Centre Africain d'Etudes Supérieures en Gestion

Institut Supérieur de Comptabilité, de Banque et de Finance

Diplôme d'Etudes Supérieures Spécialisées en Audit et Contrôle de Gestion

Promotion 23
(2011-2012)

Mémoire de fin d'études

THEME

CONTRIBUTION DE L'AUDIT INTERNE A LA SECURITE DE L'INFORMATION EN MILIEU BANCAIRE: CAS DE ECOBANK COTE D'IVOIRE

Présenté par :

TETCHI-YAVO A. S. Stéphanie

Co Dirigé par :

BLE K. Charles
Auditeur à la BCEAO

SINIMBOU Durotimi
Consultant en Contrôle Interne

Avril 2014

DEDICACE

A mon Dieu, le Père Tout Puissant.

A mon père et ma mère Denis et Henriette TETCHI YAVO.

A mon frère et ma sœur Yves et Axelle.

REMERCIEMENTS

Permettez-moi d'exprimer ma réelle gratitude à l'endroit de :

- ✓ Monsieur Moussa YAZI, Directeur de l'Institut Supérieur de Comptabilité, de Banque et de Finance (ISCBF) du Centre Africain d'Etudes Supérieures de Gestion (CESAG) pour son encadrement et sa disponibilité ;
- ✓ Monsieur Durotimi SINIMBOU, Conseiller en contrôle interne au CTISN, pour sa disponibilité lors de la direction de mon mémoire ;
- ✓ Monsieur Charles K. BLE, Auditeur Interne à la BCEAO pour sa disponibilité à la codirection du mémoire ;
- ✓ Monsieur Charles DABOIKO, Directeur General de Ecobank Cote d'Ivoire, qui a permis mon intégration au sein de son personnel ;
- ✓ Monsieur Issa MARIKO, Directeur du Département Audit Interne de Ecobank Cote d'Ivoire, pour son accompagnement ;
- ✓ Monsieur Wilfrid AMOIKON, CISA Auditeur Interne et Maitre de stage, pour sa disponibilité, ses conseils, son soutien technique et moral ;
- ✓ Tout le corps professoral du Cesag pour la formation de qualité dont j'ai bénéficié ;
- ✓ Tout le département Audit Interne de Ecobank Cote d'Ivoire qui a su me faire travailler dans un environnement convivial d'apprentissage ;
- ✓ A toute ma famille sans laquelle je n'aurais pas joui d'une formation exemplaire au Cesag ;
- ✓ A toute la 23ème promotion du DESS Audit et Contrôle de gestion pour l'ambiance fraternelle partagée ;
- ✓ A tous ceux qui de près comme de loin m'ont soutenu dans la rédaction de ce présent mémoire.

LISTE DES SIGLES ET ABREVIATIONS

BRVM: Bourse des Valeurs Mobilières

CEDEAO: Communauté Economique des Etats de l'Afrique de l'Ouest

CI: Cote d'Ivoire

CIA: Certified Internal Auditor

CISA: Certified Information System Auditor

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

CRIPP: Cadre de Référence International des Pratiques Professionnelles

EBIOS: Expressions des Besoins et Identification des Objectifs de Sécurité

ETI: Ecobank Transnational Incorporated

IEC: International Electrotechnical Commission

IFACI: Institut Français des Auditeurs et Contrôleurs Internes

IFRS: International Financial Reporting Standards

IIA: Institute of Internal Auditors

ISA: International Society of Automation

ISACA: Information System Audit and Control Association

ISO: International Standards Organization

LSF: Loi de la Sécurité Financière

MEHARI: Méthode Harmonisée d'analyse des Risques

MPA: Modalité Pratique d'Application

OCTAVE: Operationally Critical Treat and Vulnerability Evaluation

RM: Risk Manager

RSI: Responsable de la Sécurité de l'Information

RSSI: Responsable de la Sécurité des Systèmes d'Information

SI: Système d'information

SMSI: Système de Management de la Sécurité de l'Information

SOX: Sarbanes Oxley Act

SSI: Sécurité des Systèmes d'Information

TI: Technologie de l'Information

WLAN: Wide Local Area Network

LISTE DES TABLEAUX ET FIGURES

TABLEAUX

FIGURES

LISTE DES ANNEXES

TABLE DE MATIERES

INTRODUCTION GENERALE

Parmi les structures de contrôle présentes dans l'entreprise pour notamment aider le management dans la prise de décisions, on retrouve l'audit interne. C'est une fonction communément admise comme étant un moyen à la disposition du management dans le cadre du processus de gestion des risques et d'évaluation du dispositif de contrôle interne en place. L'audit interne est défini comme 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. Historiquement orienté vers la gestion financière et comptable, son champ d'action s'est étendu à tous les domaines de l'entreprise.

Les missions de contrôle et d'évaluation de la maîtrise des activités ainsi que de conseils ont suivi l'évolution économique et la croissance des organisations. De nos jours, « le management gagnant[1] » impose l'atteinte des objectifs dans tous les domaines. L'audit interne, par son approche systématique et méthodique, accompagne les opérationnels dans l'identification et la maîtrise des risques, en vue d'atteindre les objectifs fixés par la Direction Générale. Dans le contexte actuel d'amélioration continue des technologies d'information et de communication, les risques liés aux systèmes d'information sont en général suivis de près dans les cartographies des risques des auditeurs. Dans le cadre de cette surveillance accrue, une attention particulière est accordée à la sécurité de l'information. En effet, l'information est essentielle, voire déterminante pour la pérennité de l'entreprise.

La finalité de beaucoup d'activités et d'opérations effectuées en entreprise est de produire des informations financières et opérationnelles fiables dont il faut assurer l'intégrité et la protection. Ainsi des normes internationales telles que l'ISO 27000 définissent les exigences requises pour mettre en place un système de gestion de la sécurité de l'information. Elles sont conçues pour garantir la sélection de contrôles de sécurité adéquats et proportionnels au niveau du contrôle interne établit par la structure. Elles indiquent aux entreprises les règles de protection des données permettant de garantir la confiance des parties intéressées, notamment des clients. Les

[1] *Le management gagnant* est un mix du style directif et du style participatif. L'objectif est d'arriver à combiner ces différents styles de management afin de gérer au mieux des équipes aux multiples personnalités et de permettre à chacun des acteurs de l'entreprise d'atteindre ses objectifs.

normes adoptent une approche basée sur les processus pour la création, la mise en œuvre, l'utilisation, la surveillance, l'analyse, le maintien et l'amélioration des systèmes de gestion de la sécurité de l'information.

Dans les établissements de crédit, notamment les banques, les systèmes d'informations très performants sont devenus les outils de gestion par excellence. Ils occupent une place stratégique dans le pilotage et le traitement des opérations des banques. L'évolution du monde financier et de ses règlementations, et l'importance de la gestion des flux informationnels font de ces systèmes un volet incontournable. En revanche, dans cet environnement bancaire très concurrentiel, un défaut de gestion rigoureuse de cet outil peut se révéler comme une source de vulnérabilité. La gestion des flux informationnels comporte des risques qu'il faut identifier et maitriser pour préserver la disponibilité, l'intégrité et la confidentialité des informations.

Au regard de ce constat, nous nous interrogeons sur la contribution de l'audit interne à la sécurité de l'information. Comment les auditeurs internes s'inscrivent-ils dans une dynamique de maintien et d'amélioration continue de la sécurité de l'information au sein d'une banque?

La complexité des tâches de l'auditeur interne quant à la sécurité de l'information vient dans certains cas, d'un manque de connaissance ou d'une formation inadéquate sur les systèmes d'information électroniques modernes et d'autres domaines hautement sophistiqués. Plusieurs autres raisons peuvent être évoquées : l'une pourrait être le fait que certains auditeurs ont quelque fois une tendance naturelle à ne pas changer leurs habitudes ; une autre pourrait être la peur du changement. En dehors de celles précitées, nous avons d'autres difficultés rencontrées par les auditeurs internes telles que le manque de compréhension globale des processus d'activités et le suivi inadéquat des problèmes après leur détection. L'audit interne pourrait s'avérer inefficace si la direction n'assure pas toujours un suivi approprié des problèmes décelés. On pourrait parler dans ce cas-ci d'un manque d'accompagnement du management dans le processus audit interne.

Les conséquences qui en résultent sont de plusieurs ordres :

- ✓ non détection en temps réel des risques liés aux activités du système d'information ;
- ✓ mauvaise utilisation des données nécessaires à l'évaluation des risques ;

- ✓ fraude ;
- ✓ exposition directe de la banque à des risques pouvant entrainer une interruption d'activités
- ✓ mauvaise orientation du business ;
- ✓ perte de l'image et de la crédibilité de la banque ;
- ✓ non atteinte des objectifs assignés par l'entreprise.

Pour pouvoir apprécier le rôle de l'audit interne dans la gestion de la sécurité de l'information, plusieurs solutions s'offrent à nous :

- ✓ faire une enquête sur le service d'audit interne afin de comprendre son implication et sa responsabilité dans le maintien et l'amélioration de la sécurité de l'information ;
- ✓ effectuer un examen critique du système de gestion de la sécurité de l'information ;
- ✓ établir des lignes directrices pour l'auditeur interne, lui permettant d'évaluer et de suivre promptement le maintien et l'amélioration du système de sécurité de l'information.

Une seule solution retiendra notre attention pour cette étude à savoir faire une enquête sur le service d'audit interne afin de comprendre son implication et sa responsabilité dans le maintien et l'amélioration de la sécurité de l'information. Cette solution incorpore toutes les autres car il serait impossible d'apprécier la contribution de l'audit interne dans la sécurité de l'information sans faire un examen de la sécurité de l'information et sans établir de lignes directrices que pourront suivre les auditeurs internes pour être toujours plus opérationnels.

Notre enquête doit nous permettre de répondre à cette question fondamentale : **comment l'audit interne contribue-t-il au maintien et à l'amélioration continue de la sécurité de l'information ?** De cette question principale découlent d'autres spécifiques :

- ✓ qu'est-ce que l'information ?
- ✓ Qu'est-ce que la sécurité de l'information ? de quoi s'agit-il en milieu bancaire ?
- ✓ Quels sont les risques inhérents à l'insécurité de l'information et comment y remédier ?
- ✓ Par quelle approche, l'auditeur interne s'assurera-t-il de la maitrise ou non des risques sécuritaires liés à l'information?
- ✓ Sur quels référentiels, normes ou bonnes pratiques doit-il se baser ?

- ✓ De quelles compétences et connaissances l'auditeur interne a-t-il besoin ?
- ✓ Enfin, quelles recommandations fera-il pour améliorer le dispositif de contrôle interne existant dans la banque, en vue de créer une valeur ajoutée?

Nous essayerons de répondre à toutes ces questions à travers l'étude du thème suivant : **Contribution de l'audit interne à la sécurité de l'information en milieu bancaire : cas de ECOBANK Cote d'Ivoire**.

Notre choix s'est porté sur Ecobank Cote d'Ivoire premièrement parce qu'elle nous a permis d'effectuer un stage de 3 mois en son sein ; et deuxièmement parce que c'est une banque de plus de 20 ans d'existence qui connait actuellement une croissance accélérée de par sa présence sur le marché bancaire, de par ses nouveaux produits et de par sa forte influence sur les populations de tout type de revenu et de toute profession. Pour cela, elle a choisi un système technologique de pointe qui lui permet de répondre aux besoins de la clientèle exigeante. La concurrence étant de plus en plus accrue et l'utilisation des nouvelles technologies de l'information de plus en plus complexe, Ecobank CI nécessite qu'une attention particulière soit accordée à son système de gestion de la sécurité de l'information pour lui permettre d'assurer sa pérennité. Notre étude tentera d'apporter des solutions adéquates et efficaces pour le bon fonctionnement et la continuité d'exploitation de cette banque.

Notre objectif principal par cette étude, est de connaitre et apprécier le rôle et la contribution de l'audit interne dans le maintien et l'amélioration continue de la sécurité de l'information. De cet objectif, dérivent les objectifs spécifiques suivants :

- ✓ identifier les bonnes pratiques en matière de sécurité de l'information
- ✓ mettre en exergue le type d'organisation que la banque devra mettre en place pour assurer un bon fonctionnement de son système de sécurité de l'information
- ✓ connaitre les risques relatifs à un manque de sécurité de l'information
- ✓ apprécier les caractéristiques de l'audit interne qui pourraient aider la banque à atteindre ses objectifs

Pour le développement de notre étude, nous ne nous limiterons qu'aux 11 thèmes du cadre de gestion de la sécurité de l'information selon la norme ISO 27002 et aux normes internationales

pour la pratique professionnelle de l'audit interne. Notons que cette étude ne s'abstiendra pas de faire référence au référentiel CobiT et aux recommandations pratiques établies par la commission bancaire européenne et le comité de Bâle en matière de sécurité de l'information pour une bonne gestion des institutions financières. L'étude ne prendra en compte que les aspects ressources humaines, technologie et organisationnel liés à la sécurité de l'information.

L'intérêt que revêt notre étude peut être situé à un double niveau:

- **Pour l'entreprise :** elle disposera des meilleures pratiques en termes de maintenance et amélioration continue du système de sécurité de l'information. Aussi elle saura ce dont elle a besoin en matière d'outils, de techniques et de moyens tant humains que matériels pour une bonne gestion de la sécurité de ses informations et une maitrise totale du système d'information. Cette étude éclaircira davantage le rôle que l'audit interne devra jouer afin d'aider le management dans la prise de décisions et dans l'atteinte efficace et effective des objectifs en matière de sécurité de l'information.
- **Pour nous même :** cette étude sera une occasion pour nous de confronter nos connaissances théoriques à celles pratiques acquises pendant nos moments de formation professionnelle. Il s'agira pour nous d'avoir une connaissance plus élaborée sur la gestion de la sécurité de l'information du SI bancaire et aussi sur la contribution de l'audit interne à son maintien et à son amélioration.

Pour atteindre les objectifs que nous nous sommes fixés, notre étude se fera en deux (02) grandes parties qui nous permettront :

- d'abord à travers une première partie théorique, de présenter les avis de différents auteurs qui seront contenus dans une revue de littérature ;
- ensuite nous aborderons une deuxième partie, pratique, avec Ecobank Cote d'Ivoire comme exemple d'illustration dans le but de confronter la pratique de l'audit interne dans la gestion de la sécurité de l'information dans une banque d'avec la théorie.

PARTIE 1 : CADRE THEORIQUE DE L'ETUDE

La sécurité des systèmes d'information est un domaine très vaste puisqu'elle fait appel à toutes les entités de l'entreprise et à des connaissances techniques et technologiques de pointe. L'une des forces et en même temps une problématique du monde des affaires actuel est l'évolution constante des technologies de l'information. Il est vrai que plus les technologies évoluent, plus elles offrent une plus grande mobilité aux utilisateurs et révolutionnent les habitudes et les façons de travailler. Cependant elles sont empreintes de risques de plus en plus forts. Il faudrait donc trouver des solutions de sécurité de l'information pour mieux préserver la sécurité des systèmes d'information et aussi les intérêts de l'entreprise.

Dans cette quête de solutions et bonnes pratiques de sécurité, l'entreprise dispose d'agents régulateurs et garant des dispositifs de contrôle interne tel que l'audit interne. A cet effet, des auteurs divers ont développés plusieurs théories et avis mettant en exergue le rôle de l'audit interne dans la sécurité informationnelle. Nous nous sommes par conséquent atteler à présenter ces différentes opinions dans notre cadre théorique afin de mieux apprécier le concept de l'audit interne dans la sécurité des systèmes d'information de l'entreprise.

