, acteur opérationnel de l'organisation doit être sensibilisé aux enjeux d'une maîtrise des risques informatiques et se sentir tout simplement concerné par la démarche. En réalité, ce dont il est question ici, c'est la notion de culture du risque au sein de l'entreprise.

CALE & al. (2007 : 157), rajoutent que l'être humain est généralement le maillon le plus faible de la sécurité des systèmes d'information. Il est donc primordial pour toute bonne maîtrise des risques que les acteurs de l'organisation comprennent exactement quels sont les enjeux de cette démarche.

- **Vecteur 2** : **le traitement effectif des risques entrants**

Chaque dysfonctionnement ou risque entrant doit être collecté, traité, analysé dans ses causes de survenance et faire l'objet de plans de correction, de suivi de traitement effectif de risque et de veille.

- **Vecteur 3** : **la mise en place d'indicateurs et de dispositif de pilotage et de suivi des risques**

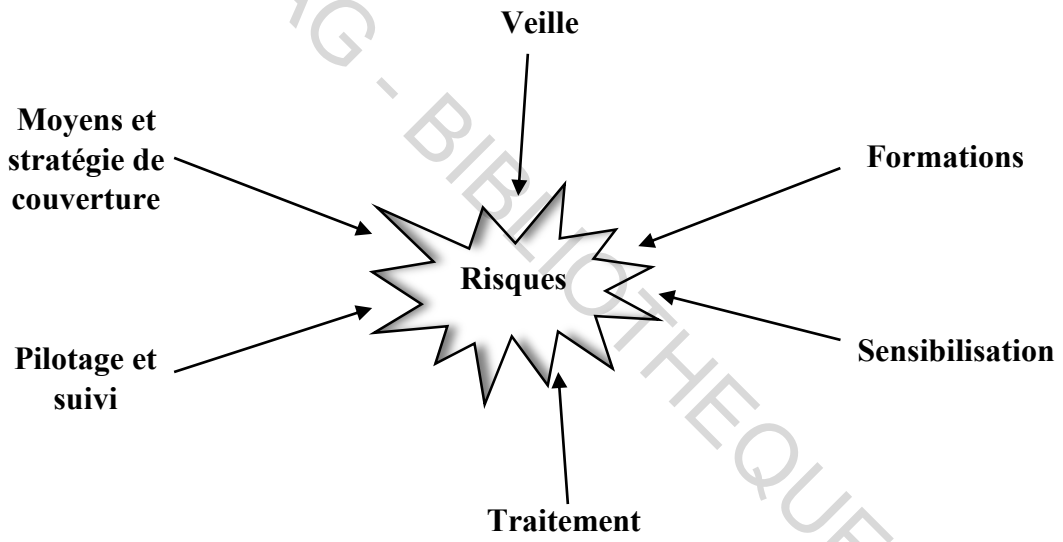
Dans la pratique ce sont principalement des « tableaux de bords » qui font la synthèse des contrôles mis en place et présente l'état d'analyse selon (DELEUZE, 2013: 227).

Dans certaines organisations, la construction de ce tableau est orientée sur le style de Balanced scorecard.

- **Vecteur 4** : **la définition, la mise en œuvre et le maintien opérationnel des dispositifs de gestion de crise et de continuité**

Ils permettent de limiter les impacts sous-jacents les risques en cas de survenance. Enfin « last but not least », la définition, la mise en œuvre et la sélection des stratégies de couvertures appropriées s'imposent.

Figure 3 : Schéma de la maîtrise des risques



Source : DARSA (2013).

2.3. Apport de l'audit interne dans le processus de maîtrise des risques informatiques

Comme évoqué plus haut (voir 2.1.4.1, page 28), l'audit interne mène des activités d'assurance et de conseil pour contribuer à la création de la valeur ajoutée. La réalisation de ces deux (02) missions passe indéniablement par une évaluation du contrôle interne. Précisons que quelle que soit l'activité menée, il y a création de la valeur ajoutée. Néanmoins, nous présenterons la contribution de l'audit interne à travers ses principales missions et nous consacrerons un point à la contribution de l'audit interne à la création de la valeur ajoutée de l'entreprise.

2.3.1. Apport de l'audit interne du point de vue de l'assurance

D'après HERVE (2014 : 13), l'auditeur interne est chargé de donner une assurance aux organes de gouvernance et au CA sur l'efficacité et l'efficience du dispositif de maîtrise des risques. L'activité d'assurance à ce niveau réside dans l'audit de conformité qu'effectue l'auditeur interne dans le cadre de sa mission.

En effet, pour un responsable d'audit interne, il est impératif de bien jauger l'appétence et la tolérance aux risques de l'entreprise. Aussi, il s'assure :

- que l'environnement de contrôle du système d'information en général est aligné sur le seuil de tolérance aux risques informatiques fixés par le CA ;
- que la vision et la stratégie des instances de gouvernance sont bien déclinées au niveau de la politique de gestion des risques ;
- de l'existence d'une culture du risque informatique au sein de l'entreprise ;
- de la conformité du dispositif de maîtrise de risques informatiques avec les lois et réglementations en vigueur (conformité avec Bale II[10]…) ;
- de la conformité du programme de mise en place du dispositif de maîtrise des risques informatiques avec les politiques internes de l'organisation ;
- que les stratégies de mitigation des risques sont bien comprises et appliquées au niveau du dispositif de maîtrise des risques informatiques ;
- que le cadre de contrôle interne des TI permet d'accroitre les performances de l'organisation facilitant ainsi l'atteinte des objectifs de l'organisation GTAG 1(in Thornton & al., 2012 : 13-16).

Le but de l'audit interne à ce niveau est de s'assurer que l'organisation dispose du juste niveau de résistance aux risques informatiques. Par ailleurs, il vérifie que :

- l'environnement de l'entreprise favorise la sensibilisation au risque (informatique) et au contrôle ;
- les objectifs de l'entreprise ont été fixés et compris par tous les acteurs de la gestion des risques ;
- des procédures écrites qui décrivent les activités interdites et les mesures à prendre en cas d'infractions avérées existent ;

[10] Dispositif prudentiel destiné à mieux appréhender les risques bancaires.

- des politiques, des pratiques, procédures et rapports et autres mécanismes sont mis au point pour piloter les activités et protéger les actifs, en particulier ceux des domaines à hauts risques (serveurs, réseaux, etc.) ;
- des canaux de communication donnent à la direction des informations fiables et pertinentes selon IFACI (2013).

Pour GAULTIER-GAILLARD & al. (2014 : 33), dans la mesure où le gestionnaire des risques est un « consultant interne », l'auditeur interne doit s'assurer de la bonne exécution du programme et de son efficacité. L'audit doit consister à faire une comparaison de la réalité avec un ensemble de bonnes pratiques, l'objectif étant de mesurer des écarts entre celles-ci et la réalité, et envisager les actions correctives pour les réduire.

Il s'agira à ce niveau d'analyser la gouvernance institutionnelle car, elle se focalise sur la conformité, le contrôle, et assure la légalité et la responsabilité.

Rajoutons à cette affirmation qu'un écart est exprimé à partir d'un risque c'est-à-dire, s'il y a pas de risque, il y' a pas d'écart selon VINCENT (2010 : 67). C'est dire donc que l'une des contributions de l'auditeur interne dans son audit de conformité ici, réside aussi dans l'identification de nouveaux risques informatiques. En effet, un dispositif de maîtrise de risques informatiques ne couvrant pas l'ensemble des risques informatiques ne peut être efficace.

2.3.2. Apport de l'audit interne du point de vue du conseil

Il s'agit principalement ici des recommandations et informations fournies par l'auditeur interne aux différents métiers notamment au gestionnaire des risques informatiques.

Selon IFACI (2015 : 7-32), l'auditeur interne peut réaliser des activités de conseils dans le but d'aider le management à traiter les nouveaux risques SI (risques informatiques inclus) au fur et à mesure qu'ils émergent. Rajoutons que le traitement de ces nouveaux commence par leur identification.

- **Apport de l'audit interne par identification de nouveaux risques**

Selon BASPT (2004 : 125), « la cartographie des risques est un document permettant de recenser les principaux risques d'une organisation et de les présenter systématiquement sous une forme hiérarchisée pour assurer une démarche globale d'évaluation des risques ».

En effet, c'est la résultante du processus d'identification des risques de l'entreprise.

Pour HERVE (2014 : 17), l'audit interne contribue à la mise à jour de la cartographie des risques. En effet, l'auditeur interne doit contribuer à la détection des risques informatiques qui pourraient échapper au dispositif de contrôle interne. Cela est justifié par la norme 2120.C1 de l'IIA (in IFACI, 2013 : 51) qui stipule : « au cours des missions de conseil, les auditeurs internes doivent couvrir les risques liés aux objectifs de la mission et demeurer vigilants vis-à-vis de l'existence de tout autre risque susceptible d'être significatif ».

Ainsi, à travers son activité d'évaluation du dispositif de contrôle interne, l'auditeur interne évalue la conception et l'installation des contrôles mis en place, ensuite procède à une vérification de leur fonctionnement et enfin effectue la communication de la revue des contrôles assortis d'éventuelles recommandations.

Pour BARRY (2009 : 17), « l'appréciation du système de contrôle interne passe par le découpage de l'entreprise en cycles d'activités et par l'évaluation des procédures mises en place pour atteindre les objectifs de contrôle pour chacun des cycles ». La finalité de l'audit interne ici est de renforcer le contrôle interne sur les différents processus et d'identifier les risques qui auraient échappé au contrôle interne. L'objectif de contrôle à ce niveau dépend de la nature de l'activité ou sous processus.

Le tableau ci-dessous présente une esquisse d'évaluation du contrôle interne des risques informatiques :

Tableau 2 : Exemple d'évaluation du contrôle interne des risques informatiques

Sous processus ou Activités	**Processus COBIT concernés**	**Objectifs de contrôle**	**Commentaires**
Gestion des accès des utilisateurs	DS5[11]	S'assurer que chaque utilisateur est limité au niveau d'accès qui lui a été accordé pour accomplir sa mission.	

[11] Domaine Stratégique

Conformité des systèmes avec la politique de gestion des risques informatique	DS5	S'assurer que tous les systèmes installés sont en cohérences avec les exigences de la politique de gestion des risques informatiques.	
Accès aux programmes et aux données	DS5	S'assurer que l'information critique et confidentielle n'est accessible qu'à ceux qui doivent y accéder.	
Surveillance des accès logiques	DS5	S'assurer que les différents responsables opérationnels participent à cette tâche quotidiennement.	
Sécurité réseaux	DS5	S'assurer que l'intégrité de l'information et de l'infrastructure de traitement est maintenue en continu.	
Gestion des failles de sécurité	DS5	S'assurer que les services et l'infrastructure informatique peuvent résister/se rétablir convenablement en cas de panne due à une erreur, à une attaque délibérée ou à un sinistre.	
Accès aux locaux	DS12	S'assurer que seules les personnes autorisées peuvent entrer dans les locaux.	

Source : Nous-mêmes à partir de MOISAND & al. (2009) et CIGREF (2009).

En effet, l'ensemble des risques informatiques découverts à l'issu de l'évaluation du dispositif de contrôle interne fait l'objet d'un rapport généralement assorti de recommandations. Ce

rapport est pris en compte par le Risk Manager/RSSI pour actualiser la cartographie des risques informatiques et orienter le déploiement de la stratégie de maîtrise des risques informatiques.

- **Audit interne et proposition/vérification des contrôles visant à mitiger les risques informatiques**

Sans un contrôle, la maîtrise des risques informatiques ne peut être assurée. Une attention particulière doit y être portée à travers les différents moyens disponibles : autocontrôle, surveillance, contrôle hiérarchique, vérification (DELEUZE, 2013 : 246).

Les risques informatiques figurant dans la cartographie des risques concernent généralement les activités courantes de l'entreprise. Elle présente les risques bruts et les risques résiduels (risques obtenus après mise en place des mesures de contrôle). Il est nécessaire de procéder à une revue périodique des mesures de contrôle mises en place pour maîtriser les risques informatiques.

D'après la norme 2130 de l'IIA in IFACI (2013 : 52), « l'audit interne doit aider l'organisation à maintenir un dispositif de contrôle approprié en évaluant son efficacité et son efficience et en encourageant son amélioration continue ». Dans la majorité des cas, pour effectuer cette tâche, l'auditeur interne devra effectuer des tests sur ces contrôles dans le but de juger de leur efficacité.

Les tests peuvent aider à déceler un déroulement inhabituel des activités et à éviter d'importants problèmes, dysfonctionnements ou attaques. C'est aussi l'occasion pour l'audit interne de faire des propositions de plans de contrôle pour les risques informatiques non couverts. D'après l'ISACA (2011 : 51), comme outils de tests et de contrôle, les auditeurs peuvent utiliser les questionnaires de contrôle interne, l'interview, les enquêtes, la revue de la documentation (les procédures, politiques de sécurité, etc.), l'observation, les logiciels d'audits spécialisés, les tests de corroborations, les tests de conformité et les tests de cheminement.

Selon HERVE (2014 : 22), le plan de contrôle liste l'ensemble des contrôles qui seront effectués par les trois (03) niveaux de maîtrise des risques informatiques. Ces contrôles sont le plus souvent fixés sur la base des risques survenus au cours de l'exercice précédent.

Il appartient donc à l'auditeur interne d'établir une liste de contrôles à réaliser pour maîtriser les risques informatiques. De plus, en complément des contrôles de routine effectués, il incombe à l'audit interne de procéder au moins une fois par an, à un audit global. Cet audit portera aussi

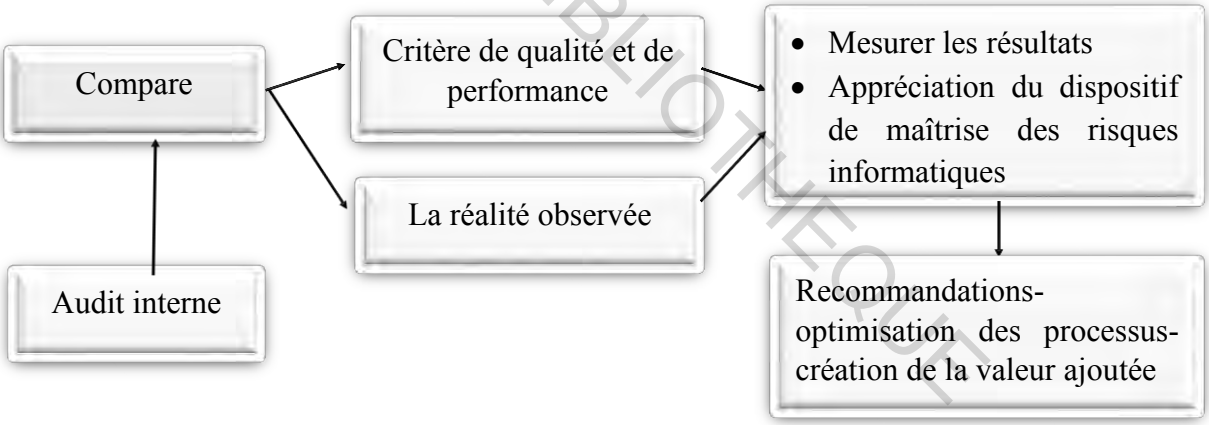
bien sur les aspects organisationnels que techniques, afin de contrôler l'efficacité et la pertinence des moyens mis en œuvre selon CALE & al. (2007 : 163).

La fonction d'audit interne est également concernée par le suivi des actions relatives à des incidents ou des carences du dispositif de contrôle interne de l'entreprise. En effet, pour CALE & al. (2007 : 166), de nouvelles menaces et vulnérabilités apparaissent tous les jours et le « bouclier » qui est parfaitement adapté aujourd'hui pour parer aux attaques, se retrouvera bien vulnérable demain. Il faut donc connaitre les dernières évolutions en termes technologiques (derniers outils utilisés par les pirates, nouvelles solutions de protection, dernières failles découvertes, etc.), législatives et aussi règlementaires.

2.3.3. Contribution de l'audit interne à la création de la valeur ajoutée

Le schéma ci-dessous présente l'approche généralement utilisée par l'auditeur interne pour contribuer à créer de la valeur ajoutée.

Figure 4 : Procédure de création de la valeur ajoutée par l'audit interne



Source : Nous-mêmes inspiré de DELOITTE (2006 : 33).