CHAPITRE 1 : CADRE CONCEPTUEL DE L'AUDIT INTERNE ET DE LA SECURITE DE L'INFORMATION

«Parce qu'il décuple la qualité et la rapidité des décisions, le système d'information est aujourd'hui au cœur des processus, des produits et du management de l'entreprise : il est devenu un actif stratégique». Cette phrase de Deyrieux (2004) traduit bien l'importance du système d'information pour les entreprises. Pour fonctionner correctement, les entreprises doivent s'assurer de la continuité et de la qualité de service de leur système d'information. En effet le système d'information est une organisation des ressources destinées à traiter l'information, soit pour produire, soit pour piloter. Le but de la sécurité de l'information est de mettre en place des méthodes et des technologies afin d'éliminer, ou du moins de minimiser, les menaces qui planent sur le système d'information. En outre, la complexité des systèmes informatiques, leur interconnexion en réseaux internes et externes, les applications informatisées et développées à l'aide de méthodologies et techniques de pointe et leur rôle stratégique pour la survie de l'entreprise, rendent de plus en plus nécessaires les missions d'audit interne permettant de répondre aux interrogations des dirigeants d'entreprise.

L'auditeur interne doit être alerté devant l'évolution sans cesse croissante des technologies de l'information et les risques y afférent pour toute organisation qu'elle soit de grande ou de petite taille. Il va devoir appréhender cette nouvelle dimension technologique afin de mieux remplir son rôle d'informateur et de conseiller auprès de la direction générale et du conseil d'administration.

A travers différentes étapes, nous aborderons les notions d'audit interne et de sécurité de l'information. Ensuite nous établirons une relation entre ces deux concepts afin de faire ressortir la contribution de l'audit interne, de par ses missions et objectifs, au maintien de la sécurité de l'information au sein même d'un organisme de crédit notamment la banque.

1.1 Historique et cadre de référence de l'audit interne

La création de la fonction d'audit interne dans les entreprises s'inscrit dans un cadre plus général de la notion d'audit. Bertin (2007 : 17 – 18) dans son ouvrage nous décrit l'historique de l'audit interne. En effet, le précurseur de l'audit connu sous le nom de révision des comptes, a été institué par la loi du 24 juillet 1867 en France. On parlait de révision des comptes avant de lui préférer le nom « audit ». Le manuel du CIA (rédigé par l'IIA) explique que l'audit a véritablement évolué après la deuxième guerre mondiale (1945). Progressivement, le terme « audit » connu un élargissement plus qu'important. Etant premièrement axé essentiellement sur les aspects financiers et comptables, il a commencé par couvrir toutes les activités opérationnelles et stratégiques de l'entreprise. Il considérait l'image de rigueur de l'entreprise, les risques liés aux différentes activités, les politiques et plans, les instabilités de l'environnement et les complexités des paramètres de gestion et de contrôle.

Cependant les crises économiques de 1929 aux USA et l'instauration de la loi Sarbanes-Oxley (SOX) et de la LSF ont déclenché une diversité d'audit notamment l'audit interne et l'audit externe appelé également audit comptable et financier. La SOX a été établie pour règlementer et rendre obligatoire les pratiques de l'audit au sein des entreprises. Renard (2010 : 36) explique que la fonction d'audit interne n'est réellement apparue en France dans les entreprises qu'à partir de 1960 et un peu partout dans le monde à partir de 1980. Car dans un souci de réduction des charges dues à la récession économique, les entreprises en vinrent finalement à suggérer de faire assumer certains des travaux préparatoires des cabinets d'audit externes, par leur propre personnel. De plus le besoin était présent de disposer en interne d'un outil d'évaluation et d'amélioration des processus de management des risques, de contrôle et de gouvernement d'entreprise.

Aujourd'hui l'audit interne a pénétré tous les domaines, toutes les fonctions, activités, opérations, tous les stades décisionnels de l'entreprise. A travers les notions et missions de l'audit interne et les responsabilités des auditeurs internes, nous verront quel est le rôle de l'audit interne dans une organisation et en quoi est-il important.

1.1.1 Notion d'audit interne

Lacolare (2010 : 10) explique que selon les normes ISO 9000:2005 et ISO 19011:2002, l'audit est défini comme un processus méthodique, indépendant et documenté permettant d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits. En plus de lui, plusieurs comités et organismes ont tenté de donner une définition à l'audit interne.

Cependant ils s'accordent tous sur cette définition de l'IFACI, approuvée par l'IIA le 29 juin 1999 :

« 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 systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité. »

Cette définition implique l'Audit Interne dans la fonction de conseiller, de perfectionniste, d'améliorateur. Son rôle est d'assurer la bonne santé de toutes les fonctions au sein même de l'organisation.

L'audit interne est le mieux à même d'alimenter le conseil d'administration et la direction générale en informations sur les faiblesses du système de contrôle interne ou sur les zones de risques susceptibles de nuire à l'atteinte des objectifs stratégiques, opérationnels, informationnels et de conformité (Bertin 2007 : 25 – 26). Le blog SSI Conseil, dans son article sur l'audit interne du SSI, explique que dans le cadre de la sécurité ses systèmes d'information, l'audit interne est une des mesures de sécurité du Système de Management de la sécurité du SI. C'est une des clauses obligatoires de la mise en œuvre d'un SMSI conforme à l'ISO 27001 : Clause 6. Il contribue à vérifier de façon indépendante et objective :

- ✓ l'efficience des dispositions du SMSI

- ✓ l'efficacité des mesures de sécurité organisationnelles, procédurales ou techniques choisies pour réduire les risques à un niveau acceptable.

Ainsi l'audit interne est l'organe qui, mandaté par la direction, intervient pour examiner et établir un diagnostic attestant du plus ou moins bon fonctionnement de son système d'information et de son dispositif de contrôle interne. Il établit également un pronostic alertant les responsables et la direction sur la sécurité des actifs, la fiabilité des informations et aussi de l'efficacité des opérations qui en découlent.

1.1.2 Missions, Objectifs et Champ d'application de l'audit interne

L'audit interne, comme nous l'avons notifié plus haut, connait une évolution constante du fait des changements réguliers de l'environnement dans lequel il est employé. En fonction de la définition de l'audit interne, nous ferons ressortir ses missions, ses objectifs et son champ d'application pour une meilleure compréhension de son rôle au sein de l'entreprise.

1.1.2.1 Les missions

Suivant la définition de l'IFACI, l'audit interne présente 3 missions :

- ✓ **Contribuer à la création de valeur ajoutée** : selon l'IFACI (CRIPP 2013 : 72), l'audit interne apporte de la valeur ajoutée à l'organisation lorsqu'il fournit une assurance objective et pertinente et qu'il contribue à l'efficience et à l'efficacité des processus de gouvernement d'entreprise, de management des risques et de contrôle ;
- ✓ **Améliorer le fonctionnement de l'organisation** : par la réalisation de missions d'audit et d'apport de conseils ;
- ✓ **Aider l'entreprise à atteindre ses objectifs** : par l'évaluation des processus de management des risques, de contrôles et de gouvernement d'entreprise, à l'aide d'une approche systématique et méthodique.

Ainsi, l'Audit Interne étant une entité à part entière, doit être capable de rassurer l'entreprise sur la continuité d'exploitation, sur la maitrise des opérations (gestion des risques) et donner une

garantie pas absolue mais raisonnable du succès des activités et de l'atteinte effective des objectifs.

1.1.2.2 Les objectifs

Dans la Modalité Pratique d'Application (MPA) 2120.A1 de l'audit interne contenu dans le CRIPP, il est spécifié les aspects sur lesquels doit porter l'évaluation du contrôle interne. Toujours dans la tendance de l'analyse par les risques, il est dit que 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.

Bertin (2007 : 21 – 22) pouvait dire l'audit interne est devenu un acteur majeur du dispositif de maîtrise des risques, du contrôle interne et de la gouvernance des sociétés. Il n'y a pas d'audit interne sans dispositif de contrôle interne. De ce fait, l'audit interne est une fonction d'appréciation et d'évaluation dont la tâche essentielle est notamment la validation et le maintien du contrôle interne. Sa mission principale est de s'assurer que les objectifs de contrôle interne s'inscrivent dans une approche globale du management des risques (COSO I et COSO II) et qu'ils sont relativement atteints.

L'interprétation de la norme 2120 donnée par L'IFACI (CRIPP 2013 : 165), soutenue par Renard (2010 : 144) souligne que pour atteindre les objectifs en matière de management des risques, les auditeurs internes doivent s'assurer que :

- ✓ les objectifs de l'organisation sont cohérents avec sa mission et y contribuent ;
- ✓ les risques significatifs sont identifiés et évalués ;
- ✓ leurs modalités de traitement des risques sont appropriées et en adéquation avec l'appétence pour le risque de l'organisation ;

- ✓ les informations relatives sont recensées et communiquées en temps opportun au sein de l'organisation pour permettre aux collaborateurs, à leur hiérarchie et au conseil d'exercer leur responsabilité.

1.1.2.3 Le champ d'application

Depuis son établissement en 1929, la fonction d'audit interne a commencé à prendre de l'ampleur, à élargir son champ d'application et à modifier ses objectifs.

Etant concerné dorénavant par toutes les fonctions de l'entreprise, l'audit interne revêt plusieurs formes selon les objectifs à atteindre lors de la réalisation d'une mission. Selon Renard (2010 : 48 – 55), nous avons :

- ✓ l'audit de conformité ;
- ✓ l'audit d'efficacité ;
- ✓ l'audit de management ;
- ✓ l'audit de stratégie ;
- ✓ le conseil.

1.1.3 Compétences et responsabilités des auditeurs

Du fait de la variété des domaines à couvrir et des missions à conduire, l'audit interne doit disposer d'une gamme de compétences toujours plus étendue. La formation permanente constitue donc un facteur clé de performance au plan individuel et collectif. Aussi, le respect des Normes internationales pour la pratique professionnelle de l'audit interne est essentiel pour que les auditeurs internes puissent s'acquitter de leurs responsabilités. Les normes relatives aux responsabilités des auditeurs internes sont appelées des **normes de qualification** (normes 1000 – CRIPP 2013). Ces normes doivent être définies dans une charte formelle d'audit interne. De ces normes, découlent les caractéristiques de l'auditeur interne :

- ✓ **indépendance** : capacité à assumer de manière impartiale, les responsabilités. L'audit interne doit être positionné à un niveau suffisamment élevé de la hiérarchie pour pouvoir être totalement indépendant et objectif. Pour cela, selon la norme 1100, l'audit interne

doit être doublement rattaché à la direction générale et au conseil d'administration (au comité d'audit plus précisément) ;

- ✓ **objectivité** : avoir un jugement impartial et sans aucune forme de subordination à celui d'autres personnes (normes 1100 et 1120);
- ✓ **compétence et Conscience professionnelle** : le savoir-faire, la diligence dans le travail, des connaissances et autres compétences relatives à l'exercice de leur fonction. Aussi faire preuve d'une formation professionnelle continue (norme 1200).

Concernant le système d'information et la sécurité de l'information, la MPA 1210.A3 (IFACI, 2013 : 36) précise que les auditeurs internes doivent posséder une connaissance suffisante des principaux risques et contrôles relatifs aux technologies de l'information, et des techniques d'audit informatisées susceptibles d'être mises en œuvre dans le cadre des travaux qui leur sont confiés. Toutefois, tous les auditeurs internes ne sont pas censés posséder l'expertise d'un auditeur dont la responsabilité première est l'audit informatique. La MPA 1220.A2 (IFACI, 2013 : 37) ajoute que pour remplir ses fonctions avec conscience professionnelle, l'auditeur interne doit envisager l'utilisation de techniques informatiques d'audit et d'analyse des données. Ces normes démontrent l'importance mise sur l'éventail de connaissance et compétence que doit avoir l'auditeur interne pour mener à bien ses missions d'audit de sécurité de l'information.

Selon Villalonga (2011 : 25), l'auditeur interne doit avoir les qualités nécessaires suivantes :

- ✓ ouvert d'esprit,
- ✓ diplomate,
- ✓ observateur,
- ✓ perspicace,
- ✓ polyvalent,
- ✓ autonome,
- ✓ synthétique,
- ✓ empathique.

Toutes ces caractéristiques citées plus haut sont celles dont l'auditeur doit se revêtir pour ainsi assurer et contribuer au maintien et à l'amélioration du système d'information, notamment de la

sécurité de l'information dans l'entreprise ; sécurité sans laquelle l'entreprise serait incapable de poursuivre correctement ses opérations et ainsi s'exposer à des pertes financières énormes.

1.2 La sécurité de l'information

Avec la mondialisation, l'évolution des technologies de l'information, l'ouverture des systèmes d'information au monde extérieur et la dépendance accrue des organisations vis-à-vis des données et ressources informatiques, la sécurité est aujourd'hui indispensable à la bonne marche de la plupart d'entre elles. En effet, aucune entreprise ne pourrait survivre aux conséquences notamment en termes de couts et de la perte d'intégrité de l'ensemble des données de son système.

Avant d'aborder la sécurité de l'information, nous définirons d'abord ce que l'on entend par information et quelle est son importance au sein de l'entreprise.

1.2.1 Notion d'information

Nous allons d'abord définir l'information et ensuite donner ses caractéristiques et son importance pour l'entreprise.

1.2.1.1 Définition de l'information

L'information est constituée de deux éléments :

- ✓ des données,
- ✓ un sens qui dépend de chaque individu.

L'information est un concept qui présente plusieurs sens. Elle désigne à la fois le message à véhiculer et les signes utilisés pour l'écrire. Au sens étymologique, l'information est ce qui donne une forme à l'esprit. Elle vient du verbe latin « *informare* », qui signifie "donner forme à" ou "se former une idée de". L'information utilise un code de signes, porteur de sens et destiné à la compréhension unique du destinataire. Le manuel de préparation CISA (ISACA, 2011 : 101) définit l'information comme étant des « données dotées de sens et d'objet ». Di Scala (2005 : 12) ajoute que l'information est le support formel d'un élément de connaissance humaine susceptible

d'être représenté à l'aide de conventions (codages) afin d'être conservé, traité, ou communiqué au sein de l'organisation ou auprès de ses partenaires.

1.2.1.2 Les caractéristiques de l'information

Le site « formaplace » identifie les caractéristiques suivantes de l'information :

- ✓ **sa forme** : orale, textuelle, visuelle, sonore
- ✓ **son mode de présentation** : numérique, alphabétique ou alphanumérique sous un support physique ou électronique
- ✓ **ses qualités** : fiable, précise, objective, stable, actuelle, pertinente, confidentielle
- ✓ **son coût**.

Selon Moisand et Garnier De Labareyre (CobiT, 2009 : 31), l'information présente 7 critères précis significatifs pour chacune des entités de l'entreprise :

- ✓ **efficacité** : la mesure par laquelle l'information contribue au résultat des processus métier par rapport aux objectifs fixés ;
- ✓ **efficience** : la mesure par laquelle l'information contribue au résultat des processus métier au meilleur coût ;
- ✓ **confidentialité** : la mesure par laquelle l'information est protégée des accès non autorisés;
- ✓ **intégrité** : la mesure par laquelle l'information correspond à la réalité de la situation ;
- ✓ **disponibilité** : la mesure par laquelle l'information est disponible pour les destinataires en temps voulu ;
- ✓ **conformité** : la mesure par laquelle les processus sont en conformité avec les lois, les règlements et les contrats ;
- ✓ **fiabilité** : la mesure par laquelle l'information de pilotage est pertinente.

1.2.1.3 L'importance de l'information

Le site formaplace stipule que l'information, en optimisant la perception des situations, permet quatre (4) fonctions essentielles :

- ✓ réduire l'incertitude sur un évènement donné ;
- ✓ modéliser la complexité de l'entreprise et de son environnement par la mise en place de procédures et processus ;
- ✓ prendre des décisions pour la réalisation des opérations et des objectifs de l'entreprise
- ✓ diriger : la direction de l'entreprise se sert de l'information pour piloter, mener des actions et contrôler les accomplissements.

L'information est une ressource fondamentale pour l'entreprise. Elle est un actif intangible, une ressource immatérielle qu'il faudrait traiter, décrypter, sélectionner en fonction des besoins. Pour cela, l'entreprise développe la veille informationnelle stratégique qui consiste à organiser la collecte des informations nécessaires aux prises de décisions.