Pour assurer la création de la valeur ajoutée, l'auditeur interne doit analyser la gouvernance d'activité de l'entreprise relative au processus de maîtrise des risques informatiques. Pour ce faire, il peut se fonder sur les bonnes pratiques du COBIT pour effectuer un certain nombre de vérifications par rapport à ce qui est mis en place dans l'entreprise et formuler des recommandations. Une bonne gouvernance d'activité conduit automatiquement à la

performance de l'entreprise et donc à une création de la valeur ajoutée d'après l'AFAI[12] & al. (2005 : 4).

En effet, la gouvernance d'activité concerne le « comment » des choses. L'auditeur devra vérifier :

- comment sont identifiés les risques informatiques ?
- comment sont appliquées les méthodologies d'analyse et de gestion des risques informatiques (EBIOS, MEHARI, etc.) ?
- comment sont fixés les objectifs du processus de maîtrise des risques informatiques ?
- comment est fixé le seuil de tolérance du risque informatique par le CA ?

Ainsi, en fonction des réponses obtenues, l'auditeur interne devra faire des recommandations au regard des bonnes pratiques du COBIT en vue de leurs optimisations.

CONCLUSION DU DEUXIEME CHAPITRE

En conclusion, ce chapitre nous a permis de cerner la notion d'audit interne, et les étapes qui constituent un bon dispositif de maîtrise des risques informatiques selon deux (02) auteurs.

Par ailleurs, nous avons présenté l'apport de l'audit interne dans la maîtrise des risques informatiques ainsi que sa participation à la création de la valeur ajoutée. Le chapitre suivant consistera à présenter les outils utilisés pour collecter les données ainsi que le modèle d'analyse de données.

[12] Association Française de l'Audit et du conseil Informatique.

CHAPITRE 3 : METHODOLOGIE DE RECHERCHE

Dans le souci de présenter l'apport de l'audit interne dans la maîtrise des risques informatiques exposés au précèdent chapitre, nous avons découpé ce chapitre en deux (02) sections à savoir le modèle d'analyse d'une part et, d'autre part, la collecte et l'analyse de données.

3.1. Modèle d'analyse

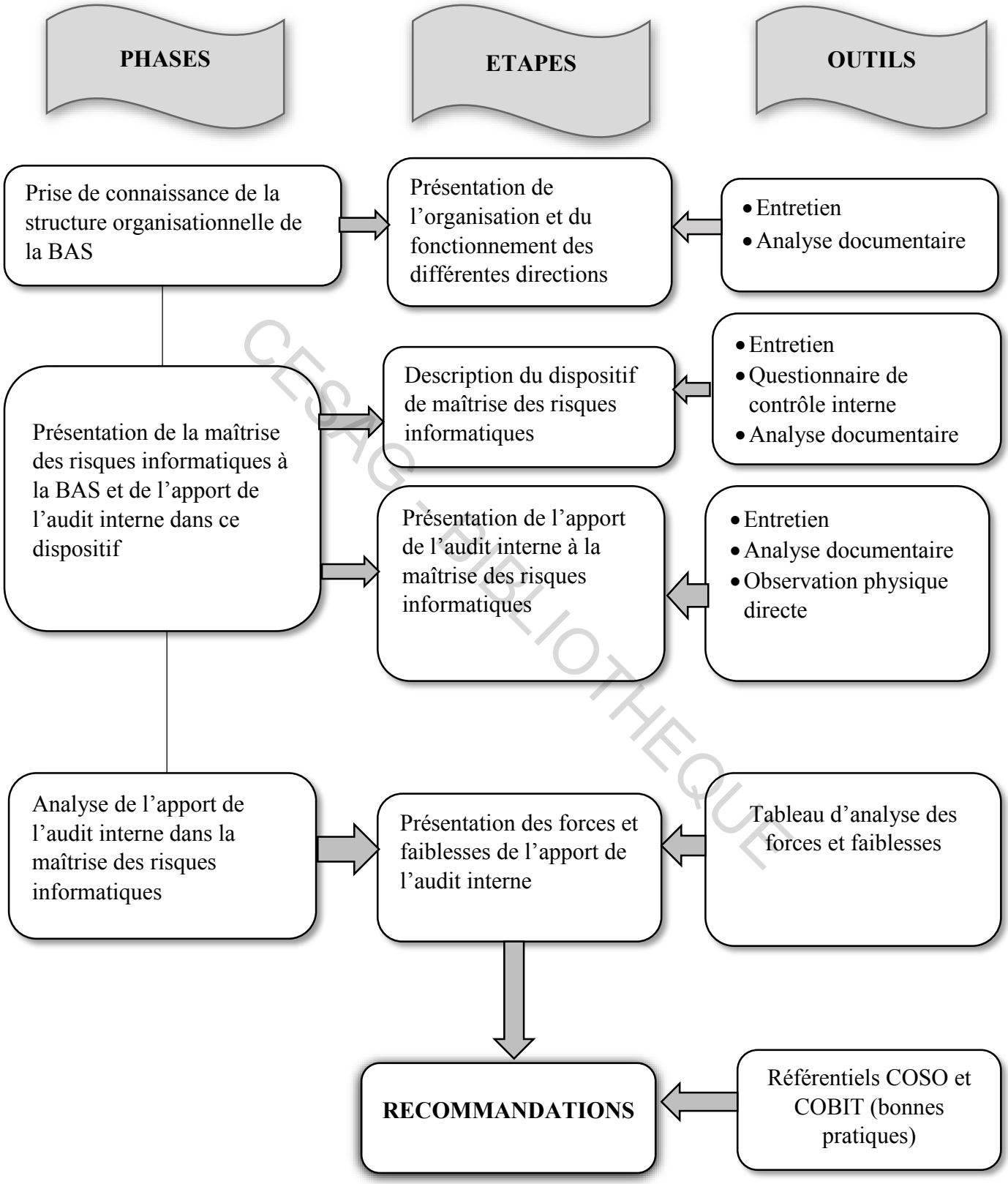
Le modèle d'analyse représente pour nous, la démarche que nous envisageons utiliser pour réaliser notre étude.

Présenté sous forme schématique, notre modèle est construit autour de trois (03) phases que sont :

- une phase de prise de connaissance de la structure organisationnelle de la BAS ;
- une phase de présentation du dispositif de maîtrise des risques informatiques et l'apport de l'audit interne dans celui-ci ;
- une phase d'analyse de l'apport de l'audit interne à la maîtrise des risques informatiques.

Chacune de ces phases contient une (01) ou deux (02) étapes auxquelles nous avons associés des outils permettant de collecter et d'analyser les données.

Figure 5 : Modèle d'analyse



Source : Nous- mêmes.

3.2. Les outils de collecte et d'analyse de données

Les principaux outils retenus pour la réalisation de ce travail seront présentés en fonction des différentes étapes.

3.2.1. Etape 1 : Présentation de l'organisation et du fonctionnement des différentes directions

Dans cette étape, nous utiliserons principalement l'entretien et l'analyse documentaire.

3.2.1.1. Entretien

L'entretien est une source importante d'information. En effet, il s'agit d'un échange interactif avec un interlocuteur ciblé et s'effectuant généralement en face à face (rarement par téléphone). Au cours de cette étape, l'entretien consistera à échanger principalement avec le Directeur des Ressources Humaines (DRH) de la BAS afin que celui-ci nous présente les principales directions de la BAS, leurs fonctionnements et leurs objectifs. Ce sera aussi l'occasion pour nous d'obtenir l'organigramme de la banque.

3.2.1.2. Analyse documentaire

L'analyse documentaire consistera à consulter les documents internes mais aussi externes à la banque en vue de recueillir les données utiles pour notre étude. Ainsi, dans le cadre de ce travail, nous consulterons la fiche de présentation de la Banque Atlantique du Sénégal, les rapports d'activité des trois (03) dernières années et l'organigramme de la BAS. L'analyse documentaire nous permettra d'acquérir une bonne connaissance de la BAS.

3.2.2. Etape 2 : Description du dispositif de maîtrise des risques informatiques

Comme outils, nous utiliserons, l'entretien, le questionnaire de contrôle interne et l'analyse documentaire.

3.2.2.1. Entretien

A l'aide d'un guide d'entretien construit à l'avance (voir annexe 2, page 102), notre entretien sera semi directif avec le responsable IT du service informatique et nous permettra d'avoir une meilleure description du processus de maîtrise des risques informatiques. Ceci nous permettra

ensuite de pouvoir confirmer ou d'infirmer certaines hypothèses formulées au début de notre travail.

3.2.2.2. Questionnaire de contrôle interne

Notre QCI ne sera composé que de questions fermées c'est-à-dire des questions qui ne nécessiteront qu'un OUI ou NON comme réponse (voir annexe 3, page 104). Le but de ce questionnaire est de s'assurer de l'existence d'un dispositif de maîtrise des risques informatiques à la BAS, de ressortir les principaux éléments constituants ce dispositif de maîtrise des risques s'il existe et enfin d'identifier les éventuelles faiblesses de ce dispositif. Il sera administré au responsable IT.

3.2.2.3. Analyse documentaire

A ce niveau, nous consulterons les politiques et documents relatifs à la maîtrise des risques informatiques notamment la politique de gestion des risques informatiques, la charte informatique, la politique informatique, la cartographie des risques informatiques, la politique informatique. A l'issu de cette étape, on pourra faire un premier diagnostic de notre thème d'étude.

3.2.3. Etape 3 : Présentation de l'apport de l'audit interne à la maîtrise des risques informatiques

Nous aurons recours à l'entretien, à l'analyse documentaire et à l'observation physique directe.

3.2.3.1. Entretien

A l'aide d'un guide d'entretien conçu à l'avance (voir annexe 4, page 107), notre entretien se fera face à face avec le Directeur d'Audit Interne de la BAS afin de ressortir la contribution des auditeurs internes dans la maîtrise des risques informatiques.

3.2.3.2. Analyse documentaire

Dans le cadre de ce travail, nous consulterons principalement, la charte d'audit interne de la BAS ainsi les rapports de missions réalisées au niveau du service informatique dans le cadre de la maîtrise ou la gestion des risques informatiques.

3.2.3.3. Observation physique directe

L'observation est une technique de collecte d'informations qui se fonde sur l'étude du comportement ou de l'attitude d'un individu en train de réaliser ses activités. Contrairement à l'entretien, cette méthode prend beaucoup plus de temps à réaliser. Au cours de celle-ci, l'attitude observée peut parfois être biaisée à cause de la présence de l'expérimentateur alors notre observation sera menée avec une grande discrétion.

Le but principal de cette observation dans le cadre de ce travail est de faire une comparaison entre ce qui est prescrit dans la charte d'audit interne et la pratique en ce qui concerne le processus de maîtrise des risques informatiques à la banque.

3.2.4. Etape 4 : Présentation des forces et faiblesses de l'apport de l'audit interne

Nous utiliserons principalement le tableau d'analyse des forces et des faiblesses lors de l'examen. Il nous permettra de ressortir les forces et faiblesses décelées au niveau de la contribution de l'audit interne dans la maîtrise des risques informatiques.

3.2.5. Etape 5 : Recommandations

Comme présenté au niveau du modèle d'analyse, en fonction des faiblesses relevées, nous formulerons des recommandations au regard des bonnes pratiques.

CONCLUSION DU TROISIEME CHAPITRE

Parvenu au terme de ce chapitre ayant porté sur la méthodologie de recherche, élément primordial pour juger de la pertinence des informations que nous présenterons au niveau de la partie pratique, nous avons jugé bon de retenir comme outils de collecte et d'analyse de données, l'entretien, l'observation physique directe, l'analyse documentaire, le QCI, et le tableau d'analyse des forces et faiblesses.

L'usage de chaque outil dépendra de l'étape à laquelle nous nous situons et des types d'information que nous souhaiterions recueillir.

CONCLUSION DE LA PREMIERE PARTIE

Parvenu au terme de cette première partie, consacrée à l'aspect théorique de notre recherche, nous avons jugé capital de développer trois (03) thématiques clés : la gestion des risques liés au système d'information, l'apport de l'audit interne à la maîtrise des risques informatiques et la méthodologie de recherche devant nous permettre d'atteindre nos objectifs.

Concernant la gestion des risques lié au système d'information, retenons que le système d'information est devenu le socle de la quasi-totalité des processus de l'entreprise ; son importance n'est plus à prouver. Un certain nombre de référentiels existent autour des systèmes d'information et l'utilisation d'un SI engendre généralement des risques dont la gestion et la maîtrise sont primordiales. Pour ce faire, des clubs et associations à l'instar du CIGREF, CLUSIF ou encore ANSSI ont développé des outils/méthodologies destinés à gérer ces risques tels que EBIOS, MEHARI, etc.

Dans la maîtrise des risques plus précisément celle des risques informatiques, l'audit interne a une grande part de responsabilité. En effet, à travers ses missions d'assurance et de conseils, l'audit interne apporte une plus-value significative à l'efficacité et l'efficience de tout dispositif de maîtrise des risques informatiques.

Dans le souci de démontrer tout ce qui a été précédemment dit, à travers un modèle d'analyse construit en trois (03) phases, nous avons retenu un certain nombre d'outils de collecte et d'analyse de données que sont : l'entretien, l'analyse documentaire, le questionnaire de contrôle interne, les tests de permanence et de corroboration et le tableau d'analyse des forces et des faiblesses.

La pratique étant parfois différente de la théorie, penchons-nous sur le cas des auditeurs internes de la Banque Atlantique du Sénégal afin d'examiner la façon dont ceux-ci contribuent à la maîtrise des risques informatiques liés aux activités de la banque.

DEUXIEME PARTIE : CADRE PRATIQUE DE LA CONTRIBUTION DE L'AUDIT INTERNE A LA MAITRISE DES RISQUES LIES AU SYSTEME D'INFORMATION

INTRODUCTION DE LA DEUXIEME PARTIE

Comme exposé à la première partie, la maîtrise des risques est une affaire de tous, y compris des auditeurs internes de la banque. L'impact causé par la survenance d'un risque informatique est de nos jours significatif aussi bien pour un auditeur interne que pour un responsable IT d'une banque.

Généralement, une grande différence est observée entre ce qui est dit en théorie et ce qui est fait en pratique, et ceci pour diverses raisons notamment l'influence de l'environnement économique et socio-culturel. L'objectif de cette partie est par conséquent de présenter l'apport des auditeurs internes de la Banque Atlantique du Sénégal à la maîtrise des risques informatiques.

Cette partie sera construite autour de trois (03) chapitres. Nous commencerons par la présentation de notre entité d'accueil, la Banque Atlantique du Sénégal. Par la suite, il s'agira pour nous de présenter le dispositif de maîtrise des risques informatiques à la BAS. Enfin, après avoir présenté l'apport de l'audit interne à la maîtrise des risques informatiques, nous analyserons cette contribution afin de ressortir les forces et les faiblesses de celle-ci.

CHAPITRE 4 : PRESENTATION DE LA BANQUE ATLANTIQUE DU SENEGAL

La Banque Atlantique du Sénégal (BAS) est une banque commerciale constituée sous la forme d'une société anonyme, appartenant au groupe privé Atlantique composé de la holding Atlantic Business International (ABI) et de ses filiales.

Créée en 2005, la Banque Atlantique du Sénégal est comptée parmi les banques les plus anciennes du Sénégal. Elle est présente sur la majeure partie du territoire sénégalais (Dakar, Thiès, Kaolack, Touba, Saint-Louis, Mbour et Louga), et dans sept (07) pays de la zone UEMOA (Cote d'Ivoire, Benin, Burkina Faso, Mali, Niger, Sénégal et Togo) sous des dénominations différentes. La présentation de la Banque Atlantique du Sénégal va se faire à travers son historique, ses missions, ses dates et faits marquants, ses produits et services et enfin son organisation

4.1. Historique de la banque

La Banque Atlantique du Sénégal occupe une place importante dans l'environnement économique du Sénégal. Elle a été créée le 26 avril 2005 avec un capital de deux (02) milliards de FCFA dans le but de servir d'intermédiaire entre ceux qui ont un excédent de trésorerie et ceux qui en ont un déficit. Le 28 décembre 2005, la BAS obtient auprès de la BCEAO[13] son agrément et commence à mener ses activités bancaires.

Au cours de sa vie, la BAS a subi deux augmentations de capital. La première augmentation à hauteur de 1,5 milliards a eu lieu en juin 2008 et la seconde augmentation en décembre de la même année portant ainsi son capital à cinq (05) milliards de FCFA. Actuellement le capital de la BAS est porté à plus de 13 502 730 000 de FCFA.

En 2012, le Groupe Banque Centrale Populaire du Maroc (BCP), l'une des premières institutions bancaires du Maroc est entré dans le capital du groupe Atlantique et représente actuellement l'actionnaire majoritaire. Le 07 juin 2012, BCP et Atlantic Financial Group (AFG) ont conclu un partenariat et ont créé une holding dénommée Atlantic Bank International

[13] Banque Centrale des Etats de l'Afrique de l'Ouest

(ABI). Ce partenariat, gage de solidité financière, permet à la banque d'asseoir et de propulser sa croissance sur le marché Sénégalais.

4.2. Missions de la BAS

Les principales missions de la Banque Atlantique du Sénégal sont :

- le financement de l'économie sénégalaise par divers moyens ;
- la préservation de l'intérêt de ses actionnaires, de ses clients et des différentes parties prenantes.

4.3. Dates clés et faits marquants

La compréhension du parcours de la BAS à ce jour, passe par la présentation de ses principales dates clés et faits marquants :

- 26 avril 2005 : création de la société anonyme Banque Atlantique Sénégal ;
- 28 décembre 2005 : arrêté n°005988/DMC matérialisant l'obtention par la BAS de son agrément ;
- 28 janvier 2006 : entrée du groupe d'assurances SONAM dans le capital à hauteur de 25% ;
- juin 2008 : augmentation du capital de 1,5 milliard le portant à 3,5 milliards ;
- décembre 2008 : augmentation du capital porté à 5 milliards ;
- mars 2011 : convention de financement SUNEOR-BANQUE ATLANTIQUE SENEGAL dont le but est de soutenir le développement du monde rural. La BAS a arrangé pour le compte de la SUNEOR, un financement structuré de douze (12) milliards de FCFA destinés à achever la commercialisation arachidière de cette dernière ;
- juillet 2011 : la Banque Atlantique et le FSE (Fonds de soutien à l'énergie) signent une convention de 347 milliards de FCFA destinés à l'apurement des dettes de la SENELEC (Société nationale d'électricité) ;
- novembre 2011 : la Banque Atlantique du Sénégal et ECI Co-arrangeurs financent la campagne arachidière de 2012 de SUNEOR pour un montant de 50 milliards de FCFA ;
- 2012 : prix EMEA (Europe, Moyen Orient et en Afrique) Deal of the year 2012, décerné à la BAS par le magazine londonien Trade Finance dans la catégorie financement des

matières premières « Structured Trade Finance and Commodity Finance » pour le financement de cinquante (50) milliards de FCFA de la campagne arachidière de 2011/2012 en faveur de la SUNEOR, conjointement Co-arrangé par ECI et BAS ;

- 2012 : la BAS reçoit le prix « best innovative card program » attribué par le forum africain des métiers et technologies de la carte en partenariat avec mastercard. Ce forum organise « les Cartes Afrique Awards » et récompense l'excellence en décernant des prix aux opérateurs les plus dynamiques et aux projets les plus innovants dans la région ;
- mai 2013 : la BAS reçoit le trophée SEDAR 2012 destiné à récompenser la banque la plus dynamique dans son secteur.

4.4. Produits et services de la BAS

La BAS offre une palette de produits et services spécifiques à chaque type d'agent économique (professionnels, fonctionnaires, salariés du privé et sénégalais de la diaspora). Parmi ses principaux produits et services, nous avons :

4.4.1. La collecte de l'épargne

La BAS propose quatre (04) types d'épargnes :

- les épargnes ordinaires ;
- les épargnes atlantiques ;
- les épargnes pour les sénégalais de la diaspora ;
- les bons de caisse.

4.4.2. Les opérations de crédit

Comme opérations de crédit, la BAS octroie : les découverts sur compte, des découverts sur cartes privilégiées, des escomptes, des avances sur marché, des avances sur bon de commande, des crédits à court terme, des crédits d'équipement des cautions en douanes, des cautions de marché, des crédits documentaires d'impôts, des crédits SPOT, des financements du commerce extérieur et des encagements par signature (caution/garanties /aval).

4.4.3. Les moyens de paiement

Comme moyens de paiement, la BAS a mis à la disposition de sa clientèle des chèques, des virements bancaires et des ordres de prélèvement.

4.4.4. La monétique

Il s'agit des différentes cartes que la BAS propose à ses clients. Il s'agit de :

- gamme visa : carte internationale de retrait et de paiement utilisable sur l'ensemble des distributeurs et terminaux de paiements électroniques affiliés au réseau VISA ;
- cartes prépayées : nous avons les cartes Atlantique Traveler (Mastercard), Atlantique Cash et Atlantique Hajj (pour ceux qui vont à la Mecque) ;
- cartes d'épargne : carte pour le retrait sur les comptes d'épargne.

4.4.5. La bancassurance : Atlantique quietus

Il s'agit de l'assurance vie adossée au compte du client et qui offre au souscripteur de l'offre, un double avantage : le versement à l'assuré ou à ses ayants droit d'un capital en cas de décès ou d'invalidité absolue et définitive, et le versement d'un capital fixe et unique en guise d'indemnité de frais funéraires (en cas de décès) ou de frais d'assistance (en cas d'invalidé absolue et définitive).

4.4.6. Les autres produits de la BAS

Nous distinguons dans cette catégorie :

- l'anet ;
- les sms banking ;
- les transferts d'argent (money gram, money cash ou western-union, et ria) ;
- les guichets automatiques de la banque ;
- les terminaux de paiement électronique ;
- l'e-relevé ;
- l'alerte e-mail ;
- de carte Visa.

4.5. Organisation de la BAS

La BAS est dirigée par un Conseil d'Administration composé d'un Président et des administrateurs chargés de fixer les grandes orientations de la banque (politique générale) ainsi que ses objectifs stratégiques. Il existe plusieurs directions au sein de la BAS ayant comme objectif commun : la contribution à l'atteinte des objectifs de la banque.

La Banque Atlantique du Sénégal compte aujourd'hui dix-huit (18) agences et bureaux et trois cent trente-sept (337) points de transfert d'argent. Néanmoins, elle poursuit en parallèle l'extension de son réseau existant. Le tableau ci-dessous présente l'ensemble des agences de la BAS :

Tableau 3 : Les principales agences de la BAS

N°	AGENCES	N°	AGENCES
1	Principale (siège)	**10**	Mbour
2	Parcelles	**11**	Saint- Louis
3	Thiaroye	**12**	Thiès
4	Pikine	**13**	Louga
5	Campus	**14**	Ziguinchor
6	Zone industrielle	**15**	Hlm
7	Vdn	**16**	Touba
8	Abdou karim bourgi	**17**	Km 18
9	Kaolack	**18**	Km 20

Source : Nous-mêmes à partir de la BAS (2015).

L'organigramme de la banque (voir annexe 5, page 109) montre que l'ensemble de ses activités est piloté par un Président du Conseil d'Administration, une Direction Générale aidée des Directions fonctionnelles, des départements et des services. Ainsi, on distingue :

4.5.1. Le Conseil d'Administration

Organe délibérant de la filiale, il est investi de tous les pouvoirs pour agir en toutes circonstances au nom de la banque dans la limite de l'objet social et des compétences réservées à l'Assemblée Générale. Il approuve l'organisation générale de la filiale. Il adopte la politique en matière de contrôle, s'assure de la mise en place d'un dispositif adéquat et surveille régulièrement son activité et ses mesures.

Il est régulièrement tenu informé des risques majeurs auxquels l'établissement est exposé, et en fixe les limites acceptables.

4.5.2. La Direction Générale

Elle est chargée de superviser toutes les activités des différents départements. Elle assure l'intermédiation entre le conseil d'administration et les différentes directions. Ses principales missions sont les suivantes :

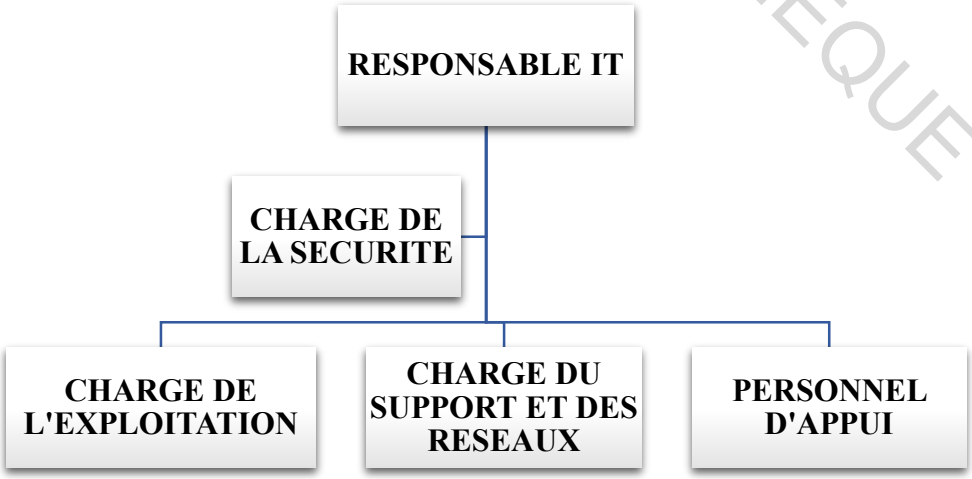
- déploiement de la politique générale de la BAS au niveau de tous les départements ;
- animer le Comité de Direction ;
- représenter la banque devant les autorités de tutelle et les clients ;
- veiller à l'application des directives du Conseil d'Administration.

4.5.3. Le Secrétariat Général

Le Secrétariat Général est rattaché hiérarchiquement à la Direction Générale. Il supervise le service informatique, le contrôle permanent, le service qualité et le responsable Business Service.

- **le service informatique** : il est composé d'un responsable IT, d'un responsable de la sécurité, d'un chargé de l'exploitation, d'un chargé du support et des réseaux et d'un personnel d'appui (voir organigramme ci-dessous).

Figure 6 : Organigramme du service informatique



Source : Nous-mêmes à partir du DRH-BAS (2015).

- **le contrôle permanent** : également chargé de la conformité, il effectue des travaux sur la base d'une check-list détaillée qui fournira l'ensemble des contrôles à vérifier au sein de chaque département. Un système de reporting mensuel est établi à l'adresse du Directeur Général de la filiale pour être informé de toute anomalie ou dysfonctionnement relevé ainsi que de tout contrôle non effectué. Ce reporting est aussi adressé au responsable de l'audit interne de la BAS, au responsable de risque management d'ABI ;
- **le service qualité** : il est chargé de la mise en application des exigences et la norme ISO 9001 : 2008 ;
- **le responsable Business Service** : il est responsable des opportunités d'affaire de la banque.

4.5.4. Le Comité d'Audit

Le Comité d'Audit prend connaissance régulièrement de l'état de mise en œuvre des recommandations de l'audit interne, se prononce sur le programme de vérification de l'audit interne, formule des recommandations visant à renforcer l'efficacité des contrôles en vue d'une maîtrise adéquate des risques inhérents et résiduels relatifs à l'activité de l'établissement.

4.5.5. La Direction de l'Audit Interne (DAI)

La position organisationnelle de la DAI est définie de sorte à lui donner une certaine indépendance vis-à-vis des autres départements et un grand champ d'action dans la banque. En effet, la DAI est rattachée d'une part, fonctionnellement du Comité d'Audit et, d'autre part, hiérarchiquement à la Direction Générale.

La Direction Audit Interne est composé d'un Directeur de l'Audit Interne, un auditeur senior, et de trois (03) autres auditeurs. Ainsi, régis par une charte d'audit interne qui tient compte des évolutions réglementaires et normatives, les auditeurs internes sont chargés de s'assurer que toutes les directions fonctionnent conformément aux procédures établies par le Groupe, agissent dans le respect des règlementations en vigueur (accord de Bâle II, commission bancaire, etc.).

Par ailleurs, la DAI est chargée :

- d'évaluer l'efficacité des différents dispositifs mis en place au sein de la BAS ;
- de réaliser régulièrement des audits de conformité dans les différentes agences de la BAS selon un plan d'audit défini ;

- de présenter les points forts et les défaillances du système de contrôle interne ;
- de formuler des recommandations pour corriger les points faibles relevés ;
- d'effectuer le suivi des recommandations formulées.

Aussi, lorsque le besoin se crée, les auditeurs internes de la BAS suivent des formations.

4.5.6. La Direction des Risques

Avec à la tête un Directeur des Risques, cette direction comprend trois (03) services à savoir : le service analyse des crédits, le service contrôle et administration de crédits et le service recouvrement.

- le service analyse de crédits est chargé d'étudier toutes les demandes de crédits formulées par la clientèle de la BAS, effectue la cotation des différents clients de la banque et les études sectorielles pour orienter la politique de crédit de la banque ;
- le service contrôle et administration de crédits est chargé du contrôle et du suivi des dossiers de crédits ainsi que l'établissement de la liste des clients précontentieux ;
- le service recouvrement est chargé d'assurer le recouvrement à l'amiable des agents et du recouvrement contentieux des agents.

4.5.7. La Direction Financière et Comptable

Cette Direction est chargée de la supervision des comptables et contrôleurs de gestion de la banque. C'est également elle qui informe l'ensemble du personnel de la banque des changements opérés au niveau de la fiscalité du pays, des éventuelles entrées en vigueur de nouvelles normes comptables, du développement de nouveaux outils de gestion. Elle comprend le service contrôle de gestion, le service comptabilité et le service contrôle comptable.

4.5.8. Les autres Directions

La Direction Générale a également mise sur pieds :

- la Direction des Opérations ;
- la Direction de la Clientèle d'Entreprise ;
- la Direction du Réseau et de la Clientèle;
- la Direction de la Trésorerie ;
- la Direction Ressources Humaines ;
- la Direction Juridique et Compliance.

CONCLUSION DU QUATRIEME CHAPITRE

Depuis sa création en 2005, la BAS a eu à faire face à de nombreux défis. La diversité culturelle de sa ressource humaine, sa culture d'entreprise orientée client, lui ont généralement permis de fidéliser sa clientèle par une approche « conseil » et d'anticiper les besoins de ses clients en leur proposant de nouveaux services innovants.

Ce chapitre, destiné à la présentation de la Banque Atlantique du Sénégal nous a permis de comprendre l'histoire de la BAS, de connaitre les produits et services qu'elle offre ainsi que les directions qu'elle a mises sur pieds pour aider la Direction Générale dans le pilotage de la banque. Le chapitre suivant présentera le dispositif de maîtrise des risques informatiques de la BAS.

CHAPITRE 5 : DESCRIPTION DU DISPOSITIF DE MAITRISE DES RISQUES INFORMATIQUES DE LA BANQUE ATLANTIQUE DU SENEGAL

L'objectif de ce chapitre est de présenter les éléments qui composent le dispositif de maîtrise des risques informatiques de la BAS.

Tout d'abord, précisons que le service informatique de la BAS ne gère pas directement tous les risques liés au système d'information. En effet, la gestion des risques informatiques à l'instar de ceux liés à la monétique ne se fait pas localement, elle est externalisée. Aussi, le système de contrôle interne de la banque repose sur une formalisation quasi-complète des procédures destinées à identifier, suivre et maîtriser les risques.

La suite de notre travail consistera à présenter les objectifs et une description du dispositif de maîtrise des risques informatiques de la banque.

5.1. Objectifs du dispositif de maîtrise des risques informatiques de la BAS

Le dispositif de maîtrise des risques informatiques de la BAS a pour objectifs de :

- définir un environnement, une méthodologie et un cadre formalisé de maîtrise des risques à même de favoriser l'émergence d'une culture de management des risques au sein de la BAS ;
- identifier, cataloguer et maîtriser les principales menaces et vulnérabilités auxquelles est exposée la banque ;
- développer et implémenter des contrôles proportionnés aux risques susceptibles d'impacter la confidentialité, l'intégrité ou la disponibilité de ses données ;
- maintenir le niveau du risque à un niveau inférieur au seuil de tolérance fixé par le management, tout en restant maître des situations susceptibles de générer un risque.

5.2. Composantes du dispositif de maîtrise des risques informatiques à la BAS

Le dispositif de maîtrise des risques informatiques à la banque comporte un cadre

institutionnel et organisationnel, une méthodologie de gestion des risques, et des stratégies de mitigations des risques.

5.2.1. Cadre institutionnel et organisationnel

Ce cadre regroupe principalement les politiques et procédures formalisées et les structures de gestion des risques.

5.2.1.1. Les politiques et procédures écrites

La politique de gestion des risques à la BAS est régie par le document de politique de sécurité informatique. Dans cette catégorie, nous présenterons la politique de sécurité des systèmes d'information, la politique informatique, et la charte de sécurité informatique.