Le manuel de préparation CISA (ISACA, 2011 : 101) explique que « l'information est devenue un élément indispensable de la conduite des affaires pour pratiquement toutes les organisations. Pour un nombre croissant de sociétés, l'information en est leur raison de vivre ». Le comité de Bale (1998 : 8) précise dans un contexte plus particulier que les objectifs d'information portent sur la préparation de rapports de qualité, pertinents, fiables et aussi récents que possible, indispensables à la prise de décision au sein de l'organisation bancaire. Ils recouvrent également la nécessité d'établir des comptes annuels, états financiers et autres communications et rapports de caractère financier et opérationnel.

Il est important de savoir que l'information est la matière première qui alimente le fonctionnement de l'entreprise. Par conséquent, un manque d'information ou une mauvaise communication entraine tout simplement la mort du système et très souvent, des pertes financières importantes et même le dépôt définitif de bilan. C'est la raison pour laquelle elle a besoin d'être contrôlée et sécurisée.

1.2.2 La sécurité de l'information

Cette partie servira à donner une définition et une explication du concept qu'est la sécurité de l'information pour l'entreprise.

1.2.2.1 Notion de sécurité de l'information

Selon le dictionnaire Larousse, la sécurité est une situation tranquille qui résulte de l'absence réelle de danger. C'est aussi un processus dont le but est de réduire les risques ou la probabilité de subir des dommages. De par cette définition, nous pouvons en déduire que la sécurité de l'information, c'est un processus permettant à une entreprise donnée de réduire les risques ou la probabilité de subir des dommages quant à la perte d'informations, à la présence d'informations biaisées, à la mauvaise utilisation ou interprétation des informations etc.

Le site Wikipédia définit la sécurité des systèmes d'information (SSI) comme étant l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour conserver, rétablir, et garantir la sécurité du système d'information. Le gouvernement québécois dans sa politique de sécurité de l'information (2009 : 2) ajoute que la sécurité de l'information est l'ensemble des activités qui préservent la disponibilité, l'intégrité et la confidentialité de l'information, et ce, peu importe le support utilisé pour la conserver ou la transmettre. C'est aussi un ensemble de mesures de sécurité mis en place pour assurer l'authentification des personnes et des dispositifs ainsi que l'irrévocabilité des actions qu'ils posent. Autrement dit, la sécurité de l'information désigne donc les mesures préventives qu'il faudrait mettre en place pour préserver les informations et les moyens.

La sécurité de l'information, selon le manuel de préparation CISA (ISACA, 2011 : 103), doit couvrir tous les processus physiques et électroniques relatifs à l'information peu importe s'ils concernent les gens et la technologie, ou les relations avec les partenaires commerciaux, les clients ou des tiers. La sécurité de l'information s'intéresse à tous les aspects de l'information et de sa protection à tous les points de son cycle de vie au sein de l'organisation.

La sécurité de l'information introduit le concept de gestion des risques. Les normes ISO 2700x qui sont des normes de la sécurité de l'information, sont établies pour permettre d'organiser sereinement le Système de Management de la Sécurité de l'Information (SMSI) de l'entreprise mais aussi de le contrôler et l'améliorer tout en restant dans une idéologie de gestion par les risques. Une entreprise peut et doit anticiper les menaces, les risques et leurs conséquences qui pèsent sur son système d'information en faisant une analyse complète de celui-ci et de son

environnement. Lorsque l'on réfléchit en termes de sécurisation du SI, il faut garder à l'esprit que le niveau de sécurité à appliquer doit toujours être basé sur la sécurité du maillon le plus faible de la chaîne des systèmes mis en jeu car un seul détail ignoré peut conduire l'entreprise à une fermeture certaine.

M. Cochard, Directeur Général du Consortium Internationale e-Miage, lors d'une présentation sur la sécurité des systèmes d'informations à l'université Picardie Jules Vernes en France (site foad.refer) a défini plusieurs facettes de la sécurité de l'information qui sont:

- ✓ la sécurité physique : liée aux systèmes matériels et à l'environnement (locaux, alimentation électrique, climatisation …) ;
- ✓ la sécurité logique et applicative : liée aux logiciels et applications (contrôle d'accès et protection de données) ;
- ✓ la sécurité de l'exploitation : procédures de maintenance des systèmes, les mises à jour, plan de sauvegarde et plan de secours ;
- ✓ la sécurité des télécommunications : liée aux infrastructures de réseaux.

1.2.2.2 Principes fondamentaux de la sécurité de l'information

Selon la norme ISO/IEC 27001 : 2005, la sécurité de l'information se caractérise par les cinq piliers suivants de l'information :

- ✓ **l'intégrité** : qui assure que la donnée reçue est la même que celle qui a été émise, c'est à dire qu'elle n'a pas été corrompue. L'altération des données (le manque d'intégrité) peut conduire à la prise de mauvaises décisions.
- ✓ **la confidentialité** : qui assure que la donnée reste privée durant la transmission pour que seules les personnes concernées aient la possibilité de la traiter. Il faudrait pour cela un message crypté ou une clé d'accès détenue uniquement par le(s) destinataire(s) concerné(s). La divulgation d'informations privées (perte de la confidentialité) ou le transfert d'informations privées à un destinataire autre que celui concerné, peut affecter la crédibilité de l'entreprise et surtout favoriser la concurrence.
- ✓ **la disponibilité** : qui assure que la donnée est présente et accessible à tout moment. L'indisponibilité des informations en temps réel pourrait entrainer un retard considérable

dans les tâches à accomplir et occasionner par la suite la perte de clients et donc des pertes financières.

- ✓ **la non-répudiation** : qui permet de s'assurer de l'identité réciproque à la fois de l'émetteur et du destinataire. Aussi qui permet de garantir qu'une transaction ne peut être niée par aucun des correspondants. Déroger au principe de non répudiation entraine une non-traçabilité des conversations ou messages entre l'émetteur et le destinataire et donc un non suivi quant au respect de la confidentialité des informations (divulgation frauduleuse d'informations).
- ✓ **l'authentification** : qui permet de s'assurer de la véracité de l'identité de l'utilisateur qui souhaite accéder à des données à accès restreint.

1.2.2.3 Missions et Objectifs de la sécurité de l'information

L'objectif principal de la sécurité de l'information est d'assurer la continuité d'exploitation de l'entreprise. C'est aussi de minimiser le risque de dommages éventuels par la prévention des incidents de sécurité et la réduction de leur impact potentiel. Aucune protection aussi sophistiquée soit-elle, ne peut garantir durablement l'inviolabilité d'un système d'information car la sécurité à 100% n'existe pas. Dès lors, l'entreprise doit classer les sinistres selon leur probabilité de survenance et leur impact, et prendre des mesures pour diminuer ces deux facteurs. Ghernaouti-Helie (2000 : 20), Professeur à l'institut d'informatique et d'organisation de HEC Lausanne, appuie cette idée en disant que l'objectif de la sécurité des systèmes d'information est de garantir qu'aucun préjudice ne puisse mettre en péril la pérennité de l'entreprise. Cela consiste à diminuer la probabilité de voir des menaces se concrétiser, à en limiter les atteintes ou dysfonctionnements induits, et à autoriser le retour à un fonctionnement normal à des coûts et des délais acceptables en cas de sinistre. La sécurité ne permet pas directement de gagner de l'argent mais permet d'éviter d'en perdre. Ce n'est rien d'autre qu'une stratégie préventive qui s'inscrit dans une approche d'intelligence économique.

La sécurité de l'information, dans un système d'information automatisé ou non, est importante voire primordiale pour toute entreprise qui souhaite assurer sa pérennité dans le monde des affaires actuel. Avec la mondialisation et l'avènement des nouvelles technologies de l'information qui marquent l'ère actuelle, les systèmes d'information aujourd'hui, sont basés sur

des infrastructures informatiques et de télécommunication. La vulnérabilité de ces infrastructures implique donc la vulnérabilité des systèmes d'information.

De plus, les systèmes d'information sont ouverts au monde extérieur (clients, fournisseurs d'accès internet, partenaires etc.), la probabilité qu'il y ait perte ou divulgation non autorisée d'informations est relativement élevée ; sachant que la perte de l'un des cinq piliers de l'information cités plus haut peut être dommageable pour l'entreprise. Les conséquences qu'elle pourrait encourir sont de plusieurs ordres dont les plus importants sont l'impact financier, l'impact sur l'image, l'impact juridique et dans le cas extrême l'interruption partielle ou définitive de l'activité.

Ainsi mettre en place la sécurité de l'information dans le système d'information, consent l'entreprise à prévenir et éviter des incidents majeurs de même que la propagation de leur impact néfaste sur l'ensemble de son environnement.

L'étape que nous aborderons maintenant est celle qui nous aidera à comprendre comment se fait la mise en œuvre de la sécurité de l'information et quels en sont les constituants, en d'autre termes savoir en quoi consiste la mise en place d'un cadre de gestion de la sécurité de l'information.

1.2.3 Mise en œuvre du cadre de gestion de la sécurité de l'information

Le facteur essentiel dans la protection des actifs informationnels et de la confidentialité est de jeter les bases d'une gestion efficace de la sécurité de l'information. Tous les acteurs de l'entreprise doivent prendre connaissance et conscience et s'engager dans le maintien de la sécurité de l'information afin d'atteindre les buts et objectifs fixés.

1.2.3.1 Engagement de la Haute Direction

En matière de systèmes d'information, selon l'IFACI (1993 : 2), la direction générale est responsable de l'évaluation des risques, de l'établissement de la politique de sécurité et de la mise en œuvre d'une structure organisationnelle. Son rôle lui est délégué par le conseil d'administration, détenteur légal et suprême des actifs informationnels. ISACA (2011 : 105)

ajoute que la mise en place d'une gouvernance efficace de la sécurité de l'information et la détermination des objectifs de sécurité stratégique de l'organisation dépendent et doivent rencontrer l'appui de la haute direction. Le développement d'une stratégie de sécurité de l'information nécessite qu'elle soit intégrée et alignée aux objectifs globaux de l'entreprise.

Selon l'IFACI (1993 : 2) : l'engagement de la haute direction consiste à :

- ✓ **effectuer une évaluation des risques** liée à la confidentialité, l'intégrité et la disponibilité des données et des ressources ;
- ✓ **établir une politique de sécurité** à l'échelle de l'organisation dans le but de canaliser le développement efficace des procédures et des pratiques de sécurité, de protéger les infrastructures et actifs critiques de l'entreprise et de responsabiliser l'ensemble du personnel. Une politique de sécurité de l'information est un ensemble de documents indiquant les directives, procédures, lignes de conduite, règles organisationnelles et techniques à suivre relativement à la sécurité de l'information et à sa gestion. C'est une prise de position et un engagement clair et ferme de protéger l'intégrité, la confidentialité et la disponibilité de l'actif informationnel de l'entreprise ;
- ✓ **mettre en place une structure organisationnelle** afin de contrôler régulièrement la conformité des opérations avec la politique de sécurité. Peter Drucker pouvait dire dans l'énonciation de sa théorie sur le management des entreprises « *une structure organisationnelle solide est un prérequis à la santé et à la performance d'une organisation. Et le test d'une entreprise en bonne santé se définit par la performance de son personnel*».

La direction générale doit s'atteler à mettre en place, par le biais d'un service dédié à la sécurité de l'information du système d'information, des dispositifs sécuritaires adéquats à l'entreprise toute entière. Notons que les politiques, objectifs et activités de sécurité doivent être en phase avec les objectifs et buts globaux de l'entreprise et s'inscrire dans une approche conforme à sa culture. Il lui faut pour cela un plan de sécurité adapté à ses activités. Selon Pipkin (2000), cinq (5) phases sont importantes pour élaborer un plan de sécurité à savoir :

- ✓ **inspection** : Identifier les fonctionnalités qui sont à la base des activités de l'entreprise. Évaluer les besoins en sécurité de l'organisation.
- ✓ **protection** : Mettre en place des moyens pour une réduction dynamique des risques.
- ✓ **détection** : Mettre en place des moyens pour une réduction réactive des risques.
- ✓ **réaction** : Mettre en place un plan de secours d'urgence.
- ✓ **réflexion** : Une fois l'incident terminé et tout remis en place, procéder à l'étude de l'événement.

La direction générale a l'autorité et doit s'engager à représenter l'organisation dans la protection et la sécurité de l'information. Elle doit définir les grandes lignes de sécurité qui doivent être suivies et appliquées par l'ensemble du personnel. La direction générale doit communiquer ses exigences concernant la protection de ses systèmes d'information afin que chaque acteur interne ou externe à l'entreprise, puisse s'y conformer pour le maintien de l'intégrité, la confidentialité et la disponibilité des informations. Elle doit également rendre compte au conseil d'administration, de la bonne fonctionnalité des systèmes de contrôle et de sécurité des informations. La direction générale doit apporter son soutien clair et massif à la démarche de sécurité et favoriser l'implication, la sensibilisation et la participation de tous les salariés.

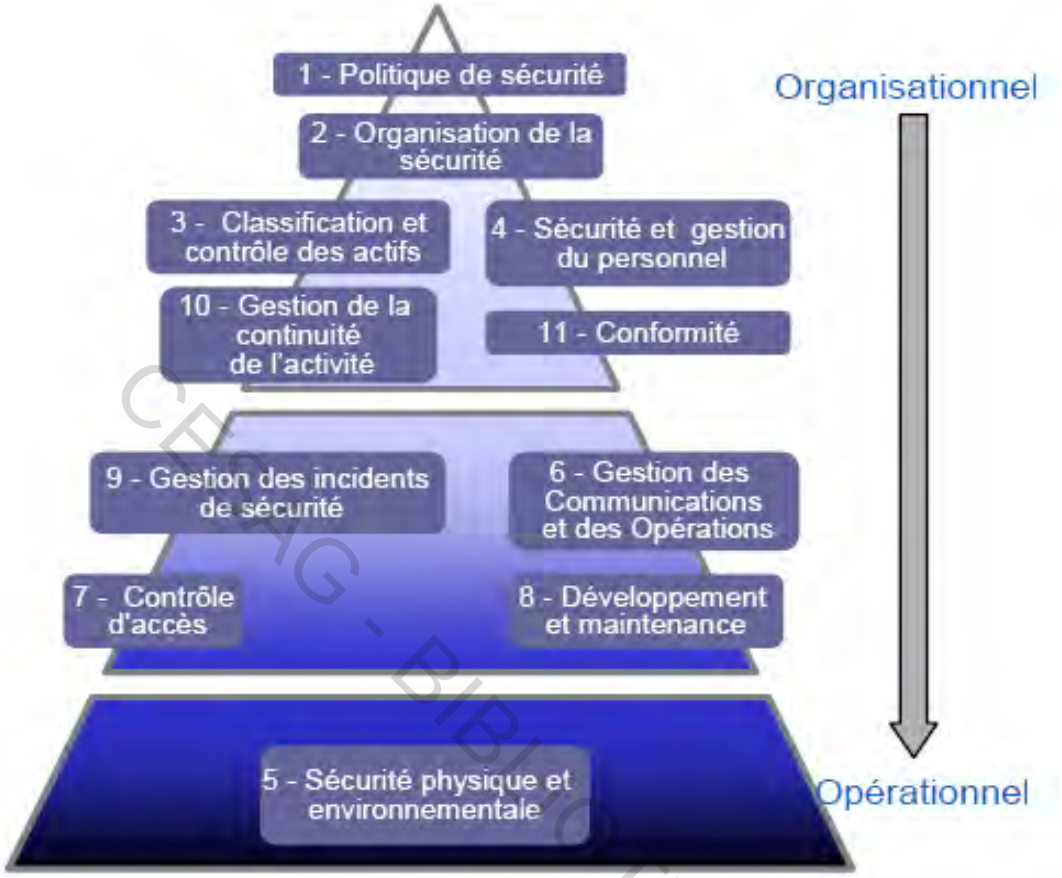
1.2.3.2 La constitution de la structure de mise en œuvre de la sécurité de l'information

Pour que le système d'information soit efficace, il faut mettre en place un cadre de gestion adéquat de la sécurité de l'information. Le cadre de gestion sert de fondement pour la mise en place de processus formels de gestion intégrée et continue de la SI, ainsi que des risques afférents. Il doit tenir compte des changements divers (technologique, juridique, social etc.) qui peuvent avoir une influence sur le système d'information. Le cadre de gestion vise principalement à établir une structure de gouvernance et de coordination et à énoncer formellement un ensemble de rôles et de responsabilités en SI.