5.2.1.1.1. La politique de sécurité informatique

La politique de sécurité informatique de la BAS présente :

- les objectifs de celle-ci et la nécessité d'une sécurité à l'instar de la préservation de la vie privée de ses clients ;
- le seuil de tolérance aux risques informatiques retenu ;
- les différentes stratégies de mitigation des risques informatiques définies (acceptation, évitement, partage et réduction) ;
- les procédures de sécurité physiques, du personnel et de l'information. Elle décline entre autres, l'ensemble des moyens nécessaires pour éviter l'intrusion dans les locaux du service informatique, la divulgation des données confidentielles de la part des agents de la banque, accès aux données sans autorisation pour les employés n'ayant pas le niveau d'habilitation requis ;
- les procédures de sécurité logique notamment, toutes les dispositions sécuritaires liées à la partie software du système d'information bancaire de la BAS ;
- les responsabilités, les rôles des personnes impliquées. En effet, la politique informe toutes les personnes utilisant le système informatique des enjeux d'une sécurité informatique dans le but de s'assurer qu'elles sont parfaitement conscientes de leurs responsabilités. C'est à ce niveau que sont déclinées les responsabilités du responsable IT et de son équipe.

Par ailleurs, la politique présente les exigences en matière de confidentialité des données, d'intégrité des systèmes et des applicatifs, de données et de traitements et de disponibilité des

informations. En effet, l'information constitue la pierre angulaire de la banque. Une importance primordiale lui est accordée.

5.2.1.1.2. La politique informatique

La politique informatique de la BAS fournit à l'ensemble des agents de la banque utilisant les ressources informatiques (ordinateurs, réseaux internes de la banque, connexion internet, etc.) un ensemble de directives quant à l'utilisation de celles-ci.

En effet, afin d'éviter à la banque l'exposition aux risques de perte d'intégrité de ses données, de développements et des installations de logiciels incompatibles et non contrôlées, cette politique interdit l'installation d'un quelconque logiciel sur un poste de travail sans approbation préalable du chargé de la sécurité de la banque. Aussi, chaque poste de travail ne peut se connecter qu'à partir d'un câble internet personnalisé et identifié.

5.2.1.1.3. La charte informatique

La charte informatique présente les conditions générales d'utilisation du système d'information bancaire, d'accès à internet, d'accès aux réseaux et aux services multimédias au sein de la banque.

Par ailleurs, elle recense l'ensemble des règles fondamentales liées à l'attitude que doit adopter le personnel de la banque en matière d'utilisation des ressources informatiques et de communication électronique. Son institution est faite dans le but d'éviter toute forme d'abus sur l'usage des outils informatiques et aussi de servir de référence en cas de conflit au sein de la BAS.

5.2.1.2. Les structures de gestion des risques

La BAS dispose d'un Comité de Risque opérationnel et de cinq (05) autres acteurs impliqués dans la maîtrise des risques informatiques.

5.2.1.2.1. Le Comité de Risque opérationnel

Ce comité est chargé de dérouler les choix et orientations stratégiques en matière d'identification des risques informatiques, de fixation du seuil de tolérance, et de définition des stratégies de mitigation de ces risques. Il est composé par le RSSI du groupe, le Directeur Général, le Responsable du Contrôle Permanent et le Responsable IT du Service Informatique et du Directeur d'Audit Interne. Le comité se réunit au moins deux (02) fois par an pour dérouler

les grandes lignes directrices décidées par le Groupe Banque Atlantique sis à Abidjan (Côte d'Ivoire).

Bien qu'ils s'agissent des mêmes membres, précisons que le Directeur Général, le RSSI du Groupe, le Responsable IT, le Responsable du Contrôle Permanent et le Directeur de l'Audit Interne ont des responsabilités distinctes selon qu'ils sont membres du Comité de Risque ou de acteurs de la BAS.

5.2.1.2.2. Les autres acteurs de la maîtrise des risques informatiques

Cinq (05) acteurs clés agissent dans la maîtrise des risques informatiques de la BAS. Une relation de continuité existe entre ces acteurs. L'activité de l'un des acteurs est le prolongement de l'activité de l'autre dans la maîtrise des risques informatiques.

Il s'agit du Directeur Général, du RSSI du Groupe, du responsable IT du service informatique, du responsable du contrôle permanent et du Directeur de l'Audit interne. Le Risk Manager n'est impliqué que dans la maitrise du risque de crédit. En effet :

- **le Directeur Général** est chargé de définir la politique de gestion des risques informatiques, de décliner les stratégies de mitigation du risque informatique et définir les dispositions d'une bonne maîtrise des risques informatiques ;
- **le RSSI du Groupe** il est chargé de sensibiliser l'ensemble du personnel de la BAS sur l'existence des risques informatiques et des dispositions à prendre pour pallier à ceux-ci ; généralement, il procède par envoie des messages e-mails pour la communication ;
- **le Responsable IT** il a pour principale responsabilité d'identifier l'ensemble des risques informatiques de la BAS ; aussi, il est de la responsabilité de son service d'assurer l'entretien des accessoires, la surveillance des liaisons, la sécurité de la banque, le câblage, la configuration du réseau, l'installation des postes et assistance aux utilisateurs d'après la politique de sécurité informatique dont la publication ne peut être faite pour des raisons de confidentialité ;
- **le Responsable du Contrôle Permanent** qualifié de contrôle de deuxième niveau à la banque, il est chargé d'établir la cartographie des risques informatiques, de s'assurer que tous les risques informatiques sont recensés, et de proposer des plans d'action pour les contrôler. Notons que la définition des plans d'action se fait conjointement avec le responsable IT du service informatique ;

- **le Directeur de l'Audit Interne** intervient conformément aux objectifs qui lui sont assignés dans la charte d'audit interne. Cette charte ne peut être jointe à ce travail pour des raisons de confidentialité.

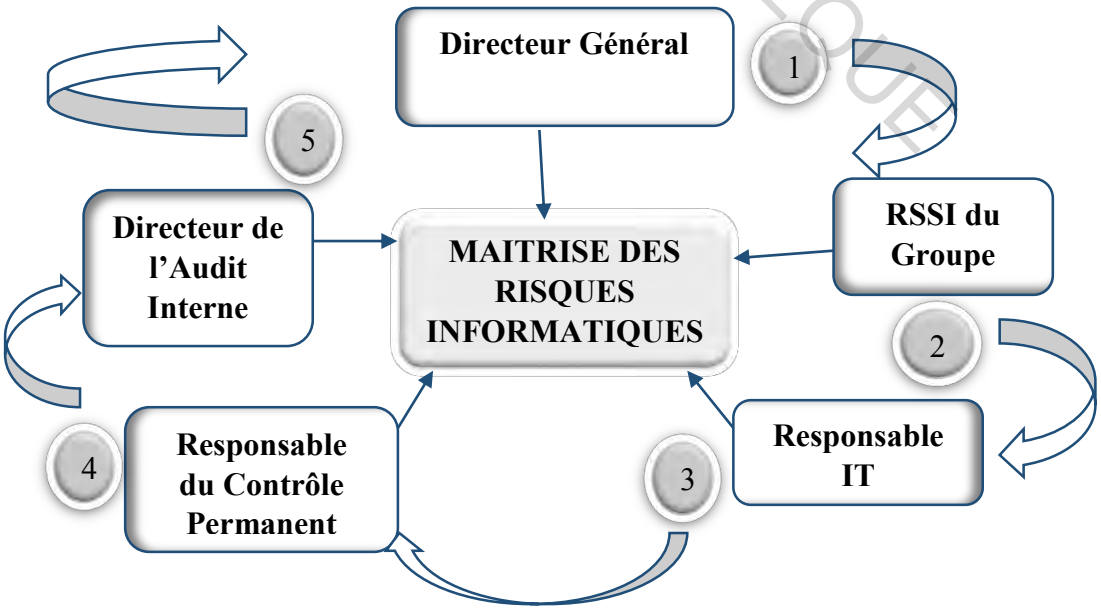
L'audit interne représente le contrôle de troisième niveau après le contrôle de premier niveau réservé aux opérationnels et le contrôle de deuxième niveau réalisé par le contrôle permanent. Ce contrôle de troisième niveau est constitué de contrôles périodiques, ponctuels ou inopinés effectués par les auditeurs internes.

D'après la charte d'audit interne, l'audit interne est chargé, en s'appuyant sur une méthodologie permettant d'identifier les risques significatifs, de vérifier particulièrement :

- ✓ la conformité des procédures aux dispositions régissant l'activité ;
- ✓ le respect de ces procédures, des modèles et dispositif de suivi des différents risques ;
- ✓ la fiabilité et la sécurité des systèmes d'information, de l'organisation des services ainsi que la mise en œuvre des recommandations précédemment faites par lui-même.

La figure ci-dessous illustre ces relations entre les acteurs par ordre d'intervention :

Figure 7 : Acteurs du dispositif de maîtrise des risques informatiques de la BAS



Source : Nous-mêmes.

Ce schéma laisse clairement entrevoir la relation de continuité existant entre ces acteurs. La maîtrise des risques est un cycle continu à la banque. Ainsi, le Directeur Général instaure la culture du risque au sein de l'établissement, le RSSI procède ensuite à la sensibilisation et à la formation de l'ensemble du personnel notamment sur la conduite à tenir face à un risque. Le responsable IT lui procède au recensement des risques, le responsable du contrôle permanent définit les plans d'action et le Directeur d'Audit Interne procède à une revue de ces plans d'action.

5.2.2. Méthodologie de gestion des risques informatiques

La présentation de la méthodologie de gestion des risques informatiques à la BAS consistera à présenter principalement la méthode d'identification des risques, leur analyse et évaluation, les étapes de leur gestion ainsi que leur cartographie.

5.2.2.1. Méthode d'identification et d'analyse des risques

Aucun outil d'identification et d'analyse des risques n'a encore été mis en place par la BAS. De même aucun référentiel de gestion des risques informatiques n'est formalisé.

Toutefois, la démarche d'identification des risques informatiques adoptée à la BAS est la méthode bottom-up (analyse active). En effet, l'identification des risques informatiques par cette méthode consiste pour le contrôle permanent, à s'entretenir avec le responsable IT du service informatique (détenteur des risques informatiques) de la BAS dans le but de recenser l'ensemble de ses risques. A ce niveau, l'auditeur interne intervient souvent comme conseiller.

5.2.2.2. Les étapes de la gestion des risques

La gestion des risques informatiques au sein de la BAS regroupe trois (03) étapes à savoir l'identification, l'analyse, évaluation et le choix de la stratégie de mitigation.

5.2.2.2.1. Identification des risques

A la BAS, chaque responsable de service/direction est propriétaire des risques de ses processus métiers. Ainsi, il est de la charge de chaque responsable de recenser l'ensemble des risques de son service ou de sa direction et de le soumettre au responsable du contrôle permanent.

5.2.2.2.2. Analyse et évaluation des risques

Après que l'identification des risques ait été effectuée, le contrôle permanent conjointement

avec le responsable IT, les hiérarchise par niveau de criticité (probabilité d'occurrence x gravité du risque) décroissant. Ce niveau de criticité obtenu a pour but de qualifier les risques identifiés (élevé, moyen et faible). Le responsable du contrôle permanent s'assure à ce niveau que les moyens de maîtrise et les plans de management sont appropriés au risque, à sa vraisemblance et à ses conséquences.

5.2.2.2.3. Stratégies de mitigation

Il s'agit encore des plans de réponse aux risques. Elles permettent de mettre en place pour chaque risque, une stratégie d'intervention et de définir la personne qui sera chargée des actions préventives relatives à ce risque.

La BAS a défini quatre (04) stratégies de mitigation des risques comme préconisés par les bonnes pratiques en la matière. Il s'agit de :

- l'évitement : lorsque la banque se rend compte qu'un risque peut provoquer de lourdes conséquences, elle cesse soit l'activité génératrice du risque, soit elle supprime le produit ou service bancaire qui le génère ;
- l'acceptation : il y a acceptation du risque lorsque l'impact que causerait la réalisation d'un risque n'est pas assez significatif pour empêcher la banque d'atteindre ses objectifs ;
- le partage : la banque partage régulièrement certains risques avec des sociétés d'assurance dont les noms ne peuvent être mentionnés par souci de confidentialité ;
- la réduction : principale stratégie utilisée, le contrôle permanent met régulièrement sur pied des plans d'action visant à mitiger les risques informatiques.

L'ensemble des points précédemment développés conduisent à l'élaboration de la cartographie des risques qui sera présenté au point suivant.

5.2.2.3. Cartographie des risques

La cartographie est un document capital pour la banque dans le processus de maîtrise des risques. En ce qui concerne les risques informatiques, les plans d'action mis sur pieds tiennent compte principalement du niveau de criticité du risque. Les travaux effectués à ce niveau sont faits sur la base de check-lists détaillées ou sur la base des bonnes pratiques en la matière.

Le tableau ci-dessous, présente un extrait de cartographie des risques informatiques de la BAS.

Tableau 4 : Extrait de cartographie des risques informatiques de la BAS

Risques informatiques	**Plans d'action**
Couverture incomplète de la procédure de sécurité définie par ATECH (Atlantique Technologie)	Mettre en place une procédure de sécurité formalisée
Gestion inappropriée des rebuts informatiques	Formaliser une procédure de gestion des rebuts informatiques et proposition de perforer les disques non réutilisables et effacer ceux réutilisables
Défaillance de sécurité des actifs informatiques (inexistence de câble de sécurité pour les ordinateurs portables)	Acheter des applicatifs de cryptage de disques durs. Ainsi, en cas de perte d'ordinateur ou d'erreur sur le mot de passe, le disque dur s'efface automatiquement
Défaillance de sécurité chez les tiers ayant accès au système d'information de la banque	Organisation des missions d'audit pour s'assurer du respect des normes de sécurité
Indisponibilité des réseaux de télécommunications	Formaliser une procédure
Indisponibilité des systèmes en raison de l'absence de suivi dès l'échéance de contrats de maintenance	Mettre en place un contrat de maintenance pour les systèmes de gestion en interne, formaliser le processus de suivi des contrats de maintenance
Modification du nombre de validation nécessaire pour une opération	Rédiger une procédure de gestion des paramétrages, un état quotidien recensant les modifications effectuées sur le paramétrage : poids et signature
Non renseignement des jours fériés dans le système d'information bancaire	Mettre en place une procédure et un contrôle sur les jours fériés invariable en début d'année (ils sont normalement paramétrés le 31 décembre n pour l'année n+1)
Non alignement des projets informatique à la stratégie des besoins métiers de la banque	Pour les projets de groupe, s'assurer de la validation du cahier de charges par le comité projet de chaque filiale concernées, s'assurer

	également du recetage dans chaque filiale avant mise en production

Source : Nous-mêmes à partir de la cartographie informatiques de la BAS (2014).

5.2.3. Les contrôles

Les contrôles constituant le dispositif de maîtrise des risques regroupent l'ensemble des parades mises sur pieds pour assurer une résistance du système informatique face aux attaques. Ainsi, il a été prévu principalement trois (03) types de contrôle au niveau du dispositif de maîtrise des risques informatiques de la BAS à savoir les contrôles organisationnels, physiques et logiques ou techniques.

5.2.3.1. Contrôles organisationnels

Les principaux contrôles organisationnels concernent la séparation des tâches incompatibles, la protection du matériel de bureau, la gestion des accès logiques et la sauvegarde des données de la banque.

5.2.3.1.1. La séparation des tâches incompatibles

La BAS a défini des règles visant à empêcher tout cumul de fonctions incompatibles. Ainsi, la personne chargée d'enregistrer les données dans le système de la banque ne peut être la même personne qui la modifie ou la supprime. Ce dispositif a pour but de prévenir tout risque de malversation, d'altération ou de destruction volontaire ou involontaire des informations de la BAS.

De plus, il est prévu une séparation de fonctions entre le chargé de la sécurité et les autres fonctions informatiques. Par exemple, la BAS a prévu une séparation de fonction entre le chargé de la sécurité du réseau et celui qui en assure son exploitation, ou encore entre le chargé de la sécurité et celui en charge de l'exploitation du système d'information bancaire.

5.2.3.1.2. La protection du matériel de bureau

Il est interdit à tout agent de rentrer chez soi avec son ordinateur portable à usage professionnel. Cette mesure rentre dans le cadre de la protection du patrimoine (actif informatique) de la banque.

5.2.3.1.3. La gestion des accès logiques

Elles concernent l'attribution des niveaux d'habilitations et des droits d'accès. La procédure d'attribution des niveaux d'habilitation à la BAS consiste à définir les niveaux d'habilitations compte tenu de la fiche de poste de chaque membre. Au sein de la banque, cette procédure concerne un aspect organisationnel.

Ainsi, il est prévu un contrôle régulier à ce niveau compte tenu des changements réguliers dans le milieu salarial. La procédure d'attribution des droits d'accès consiste exclusivement à autoriser les agents de la banque à n'accéder qu'aux informations dont ils ont besoin pour accomplir leurs tâches. Par conséquent, les informations dont aura accès une caissière de la banque ne sont pas de même envergure que celles dont a accès un chef d'agence. Il en est de même en ce qui concerne un analyste de crédit et le directeur de crédit. Un mot de passe est attribué à chaque agent de la banque au moment de son embauche en conformité avec la stratégie de mot de passe préalablement définie par la banque et dont le format ne peut être présenté pour des raisons de confidentialité.

5.2.3.1.4. La sauvegarde des données

Le service informatique de la banque effectue des sauvegardes journalières, hebdomadaires, et mensuelles de ses données afin d'éviter le risque de perte des données de la banque. Ainsi, à partir d'un serveur de partage, un répertoire est créé par département et par agents dans lequel sont déversées les données journalières. Ensuite, une sauvegarde différentielle est opérée quotidiennement à la clôture de la journée à une heure tenue confidentielle. Au cours de la procédure de sauvegarde, il ne doit pas avoir écrasement de données. Seules les données ayant subi une modification subissent un changement. L'ensemble de ces données est dupliqué par le service informatique dont une partie est cryptée et envoyée dans un serveur externe tenu confidentiel.

En effet, un certain nombre de paramétrages sont opérés au niveau du système d'information bancaire de la BAS. Ainsi, au moment de se connecter sur le système, chaque agent procède obligatoirement à son authentification (nom et mot de passe).

5.2.3.2. Contrôles physiques

La BAS a prévu un certain nombre de règles destinées à maîtriser les évènements pouvant affecter l'établissement. Ainsi, il a été instauré :

- le port obligatoire d'un badge afin d'éviter tout risque d'intrusion ;
- l'installation d'un système de paratonnerre et des prises terres afin de préserver l'architecture matériel informatique contre les sinistres (éclair, tonnerre) ;
- l'équipement de la salle des machines d'un système de climatisation afin de prévenir le risque de destruction des machines dû à l'hygrométrie ;
- l'installation des caméras de surveillance pour limiter le risque d'intrusion ;
- l'équipement des machines d'un onduleur afin de prévenir la destruction des machines du fait des coupures de courant ;
- la conservation des matériels réseaux, tels que les serveurs, routeurs, commutateurs et modems dans une salle ou une armoire verrouillée ;
- la mise en place d'un programme de maintenance des machines afin d'éviter le risque de détérioration des machines ;
- la non-installation du service informatique au niveau du sous-sol du bâtiment afin d'éviter tout risque d'inondation.

5.2.3.3. Contrôles logiques ou techniques

Les contrôles logiques à la BAS représentent l'ensemble des mécanismes mis en place pour protéger la partie immatérielle ou software du système d'information. Ainsi, il a été mis en place :

- une fonction pare-feu (firewall) afin de répondre au besoin de protection du réseau interne de la banque contre les attaques extérieures venant d'internet, de filtrer les communications internes et externes, et d'authentifier les utilisateurs du système ;
- une surveillance du réseau informatique destinée à détecter les pannes, de déceler les engorgements et de répartir les charges informatiques ;
- des fonctionnalités du serveur proxy consistant à enregistrer automatiquement l'ensemble des pages WEB consultées par le personnel. Celles-ci sont mises en place dans le but de surveiller l'utilisation d'internet par le personnel de la banque car l'homme constitue la plus grande source de risques ;
- un système de messagerie afin de conserver une trace de tous les messages reçus et envoyés (e-mails) par les employés de la banque. Ceci a été fait dans le but de respecter le principe de non-répudiation. A tout moment, il est possible de retracer les opérations effectuées par un agent ;

- un système de cryptage des informations à travers l'usage des clés pour éviter que les informations qui sortent de la banque ne soient interceptées et utilisées par une personne externe (sécurisation des données en transit) ;
- un pare-feu visant à empêcher tout agent de se connecter au réseau de la banque à partir d'un réseau externe à celle-ci ;
- une solution antivirale afin de protéger le système contre les attaques dues aux virus informatiques. Cette solution est mise à jour régulièrement ;
- une protection visant à empêcher tout agent d'opérer un transfert de fichier à partir d'une clé USB sur l'un des postes du service informatique ;
- une procédure de mise en veille des machines non utilisées dans un délai très court (le délai ne peut être communiqué par souci de confidentialité) afin d'éviter le risque de vol de données ;
- des connections exclusivement par câble afin d'éviter des intrusions liées aux réseaux internet ;
- un système d'alerte visant à prévenir les attaques par des vers informatiques ;
- un système de mot de passe/login pour toute ouverture d'une session utilisateur ;
- une protection du réseau informatique contre les intrusions (hacker).

CONCLUSION DU CINQUIEME CHAPITRE

Ce chapitre a reposé principalement sur la description du dispositif de maîtrise des risques informatiques de la BAS et sur la présentation de ses objectifs. Ce dispositif est construit autour d'un cadre institutionnel et organisationnel, d'une méthodologie de gestion des risques et des contrôles.

Le cadre institutionnel et organisationnel regroupe d'une part, les politiques et procédures écrites à savoir la politique de sécurité du système d'information, la politique informatique et la charte informatique et d'autre part, les structures de gestion des risques (le Comité de Risque, le Directeur Général, le RSSI, le responsable IT, le responsable du contrôle permanent et le Directeur d'Audit Interne).

La méthodologie de gestion des risques regroupe la méthode d'identification et d'analyse des risques et l'établissement d'une cartographie des risques. Quant aux contrôles mis en place au niveau du dispositif, ils sont constitués des contrôles organisationnels, physiques et logiques.

La suite de ce travail consistera à présenter la contribution de l'audit interne à la maîtrise des risques informatiques de la BAS ainsi que son analyse.

CHAPITRE 6 : PRESENTATION ET ANALYSE DE L'APPORT DE L'AUDIT INTERNE DE LA BAS A LA MAITRISE DES RISQUES INFORMATIQUES ET RECOMMANDATIONS

Dans le présent chapitre, nous nous sommes intéressés principalement au rôle de l'audit interne dans le dispositif de maîtrise des risques informatiques décrit dans le précédent chapitre. Les informations présentées dans ce chapitre ont été recueillies à partir d'un entretien effectué avec le Directeur de l'Audit interne de la BAS sur la base d'un guide d'entretien (voir annexe n°4, page 107).

Ainsi, après avoir présenté le plan d'audit de la BAS, nous présenterons les différentes contributions de l'audit interne de la BAS dans le cadre de la maîtrise des risques informatiques. Aucune œuvre humaine n'étant pas parfaite, il consistera ensuite pour nous, d'analyser cette contribution afin de ressortir des manquements et d'y formuler des recommandations en vue de leurs corrections.

6.1. Plan d'audit interne de la BAS

Les auditeurs internes de la BAS mènent leurs activités sur la base d'un plan d'audit interne quinquennal soumis à l'inspection générale du groupe (quatrième niveau de contrôle) pour validation avant leur approbation par le CA de la filiale sur proposition du Comité d'Audit. Ensuite, ce plan est décliné en plan d'audit annuel. Le tableau ci-dessous nous donne un aperçu du plan d'audit interne de la BAS.

Tableau 5 : Exemple de plan d'audit interne de la BAS

ESQUISSE DU PLAN D'AUDIT QUINQUENNAL	Année N	Année N+1	Année N+2	Année N+3	Année N+4
MISSIONS D'AUDIT PAR THEMATIQUE					
Audit de la DFC	✓	✓			

Audit des moyens généraux		✓			
Audit de l'activité monétique	✓				
Audit de département juridique et compliance	✓		✓		✓
Audit de la sécurité physique et informatique	✓				✓
Audit de la gestion des habilitations	✓				✓
Audit de la direction des opérations	✓	✓	✓	✓	✓
Audit du risque de crédit	✓		✓		✓
Audit de la gestion de a trésorerie	✓				
MISSION D'AUDIT DE CONFORMITE					
Ensemble des agences de la Banque Atlantique du Sénégal	✓	✓	✓	✓	✓
SUIVI DES RCOMMANDATIONS					
REPORTING					

Source : Nous-mêmes inspiré du plan d'audit quinquennal de la BAS (2010).

Au sein de la Direction Audit Interne, le déroulement des missions se fait sur la base d'un plan de mission établi par le Directeur d'Audit Interne de la BAS. En effet, il élabore un programme annuel d'audit couvrant le cycle des investigations. Ce programme est également soumis à l'inspection générale du groupe pour validation avant leur approbation par le CA de la filiale sur proposition du Comité d'Audit.

L'élaboration du plan d'audit interne est faite sur la base d'une évaluation annuelle des risques de l'année précédente et ne prévoit pas de missions d'audit au niveau du service informatique de façon régulière.

6.2. Apport de l'audit interne de la BAS dans la maîtrise des risques informatiques

L'apport de l'audit interne dans la maîtrise des risques informatiques de la banque se retrouve dans ses principales missions, seul ou conjointement avec des cabinets, mais aussi à travers sa collaboration avec les autres acteurs de la maîtrise des risques informatiques.

6.2.1. Apport de l'audit interne à travers ses missions

A ce niveau, l'apport de l'audit interne dans la maîtrise des risques se trouve principalement dans ses travaux de vérification portant sur le dispositif de maîtrise des risques informatiques et des recommandations qu'il formule.

En effet, la Direction d'Audit Interne de la BAS conjointement avec un cabinet de renom dont le nom est tenu confidentiel ont procédé quelque fois à une revue des contrôles généraux informatiques sur les domaines suivants :

- l'accès aux applications et aux données ;
- l'évolution des systèmes ;
- l'exploitation informatique (les usages qui se font des ressources informatiques);
- l'informatique des utilisateurs finaux.

Cette intervention visait à acquérir une meilleure compréhension des procédures et des systèmes concourant à la production de l'information, et à confirmer que les dispositions essentielles qui ont été prises en matière de contrôle interne afin d'assurer une fiabilité raisonnable des informations traitées.

Certains tests de conception et d'efficacité sur les contrôles généraux informatiques ont également été effectués par le cabinet exclusivement à savoir le test sur la procédure de droit d'accès et le test sur le système de messagerie.

L'approche adoptée reposait principalement sur les informations collectées au travers d'entretiens avec le service informatique et certains utilisateurs clés et sur la revue documentaire. L'accomplissement de cette mission a nécessité de vérifier l'existence des thématiques suivants :

- la politique de sécurité informatique ;
- la gestion de la sécurité physique (accès et moyens de protection environnementale) ;
- la séparation des tâches incompatibles ;
- la gestion des accès des utilisateurs et des administrateurs (création, modification, suppression et revue des accès) ;
- la gestion des sauvegardes de données ;
- la protection antivirus.

L'examen de chacune de ces thématiques a reposé sur une comparaison de leur contenu avec les bonnes pratiques en la matière notamment la norme ISO 27 005[14]. Ainsi, concernant la politique de sécurité informatique, il a été question de vérifier si la politique de sécurité informatique comporte les quatre (04) rubriques que sont : la politique de gestion des risques informatiques clairement définie avec leurs stratégies de mitigation, la classification de l'information destinée à attribuer le niveau de protection correspondant, la conformité des systèmes avec la règlementation en vigueur et enfin le volet sensibilisation de l'ensemble des utilisateurs. Les insuffisances qui ont été relevées à ce niveau ont fait l'objet de recommandations.

En ce qui concerne la sauvegarde des données, il a été question de vérifier si le délai de sauvegarde des données est conforme à ce qui a été prévu par les procédures. Pour confirmer le respect du système de sauvegarde, un échantillon a été prélevé par le cabinet afin d'effectuer un test de sauvegarde.

[14] Norme des séries ISO 27 000 et relatives au Management des risques.

La vérification antivirale consistait exclusivement à se rassurer de son existence, l'existence d'une licence et de la fréquence de sa mise à jour.

Par ailleurs, le déroulement des autres contrôles s'est fait avec attribution d'un niveau aux risques. Les recommandations de ce tableau ont été formulées au regard des insuffisances qui ont été relevées. Le tableau ci-dessous donne une vue des contrôles et des recommandations formulées compte tenu des faiblesses qui ont été relevées par l'audit interne et le cabinet.

Tableau 6 : Les contrôles effectués sur le dispositif de maîtrise des risques informatiques

CONTRÔLES	NIVEAU DE RISQUE	RECOMMANDATIONS
Vérifier si la matrice de séparation des tâches destinée à assurer la cohérence des droits d'accès attribués aux comptes utilisateurs avec leurs degrés de responsabilités est définies	Elevé	Formaliser totalement une matrice de séparation des taches définissant les incompatibilités en accord avec la structure organisationnelle de la BAS
Vérifier l'existence d'une procédure de gestion des mots de passe	Elevé	Renforcer la procédure de gestion des mots de passe
S'assurer de l'existence d'une procédure de gestion des droits d'accès relatifs aux comptes réseau et le système d'information bancaire.	Elevé	Formaliser totalement une procédure des droits d'accès des comptes génériques en cas d'impossibilité de leur suppression
Vérifier l'existence et la pertinence d'une charte d'utilisation des ressources informatiques (politique informatique).	Moyen	Inclure dans la charte, les clauses de non diffusion de mots de passe, d'installation de programmes non autorisés, d'utilisation d'internet et de la messagerie électronique.

S'assurer de l'existence d'une procédure de suppression des comptes utilisateurs dans le système d'information de la banque une fois l'agent ayant quitté la BAS.	Elevé	Formaliser une procédure de suppression des comptes dans SI de la banque et prévoir dans la procédure une revue régulière des comptes actifs pour tous les utilisateurs de la BAS.

Source : Nous-mêmes inspiré du rapport IT Risk (2010).

Les recommandations formulées à ce niveau sont destinées à renforcer les composantes du dispositif de maîtrise des risques informatiques de la BAS. Le niveau de risque présenté dans ce tableau a été fixé compte tenu des anomalies relevées et du niveau d'importance accordée à l'objet de la vérification.

Aussi, les auditeurs internes de la BAS ont été associés à certains projets informatiques tenus confidentiels au cours desquels il a été de leur ressort d'identifier les risques informatiques au fur et à mesure qu'ils se présentaient. L'ensemble des nouveaux risques identifiés ont servi à enrichir la cartographie des risques informatiques.

Par ailleurs, au cours des six (06) derniers mois, deux (02) missions se sont déroulées dans le cadre de la maîtrise des risques informatiques. La première a été réalisée par un cabinet externe avec l'implication des auditeurs internes de la BAS. La deuxième mission relative au contrôle des niveaux d'habilitations des agents de la BAS a été effectuée par les auditeurs internes de la banque.

En effet, cette dernière mission a consisté pour l'audit interne de la banque à vérifier si les niveaux d'habilitations octroyés aux différents agents de la banque étaient en conformité avec leurs profils de poste. De plus, dans le cadre de l'exercice de leurs activités d'assurance et de conseil, l'audit interne se rassure que l'attribution des mots de passe est conforme à la stratégie d'attribution des mots de passe définie dans la politique de sécurité informatique. En effet, l'attribution des mots de passe ou encore la gestion des accès constitue un risque informatique significatif au sein de la BAS compte tenu de la clause de confidentialité qui repose sur la banque.

6.2.2. Apports de l'audit interne à travers ses relations avec les autres acteurs de la maîtrise des risques informatiques

L'apport à ce niveau se situe dans les relations que l'audit interne entretient avec les autres acteurs de la maîtrise des risques informatiques. La plupart du temps, il s'agit des conseils ou recommandations formulées. Dans cette section, nous présenterons les relations entre l'audit interne et le service informatique d'une part, l'audit interne et la Direction Générale d'autre part, et enfin, la relation entre l'audit interne et le contrôle permanent.

6.2.2.1. Relation audit interne et service informatique dans le cadre de la maîtrise des risques

L'informatique n'est plus un outil accessoire mais indispensable aux auditeurs internes de la BAS. Quotidiennement, ils recourent aux instruments et matériels informatiques à l'instar des machines, logiciel dans l'exercice de leurs fonctions.

Il existe une coordination entre les travaux de l'audit interne et ceux du service informatique. La Direction d'Audit Interne en collaboration avec le service informatique veille constamment à améliorer les niveaux de contrôle qui doivent garantir :

- la mise à jour quotidienne des habilitations du personnel de la banque ;
- l'impossibilité pour un agent d'accéder à distance au système d'information de la BAS à partir d'un poste externe à celle-ci sans être identifié ;
- l'existence d'un programme de maintenance des machines afin d'éviter le risque de détérioration des machines.