Afin d'encadrer la démarche de mise en œuvre du cadre de gestion de la sécurité de l'information, notre étude se réfèrera à la norme ISO/IEC 17799 :2000, aujourd'hui appelé Norme ISO 27002. La norme ISO/IEC 27002 considère que beaucoup de systèmes d'information

n'ont pas été conçus pour être sécurisés. Ainsi la mise en œuvre de moyens techniques de protection a un impact limité et doit être soutenue par une organisation appropriée et par des procédures. Ladite norme propose 133 règles regroupées en 11 thèmes décrivant les meilleures pratiques en matière de sécurité de l'information. Linlaud (2003 : 55 – 80) par un tableau d'analyse des thèmes de la norme ISO/IEC 27002 et Hollo (2009 : 12) par son diagramme de répartition des catégories ISO 27002, ont défini chacun des éléments du cadre de gestion de la sécurité de l'information. Ainsi, le cadre de gestion de la sécurité de l'information prend donc en compte les 11 étapes suivantes :

Figure 1 : Le diagramme de répartition des catégories ISO 27002



Source : Laurent Hollo (2009)

- **Thème 1 : la gestion de la politique de sécurité** : elle traduit l'engagement de la direction à fournir une orientation stratégique et un support en ce qui concerne la gestion de la sécurité de l'information par l'établissement d'une politique de sécurité approuvée, publiée et communiquée par elle à tous les employés. Cette politique doit faire l'objet d'une révision constante et doit être en phase avec les objectifs de l'entreprise.
- **Thème 2 : l'organisation de la sécurité** : il s'agit de l'organisation interne et externe liées à la sécurité de l'information de l'entreprise. L'organisation interne doit prendre en compte un cadre adéquat de gestion de la sécurité par la présence d'un comité de gestion de la sécurité de l'information émanant de la direction, la répartition claire des responsabilités en matière de sécurité de l'information, les procédures de sécurité mises en place et les dispositifs de contrôle. Pour l'organisation externe en particulier pour la sécurité d'accès des tiers et les contrats d'externalisation, la politique de sécurité doit tenir compte des risques associés à l'accès des tiers au système d'information de l'entreprise ainsi que des contrôles adaptés qui doivent être mis en œuvre. Elle doit également prendre en compte le fait que les contrats d'externalisation fassent l'objet d'engagements contractuels très précis.
- **Thème 3 : la classification et le contrôle des actifs** : Deux points importants : la responsabilité liée aux actifs et la classification de l'information. Concernant la responsabilité liée aux actifs, l'entreprise doit réaliser un inventaire régulier de tous ses actifs liés à son SI. En délégant des responsables de gestion de ces actifs, elle peut mieux contrôler et s'assurer qu'une mise à jour récurrente de l'inventaire est effectuée. Concernant la classification de l'information, elle doit être accompagnée de procédures formelles et être exécutée en tenant compte des besoins liés à l'exploitation, de la sensibilité des informations, des restrictions éventuelles et du degré d'impact des évènements nuisibles à leur exploitation.
- **Thème 4 : les éléments de sécurité liés aux ressources humaines** : il s'agit ici d'intégrer la sécurité de l'information dans la description des tâches ; de sélectionner le personnel permanent, contractuel ou intérimaire en fonction des critères liés à la sécurité de l'information conformément à la politique de sécurité ; de faire signer au personnel des accords de confidentialité ; de sensibiliser et de former tous les employés de

l'organisme et les tiers utilisateurs si nécessaire à l'application et au respect des procédures et politique de sécurité de l'information ; d'inciter les employés à réagir face aux incidents et aux défauts de sécurité en signalant toute forme de défaillance ou dysfonctionnement.

- **Thème 5 : la sécurité physique et la sécurité de l'environnement** : consiste en la mise en place de périmètres de sécurité dans le but de protéger les secteurs physiques qui abritent les équipements de traitement des informations de même que les équipements eux-mêmes. Il s'agira de protéger ces secteurs ainsi que leurs accès afin de garantir que l'entrée n'est accordée qu'aux personnes autorisées. Les équipements et les secteurs physiques doivent être protégés contre tout sinistre (coupure de courant intempestive, tentative d'interception causée par une défaillance du câblage électrique, crise, guerre etc.).
- **Thème 6 : la gestion des communications et des opérations** : inclut plusieurs objectifs. L'organisme doit mettre en place des procédures et documents formels d'exploitation afin de définir les responsabilités et de séparer au mieux les tâches qui s'avèrent incompatibles. Ces procédures devront prendre en compte la gestion des incidents, la gestion des réseaux, l'utilisation de services extérieurs, la protection contre les logiciels malveillants, la sauvegarde de l'information, l'accès du système aux parties externes (prestataires, clients, public…), la sécurisation du E-commerce, la sécurisation du courrier électronique et des systèmes bureautiques. Ces procédures doivent s'encadrer de dispositifs de contrôles adaptés aux technologies de l'entreprise.
- **Thème 7 : le contrôle des accès logiques** : il s'agira ici de contrôler les accès à l'information. Les exigences concernant ce contrôle doivent être documentées et contenues dans la politique de sécurité de l'information. Ce contrôle inclut que chaque utilisateur soit clairement identifié par une authentification et un mot de passe forts et uniques (pour le respect du principe de traçabilité) ; que les attributions et utilisations des privilèges sont limitées et contrôlées ; que les procédures d'enregistrement, de modification ou de suppression des droits d'utilisateurs existent et sont respectées et utilisées au moment opportun ; que les accès aux réseaux et aux applications sont restreints ; que les accès aux matériels, systèmes, applications, réseaux, ont été délivrés aux personnes indiquées.

- **Thème 8 : le développement et la maintenance des systèmes** : il s'agit de mettre en place des sécurités dans les applications et les systèmes de fichiers (système de validation des données entrantes et sortantes, contrôle du traitement interne), et aussi des mesures de cryptographie (code, signature numérique etc.) dans le but d'assurer la confidentialité des informations. Il faut également que les processus de maintenance des systèmes soient adaptés et mis régulièrement à jour et en œuvre. Les logiciels et progiciels doivent être protégés contre toute attaque virale et les systèmes doivent être révisés lorsque qu'une modification se produit. Les évènements des systèmes doivent être générés et conservés (journalisation des évènements).
- **Thème 9 : la gestion des incidents de sécurité** : consiste d'abord en la journalisation ou l'élaboration d'un rapport des évènements exceptionnels et significatifs ayant attrait à la sécurité de l'information. Cela permet de surveiller les opérations et d'apporter en temps réel les corrections qui s'y rapportent. Ensuite il faudrait gérer à proprement dit les incidents en définissant les responsabilités et en développant un processus d'amélioration continue qui prend en compte l'arsenal technologique de l'entreprise de même que les objectifs globaux.
- **Thème 10 : la gestion de la continuité de l'activité** : l'entreprise doit mettre en place un processus pour gérer les interruptions des activités d'exploitation causées par des défaillances majeures ou des sinistres. Ensuite elle doit développer non seulement un plan stratégique basé sur l'évaluation des risques afin de déterminer l'approche complète de la continuité d'activités, mais en plus elle doit définir des plans de continuité pour maintenir ou rétablir le fonctionnement de l'exploitation. Ces plans doivent être de façon récurrente contrôlés, testés et réévalués.
- **Thème 11 : la gestion de la conformité** : la politique de sécurité et les procédures doivent respecter les exigences légales, règlementaires et contractuelles applicables à la structure. Ces procédures doivent être mis à jour, protégés et correctement suivis par tous les employés de l'entreprise ; le département de l'audit interne ou de la conformité devront s'en assurer. Les dispositifs de sécurité des SI doivent être régulièrement vérifiés pour assurer leur conformité technique. Les exigences d'audit des systèmes opérationnels doivent être soigneusement planifiées et approuver afin de minimiser au maximum le risque.

La mise en œuvre du cadre de gestion ainsi développé, doit permettre d'assurer une gestion efficace de la sécurité de l'information. Aussi l'entreprise désireuse d'améliorer de façon continue sa sécurité de l'information, a le choix entre prendre en compte les recommandations ou bonnes pratiques des normes ISO citées plus haut ou opter pour une gestion de la sécurité de l'information par des méthodes d'analyse des risques ; toujours est-il que ces méthodes intègrent les recommandations de certaines normes ISO.

Une méthode d'analyse des risques est une démarche, un processus ou un ensemble de principes qui permet d'appliquer une norme au système d'information de l'entreprise. La méthode sert aussi à faire un audit qui donne l'occasion d'effectuer, par exemple, un état de la sécurité du système d'information. Elle est souvent accompagnée d'outils afin d'appuyer son utilisation. Selon Debrock et Gourdin (2009 : 8 – 9), on distingue 3 catégories de méthodes : les méthodes quantitatives (ex : cout, impact financier…), qualitatives (ex : classement des risques – élevé, moyen, faible) et celles avec bases de connaissance (ex : recherche de standard ou bonnes pratiques à appliquer dans la sécurisation des TI). Les méthodes les plus utilisées sont les méthodes OCTAVE, MEHARI et EBIOS. Bien que fonctionnant de façon différente, ces méthodes ont pour finalité la mise en avant des actifs importants de l'entreprise et de la vulnérabilité des infrastructures des SI, l'étude des risques et l'établissement des plans de sécurité afférents.

Une entreprise s'attelant à mettre en place un cadre de gestion de la sécurité de l'information tel que décrit par la norme ISO/IEC 27002, atteindra ses objectifs en matière d'intégrité, de confidentialité et de disponibilité de l'information. Cependant il faudrait que tous ses acteurs, contribuant à son fonctionnement, comprennent leur responsabilité directe et indirecte quant à la sécurité des informations pour une atteinte effective des buts et objectifs globaux.

1.2.3.3 Communication et responsabilité des différents acteurs

L'un des piliers de la mise en place de la gouvernance réside dans la sensibilisation et la formation des ressources humaines. Il est donc vital pour l'entreprise, d'encadrer les habitudes et méthodes de travail, de mettre un point d'honneur sur l'importance de la communication, ainsi que de détecter et corriger les comportements inappropriés.

En plus de la direction générale qui définit les grandes lignes de la sécurité informationnelle, chaque acteur de l'entreprise a la responsabilité de l'application des clauses de sécurité prescrites pour une bonne marche de la structure. Les employés doivent être sensibilisés aux risques et aux comportements suivants :

- ✓ utilisation des outils de l'entreprise à des fins personnels (internet, téléphone, courriel…)
- ✓ protection contre les virus ou autres logiciels malveillants
- ✓ gestion de l'identité informatique et contrôle d'accès aux actifs informationnels
- ✓ protection des droits d'auteur, des renseignements personnels et de la vie privée

Selon les bonnes pratiques contenues dans la norme ISO/IEC 27002, l'entreprise doit être dotée d'un Système de Gestion de la Sécurité de l'Information (SGSI) mais également de personnes ressources, responsables et garant de cette sécurité. Voici les rôles et responsabilités des groupes concernées par la gestion de la sécurité de l'information selon le manuel du CISA (ISACA, 2011 : 366) :

- ✓ **un comité directeur de la sécurité des SI** : qui se constitue des représentants des divers niveaux de direction de l'entreprise. Ils sont chargés de discuter des problèmes, d'établir et d'approuver des pratiques de sécurité qui auront un bon impact sur l'organisme. Le comité doit être établit formellement par un mandat approprié ;
- ✓ **les cadres supérieurs** : qui seront responsables de la protection générale des actifs informationnels et de la mise en place et de la maintenance du cadre stratégique ;
- ✓ **le groupe consultatif pour la sécurité** : chargée de définir le processus de gestion des risques de sécurité de l'information et le niveau de risque acceptable, ainsi que de passer en revue les plans de sécurité de l'organisation. Il doit faire savoir à l'entreprise si ses programmes de sécurité répondent aux objectifs opérationnels ;
- ✓ **le chef de la protection des renseignements personnels** : c'est un dirigeant de niveau supérieur chargée de rédiger et de faire appliquer les politiques établies pour protéger la vie privée des clients et des employés ;
- ✓ **l'officier principal de la sécurité de l'information** : dirigeant de niveau supérieur charge de rédiger et de faire appliquer les politiques conçus pour protéger les actifs informationnels ;

- ✓ **les détenteurs du processus** : assurent que les mesures adéquates de sécurité concordent avec la politique organisationnelle et qu'elles sont maintenues ;
- ✓ **les détenteurs d'actifs informationnels et détenteurs de données** : ils sont responsables des actifs possédés. Ce qui entraine l'exécution d'une évaluation des risques, la sélection des contrôles adéquats pour faire diminuer les risques à un niveau acceptable, et l'acceptation du risque résiduel ;
- ✓ **les utilisateurs et les parties externes**: suivent les procédures établies dans la politique de sécurité et adhèrent aux règlementations sur la confidentialité et la sécurité ;
- ✓ **l'administrateur de la sécurité** : chargé de fournir la sécurité physique et logique adéquate pour les programmes des SI, les données et l'équipement. Il travaille sur les recommandations de base données par la politique de sécurité de l'information ;
- ✓ **les spécialistes / conseillers en matière de sécurité** : aident à concevoir, à implanter, à gérer et à réviser la politique, les normes et les procédures de sécurité de l'entreprise ;
- ✓ **les développeurs des TI** : implantent la sécurité de l'information au sein des applications ;
- ✓ **auditeurs** : fournissent à la direction, une assurance objective et indépendante de la pertinence et de l'efficacité des objectifs de la sécurité de l'information et des contrôles connexes à ces objectifs.

L'idée dans la description des rôles et responsabilités selon ISACA est que le SMSI soit confié au personnel de l'entreprise lui-même. L'homme étant le maillon le plus faible de l'entreprise, cela lui permettra de comprendre l'enjeu de la sécurité de l'information et de mieux l'appliquer. En matière de système de sécurité de l'information, le plus important c'est la communication. Plus le personnel est informé et sensibilisé, mieux l'entreprise évite les risques qui peuvent lui coûter la fin de son existence. La communication doit être verticale (Management – Opérationnels / Opérationnels – Management) et horizontale (entre les opérationnels).

A travers ce premier chapitre, nous avons posé les bases de l'audit interne et celles de la sécurité de l'information. Ce chapitre s'applique à tout type d'entreprise. Cela nous permet donc par la suite de comprendre et d'apprécier le rôle que doit jouer l'audit interne dans la sécurisation de l'information au sein d'une banque. Dans le prochain chapitre, nous verrons quels sont les

normes et référentiels applicables à la banque et à l'audit interne et quel est l'apport de l'audit interne à la sécurité de l'information bancaire.

CHAPITRE 2 : L'AUDIT INTERNE ET LA SECURITE DE L'INFORMATION EN MILIEU BANCAIRE

Nous présenterons en premier lieu les normes et référentiels qui traitent de l'audit interne et de la sécurité de l'information. En second lieu, nous décrirons le rôle de l'audit interne en milieu bancaire et plus précisément sa méthodologie en matière de sécurité de l'information.

2.1 Les normes et référentiels afférents à l'audit interne et à la sécurité de l'information

L'audit interne et la sécurité de l'information ne sauraient être effectués sans un cadre de référence formel pour montrer leur degré d'importance non seulement pour l'entreprise mais aussi pour les législateurs et partenaires extérieurs. Nous présenterons par la même occasion les référentiels applicables au système bancaire afin de comprendre les dispositions prises pour la réglementation de l'audit interne et la sécurité de l'information au sein d'une banque.