6.2.2.2. Relation l'audit interne et le contrôle permanent dans la maîtrise des risques

Rappelons que la principale différence entre le contrôle permanent et l'audit interne au sein de la BAS est la périodicité d'intervention. En effet, le contrôle permanent effectue les contrôles de façon continue tout au long du processus de maîtrise des risques informatiques alors que le l'audit interne n'intervient que périodiquement. Néanmoins, il peut arriver que l'audit interne effectue une mission non prévue par le plan d'audit interne sur demande expresse du Directeur Général ou en cas de fraude au niveau d'un département ou service.

Ainsi, compte tenu de la fréquence de ses missions, l'audit interne vérifie les travaux effectués par le contrôle permanent dans le but de s'assurer que les plans d'action mis sur pieds par le contrôle permanent pour maîtriser les risques informatiques sont efficaces et efficients. Aussi, dans le cadre de ses missions au niveau du service informatique, l'audit interne se sert parfois des travaux qui ont déjà été réalisés par le contrôle permanent, notamment les points de dysfonctionnement qui ont été relevés afin d'orienter sa mission. Dans la majorité des cas, ces points de dysfonctionnement font l'objet d'une réévaluation par l'audit interne avant le début de toute activité. Il est important de préciser ici que pour l'audit interne, le choix des contrôles à réaliser se fait selon une démarche par les risques et non par les processus pour voir si les risques informatiques sont maîtrisés.

La principale valeur ajoutée à ce niveau se trouve dans la vérification (revue) de l'efficience et de l'efficacité des plans d'action mis sur pieds pour maîtriser les risques informatiques. Aussi, puisque ces plans d'action se trouvent dans la cartographie des risques, cela implique que l'audit interne contribue à l'amélioration de la cartographie des risques informatiques de la BAS.

6.2.2.3. Relation audit interne et Direction Générale dans la maîtrise des risques

L'audit interne étant sous le rattachement hiérarchique de la Direction Générale, l'ensemble des recommandations notamment celles destinées à améliorer le dispositif de maîtrise des risques informatiques lui est adressé directement sans intermédiaire. Cette position hiérarchique est un avantage pour l'audit interne dans le cadre de la maîtrise des risques informatiques de la BAS et aussi dans le cadre des suivis de recommandations.

6.3. Analyse de l'apport de l'audit interne dans le dispositif de maîtrise des risques informatiques

Le but de cette section est d'analyser l'apport de l'audit interne dans la maîtrise des risques informatiques de la BAS au regard des informations figurant au cinquième chapitre et à la section précédente. Aussi, les manquements ou faiblesses qui ressortiront de cette analyse feront l'objet de recommandations de notre part en vue de leur correction régularisation.

L'analyse de la contribution de l'audit interne se fera suivant le schéma de présentation du précèdent chapitre relatif à la description du dispositif de maîtrise des risques informatiques. Ainsi, nous ferons l'analyse de l'apport par rapport :

- au cadre institutionnel et organisationnel ;
- à la méthodologie de gestion des risques ;
- aux principaux contrôles.

6.3.1. Analyse au niveau du cadre institutionnel et organisationnel

L'analyse à ce niveau sera orientée vers les éléments constituant ce cadre à savoir : les politiques et procédures écrites et les structures de gestion des risques.

6.3.1.1. Analyse de l'apport au niveau des politiques et procédures écrites

L'analyse portera sur la politique de sécurité informatique, la politique informatique, la charte informatique.

6.3.1.1.1. La politique de sécurité informatique

L'audit interne ne participe pas à l'élaboration de la procédure de sécurité informatique de la BAS en raison du respect du principe d'indépendance de sa fonction qui le lie aux autres membres de la banque. Néanmoins, une revue de cette politique est faite tous les deux (02) ans par les auditeurs internes sur la base de bonnes pratiques en la matière afin de s'assurer du niveau d'efficacité de celle-ci, c'est-à-dire de vérifier par exemple si les stratégies de mitigation des risques informatiques définies sont adéquates avec l'environnement interne et externe de la banque.

Dans certaines régions géographiques par exemple, le système d'assurance ou de coassurance n'est pas très développé et solide. Alors, il ne serait pas très judicieux d'avoir recours à ce type de réponse (partage) aux risques informatiques. Aussi, les changements environnementaux et climatiques (température, mouvements des plaques, etc.) devraient également amener le gestionnaire du risque informatique à revoir sa stratégie de traitement des risques ainsi que ses parades.

6.3.1.1.2. La politique informatique

A ce niveau, l'audit interne n'intervient également pas dans la conception de ce document. Néanmoins, une revue de cette politique est faite par les auditeurs internes tous les deux (02) ans sur la base de bonnes pratiques en la matière.

Par ailleurs, il faut préciser que l'existence d'une culture au risque informatique est un préalable pour le succès et le respect de la politique informatique. L'ensemble des agents de la banque

doivent être sensibilisé sur les enjeux d'une maîtrise des risques informatiques et de l'impact que ces risques peuvent causer sur leurs activités.

Par conséquent, l'audit interne devrait de façon concomitante s'assurer de l'existence d'un programme de sensibilisation et de formation aux risques informatiques dans la banque (cela fait référence à la relation qui devrait exister entre l'audit interne et le RSSI du groupe).

6.3.1.1.3. La charte informatique

A travers les informations recueillies, nous avons constaté que l'audit interne ne participe pas à la conception de la charte du service informatique de la BAS en raison du respect de son principe d'indépendance. Néanmoins, aucune revue de cette charte informatique n'est faite par l'audit interne afin de s'assurer de la conformité de celle-ci avec les bonnes pratiques en la matière (bonnes pratiques du COBIT par exemple).

6.3.1.2. Analyse de l'apport au niveau des structures de gestion des risques

L'analyse sera relative au Comité de Risque et aux relations entretenues par l'audit interne et les autres acteurs de la maîtrise des risques.

6.3.1.2.1. Le Comité de Risque de la BAS

Les auditeurs internes de la BAS font partie de ce comité. En effet, la participation des auditeurs internes à ce comité est l'occasion pour eux d'apporter un plus qui contribue à la création de la valeur ajoutée. Les principaux apports effectués par l'auditeur interne ici sont orientés vers la gouvernance d'activité développée par le COBIT.

6.3.1.2.2. Relations avec les autres acteurs de la maîtrise des risques informatiques

Les relations qu'entretiennent les auditeurs internes de la BAS avec les autres acteurs de la maîtrise des risques sont de nature à renforcer ce dispositif. En effet, les relations entretenues par la Direction Audit Interne avec le service informatique, le contrôle permanent et la Direction Générale impactent positivement le dispositif de maîtrise des risques informatiques sur certains points du dispositif de maîtrise des risques. En effet, elles permettent :

- l'enrichissement de la cartographie des risques informatiques par identification de nouveaux risques ;
- la revue des plans d'action mis sur pieds pour maîtriser les risques informatiques ;

- l'adéquation entre le niveau d'habilitation des différents agents et leurs fiches de postes, et sa revue quotidienne ;
- la mise à jour quotidienne des habilitations du personnel de la banque ;
- l'impossibilité pour un agent de se connecter au système d'information de la BAS à distance ou à partir d'un poste externe à la banque sans être identifié ;
- l'existence d'un programme de maintenance des machines afin d'éviter le risque de détérioration des machines.

Par ailleurs, la relation entretenue par l'audit interne avec la Direction Générale est également de nature à renforcer le dispositif de maîtrise des risques informatiques de la BAS, principalement en raison de la position hiérarchique qui existe entre eux. En effet, plus la Direction Audit Interne est rattachée au plus haut niveau hiérarchique dans une organisation, plus cela favorise son indépendance, l'efficacité de ses travaux et la prise en compte de ses recommandations.

Nous n'avons relevé aucune relation particulière entre les auditeurs internes et le responsable de la sécurité des systèmes d'information.

6.3.2. Analyse au niveau de la méthodologie de gestion des risques

La contribution de l'audit interne est assez forte à ce niveau. En effet, à travers ses missions et ses relations, les auditeurs internes procèdent à l'identification des risques informatiques et à la revue de l'efficience et de l'efficacité des plans d'action qui figurent dans la cartographie des risques. Cependant, précisons que ces contrôles sont ceux relatifs à la partie physique du dispositif de maîtrise des risques informatiques. L'audit interne n'intervient pas dans le processus d'analyse et d'évaluation des risques. Cela est de la responsabilité du contrôle permanent.

En ce qui concerne les stratégies de mitigation des risques, le Directeur d'Audit Interne grâce à sa participation au Comité de Risque influence le choix de la stratégie d'intervention à travers ses conseils.

6.3.3. Analyse de l'apport de l'audit interne par rapport aux contrôles

L'analyse de la contribution se fera selon qu'il s'agit des contrôles organisationnels, physiques ou logiques.

6.3.3.1. Analyse par rapport aux contrôles organisationnels

L'analyse ici se fera au regard de la séparation des tâches incompatibles, de la protection du matériel de bureau, de la gestion des accès logiques et de la sauvegarde des données.

6.3.3.1.1. La séparation des tâches incompatibles

L'audit interne s'assure que la structure organisationnelle telles que définie par la Direction Générale de la BAS est bien celle qui existe au sein du service informatique. Aussi, dans l'exercice de ses activités d'assurance, les auditeurs internes s'assurent que le principe de séparation des tâches incompatibles tel que défini est respecté dans ce service de façon continue (existence d'une matrice de séparation des tâches).

Néanmoins, nous pensons que ces vérifications effectuées par les auditeurs internes ne sont pas suffisantes.

En effet, au cours de ces contrôles, les auditeurs internes utilisent généralement les fiches de postes qui ont été établies, l'observation physique du fonctionnement du service informatique et les informations issues des entretiens avec les principaux concernés. A partir de cette démarche, nous pensons qu'il est impossible pour l'auditeur interne de pouvoir s'assurer concrètement de la séparation des tâches entre celui qui assure la sécurité du réseau de celui qui en assure son exploitation. Cela requiert un contrôle logique approfondi. Dans le milieu bancaire, plusieurs malversations ou scandales financiers ont déjà eu lieu du fait de cette incompatibilité.

6.3.3.1.2. La protection du matériel de bureau

Ici, ce contrôle est effectué par les opérationnels et n'est pas de la responsabilité des auditeurs internes.

6.3.3.1.3. La gestion des accès logiques

La procédure d'attribution des niveaux d'habilitations au sein de la banque est revue par les auditeurs internes de la BAS afin de s'assurer de l'adéquation entre le niveau d'attribution accordé aux différents agents et leurs fiches de postes.

La procédure d'attribution des droits d'accès repose principalement sur l'octroi d'un mot de passe à chaque agent de la banque. Dans le cadre de cette procédure, les auditeurs internes

s'assurent que tous les agents nouvellement recrutés se font attribuer un mot de passe dans la banque dont le format est identique à la stratégie de mot de passe de la banque.

Cependant, rappelons que cette vérification est limitée chez les auditeurs internes. En effet, l'insuffisance d'expertise technique empêche ceux-ci de pouvoir s'assurer que la procédure de création de mots de passe respecte les directives qui ont été définies à la BAS.

6.3.3.1.4. La sauvegarde des données

L'audit interne a eu à effectuer des contrôles à ce niveau. Le contrôle visait à s'assurer qu'une sauvegarde était effectuée chaque jour dans un serveur prévu à cet effet. Pour ce faire, le contrôle a consisté pour les auditeurs internes à faire des simulations de sauvegarde à partir d'un échantillon test choisi. Toutefois, la principale limite de ces contrôles réside dans le fait qu'il est impossible pour eux, de vérifier qu'il n'y a pas d'écrasement (remplacement automatique d'une donnée par une autre) au moment de la sauvegarde d'une part, et d'autre part, que les données sauvegardées sont dupliquées comme le préconise la procédure.

6.3.3.2. Analyse de l'apport par rapport aux contrôles physiques

L'apport effectué par les auditeurs internes dans cette catégorie se trouve à plusieurs niveaux. En effet, les auditeurs internes de la BAS s'assurent que :

- la salle informatique de la banque est dotée de dispositifs de protections environnementaux tels que le paratonnerre et les prises terres ;
- les personnes accédant à la salle informatique sont identifiées au préalable et portent un badge ;
- la salle informatique est doté d'un climatiseur fonctionnant en continu afin d'éviter le risque de détérioration des ordinateurs et autres matériels informatiques dus à l'hygrométrie ;
- les machines sont équipées d'un onduleur afin de prévenir la destruction des machines du fait des coupures de courant ;
- les serveurs, routeurs, commutateurs et modems se trouvent toujours dans une salle ou une armoire verrouillée ;
- le programme de maintenance des machines est respecté afin d'éviter tout risque de détérioration des machines.

6.3.3.3. Analyse par rapport aux contrôles logiques

La contribution des auditeurs internes par rapport aux contrôles logiques est généralement effectuée avec l'assistance d'un cabinet externe spécialisé dont le nom est tenu confidentiel. Ainsi, les contrôles opérés par l'audit interne conjointement avec le cabinet ont consisté à :

- s'assurer de la surveillance du réseau informatique destiné à détecter les pannes, à déceler les engorgements et à répartir les charges informatiques ;
- s'assurer que les fonctionnalités du serveur proxy destinés à enregistrer automatiquement l'ensemble des pages WEB consultées par le personnel de la banque ;
- s'assurer que le système de messagerie installé conserve une trace des messages reçus et envoyés (e-mails) par les agents ;
- s'assurer de l'impossibilité pour un agent de se connecter au réseau de la banque à partir d'un réseau externe de la banque ;
- s'assurer que le système d'alerte destiné à prévenir les attaques par des vers informatiques est installé ;
- s'assurer de la protection du réseau informatique contre les intrusions (hacker) ;
- vérifier que les agents n'utilisent pas les réseaux sans fil dans le souci d'éviter les intrusions liées aux réseaux Internet.

Toutefois, précisons que bien que les auditeurs internes soient la plupart du temps assistés à ce niveau, il existe néanmoins des contrôles exclusivement faits par le cabinet. Il s'agit de :

- la vérification de la protection des réseaux internes de la banque contre les attaques extérieures venant d'Internet, de filtrage des communications internes/externes, d'authentification des personnes qui se connectent et de contrôle d'accès des agents de la banque ;
- la vérification du système de cryptographie du service informatique.

Cette analyse, nous a permis de relever un certain nombre de forces et faiblesses relatives à l'apport de l'audit interne dans la maîtrise des risques informatiques. Le bilan de cette analyse fera l'objet du point suivant.

6.4. Bilan de l'analyse de la contribution de l'audit interne à la maîtrise des risques informatiques de la BAS

Cette partie consiste principalement à présenter un récapitulatif des forces et faiblesses issues de notre analyse. La présentation de ces derniers se fera au moyen du tableau des forces et faiblesses.

Tableau 7: Les forces et les faiblesses de la contribution de l'audit interne à la maîtrise des risques informatiques

Bilan / Eléments		FORCES	FAIBLESSES
Contribution de l'audit interne au niveau du cadre institutionnel et organisationnel	Politique de sécurité informatique	- non implication de l'audit interne dans la conception de la charte informatique ; - revue de la politique de sécurité informatique.	
	Politique informatique	- non implication de l'audit interne dans la conception de la charte informatique ; - revue de la politique informatique.	
	Charte informatique	- non implication de l'audit interne dans la conception de la charte informatique.	- absence de revue de la charte informatique.
	Comité de Risques	- participation de l'auditeur interne au Comité de Risques.	
	Relations avec les acteurs de la	- adéquation entre le niveau d'habilitation des différents agents avec leurs fiches de postes, et sa revue quotidienne ;	

	maîtrise des risques informatiques	- mise à jour quotidien des habilitations du personnel de la banque ; - impossibilité pour un agent de se connecter au système d'information de la BAS à distance ou à partir d'un poste externe à la banque sans être identifié ; - existence d'un programme de maintenance des machines afin d'éviter le risque de détérioration des machines ; - rattachement hiérarchique entre l'audit interne et la Direction Générale.	
Contribution de l'audit interne au niveau de la méthodologie de gestion des risques	Méthode d'identification des risques	- conseils aux différents métiers.	
	Etapes de la gestion des risques	- identification de nouveaux risques ; - influence sur le choix de la stratégie de mitigation.	
	Cartographie des risques	- enrichissement de la cartographie des risques informatiques par identification de nouveaux risques ;	- absence de contrôles approfondis sur l'efficacité et l'effectivité des plans d'action relatifs à la partie logique du dispositif.

		- revue des plans d'action mis sur pieds pour maîtriser les risques informatiques (plus partie physique du dispositif).	
Contribution de l'audit interne au niveau des contrôles	Contrôles organisationnels	- comparaison entre la structure organisationnelle mise en place et la structure organisationnelle défini dans la politique de sécurité informatique ; - contrôle de la matrice de séparation des tâches incompatibles ; - revue de la procédure d'attribution des niveaux d'habilitations ; - vérification de l'existence d'une procédure de gestion des mots de passe ; - vérification de l'existence de revue formalisée des droits d'accès relatif aux comptes réseau et le système d'information bancaire ; - vérification de l'existence d'une procédure de suppression des comptes utilisateurs dans le système d'information de la banque une fois l'agent ayant quitté la BAS ;	- absence de contrôles approfondis afin de s'assurer de la séparation des tâches entre la personne en charge la sécurité du réseau de celui qui en assure son exploitation du réseau ; - absence de suivi des modifications non autorisées de programmes ou de paramètres liés à la gestion des mots de passe ; - absence de contrôles approfondis visant à s'assurer qu'il n'y a pas d'écrasement des données au moment des sauvegardes ; - absence de contrôles approfondis afin de s'assurer que l'ensemble des données sauvegardées sont dupliquées.

		- vérification d'une sauvegarde journalière des données de la banque.	
	Contrôles physiques	- la salle informatique de la banque est dotée de moyens de protection environnementaux tels que le paratonnerre et les prises terres ; - l'ensemble des personnes pouvant entrer dans le service informatique sont identifiées au préalable et portent un badge ; - le service informatique est doté d'un climatiseur fonctionnant en continu afin d'éviter le risque de détérioration des ordinateurs et autres matériels informatiques dus à l'hygrométrie ; - toutes les machines sont équipées d'un onduleur afin de prévenir la destruction des machines du fait des coupures de courant ; - les serveurs, routeurs, commutateurs et modems se trouvent toujours dans une salle ou une armoire verrouillée ;	

		- le programme de maintenance des machines est respecté afin d'éviter tout risque de détérioration des machines.	
	Contrôles logiques ou techniques	- contrôle de la surveillance du réseau informatique destiné de détecter les pannes, de déceler les engorgements et à repartir les charges informatiques ; - contrôles sur les fonctionnalités du serveur proxy de la banque destinés à enregistrer automatiquement l'ensemble des pages WEB consultées par le personnel de la banque ; - contrôle du système de messagerie installé visant à conserver une trace des messages reçus et envoyés (e-mails) par les agents ; - contrôle de la possibilité pour un agent de se connecter au réseau de la banque à partir d'un réseau externe de la banque ; - contrôle sur système d'alerte destiné à prévenir les attaques par des vers informatiques ;	- absence de contrôle visant à s'assurer de la protection des réseaux internes de la banque contre les attaques extérieures venant d'Internet, de filtrage des communications internes/externes, d'authentification des personnes qui se connectent et de contrôle d'accès des agents de la banque ; - absence de contrôle sur le système de cryptographie du service informatique.

		- contrôle visant à s'assurer de la protection du réseau informatique contre les intrusions (hacker).	

Source : Nous-mêmes.

6.5. Recommandations

A partir des analyses effectuées au précédent point et des informations tirées du dispositif de maîtrise des risques informatiques, plusieurs faiblesses ont été relevées. Ainsi, nous nous permettons de formuler des recommandations en vue de leurs corrections.

La nature des recommandations formulées dans cette section sont de trois (03) types et réparties en cinq (05) points. La première est destinée à corriger les faiblesses relevées au niveau de l'apport des auditeurs internes de la BAS dans la maîtrise des risques informatiques compte tenu de ses composantes, la seconde est destinée à optimiser le dispositif de maîtrise des risques informatiques et la troisième est relative à l'organisation de l'audit interne.

6.5.1. Recommandation relative au cadre institutionnel et organisationnel

Concernant les faiblesses relatives au cadre institutionnel et organisationnel, nous proposons aux auditeurs internes d'intégrer dans le plan d'audit une revue périodique de la charte informatique.

6.5.2. Recommandation relative à la méthodologie de gestion des risques

Concernant les faiblesses de l'apport de l'audit interne dans cette composante, nous proposons aux auditeurs internes d'effectuer des contrôles approfondis sur l'efficacité et l'efficience des plans d'action figurant dans la cartographie des risques et relatifs à la partie logique du dispositif.

6.5.3. Recommandations relatives aux contrôles

Les recommandations seront formulées selon qu'il s'agit des contrôles organisationnels ou logiques.

6.5.3.1. Recommandations relatives aux contrôles organisationnels

Nous proposons à l'audit interne :

- d'effectuer des contrôles approfondis afin de s'assurer de la séparation des tâches entre la personne en charge la sécurité du réseau de celui qui en assure son exploitation du réseau ;

- de procéder à un suivi des modifications non autorisées de programmes ou de paramètres liés à la gestion des mots de passe ;
- d'effectuer des contrôles approfondis visant à s'assurer qu'il n'y a pas d'écrasement des données au moment des sauvegardes ;
- d'effectuer des contrôles approfondis afin de s'assurer que l'ensemble des données sauvegardées sont dupliquées.

6.5.3.2. Recommandations relatives aux contrôles logiques

A ce niveau, nous proposons à l'audit interne de la banque :

- d'effectuer des contrôles visant à s'assurer de la surveillance du réseau informatique destiné à détecter les pannes, à déceler les engorgements et à répartir les charges informatiques ;
- d'effectuer des contrôles approfondis sur le système de cryptographie du service informatique ;
- d'effectuer des contrôles du système d'alerte destiné à prévenir les attaques par des vers informatiques ;
- d'effectuer des contrôles visant à s'assurer de la protection du réseau informatique contre les intrusions.

6.5.4. Recommandations en vue d'optimiser le dispositif de maîtrise des risques informatiques

Les recommandations formulées à ce niveau sont adressées au Directeur Général. Ainsi, nous lui proposons :

- d'aménager complètement la salle de machine tout en mettant en place les mécanismes nécessaires de protection des équipements contre les pannes, les dégâts dus aux eaux (installation de faux plancher) ;
- d'impliquer le Risk Manager dans le processus de maîtrise de risques informatiques afin de renforcer les processus de maîtrise des risques informatiques ;
- de formaliser un référentiel de gestion des risques informatiques notamment le COBIT. En effet, il consistera à mette en place les bonnes pratiques du COBIT au regard de ses 34 processus et de ses 318 objectifs tout en les adaptant au contexte de la BAS ;
- d'élaborer des procédures de gestion des équipements à distance ;
- de mettre en place un système de reporting des incidents de sécurité ;

- d'élever le niveau des exigences et des spécifications de contrôle interne au regard du niveau des performances attendues ;
- de formaliser les tests de sauvegardes et de restaurations.

6.5.5. Recommandations relatives à l'organisation de la Direction Audit Interne

Nous proposons à l'audit interne de :

- développer ou acquérir au sein du Département de l'Audit Interne, les compétences en sécurité logique du système d'information. Cela constituerait un facteur clé de succès de l'accroissement des performances au plan individuel et collectif ;
- prévoir dans le plan d'audit interne des audits réguliers au niveau du dispositif de maîtrise des risques informatiques ;
- prévoir des contrôles supplémentaires sur les applications acquises, développées, mise à jour et exploitées par les utilisateurs hors de l'environnement informatique habituel de l'organisation (tableaux Excel, logiciel Access, etc.).

CONCLUSION DU SIXIEME CHAPITRE

Parvenu au terme de ce chapitre ayant porté sur la contribution de l'audit interne de la BAS dans la maîtrise des risques informatiques, il a été question pour nous de présenter tout d'abord l'apport de l'audit interne dans la maîtrise des risques informatiques, ensuite d'analyser cette contribution et enfin de formuler des recommandations.

L'apport des auditeurs internes de la banque dans la maîtrise des risques informatiques se trouve dans les missions auxquelles ils ont été associés d'une part, et d'autre part à travers les contrôles effectués dans le cadre de l'exercice de leurs fonctions. Néanmoins, cette contribution a révélé un certain nombre de faiblesses pour lesquelles nous avons proposé des recommandations.

CONCLUSION DE LA DEUXIEME PARTIE

Cette deuxième partie, réservée au cadre pratique de notre recherche, a reposé principalement sur trois (03) chapitres.

Le premier chapitre réservé à la présentation de notre entité hôte à savoir, la Banque Atlantique du Sénégal a consisté pour nous à présenter cinq (05) points primordiaux. En effet, il a été question pour nous de présenter l'historique de la BAS, ses missions, les dates et faits marquants, les produits et services qu'elle offre et enfin son organisation. Il ressort de cette présentation que cette banque reste dans un souci constant d'expansion de son réseau et d'accroissement de ses parts de marchés. Par ailleurs, elle considère sa ressource humaine comme sa première arme de réussite.

Le deuxième chapitre quant à lui a reposé sur la description du dispositif de maîtrise des risques informatiques de la banque. Au sein de la BAS, ce dispositif contient principalement trois (03) composantes à savoir une composante organisationnelle, procédurale et technique ou sécuritaire. La composante organisationnelle regroupe principalement le comité de risque, l'organisation de la fonction informatique, la séparation des tâches incompatibles et les acteurs de la maîtrise des risques. La composante procédurale regroupe la charte informatique, la politique de sécurité informatique, la politique informatique, les procédures d'attribution des niveaux d'habilitations, des droits d'accès et de sauvegarde des données et la cartographie des risques informatiques de la banque. La composante technique regroupe quant à elle le dispositif de sécurité physique et logique.

Le dernier chapitre de cette partie et également dernier de notre étude, a consisté à présenter la contribution effectuée par les auditeurs internes de la banque dans la maîtrise des risques informatiques. Aucune œuvre humaine n'étant parfaite, nous avons par la suite analysé cette contribution afin de ressortir ses forces et ses faiblesses. La dernière section de ce chapitre a consisté à formuler des recommandations relatives au cadre institutionnel et organisationnel, aux contrôles organisationnels, techniques, à l'optimisation du dispositif de maîtrise des risques informatiques et à l'organisation de la fonction audit interne.

CONCLUSION GENERALE

Parvenu au terme de notre étude, nous pouvons affirmer que l'attitude du management face à la politique et aux procédures établies liées à la maîtrise des risques est révélatrice de l'importance qu'il accorde à la sécurité.

L'objectif de cette étude était d'abord de présenter la contribution de l'audit interne à la maîtrise des risques liés au système d'information et, exclusivement des risques informatiques. Pour ce faire, nous avons construit notre travail autour de deux parties dont l'une théorique et l'autre pratique.

La partie théorique a consisté pour nous à parcourir la notion de système d'information et les éléments constituant la gestion de ses risques ainsi que les actions attendues de l'audit interne pour maîtriser ses risques informatiques.

Dans la deuxième partie, il a été question pour nous de passer en revue les pratiques en place à la banque dans la maîtrise des risques informatiques.

En somme, retenons que le système d'information de la BAS repose sur des processus quasi-informatisés. L'audit interne de la Banque Atlantique du Sénégal est impliqué dans la maîtrise des risques informatiques bien qu'il ait assez recours à des cabinets externes pour la réalisation de ses contrôles relatifs à la partie logicielle du système d'information.

Ceci s'explique certainement par le fait que les compétences en sécurité des systèmes d'information sont encore rares chez la plupart des auditeurs internes. La gestion et la maîtrise des risques informatiques demandent une connaissance transverse de l'informatique notamment en systèmes d'exploitation, réseau, programmation, en pratique de production, cryptographie, en technologies de stockage et en virtualisation pour ne citer que celles-là. Aussi, les modules dédiés à la sécurité du SI ont longtemps été peu présents dans les cursus de formation supérieure en audit des universités ou écoles de commerce il y'a quelques années.

Nous espérons que les recommandations formulées concernant d'une part, l'apport de l'audit interne au niveau du cadre institutionnel et organisationnel, de la méthodologie de gestion des risques, des contrôles logiques et d'autre part, celles visant à optimiser le dispositif et améliorer l'organisation de la Direction Audit Interne seront prises en compte par la Banque Atlantique du Sénégal.

ANNEXES

Annexe 1 : Les types de risques informatiques

	Arrêt de maintenance de logiciels par disparition de la SSII/ du fournisseur concepteur de la solution
	Divulgation des données confidentielles
	Accidents naturels
	Vandalisme sur équipement sans intrusion
	Vandalisme sur équipement avec intrusion dans les locaux
	Vol d'équipement avec intrusion dans les locaux
	Vol d'équipement sans intrusion
	Dégâts des eaux ou autre liquide
	Vol d'information (sensible ou non)
	Vol d'information et diffusion au public
	Destruction volontaire d'information
	Modification volontaire d'information
	Altération volontaire d'information
	Intrusion dans les systèmes
	Perturbation des services rendus
	Détournement d'un site, d'un service vendu (site web, contact email etc.)
	Ecoute d'information sur le réseau (intrusion réseau interne)
	Altération accidentelles des informations par l'exploitation (perte ou dégradation des données)
	Abus de pouvoir par une maintenance externe (TMA, mainteneur outrepassant droits
	Dysfonctionnement d'un matériel (panne physique)
	Dysfonctionnement d'un logiciel (panne logique)

	Dysfonctionnement d'un service externe (perte de compétence d'un tiers)
	Blocage centre informatique ou locaux métiers
	Erreur de saisie (erreur manuelle, création d'anomalie,
	Virus informatiques (attaques virale)
	Absence de données critiques (perte de données sensibles particulières)

Source : Nous-mêmes à partir de DARSA (2014).

Annexe 2: Guide d'entretien avec le responsable IT

Entité: Banque Atlantique du Sénégal	
Département /Service: Service Informatique	
Fonction: Responsable IT	
QUESTIONS	**RÉPONSES**
Quelle est l'organisation de votre service ?	
Pouvez-vous nous faire une description synoptique de l'activité de votre service ?	
Existe-t-il une coordination entre les travaux du service informatique et ceux de l'audit interne ?	
Considérez-vous que l'équipe informatique dispose d'une compétence suffisante en matière de gestion et maîtrise des risques informatiques pour pouvoir s'acquitter de manière efficace de cette tâche ?	
Quels sont les objectifs du dispositif de maîtrise des risques informatiques ?	
Qui est le gestionnaire des risques informatiques ?	
Pour quelles methodes avez vous optée dans le cadre de la gestion des risques inoformatiques? ➢ MEHARI ➢ EBIOS ➢ AUTRE ➢ AUCUNE	
Pouvez-vous nous faire une description synoptique du processus de maîtrise des risques informatiques ?	
Compte tenu du fait que la BAS n'est qu'une filiale, la maîtrise de l'ensemble des risques informatiques est-elle de votre ressort ? ➢ si non quels sont les risques qui ne sont pas gérés par votre service ?	

Pouvez-vous nous faire une description la méthodologie de gestion des risques ?	
Avez-vous une idée du rôle de l'audit interne dans la maîtrise des risques informatiques ? ➢ si oui lequel ?	
Les rapports des auditeurs internes vous aident –ils à prendre conscience des risques que vous encourez dans l'exercice de vos fonctions ?	
Les auditeurs internes vous aident-t-ils à décliner des actions pour leurs maîtrises ?	

Source : Nous-mêmes.