2.1.1 Les normes et référentiels applicables à l'audit interne

Les normes internationales applicables à l'audit interne sont celles édictées par l'IIA. Elles sont contenues dans un document appelé le Cadre de référence international des pratiques professionnel de l'audit interne (CRIPP). Chacune des normes est interprétée pour permettre à l'auditeur interne de mieux assimiler ses tâches et organiser son travail. Ces interprétations sont nommées des Modalités Pratiques d'Application (MPA). Elles sont valables autant pour les missions d'assurance que celles de conseil.

On distingue 3 types de normes dans le CRIPP : les normes de qualification (norme 1000), les normes de fonctionnement (norme 2000) et les normes de mise en œuvre. Les normes de qualification et les normes de fonctionnement s'appliquent à tous les services d'audit. Les normes de mise en œuvre précisent les normes de qualification et les normes de fonctionnement en indiquant les exigences applicables dans les activités d'assurance (A) ou de conseil (C).

L'IFACI affirme dans son commentaire (IFACI 2013 : 49) que le processus de contrôle de l'audit interne vise l'ensemble du dispositif de contrôle interne. Il ne faut pas le restreindre aux

procédures ou aux activités de contrôle, mais également prendre en compte l'organisation, le pilotage et la surveillance du processus qui se fondent sur une approche par les risques et une diffusion fiable de l'information. En matière de système d'information, selon le CRIPP (IFACI, 2013 :67), les auditeurs doivent effectuer des contrôles des technologies de l'information. Ce sont des contrôles qui viennent en appui de la gestion et de la gouvernance de l'organisation et qui comportent des contrôles généraux et des contrôles techniques sur les infrastructures des technologies de l'information dans lesquelles on retrouve les applications, les informations, les installations et les personnes.

En conclusion l'audit interne, de par ces normes, a la responsabilité d'évaluer le dispositif de contrôle interne à tous les niveaux de l'entreprise et de rendre compte fidèlement à la direction générale et au conseil d'administration.

2.1.2 Les normes et référentiels applicables à la sécurité de l'information bancaire

La sécurité de l'information évolue dans un cadre défini par les normes ISO 2700x et le CobiT. Notre étude ne saurait s'abstenir d'énoncer ces deux référentiels sans lesquels il serait quasi impossible de mettre en place un SMSI adéquat au sein d'une structure.

2.1.2.1 La norme ISO 27002

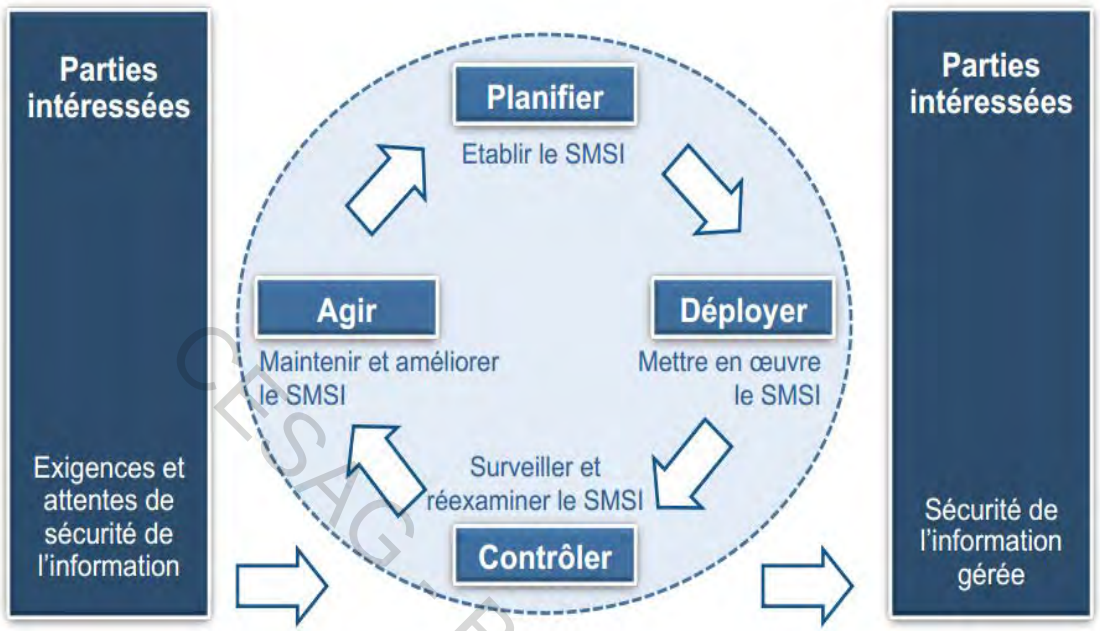
Selon le CLUSIF (2003 : 6), en 1995, la BSI (British Standards Institution) publie un document composé de 10 grands chapitres et contenant une centaine de recommandations sécuritaires sous le dénominatif de norme BS7799. En 1998, la BSI adjoint une seconde partie dénommée BS7799-2 qui précise les exigences de mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI). En 2000, suite au succès rencontré par la BS7799 dans le monde entier, l'ISO adopte la BS7799, tout en y ajoutant quelques mesures de sécurité supplémentaires et en la renommant ISO 17799. En juin 2005, l'ISO remanie et enrichit de nouvelles mesures de sécurité de l'ISO/IEC 17799, qui sera renommée en 2007, ISO 27002.

La série 27000 des normes ISO se concentre sur la gouvernance en sécurité de l'information. La liste suivante illustre les encadrements ISO prévus dans cette catégorie :

- ✓ ISO/CEI 27000 : Introduction et vue globale de la famille des normes, ainsi qu'un glossaire des termes communs (mai 2009)
- ✓ ISO/CEI 27001 : Norme de certification des SMSI (publiée en 2005, révisée en 2013)
- ✓ ISO/CEI 27002 : Guide des bonnes pratiques en SMSI (renuméroté en ISO/CEI 27002:2005 en juillet 2007, dernière révision en 2013)
- ✓ ISO/CEI 27003 : Guide d'implémentation d'un SMSI, publié le 3 février 2010 (Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information)
- ✓ ISO/CEI 27004 : Norme de mesures de management de la sécurité de l'information (publiée le 12 juillet 2009)
- ✓ ISO/CEI 27005 : Norme de gestion de risques liés à la sécurité de l'information (publiée le 4 juin 2008, révisée le 19 mai 2011)
- ✓ ISO/CEI 27006 : Guide de processus de certification et d'enregistrement (publié (en) le 1er décembre 2011)
- ✓ ISO/CEI 27007 : Guide directeur pour l'audit des SMSI (publié (en) le 14 novembre 2011)
- ✓ ISO/CEI 27008 : Lignes directrices de vérification en matière de mesures de sécurité (publiée (en) le 15 octobre 2011)
- ✓ ISO/CEI 27011 : Guide pour l'implémentation de ISO/CEI 27002 dans l'industrie des télécommunications (publié le 15 décembre 2008)
- ✓ ISO/CEI 27031 : Lignes directrices pour mise en état des technologies de la communication et de l'information pour continuité des affaires (publiée en mars 2011)
- ✓ ISO/CEI 27799 : Guide pour l'implémentation de ISO/CEI 27002 dans l'industrie de la santé (publié le 12 juin 2008),

Pour rappel, la norme ISO/IEC 17799 alias norme ISO 27002 montre les bonnes pratiques en terme d'implémentation d'un cadre de gestion adéquat et fiable pour une meilleure organisation de l'entreprise et une atteinte effective des objectifs de sécurité de l'information. La norme ISO/IEC 27002 propose un principe appelé « modèle PDCA » qui rappelle fortement le modèle du système de gestion de la qualité basé sur les processus. Soit la figure suivante :

Figure2 : Représentation schématique du PDCA



Source : asiq.org

Le modèle PDCA présente 4 étapes :

- ✓ **Plan** : élaboration de la politique de sécurité, des cibles, des objectifs, des processus et des procédures relevant de la gestion des risques et de l'amélioration de la sécurité de l'information
- ✓ **Do** : mise en œuvre de la politique de sécurité, les contrôles, les processus et les procédures
- ✓ **Check** : évaluation et définition des processus et des critères de performances de la politique de sécurité par rapport aux objectifs
- ✓ **Act** : réalisation des actions préventives et correctives, basées sur les résultats et visant à améliorer le système de gestion de la sécurité de l'information

Le modèle PDCA permet de considérer le système de gestion de la sécurité de l'information comme étant un élément stratégique de l'entreprise.

2.1.2.2 Le référentiel CobiT

Le CobiT est le résultat des travaux collectifs réalisés par les principaux acteurs de la profession, auditeurs internes ou externes, fédérés au sein de l'ISACA. Il a été publié en 1996 par l'ITGI (Information Technologies Gouvernance Institute) de l'ISACA. La généralisation de la SOX et de ses déclinaisons locales ou sectorielles (IFRS, LSF, normes Bâle II) ont considérablement renforcé le rôle des auditeurs. Ces dispositions réglementaires ont accéléré la diffusion de CobiT comme référentiel de contrôle et de gouvernance des SI.

Le CobiT formalise le contrôle des processus et le suivi de la performance et est devenu le référentiel des meilleures pratiques en technologie de l'information. Le CobiT définit l'ensemble des objectifs de contrôle reliés à l'évaluation des services TI, ainsi que la méthodologie de mise en place associée. Avec CobiT, la sécurité devient l'une des composantes de la gouvernance en proposant des bonnes pratiques de gouvernance de la sécurité de l'information. Cette dernière rejoint ainsi l'univers de la gestion des risques. La sécurité de l'information n'est plus seulement un sujet de technicien mais devient un enjeu de la direction générale et des métiers. CobiT, en développant l'alignement stratégique et l'apport de valeur des systèmes d'information, met bien en évidence les risques que l'absence de mesure de sécurité de l'information fait courir à l'entreprise (Moisand et Garnier De Labareyre, 2009 : 214).

Le CobiT aborde la gouvernance de la sécurité de l'information en s'intéressant à :

- ✓ la prise en compte de la sécurité de l'information dans l'alignement stratégique ;
- ✓ la prise de mesures appropriées pour limiter les risques et leurs conséquences potentielles à un niveau acceptable ;
- ✓ la connaissance et la protection des actifs ;
- ✓ la gestion des ressources ;
- ✓ la mesure pour s'assurer que les objectifs de sécurité sont bien atteints ;
- ✓ l'apport de valeur par l'optimisation des investissements en matière de sécurité de l'information ;
- ✓ les bénéfices retirés ;
- ✓ l'intégration de la sécurité de l'information dans les processus.

Globalement, CobiT aborde la sécurité de l'information dans plus de 20 processus sur 34. Mais les processus suivants font apparaître une dimension sécurité importante dans les objectifs de contrôle (Moisand et Garnier De Labareyre, 2009 : 214) :

- ✓ PO6 − Faire connaître les buts et orientations du management
- ✓ PO9 − Évaluer et gérer les risques
- ✓ DS4 − Assurer un service continu
- ✓ DS5 − Assurer la sécurité des systèmes

Les ressources du CobiT constituent un modèle de bonnes pratiques. Le référentiel CobiT fournit un ensemble détaillé de contrôles et de techniques de contrôle destiné aux environnements de gestion des systèmes d'information. Le CobiT estime que la gouvernance des systèmes d'information doit être constituée des structures et processus de commandement et de fonctionnement qui conduisent l'informatique de l'entreprise à soutenir les stratégies et les objectifs de l'entreprise, et à lui permettre de les élargir. Par conséquent, son utilisation permet de comprendre les objectifs de l'entreprise, de faire connaître les meilleures pratiques et d'émettre des recommandations autour d'une référence normative comprise et respectée de tous.

2.1.3 Les référentiels applicables au système bancaire

Cette partie nous montrera les réglementations prévues pour l'environnement bancaire concernant les contrôles et la sécurité des systèmes d'information. Ces dispositions sont obligatoires pour toutes les institutions financières.

2.1.3.1 La commission bancaire

La Commission bancaire est l'organe chargé de contrôler le respect par les établissements de crédit, des dispositions législatives et réglementaires qui leur sont applicables et de sanctionner les manquements constatés. Elle examine, en outre, les conditions d'exploitation de ces établissements et veille à la qualité de leur situation financière ainsi qu'au respect des règles de bonne conduite de la profession. La surveillance ou le contrôle exercée par la commission bancaire au sein des institutions de crédits notamment les banques s'étend à tous les domaines de

celles-ci. Mais pour notre étude, nous nous intéresserons essentiellement à l'aspect « gestion des systèmes d'information et sécurité de l'information » des banques.

La commission bancaire considère que la sécurité des systèmes d'information fait partie intégrante de la sécurité des établissements de crédit dont elle a la responsabilité. Ces derniers ont un devoir de sécurité vis-à-vis de leurs clients, d'eux-mêmes et de l'ensemble du système bancaire. Les SI étant, à cause de la mondialisation, tous informatisés, la menace informatique constitue un danger réel pour les banques. L'informatique est devenue un outil de production principal et inévitable : les valeurs monétaires, les informations sur les clients et partenaires, les transactions financières, les comptes bancaires etc. sont contenus, stockés et valorisés par elle.

Quelles que soient les causes, l'informatique peut jouer si la défaillance est importante, soit un rôle de déclencheur de crise, soit celui de propagateur. L'impact des problèmes que peut rencontrer une banque lorsque la sécurité de son système d'information n'est plus assurée, est important et rapide. Selon le livre blanc de la commission bancaire européenne (1996 ; page 10), les risques encourus par la banque sont :

- ✓ **le risque de non transfert**, entrainant un « cash liquidity risk » où la banque, pour des raisons diverses liées à son informatique, n'est plus capable, à tout moment, de remplir à court terme ses obligations vis-à-vis de ses clients ou de ses confrères ;
- ✓ **le risque de perte d'informations**, dû à la destruction totale ou partielle de ses fichiers stratégiques ou de sa mémoire, ou la divulgation d'informations confidentielles (fichiers clients, positions stratégiques etc.) ;
- ✓ **le risque de fraudes**, conduisant à des pertes de valeurs (coûts économiques des détournements);
- ✓ **le risque juridique** engageant la responsabilité civile éventuelle ;
- ✓ **le risque de réputation et d'image.**

Pour cela, la commission bancaire a décrit un cadre de sécurité obligatoire auquel toute institution financière doit se conformer. Il s'agit pour chaque institution financière d'évaluer de façon récurrente son système d'information ainsi que la sécurité des informations qui regorgent de ce système par une méthode d'analyse et de mesure constante des risques.

Différentes étapes sont à considérer (livre blanc de la commission bancaire européenne, 1996 : 34):

- ✓ un engagement de la direction générale, qui doit définir la politique de sécurité, le risque maximal tolérable, la liste des données stratégiques et d'autres grandes options (coûts/avantages, problèmes de personnels etc.) ;
- ✓ l'analyse du système d'information et du niveau de sécurité de celui-ci ;
- ✓ la définition du schéma directeur de la sécurité des systèmes d'information qui représente à l'arbitrage de la direction générale, le plan d'action (les mesures à prendre, l'organisation à définir, les budgets, les plannings, la politique de protections et la gestion des risques et le contrôle);
- ✓ la sensibilisation permanente de tout le personnel pour rechercher l'adhésion autour du schéma sécuritaire ;
- ✓ la cohérence et le bon sens qui permettent d'adapter la nature et l'importance des moyens aux risques et aux enjeux.

2.1.3.2 Le comité de Bâle

Le comité de Bâle est l'organe international qui régit la mise en place et les conditions de réussite d'un système de contrôle interne en milieu bancaire. C'est une institution créée en 1974 par les gouverneurs des banques centrales du G10[2]. Aujourd'hui, 10 autres pays se sont ajoutés au groupe afin de mener des réflexions plus pertinentes sur le contrôle interne bancaire. L'une de ses missions est le renforcement de la sécurité et de la fiabilité du système financier (le site Wikipédia sur le comité de Bâle). Le comité de Bâle (1998 : 20) estime qu'étant donné que l'activité bancaire est un secteur dynamique, où tout évolue rapidement, les banques doivent en permanence surveiller et évaluer leurs systèmes de contrôle interne en fonction des modifications des conditions internes et externes et les renforcer, au besoin, pour en garantir l'efficacité.

[2] Le G10 est un groupement informel de onze pays crée en 1960 et qui a pour but à l'origine, de fournir des ressources supplémentaires au Fonds Monétaire International, il se compose de l'Allemagne, la France, la Belgique, Les USA, la Canada, l'Italie, le Japon, les Pays-Bas, l'Angleterre, la Suède et la Suisse.

A titre d'information, le comité de Bâle a mis en place 29 principes fondamentaux (comité de Bâle 2012 : 10) qui servent de référence aux banques. Ces principes leur permettent d'évaluer la qualité de leur système de contrôle et de définir les travaux à mener en vue d'atteindre un niveau de base en matière de saines pratiques de contrôle toujours dans une gestion par les risques. Ces principes sont regroupés en deux grandes catégories : la première (Principes 1 à 13) porte sur les pouvoirs, les responsabilités et les fonctions des autorités de contrôle, tandis que la seconde (Principes 14 à 29) se concentre sur la réglementation prudentielle et les obligations faites aux banques. Le premier principe de la version précédente a été divisé en trois principes distincts, et de nouveaux principes ont été ajoutés sur les thèmes de la gouvernance d'entreprise ainsi que de l'information à fournir et de la transparence.

Un système de contrôle interne efficace est une composante essentielle de la gestion d'un établissement et constitue le fondement d'un fonctionnement sûr et prudent d'une organisation bancaire. En se dotant de contrôles internes rigoureux, une banque pourra mieux réaliser ses buts et ses objectifs de rentabilité à long terme, en assurant également la fiabilité de sa communication financière tant externe qu'à sa direction. Un tel système peut aussi garantir que la banque agit dans le respect des lois et réglementations ainsi que de ses politiques, programmes, règles et procédures internes; il atténue, en outre, le risque de pertes imprévues ou d'atteinte à la réputation de l'établissement (comité de Bâle, 1998 : 1).

Face aux référentiels et aux bonnes pratiques précités, l'audit interne se doit d'établir et de structurer une méthodologie de travail adéquate afin de mener ses activités dans le cadre de la règlementation sécuritaire en vigueur.

2.2 Méthodologie de l'audit interne dans le cadre de la sécurité de l'information bancaire

L'audit de la sécurité de l'information doit être compris dans le plan d'audit interne annuel. Il vise différents objectifs. D'abord, la détermination des déviations par rapport aux bonnes pratiques de sécurité et ensuite la proposition d'actions visant l'amélioration du niveau de sécurité du système d'information. L'audit de sécurité d'un système d'information se présente comme un moyen d'évaluation de la conformité d'une situation liée à la sécurité par rapport à

une politique de sécurité ou par rapport à un ensemble de règles de sécurité, de procédures ou techniques de référence.

La démarche d'audit devra suivre un plan de travail bien structuré pour l'évaluation appropriée du SMSI mis en place par le management. Pour la démarche d'analyse, l'audit interne doit prendre en compte l'environnement global de l'entreprise en vue de vérifier l'alignement du SMSI adopté avec les enjeux, les risques opérationnels et les stratégies et politique de l'entreprise. L'audit interne pourra aussi s'assurer que le SMSI est conforme aux exigences de la norme ISO 27002. La mission d'audit interne se déroule toujours de la même façon avec une phase de préparation incluant une phase de prise de connaissance du domaine à auditer, une phase de réalisation et enfin une phase de conclusion matérialisée par la rédaction d'un rapport d'audit. Ce rapport comportera des recommandations qui feront l'objet de suivi.

2.2.1 Le plan d'audit de la sécurité de l'information

L'audit du SMSI doit se faire en fonction de la taille et des activités de l'entreprise et aussi en fonction du niveau de l'appétence pour le risque défini par la structure elle-même. Plusieurs méthodes d'élaboration du plan d'audit peuvent être évoquées, mais nous, nous ne prendrons en compte que celle préconisée par ISACA (2010 ; 14 – 32).

Dans le plan d'audit, il s'agira d'évaluer :

- ✓ **Etape 1 : la gestion de la sécurité de l'information**

  L'objectif est de s'assurer que le SMSI répond effectivement aux besoins de l'entreprise. L'auditeur devra apprécier le processus de gouvernance de la sécurité de l'information en constatant l'existence d'un comité de pilotage de la sécurité dans lequel chaque corps métier clé devra être représenté. Ce comité devra se composer de la Direction de l'audit interne, de la Direction des ressources humaines, de la Direction des opérations, de la Direction des finances, de la Direction de la sécurité informatique et de la Direction juridique. A travers les rapports dudit comité, l'auditeur vérifiera si les tâches assignées et le rôle, de même que les recommandations faites, vont toujours dans l'intérêt de la bonne gestion de la sécurité de l'information.

L'auditeur interne évaluera aussi les risques en fonction du niveau de risque acceptable définit par l'entreprise. L'existence et la conformité des politiques et procédures de sécurité d'avec la stratégie de la structure devront être vérifiées. Selon la norme ISO 27001 section 2, les politiques et procédures devront au minimum inclure la politique du respect de la sécurité, la politique de l'acceptation du risque de gestion, la politique de sécurité des communications externes, la politique de pare-feu, la politique de sécurité E-mail, la politique de sécurité de l'ordinateur portable / de bureau et enfin la politique d'utilisation d'internet.

L'auditeur interne s'assurera également de l'existence d'un plan de sécurité des technologies de l'information (intégration et maintenance) selon l'infrastructure informatique et la culture de sécurité développées par l'entreprise. Le plan de sécurité doit prendre en compte la classification des données, les normes technologiques, les politiques d'accès / ressources humaines (séparation des tâches, gestion des utilisateurs clés et les contractants extérieurs), la sécurité et le contrôle, la gestion des risques et les exigences de conformité externes.

- ✓ **Etape 2 : les opérations et la gestion de la technologie de sécurité de l'information**

L'objectif sera de s'assurer de l'existence d'un dispositif clair de sécurité de l'information non seulement pour les fonctions (les corps métiers) mais aussi pour les technologies de l'information à proprement dit.

L'auditeur devra vérifier que l'intégrité, la disponibilité et la confidentialité des données ou informations ne sont pas compromises à travers l'existence et l'efficacité des dispositifs d'authentification, d'identification et de traçabilité des différents utilisateurs du système (permanent, temporaire ou extérieur). Ce contrôle prendra en compte l'analyse de la gestion des privilèges accordés aux personnes autorisées et la gestion des accès aux applications et aux zones de sécurité.

L'auditeur appréciera la vulnérabilité ou la robustesse des dispositifs de sécurité établis pour les technologies de l'information (les réseaux, le matériel informatique, les disques amovibles etc.) qui sont entre autre les pare-feu et antivirus, les systèmes de cryptographie des données, le dispositif de sécurité des réseaux (interne et externe) et le mode opérationnel d'échange des informations.

Ensuite, l'auditeur interne devra s'assurer que les moyens de gestions des incidents sont appropriés et efficaces. Il devra vérifier l'existence et du rôle d'un comité de gestion des incidents, l'existence d'un plan de classification des incidents par priorité, de l'existence des procédures et plans de gestion immédiat des incidents, l'existence, l'effectivité et la mise à jour des plans de relance après la survenance d'incidents. Le maillon faible de l'entreprise étant l'homme, l'auditeur doit s'assurer que le personnel est régulièrement sensibilise et éduqué à l'aide de formations obligatoires. Un suivi devra être fait pour évaluer les compétences et la compréhension réelle des dispositifs de sécurité de l'information mis à disposition au niveau interne et externe.

Après ces deux étapes, vient l'évaluation de l'évolution du SMSI mis en place. Basé sur les résultats de l'audit de la sécurité de l'information et ses observations, l'auditeur interne devra assigner un niveau de maturité à chacun des éléments du SMSI. Ensuite par la comparaison de ce niveau d'avec la cible de maturité que souhaiterait atteindre l'entreprise, il appréciera les écarts et émettra des recommandations qui amèneront le SMSI au niveau requis.

Pour mettre en œuvre ce plan d'audit, l'auditeur interne a besoin d'outils et de tests de contrôles. La prochaine section nous éclairera sur cet aspect.

2.3.3 Les outils et tests de contrôle

Pour qu'une mission d'audit de la sécurité de l'information soit effective, l'auditeur interne doit premièrement avoir des compétences dans le domaine à auditer. Selon la norme 1210, les auditeurs internes doivent posséder les connaissances, le savoir-faire et les compétences nécessaires pour mener correctement les missions d'audit. La compétence de l'auditeur interne doit se remarquer autant dans l'utilisation des normes et techniques que dans les domaines de l'organisation dans lesquels il intervient.

En matière de sécurité de l'information, comme le stipule la MPA 1210.A3, il n'est pas demandé à l'auditeur interne d'être un informaticien ou un auditeur informaticien mais plutôt d'avoir des compétences et connaissances dans les technologies de l'information et dans la gestion de la sécurité. Ceci pour pouvoir effectuer des évaluations professionnelles et apporter des

recommandations créatrices de valeur ajoutée. Selon l'IIA (2012 : 7), l'entreprise attend de l'auditeur interne des compétences telles que :

- ✓ la réflexion analytique / œil critique ;
- ✓ la communication ;
- ✓ le management des risques ;
- ✓ l'extraction et l'analyse des données ;
- ✓ les contrôles généraux des SI ;
- ✓ le sens des affaires.

L'auditeur interne compétent pour une mission de sécurité de l'information, doit garder à l'esprit 5 principaux domaines de risques à savoir : les risques de non-conformité, les risques opérationnels, les risques financiers, les risques informatiques et les risques stratégiques (IIA 2012 : 4). Selon l'IFACI (1993 :19), le principal risque associé à la gestion de la sécurité de l'information est que l'intégrité, la confidentialité et la disponibilité des données ou ressources du système d'information puissent être compromises.

Comme outils et tests de contrôle en matière de système d'information, selon le manuel de préparation du CISA (ISACA, 201 :57), l'auditeur interne peut utiliser les techniques d'entretien (questionnaire de contrôle interne, enquête, interview), l'examen de la documentation (les procédures, politique de sécurité, documents relatifs aux ressources humaines etc.), l'observation, l'utilisation de logiciels d'audits spécialisés, les tests de corroboration, les tests de conformité, les tests de cheminement. Il peut également procéder à des tests d'intrusion afin d'éprouver la vulnérabilité du système informatique de gestion.

L'auditeur interne effectuera ces tests de contrôles afin de s'assurer de l'efficience du dispositif de contrôle mis en place pour assurer et maintenir la sécurité de l'information. A travers son esprit d'analyse et ses outils, il contribue d'une manière ou d'une autre à la gestion de la sécurité de l'information et ainsi crée de la valeur ajoutée. La prochaine étape nous permettra de voir en quoi le plan de travail de l'audit et son évaluation crée de la valeur pour l'entreprise dans laquelle il exerce son métier.

2.3 La contribution de l'audit interne et création de valeur ajoutée

En matière de sécurité de l'information, le cadre de gestion doit faire partie intégrante du contrôle interne car la protection des ressources et des données utilisées ou produites par le système d'information nécessite une forte structure de contrôle. Le comité de Bâle (1998 : 20) explique que surveiller l'efficacité des contrôles internes est une tâche qui peut être accomplie par du personnel de plusieurs secteurs différents, dont celui en charge des opérations elles-mêmes, le contrôle financier et l'audit interne. Selon lui, le système de contrôle de la banque se constitue en contrôle interne en amont et d'audit interne en aval. Par ricochet, l'audit interne doit s'assurer qu'un dispositif de contrôle interne existe à tous les niveaux de la chaîne de traitement de l'information, qu'il est conforme aux orientations du business et adapté à l'environnement de travail. Autrement dit, il doit veiller à ce que ce dispositif de contrôle interne réponde convenablement aux besoins de sécurité de l'entreprise en l'évaluant et en apportant des recommandations pour son amélioration continue.

Dans le secteur bancaire, étant fortement concurrenciel, la réussite dépend de la sécurité, de l'exactitude, de la fiabilité et de la disponibilité des données ou de l'information que les technologies mettent à la disposition de la direction et des employés au besoin. L'audit interne est donc cette entité capable d'assurer que les systèmes d'information sont bien gouvernés et la sécurité de l'information bien gérée afin que les décisions prises par le management créent de la valeur ajoutée. Par ailleurs, une solide gouvernance d'entreprise constitue le fondement d'une gestion efficace des risques et de la confiance du public dans les banques et dans le système bancaire (le comité de Bale, 2012 : 2). L'audit interne est chargé de vérifier la régularité des activités de la banque. À cette fin, il fournit, à tous les niveaux de responsabilité de la banque, des assurances, des analyses, des plans d'actions approuvés ou des recommandations, des conseils et des informations concernant les activités qu'il a vérifiées (Banque Européenne d'investissement, 2007 : 2).

L'audit interne contribue à la détection des risques de sécurité qui pourraient échapper au dispositif de contrôle interne en place. Il redore ainsi par ses recommandations, l'image de l'entreprise devant le monde extérieur. L'auditeur interne doit être celui qui a une vue et une compréhension approfondie des risques inhérents à la sécurité de l'information. C'est la raison

pour laquelle il lui est recommandé une formation continue et une connaissance approfondie des technologies de l'information modernes.

L'audit est rendu obligatoire par la clause 6 de la norme ISO 27001 qui précise que des audits doivent être conduits à intervalles planifiés pour s'assurer que les objectifs et mesures de sécurité, les processus et procédures du SMSI sont :

- ✓ conformes au standard (ISO 27001 et son Annexe A) et aux législations et règlements en vigueur,
- ✓ conformes au SOA,
- ✓ effectivement implémentées et mises à jour,
- ✓ fonctionnent comme prévu.

Selon le site SSi-conseil, l'audit participe au processus d'amélioration continu permettant de contrôler, de corriger ou d'améliorer les mesures de sécurité mises en place grâce à 3 types d'actions :

- ✓ les audits internes (planifiés)
- ✓ les contrôles internes (inopinés mais plus ciblés)
- ✓ les revues de management (généralement planifiées sauf événement exceptionnel).

L'audit Interne a une approche factuelle basée sur des tests, des interviews, des observations. Cela lui permet de donner un point de vue indépendant sur ce qui est appliqué et la conformité aux bonnes pratiques en matière de gestion de sécurité de l'information.

Toute entreprise espère assurer intégrité, confidentialité et disponibilité de ses informations pour les parties prenantes. Ainsi, les vérifications et recommandations de l'auditeur interne crée de la valeur ajoutée pour cette entreprise à différents niveaux :

- **au niveau de la gestion de la sécurité de l'information** :

  L'entreprise aura une approche cohérente de la définition des processus IT et connaitra l'importance d'un comité de pilotage de la sécurité de l'information et son rôle. Elle

comprendra mieux son environnement de contrôle informatique et l'importance des politiques de sécurité informationnelle. Elle saura sur quels points mettre l'accent afin d'aligner sa stratégie informatique avec sa stratégie globale.

L'entreprise pourra aisément mettre à jour ses procédures et politiques en matière de sécurité de l'information et les suivre en fonction de son changement d'environnement ou de stratégie. Elle aura connaissance des risques liés à la sécurité de l'information susceptibles d'avoir un impact négatif sur ses activités et pourra mieux les classer par priorité. Par la compréhension des risques de sécurité, l'entreprise sera à même de prendre des décisions qui s'alignent aisément à ses objectifs.

Chaque corps métier saura ce qu'il faut faire pour maintenir et améliorer la sécurité de l'information dans son domaine. L'entreprise saura de quelles compétences elle a besoin pour son fonctionnement et pourra ainsi attribuer convenablement les rôles et responsabilités. De même, cela favorisera une bonne protection et une bonne utilisation des actifs liés aux TI.