Annexe 3: Test d'existence du dispositif de maîtrise des risques informatiques

Entité: Banque Atlantique du Sénégal **Processus:** Maîtrise des risques informatiques	**Question de contrôle interne**			**2014-2015** **Folio :**
Objectif du questionnaire : s'assurer de l'existence d'un dispositif de maîtrise des risques informatiques				
Questions	**Oui**	**Non**	**N/A**	**Commentaires**
Un référentiel de gestion des risques informatiques existe-t-il ?		✓		
Existe-t-il une méthodologie de gestion des risques ?	✓			
Existe-t-il une politique de sécurité informatique? ➢ si oui présente-t-elle les différentes stratégies de mitigation des risques informatiques ?	✓ ✓			
Existe-t-il une charte informatique ? ➢ si oui est-elle est régulièrement mise à jour ?	✓ ✓			
Existe-t-il une politique informatique ? ➢ si oui est-elle régulièrement mise à jour?	✓ ✓			
Existe-t-il une procédure d'attribution des niveaux d'habilitations ? ➢ si oui est-elle régulièrement revue?	✓ ✓			
Existe-t-il une procédure d'attribution des droits d'accès ? ➢ si oui est-elle régulièrement revue ?	✓ ✓			
Existe-t-il une procédure de sauvegarde des données ? ➢ si oui est-elle régulièrement revue ?	✓ ✓			

Existe-t-il un programme de communication et de sensibilisation aux risques informatiques au sein de la banque ?	✓			
Les principales menaces sont-elles identifiées ?	✓			
Disposez-vous d'une cartographie des risques ? ➢ si oui, prend-elle en compte les risques informatiques ? ➢ est-elle régulièrement mise à jour régulièrement ?	✓ ✓ ✓			
Une politique de protection des réseaux est-elle mise en place ? Si oui est-elle mise à jour périodiquement ?	✓			
Est-ce qu'il existe une procédure de sauvegarde des données clairement définie ?	✓			
Existe-t-il un dispositif de sécurité physique de gestion des risques informatiques ? ➢ si oui est-elle revue périodiquement ?	✓ ✓			
Existe-t-il un dispositif de sécurité logique des risques informatique ? ➢ si oui est-elle revue périodiquement ?	✓ ✓			
Existe-t-il une matrice de séparation des tâches incompatibles ? ➢ si oui fait-elle l'objet de revue périodique ?	✓ ✓			
Disposez-vous d'un comité de gestion des risques de la banque ?	✓			
Un plan d'action de correction des risques informatiques est-il mis en place ? ➢ si oui fait-il l'objet d'une revue périodique ?	✓ ✓			

Les auditeurs internes font ils partie de ce comité ? ➢ si oui quels sont leurs rôles ?	✓ ✓			
Existe-t-il une collaboration efficace les principaux acteurs de la maîtrise des risques informatiques ?	✓			

Source : Nous-mêmes.

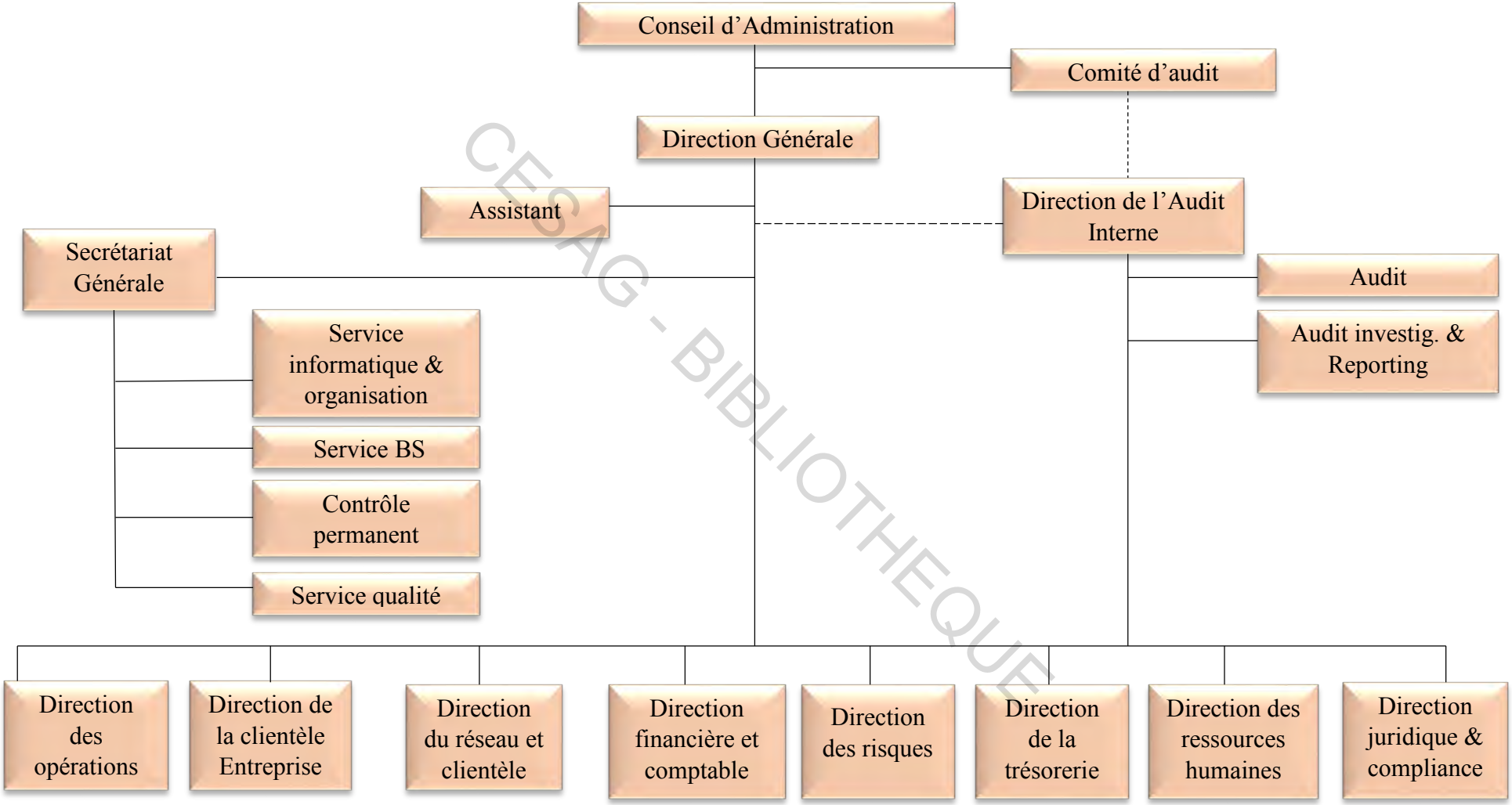
Annexe 4: Guide d'entretien avec le Directeur de l'Audit Interne

Entité : Banque Atlantique du Sénégal	
Département/Service : Département Audit interne	
Fonction : Directeur de l'Audit Interne	
QUESTIONS	**RÉPONSES**
Quelle est l'organisation de votre département ?	
Quel est le rattachement hiérarchique de votre département ?	
Votre charte d'audit tient elle compte des évolutions normatives ?	
Pouvez-vous nous faire une description synoptique de votre activité ?	
L'équipe d'audit interne bénéficie-t-elle d'un programme de formation continue adéquat ?	
Existe-t-il une coordination efficace entre les travaux de l'audit interne et ceux du service informatique ?	
Considérez-vous que l'équipe d'audit interne dispose d'une compétence suffisante en matière de gestion des risques SI pour pouvoir s'acquitter de manière efficace de cette tache? ➢ quelles sont les domaines à compléter ?	
Selon la norme 2120, l'audit interne doit évaluer l'efficacité des processus de management des risques et contribuer à leur amélioration. Dans l'exercice de votre fonction d'auditeur interne, évaluez-vous effectivement ce processus ?	
Quelle responsabilité vous a été attribuée au sein de l'entreprise en ce qui concerne la maîtrise des risques informatiques ?	
Comment décrivez-vous votre contribution dans le processus de maîtrise des risques au regard de vos activités ?	
Vous arrive-t-il de faire des tests sur ces dispositifs ?	
Quel est votre degré d'implication dans la mise en place des éléments constituant le dispositif de maîtrise des risques informatiques ?	

Quelle est votre approche pour l'élaboration de vos plans d'audit annuel ?	
Inscrivez-vous des missions d'audit des systèmes informatiques dans votre plan d'audit ? ➢ si oui à quand date la dernière mission ?	
Pouvez-vous nous parler des relations que vous entretenez avec le Directeur Général, le Responsable IT, la Responsable du Contrôle Permanent, RM et le RSSI dans le cadre de la maîtrise des risques informatiques de la banque?	
Etes-vous associé à la formation et la sensibilisation des agents sur les risques informatiques ?	
Quelle est la périodicité de vos revues des procédures des systèmes informatiques ?	
Participez-vous à la conception de la politique de sécurité informatique, de la charte informatique, de la politique informatique, de la procédure d'attribution des niveaux d'habilitations, d'attribution des droits d'accès, de sauvegarde des données et la cartographie ? ➢ procédez-vous à leur revue ?	
Comment s'assurez-vous que les risques que vous identifiez dans le cadre de votre mission sont prises en compte dans la mise à jour de la cartographie des risques ?	
Quelle est votre part de responsabilité dans la gestion des risques informatiques ?	

Source : Nous-mêmes.

Annexe 5 : Organigramme de la Banque Atlantique du Sénégal



Source : Nous-mêmes à partir de DRH-BAS (2015).

BIBLIOGRAPHIE

OUVRAGES

1. BARRY Mamadou (2009), *Audit contrôle interne,* Editions Achevé sous les presses de la Sénégalaise de l'Imprimerie, Dakar, 371 pages.
2. BARTHELEMY Bernard (2004), *Gestion des risques : méthode d'optimisation globale*, Editions d'Organisation, Paris, 409 pages.
3. BERTIN Elisabeth (2007), *Audit interne*, Editions Groupe Eyrolles, Paris, 320 pages.
4. BIZINGRE Joël, PAUMIER Joseph et RIVIERE Pascal (2013), *Référentiel du système d'information,* Editions Dunod, Paris, 317 pages.
5. CIGREF (2009), *le contrôle interne du système d'information des organisations*, Editions CIGREF, Paris 152 pages.
6. CLAUDE Pinet (2012), *10 clés pour la sécurité de l'information : ISO/CEI 27001*, Editions AFNOR, Paris, 135 pages.
7. DARSA Jean-David (2013), *La gestion des risques en entreprise : identifier, comprendre, maîtriser. Les risques économiques, stratégiques, financiers, opérationnels, juridique*, 3ème édition, Editions Gereso, Paris, 333 pages.
8. DARSA Jean-David (2014), *365 risques en entreprise : une année en risk management,* 2ème édition, Editions Gereso, Paris, 422 pages.
9. DARSA Jean-David (2013), *Les risques opérationnels de l'entreprise : un environnement toujours plus risqué ?*, Editions Gereso, Paris, 267 pages.
10. DAYAN Armand (2008), *Manuel de gestion, vol.1*, 2ème édition, Editions Ellipses/AUF, Paris, 1088 pages.
11. DELEUZE Gilles (2013), *Analyse des risques : concepts, outils, gestion, maîtrise*, Editions EMS, Paris, 339 pages.
12. DELMOND Marie-Hélène, PETIT Yves et GAUTIER Jean-Michel (2008), *Management des systèmes d'information,* 2ème édition, Editions Dunod, Paris, 249 pages.
13. DESMOULINS Nicolas (2009), *Maîtriser le levier informatique : accroitre la valeur ajouté des systèmes d'information,* Editions Pearson, Paris, 286 pages.

14. DESROCHES Alain, LEROY Alain, et VALLEE Frédérique (2007), *La gestion des risques*, 2ème édition, Editions Lavoisier, Paris, 298 pages.

15. DEYRIEUX André (2003), *le système d'information : nouvel outils de stratégie, direction d'entreprise et direction du système d'information*, Editions Maxima, Paris, 135 pages.

16. GAULTIER-GAILLARD Sophie et LOUISOT Jean-Paul (2014), *Diagnostic des risques : identifier, analyser et cartographier les vulnérabilités*, Editions Afnor, Paris, 209 pages.

17. GILLET Michelle et GILLET Patrick (2013), *Management des systèmes d'information : Manuel et Application*, 3ème édition, Editions Dunod, Paris, 497 pages.

18. GILLET Michelle et GILLET Patrick (2011), *Les systèmes d'information de A à Z,* Editions Dunod, Paris, 217 pages.

19. GRAEVE Jean de et POTIER Jean (2001), *Système d'information, Management et Acteurs,* Editions Sapienta, Paris, 135 pages.

20. GREUNING Hennie Van et BRATANOVIC Sonja Barjovic (2004), *Analyse et gestion du risque bancaire,* Editions ESKA, Paris, 384 pages.

21. HERVE Fratta, MADERS Henri- Pierre et MASSELIN Jean-Luc (2014), *Les métiers d'auditeur interne et de contrôleur permanent*, Editions Eyrolles, Paris, 345 pages.

22. IFACI (2013), *Cadre de Référence International des Pratiques Professionnelles de l'Audit Interne*, Editions Ebzone, Paris, 238 pages.

23. IFACI (2015), *Manuel d'audit interne : améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*, Editions Eyrolles, Paris, 733 pages.

24. ISACA (2011), *Manuel de préparation CISA 2011*, ISACA, USA, 505 pages.

25. LAUDON Jane et LAUDON Kenneth (2011), *Management des systèmes d'information,* 11ème édition, Editions Pearson, Paris, 631 pages.

26. MOISAND Dominique et GARNIER DE LABAREYRE Fabrice (2009), *Cobit pour une meilleure gouvernance des systèmes d'information*, Editions Eyrolles, Paris, 258 pages.

27. MONACO Laurence (2014), *Les carrés DCG 8 : Système d'information de gestion 2014-2015*, Editions Guialino, Paris, 91 pages.

28. O'BRIEN James (1995), *Les système d'information de gestion,* Editions du Renouveau Pédagogique, Montréal, 768 pages.

29. PILLOU Jean-François et CAILLEREZ Pascal (2011), *Tout sur les systèmes d'information Grandes, moyennes et petites entreprises,* 2ème édition, Editions Dunod, Paris, 189 pages.

30. Price Waterhouse Coopers et IFACI (2014), *Référentiel intégré de contrôle interne*, Editions Eyrolles, Paris, 264 pages.

31. REIX Robert, FALLERY Bernard et KALIKA Michel (2011), *Système d'information et management des risques*, 6ème édition, Editions Vuibert, Paris, 475 pages.

32. RENARD Jacques (2010), *Théorie et Pratique de l'Audit Interne,* 7ème édition, Editions d'Organisation, Paris, 469 pages.

33. RENARD Jacques (2013), *Théorie et pratique de l'audit interne*, 8ème édition, Editions Eyrolles, Paris, 453 pages.

34. SATZINGER John W, JACKSON Robert B et BURD Stephen D (2003), *Analyse et conception de systèmes d'information,* 2ème édition, Editions Renard Goulet, Paris, 705 pages.

35. SCHICK Pierre (2007), *Mémento d'audit interne*, Editions Dunod, Paris, 217 pages.

36. SCHICK Pierre, VERA Jacques, BOURROUILH PAREGE Olivier (2010), *Audit internes et référentiels de risques*, Editions Dunod, Paris, 340 pages.

37. TENEAU Gilles et AHANDA Jean-Guy, *Guide commenté des normes et référentiels*, Editions Eyrolles, Paris, 370 pages.

38. VINCENT Lacolare (2010), *Pratiquer l'audit à valeur ajoutée*, Editions AFNOR, Paris, 197 pages.

39. VOLLE Michel (2004), *Lexique du système d'information,* Club des maitres d'ouvrage des systèmes d'information & Michel VOLLE, Editions GNU Free Documentations, Paris, 23 pages.

WEBOGRAGHIE

40. AFAI et CIGREF (2005)*, Place de la gouvernance du système d'information dans la gouvernance générale de l'entreprise,* http://www.itgi-france.com.

41. AMF (2010), *Cadre de référence des dispositifs de gestion des risques et de contrôle interne,* http://www.amf-france.org.

42. AMRAE-CLUSIF(2006), *RM et RSSI: Deux métiers qui s'unissent pour la gestion des risques liés au système d'information*, https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-RM-RSSI-GESTION-DES-RISQUES.pdf.

43. ANSSI (2010), *EBIOS*, http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/.

44. CIGREF (2009), *Les référentiels de la DSI,* http://www.cigref.fr/cigref_publications/RapportsContainer/Parus2009/Referentiels_de_la_DSI_CIGREF_2009.pdf.

45. CLUSIF (2010), *MEHARI*, http://www.clusif.asso.fr/fr/production/mehari/.

46. COMMISSION BANCAIRE (2011), *Circulaire n° 003-2011/CB/C*, http://www.bceao.int/IMG/pdf/circulaire_0030001.pdf.

47. DELOITTE (2006), *Les fondamentaux du contrôle interne et de l'audit interne*, http://fr.slideshare.net/YoussefBensafi/les-fondamentaux-de-laudit-interne? http://www.rcgt.com/wp-content/uploads/2012/09/Guides-pratiques-audit-TI-Presentation-2012.pdf.

48. NIST (2002), *Risk Management guide for IT*, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.

49. THORNTON Grant et CHABOT Raymond (2012), *Présentation des guides GTAG pouvant être utilisés par un auditeur interne lors de mandats d'audit TI*,

50. ZAAFOURI Sawsen (2014), *La sécurité du matériel informatique*, https://www.securiteinfo.com/conseils/securite-physique-et-logique-du-materiel-informatique.shtml.

REVUES

51. BAPST Pierre Alexandre, BERGERET Florence (2002), Pour un management des risques orienté vers la protection de l'entreprise et la création de la valeur ajoutée (deuxième partie), *Revue française de l'audit interne,* N°162 : 31-33.