- **Au niveau des opérations et de la technologie de sécurité de l'information**

  L'évaluation de ce facteur permettra à l'entreprise de mieux identifier les risques liés aux technologies de l'information. Elle sera à même de palier rapidement aux incidents de sécurité qui surviendront par la mise en place d'un comité de gestion des incidents. En adoptant un système de management de qualité pour la sécurité de l'information, l'entreprise rencontrera la satisfaction de ses partenaires de même que la compréhension et la motivation de son personnel.

  L'entreprise saura quels sont les moyens et méthodes techniques modernes à adopter pour sauvegarder et protéger ses informations, comment les utiliser et comment les faire respecter. Les technologies seront utilisées de manière efficiente et efficace pour permettre la réalisation des objectifs au moment opportun. Il y aura une amélioration de la satisfaction de la clientèle puisque la gestion de la qualité du SMSI et des services sera alignée à leurs attentes. Les rôles seront également clairement définis et les attributions et privilèges, nettement repartis.

Ce chapitre nous a permis de comprendre le cadre normatif et référentiel dans lequel se trouve le système bancaire. Nous avons également fait référence à l'apport de l'audit interne dans la

gestion de la sécurité de l'information. De façon générale, son rôle est de veiller à l'atteinte des objectifs assignés par la Direction Générale dans ses procédures de sécurisation des actifs informationnels de la structure.

Notre étude a pour exemple de travail, la banque ECOBANK Cote d'Ivoire. Pour l'obtention des informations et leur analyse et interprétation, nous avons suivi une démarche qui sera présentée dans ce dernier chapitre de notre partie théorique. A travers un modèle d'analyse précis, nous vérifierons non seulement l'existence du SMSI de ECOBANK CI mais nous évaluerons aussi ses forces et ses faiblesses. Enfin nous montrerons ce que l'audit interne peut apporter pour pallier les éventuelles défaillances à travers nos recommandations.

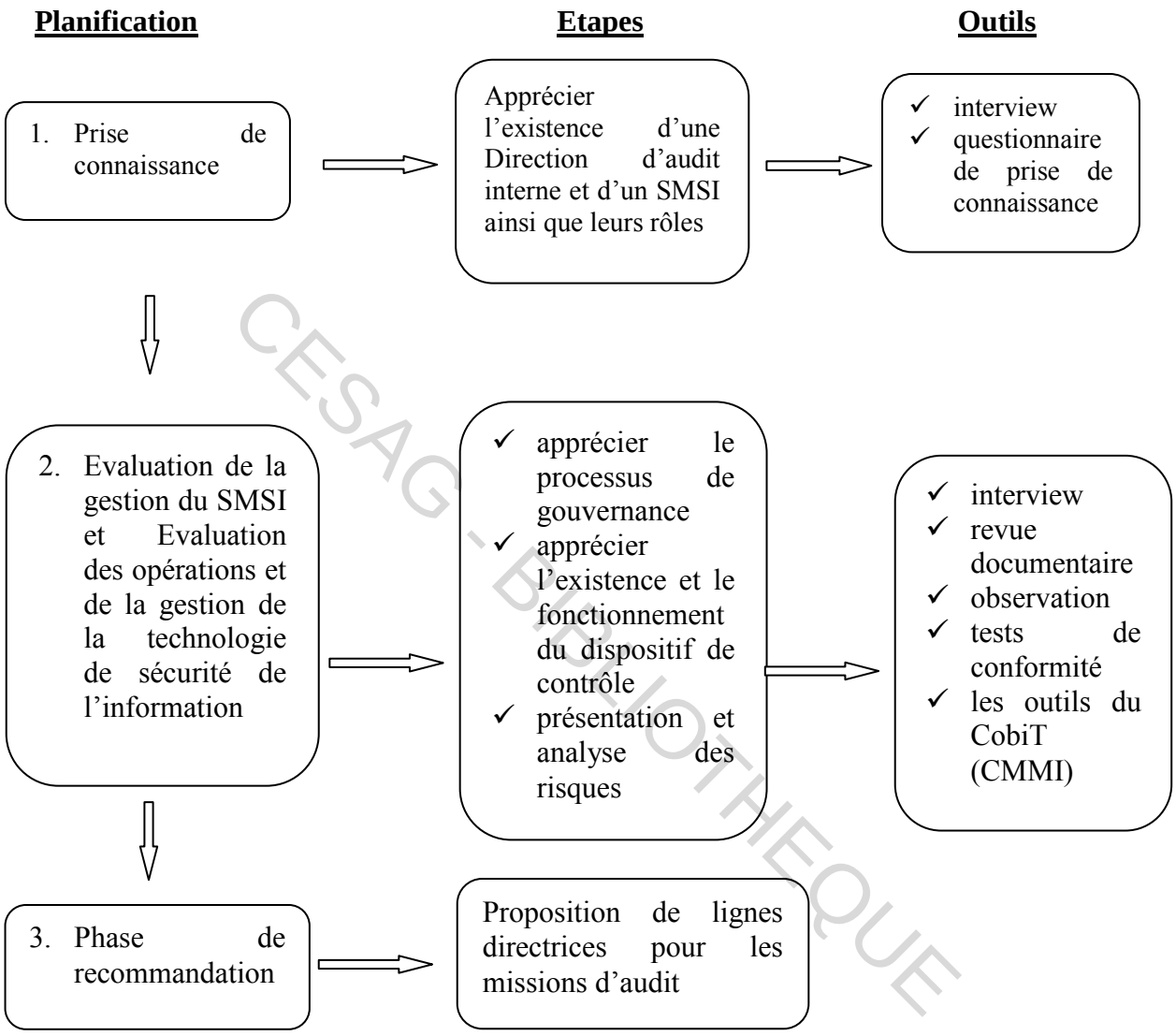
CHAPITRE 3 : METHODOLOGIE DE LA RECHERCHE

Après avoir émis la théorie concernant la sécurité de l'information et sa gestion ainsi que le cadre référentiel, nous allons avec l'exemple de ECOBANK CI, comprendre dans la pratique comment est gérée la sécurité de l'information en milieu bancaire et quelle est la contribution de l'audit interne à son bon fonctionnement et à son maintien face aux risques divers de sécurité. Il s'agira pour nous dans cette partie, de constater, d'observer, de diagnostiquer le SGSI quant aux normes et aux bonnes pratiques et d'en ressortir les résultats d'analyse. Les points de défaillances qui seront découverts pourront faire l'objet de missions d'audit interne pour l'apport de solutions de pérennité et de bonne gouvernance. Ceci accentuera le rôle de l'audit interne au sein de la banque et démontrera sa contribution pour l'atteinte effective des objectifs de sécurité de l'information. Notre démarche méthodologique sera présentée de manière succincte ci-après.

3.1 Le modèle d'analyse

Notre modèle d'analyse est schématisé en méthodes, étapes et outils. Ce modèle nous permettra de décrire et apprécier le cadre de gestion de la sécurité de l'information de même que le rôle de la direction de l'audit interne dans le maintien et l'amélioration de la sécurité de l'information au sein de ECOBANK CI comme suit :

Figure 3 : Modèle d'analyse



Source : Nous-même

3.2 La démarche d'analyse utilisée

Pour notre étude, nous avons opté pour un plan à 3 niveaux d'étude. Nous allons premièrement prendre connaissance du SMSI de Ecobank Cote d'Ivoire afin d'apprécier non seulement son existence mais aussi son mode de fonctionnement. Ensuite nous décrirons la fonction d'audit interne, son rôle au sein de la banque et en matière de sécurité de l'information. La prise de

connaissance du SMSI s'effectuera à l'aide des 6 éléments clés de sécurité de l'information de la norme ISO 27002 décrit par ISACA (2011 ; 365 – 366) à savoir : engagement de la direction, organisation, politiques et procédures, sensibilisation et éducation, contrôle et conformité et enfin gestion et intervention face à l'incident.

En second plan, nous effectuerons une évaluation à proprement dit de la gestion de la sécurité de l'information puis des opérations et de la gestion de la technologie de sécurité de l'information. Pour évaluer la gestion de la sécurité de l'information, nous apprécierons le processus de gouvernance du SMSI. Nous constaterons la présence ou non d'un comité de pilotage crée à cet effet ainsi que l'existence d'une stratégie de gouvernance clairement définie et respectée tout en passant par une évaluation et une analyse des risques. Ensuite pour l'évaluation des opérations de la gestion des technologies de sécurité de l'information, nous apprécierons l'existence et le fonctionnement du dispositif de contrôle relatif à la sécurité de l'information. Ceci sera également suivi d'une analyse des risques éventuels de sécurité.

Enfin à travers un système de cotation du niveau de maturité du SMSI allant de 0 à 5 et un tableau contenant les faiblesses et les risques, nous ferons ressortir des points caractériels du SMSI. Nous apporterons par la suite les recommandations jugées nécessaires qui découleront de notre synthèse.

Nous notons que différents aspects peuvent influencer la gestion de la sécurité de l'information. Nous aurons donc à apprécier dans le contexte de l'analyse par les risques:

- ✓ les ressources humaines : la direction générale, le personnel en charge de la sécurité de l'information, les autres membres du personnel etc.
- ✓ le système informatique : la gestion des applications, matériels informatiques et logiciels, les réseaux, l'environnement physique etc.
- ✓ la gestion des données ou informations, classification, sauvegarde, plan de continuité d'activités et de gestion des incidents etc.
- ✓ l'organisationnel (politiques, procédures et règlements en vigueur, organigramme, conformité)

Notre évaluation aura pour but principal de s'assurer du respect de l'intégrité, de la confidentialité et de la disponibilité de l'information au sein de ECOBANK CI.

3.3 La collecte de données

Les données seront recueillies à travers différentes techniques. Celles assorties à notre recherche sont la revue documentaire, l'interview, l'observation et les tests de conformité. Ces données seront analysées à travers les normes et référentiels applicables à la sécurité de l'information.

3.3.1 Les outils de collecte des données

Les outils sont :

- ✓ **la revue ou analyse documentaire**: elle sera utilisée dans l'étape de l'évaluation de la gestion de la sécurité de l'information et des opérations et technologies de sécurité informationnelle. Il s'agit d'étudier de façon attentive et intellectuelle tout type de document relatif à la sécurité de l'information, édité bien évidemment par la banque. Cela nous permettra d'avoir une meilleure compréhension des processus de la banque. Ces documents sont entre autre la politique de sécurité, les procédures de sécurité de l'information, les mémorandums, les états de gestion des réseaux, les révélés d'évènements inhabituels (s'il en existe), les « jobs descriptions » pour les employés chargés de la gestion de la sécurité de l'information, les anciens rapports d'audit et tout autre type de document susceptible de nous aider dans notre étude.
- ✓ **l'interview** : il s'agit ici de rencontrer des personnes ressources dans les domaines du management des systèmes d'information, de la sécurité du système d'information et de l'audit interne. Ces entretiens nous permettront d'avoir des informations pertinentes sur le processus de gouvernance du SI et la sécurité du SI d'une part et d'autre part sur l'audit interne face à la sécurité de l'information. L'interview se fera sous forme de questionnaire de prise de connaissance et également à certaines étapes sous le style narratif.
- ✓ **l'observation** : il s'agit d'observer les évènements à travers les tests d'intrusion dans le système, aussi apprécier l'environnement physique où sont stockés les matériels informatiques (serveurs, câblages, lieux physiques, ordinateurs…). On pourra aussi

observer et apprécier l'attitude des agents face au maintien et au respect des règles et procédures de sécurité de l'information (étant entendu qu'eux aussi traitent et véhiculent l'information).

- ✓ **les tests de conformité** : à travers ces tests, nous pourrons apprécier la conformité des actions menées par rapport aux procédures et politiques de l'entreprise en matière de sécurité de l'information.

3.3.2 Les outils d'analyse des données

Pour évaluer la conformité du SMSI de Ecobank CI d'avec les critères ou exigences de la norme ISO 27002, comme nous l'avons dit plus haut, nous établirons un système de cotation du SMSI. C'est un système de cotation établit par le CobiT (cotation CMMI). Ce système allant de 0 à 5 nous permettra d'évaluer le niveau de maturité du SMSI de Ecobank CI. Il mettre en exergue la maturité souhaite par l'entreprise qui est normalement notée à 5 et le niveau actuel du SMSI. Les significations sont les suivantes :

- 0 : le critère n'est absolument pas rempli
- 1 : le critère est insuffisamment rempli et présente plusieurs carences majeures
- 2 : le critère est insuffisamment rempli et présente une seule carence importante
- 3 : le critère est insuffisamment rempli mais ne présente que des carences mineures
- 4 : le critère est rempli (situation acceptable)
- 5 : le critère est parfaitement rempli (situation optimale)

Les notations 0,1 et 2 démontreront une non-conformité avec les critères ou exigences de la norme ISO 27002 ; les notations 3 et 4 attesteront d'une conformité plus ou moins complète. Seule la notation 5 pourra confirmer une conformité parfaite au exigences de la norme ISO 27002

Pour l'analyse des données, nous établirons un tableau des risques qui ressortent des carences constatées afin de mieux appréhender les points de contrôle de la banque, auxquels pourra s'intéresser l'auditeur interne en matière de sécurité de l'information. Dans ce même tableau seront présente les faiblesses recueillies du SMSI. Ensuite des recommandations, découlera la

contribution que peut apporter l'audit interne au maintien et à l'amélioration continue de la sécurité de l'information.

Conclusion de la première partie

Au terme de l'étude théorique, nous pouvons dire que l'information est un capital essentiel de l'entreprise qu'il faudrait sécuriser. Elle est importante en ce sens qu'elle permet la prise de décisions stratégiques et la bonne orientation des taches et actions pour l'atteinte effective des objectifs fixés. Néanmoins le manque d'intégrité, de confidentialité et de disponibilité de cet actif peut provoquer des pertes financières énormes pour l'entreprise qui la détient. Cependant il existe l'audit interne qui est un outil d'aide au management, d'évaluation de processus de gestion et qui contribue à la création de valeur ajoutée. Son rôle au sein de l'entreprise est bénéfique pour le maintien et l'amélioration continue de la sécurité de l'information. Il doit permettre à la banque de réduire l'impact des risques qui pèsent sur son SI, d'atteindre avec efficacité ses objectifs et de rehausser son image et sa crédibilité devant la concurrence sans cesse croissante. Aussi les normes ISO 27000 et les divers référentiels (CobiT et la commission bancaire) nous donnent de bonnes pratiques pour l'implémentation d'un cadre de gestion adéquat de cette sécurité dans le but unique de parvenir à la pérennisation de l'entreprise dans le monde des affaires actuel.

Ayant obtenu toute la théorie nécessaire sur l'audit interne et la sécurité de l'information en milieu bancaire, nous allons avec l'exemple de ECOBANK CI, confronter la théorie à la pratique.

PARTIE 2 : CADRE PRATIQUE DE L'ETUDE

Divers secteurs d'activités dans le monde des affaires actuel présentent des systèmes d'information dûment automatisés. Notre étude s'est portée sur le secteur bancaire car celui-ci est géré au sein d'une plateforme de hautes technologies de l'information. Il en est ainsi à cause de la multitude de transactions que requiert l'activité bancaire au sein de la banque elle-même et dans sa corrélation avec les autres banques.

Ainsi l'activité bancaire repose toute entière sur la confiance, et il ne peut y avoir de confiance sans sécurité. Il n'y a pas non plus d'activité financière, ni économique sans prise de risques. Les marchés financiers engendrent principalement divers risques. Prendre donc l'exemple d'une banque pour effectuer notre étude nous permet d'apprécier l'implémentation et la gestion d'une sécurité de l'information dans un système purement automatisé. Ecobank Côte d'Ivoire est par ricochet la cible de notre étude à cause de sa constance évolution et de la place importante qu'elle occupe aujourd'hui dans le milieu bancaire en Côte d'Ivoire.

CHAPITRE 4 : PRESENTATION GENERALE DE ECOBANK COTE D'IVOIRE

Ecobank CI fait partir du Groupe Ecobank Transnational Incorporated (ETI). Ainsi avant d'entamer la présentation de Ecobank CI, nous ferons l'historique du Groupe afin d'apprécier l'évolution et la place de cette banque dans le milieu bancaire.

4.1 Historique du Groupe Ecobank

ETI, Ecobank Transnational Incorporated, est une société anonyme à responsabilité limitée créée en 1985 comme holding bancaire à l'initiative de la Fédération des chambres de commerce d'Afrique de l'Ouest avec le soutien de la CEDEAO. Au début des années 1980 l'industrie bancaire en Afrique de l'Ouest était dominée par les banques étrangères et appartenant à l'État. Il n'existait pratiquement aucune banque en Afrique de l'Ouest appartenant ni étant gérée par le secteur privé africain. ETI a été fondée dans le but de combler ce vide. Un accord de siège a été signé avec le gouvernement du Togo en 1985 qui confère à ETI le statut d'organisation internationale jouissant des droits et privilèges nécessaires lui permettant d'exercer en tant qu'institution régionale, avec un statut d'institution financière non-résidente.

ETI a commencé ses activités avec sa première filiale au Togo en Mars 1988. Aujourd'hui avec ses filiales et ses partenaires, elle est déployée dans 34 pays africains et est cotée à la bourse nigériane, celle du Ghana et celle de la Cote d'Ivoire (BRVM). Elle était depuis 2012, sous la direction générale de M. Thierry Tanoh, et est aujourd'hui dirigée par M. Albert Essien (depuis mars 2014). Le Groupe dispose également d'une filiale à Paris et des bureaux de représentation à Dubaï, Johannesburg, Londres, Luanda et Pékin. Notons que ETI est une banque panafricaine axée sur l'Afrique offrant des services de banque de détail, banque de grand clientèle et banque d'investissement et services bancaires transactionnels aux gouvernements, aux institutions financières, aux sociétés multinationales, aux entreprises locales, aux PME et aux particuliers. Elle a aujourd'hui des représentations en Europe et en Asie et un centre mutuel de services informatiques à Accra.

4.2 Présentation, organisation et missions de Ecobank CI

En premier lieu, nous ferons la présentation de Ecobank CI ainsi que son évolution sur le marché bancaire. Puis nous décrirons son organisation fonctionnelle et structurelle et enfin ses objectifs et missions qui la poussent à une constante évolution**.**

4.2.1 Présentation de Ecobank CI

Ecobank Cote d'Ivoire est donc une filiale du groupe ETI. Elle a été implantée en Côte d'Ivoire en octobre 1989 et a son siège à Abidjan la capitale économique ivoirienne, plus précisément au Plateau dans la commune administrative. Etant une banque panafricaine ayant plus de 20ans d'existence, elle présente un atout considérable pour la clientèle ivoirienne de par ses produits divers et sa proximité et est depuis 2012 à la 2eme[3] place du marché bancaire ivoirien derrière la Société Générale (SGBCI). Elle est présente dans plusieurs villes et communes du pays et compte à ce jour 48 agences et plus de 600 employés.

4.2.2 Organisation administrative et structurelle de ECOBANK CI

Dans le but de mieux organiser et structurer la banque, chaque filiale a en son sein un conseil d'administration, une direction générale et des directions opérationnelles. Les filiales sont tenues par les mêmes objectifs globaux établis par le groupe et évoluent à travers un management centralisé. Les décisions sont prises par le Conseil d'Administration du groupe et doivent être promptement appliquées. Les filiales rendent compte directement à la maison mère.

La structure organisationnelle de Ecobank CI comporte (Voir organigramme en annexe):

- ✓ **le Conseil d'Administration :** qui détermine les grandes lignes de conduite de la structure ainsi que les objectifs globaux ;
- ✓ **la Direction Générale** : Elle coiffe toutes les directions de la banque, elle donne toutes les décisions, autorise et coordonne les changements dans chaque direction ;

[3] Tiré des nouvelles du site Abidjan.net, section économie, publié le samedi 16 février 2013

- ✓ **La direction Juridique /secrétariat Général** : C'est le conseil juridique en charge de tout ce qui est en rapport avec tous les aspects légaux de l'activité ;
- ✓ **la direction Conformité** : Elle s'assure que la banque respecte les exigences réglementaires et veille à la lutte contre le blanchiment des capitaux ;
- ✓ **la direction Audit Interne**: Par des revues programmées ou non, elle s'assure de l'existence, de l'adéquation et de l'efficience du dispositif du contrôle interne ;
- ✓ **la direction Contrôle Interne** : Elle veille à l'application effective des procédures de la banque et contribue ainsi à minimiser les pertes opérationnelles ;
- ✓ **la direction des Opérations et de la Technologie** : Elle exécute toutes les opérations ordonnées par les différents départements ;
- ✓ **la direction des Risques** : Elle évalue les risques auxquels sont confrontés la banque, notamment en matière de crédit et conseille la Direction Générale dans les prises de décision ;
- ✓ **la direction des Ressources Humaines** : Elle est en charge du recrutement, de l'encadrement et de la gestion du personnel ;
- ✓ **la direction Financiere** : Elle est responsable de la gestion financière et de la réduction des coûts de la banque ;
- ✓ **la direction de la Trésorerie** : Elle assure la gestion de la liquidité de la banque en monnaie locale et en devises. Elle est aussi en charge des opérations de la banque sur le marché des capitaux ;
- ✓ **la direction Domestic Bank** : Elle offre des produits et services financiers pratiques, accessibles et fiables aux marchés de détail, aux entreprises locales, aux clients du secteur public et de la micro finance, s'appuyant sur un important réseau d'agence et de Distributeurs Automatiques de Billet (DAB) aussi bien que les plates-formes bancaires mobiles, de banque par Internet et les transferts de fonds.
- ✓ **la direction Corporate Bank** : Elle offre des solutions financières aux entreprises mondiales et régionales, aux entreprises publiques, institutions financières et organisations internationales et s'occupe de la gestion de leur compte.

4.2.3 Mission et activités de ECOBANK CI

La mission de Ecobank CI découle de celle de la maison mère c'est-à-dire bâtir une banque panafricaine d'envergure mondiale et contribuer à l'intégration et au développement économique et financier du continent africain. Par cette mission, elle entend fonctionner à l'échelle mondiale comme une banque unique : les mêmes objectifs, les mêmes procédures et pratiques, la même offre de services caractérisent toutes les agences de Ecobank à travers le monde. De façon particulière, Ecobank CI a pour vision d'être le premier choix de la clientèle ivoirienne et donc le leader des banques en Côte d'Ivoire.

Pour atteindre sa vision, elle s'est fixé des objectifs stratégiques qui sont les suivants :

- ✓ augmenter la taille de la banque par le biais de la croissance organique et les acquisitions ;
- ✓ accroitre le volume des opérations sur les marches ou la banque est déjà présente ;
- ✓ poursuivre l'expansion sur de nouveaux marchés;
- ✓ développer de nouveaux produits et pénétrer d'autres segments de clientèle ;
- ✓ satisfaire les attentes de la clientèle en leur offrant des opportunités d'affaires, des produits et des services d'excellente qualité.

Pour mener à bien sa mission, Ecobank CI offre des services de trésorerie, de financement d'entreprise et de banque d'investissement bancaires, des solutions de gestion des valeurs mobilière et d'actif pour des entreprises clients et gouvernement.

Ecobank CI dispose d'une gamme de produits et services bancaires répondant aux besoins divers de la population (entreprises et particuliers). Nous avons : des comptes courant ; comptes épargne ; cartes bancaires ; dépôts à terme ; crédit particulier ; crédit auto/moto ; crédit immobilier ; crédit commercial ; crédit documentaire ; transferts & règlements ; opérations de change ; western union.

Ecobank possède une plateforme technologique intégrée supportant l'ensemble de ses opérations nommée FLEXCUBE. Les services d'Ecobank sont délivrés à travers trois secteurs d'activité axés sur la clientèle, Corporate Bank, Domestic Bank et Ecobank Capital et sont pris en charge

par une plate-forme informatique mutualisée, gérée par e-Process, la filiale technologique du groupe. Par conséquent, Ecobank CI évolue dans un système purement automatisé, ce qui ne l'exclut pas de nombreux risques de sécurité inhérents au système d'information.

Nous avons eu l'occasion de mener notre étude en étant dans la direction de l'audit interne d'Ecobank CI. Le prochain point nous donnera une brève présentation de cette direction.

4.3 Présentation de la direction de l'audit interne

La direction Audit interne est rattachée administrativement à la Direction Générale et fonctionnellement au Groupe Audit de la maison mère ETI et rend compte au Comité d'audit émanant du Conseil d'Administration de la banque. Cette direction est constituée d'un directeur, 3 auditeurs internes permanents et des stagiaires. Parmi les auditeurs internes, on en retrouve seulement un qui a des compétences en audit informatique. Ladite direction effectue des missions d'audit financier et opérationnel et veille au respect des procédures et à l'efficience du dispositif de contrôle interne dans les différentes agences d'Ecobank CI à travers tout le pays.

La direction de l'audit interne établit elle-même ses plans d'audit en fonction des insuffisances constatées et d'une cartographie des risques et en fait la proposition au Conseil qui les approuve et les valide. Chaque auditeur est tenu de participer aux formations continues afin d'améliorer ses compétences.

Il faut dire que la compréhension du rôle de l'audit interne est visible au sein de Ecobank CI puisque la Direction Générale lui accorde la place qu'il faut dans les prises de décisions et d'amélioration continue de l'entreprise. Par ses analyses et recommandations, la direction de l'audit interne peut se prévaloir d'être un des organes garant de la pérennité de Ecobank CI.

Le prochain chapitre nous donnera plus ample informations sur le cadre de gestion de la sécurité de l'information de la banque et nous décrirons la fonction de l'audit interne en matière de sécurité de l'information et le dispositif de contrôle interne établi par la banque pour protéger ses informations.

CHAPITRE 5 : DESCRIPTION ET DIAGNOSTIC CRITIQUE DE LA CONTRIBUTION DE L'AUDIT INTERNE A LA GESTION DE LA SECURITE DE L'INFORMATION AU SEIN DE ECOBANK COTE D'IVOIRE

Dans ce chapitre, nous décrirons le système de gestion de la sécurité de l'information au sein de Ecobank Côte d'Ivoire selon les 6 éléments clés de la norme ISO 27002 définit par ISACA. Ensuite nous procèderons à l'analyse et à l'interprétation de ces résultats et également à la présentation et à l'analyse des risques de sécurité dus aux insuffisances qui seront relevées.

Le système d'information de ladite banque de façon générale n'est pas soumis à un système de management décentralisé. Etant une filiale de la maison mère ETI, Ecobank Côte d'Ivoire fonctionne selon les directives du Groupe en particulier en ce qui concerne la gestion de la sécurité de son système d'information. La description de son SMSI nous donnera de plus amples informations. Les objectifs de la banque en matière de sécurité de l'information sont : fiabilité, disponibilité et sécurité.

5.1 Description du système de gestion de la sécurité de l'information

Il est important avant toute évaluation de prendre connaissance de ce qu'il faut évaluer. Ceci nous permettra d'effectuer au mieux notre analyse et d'apprécier les risques inhérents à la sécurité de l'information et donc à l'activité bancaire. Cette description déroule les 6 étapes clés de la sécurité de l'information telles qu'elles sont comprises et effectuées par Ecobank CI.

5.1.1 Engagement et soutien de la haute direction

La direction générale de Ecobank CI est a pour hiérarchie la haute direction du Groupe ETI. La haute direction du groupe établit la stratégie concernant la sécurité de l'information et les grandes lignes pour son maintien et son respect. Les directions des filiales se chargent de décliner ces directives dans les procédures et processus de la filiale.

La haute direction du groupe s'est engagée dans la gestion de la sécurité de l'information par l'établissement d'une politique de sécurité et par la mise en place d'un groupe fonctionnel

nommé « SECURITY ». Il définit les politiques et procédures applicables en matière de sécurité de l'information au niveau des filiales, toujours sous l'approbation de haute direction.

Le contrôle permanent du SI au sein des filiales est dévolu au Contrôle Interne et plus spécifiquement le Contrôle du système d'information. L'audit Interne est saisi pour des missions de contrôle périodique sur l'efficacité des contrôles en amont. Un compte rendu constant est fait au Groupe ETI sur l'évolution et l'application des stratégies de sécurité de l'information établies.

5.1.2 Politique et procédures

Il existe au sein de Ecobank CI, une politique de sécurité ainsi que des procédures bien formalisées. La politique de sécurité est approuvée par la Direction générale qui est par ailleurs garant de son exécution. En pratique, la spécificité de ces directives l'oblige à déléguer son pouvoir aux directions métiers telles que : la Direction des Opérations et de la Technologie, la Direction du Contrôle Interne et la Direction de l'Audit Interne. Le groupe SECURITY de la maison mère a défini des politiques qui régissent la sécurité de l'information concernant les points suivants: sécurité internet, contrôle d'accès, gestion d'actifs, communication, conformité, ressources humaines, gestion des incidents de manipulation, sécurité des échanges d'information, développement du système, l'organisation de l'information, l'environnement physique. Ces documents sont accessibles à tout le personnel sur l'intranet de la banque. Les processus et manuels de procédures découlent de ces politiques pour permettre à la banque de fonctionner correctement. Pour l'instant trois manuels[4] de procédures relatifs à la sécurité de l'information sont établis. Notons que ces manuels n'existaient pas avant juillet 2013. Ils concernent :

- ✓ gestion des données des ordinateurs (portable / de bureau)
- ✓ gestion du réseau pour la sécurité de l'information;
- ✓ gestion du réseau WLAN

[4] Informations reçues suite au questionnaire de prise de connaissance du SMSI

La mise à jour des procédures tient compte de l'évaluation annuelle des risques en chaque début d'année. La cartographie des risques comprend tous les risques y compris ceux relatifs aux technologies de l'information.

5.1.3 Organisation

Concernant l'organisation, il existe un responsable de la sécurité de l'information à Ecobank CI depuis 2013. Représentant du Groupe SECURITY, il est chargé de la gestion de la sécurité de l'information et de l'ensemble de son système. Il a également pour tâche la planification et la mise en œuvre effective du BCP (Business Continuity Plan). Dans la structure organisationnelle (organigramme), il est rattaché à la Direction Informatique, sous les autres directions métiers de la banque. Nous pouvons néanmoins constater l'absence d'un comité de pilotage de la sécurité au sein de la filiale. Le responsable de la sécurité de l'information collecte les informations bien évidemment auprès des autres corps métiers mais établit seul les stratégies et l'approche adéquate de la gestion de la sécurité pour les différentes activités de la banque.

Il existe aussi une division IT en charge de la maintenance, de la gestion des applications fonctionnelles de base (système d'exploitation, email etc.) et de l'apport de solutions informatique pour supporter le business. Le responsable de la sécurité de l'information est chargé du suivi de l'exécution des grandes lignes de sécurité définie par le Groupe Ecobank. Sur le plan fonctionnel, il fait partie du Groupe Security. Celui-ci émet aussi les objectifs de contrôle à atteindre en matière de sécurité de l'information. Cet organe a une forte implication et assure la promotion de la sécurité de l'information par la sensibilisation et la formation du personnel et aussi par l'acquisition de moyens de contrôle.

Aussi l'audit interne au niveau des filiales s'assure de l'application des procédures établies pour le bon fonctionnement du SMSI et de l'alignement continu du dispositif de contrôle interne aux objectifs fixés par la banque.

Concernant l'organisation des données numériques à traiter, Ecobank CI s'est approprié une application bancaire nommée FLEXCUBE. Cette application a remplacé une autre du nom de GLOBUS qui était devenu obsolète pour l'activité de la banque. Quant aux données matérielles

ou physiques, elles sont classées et conservées dans des armoires ou des cartons sans ordre de priorité particulier à l'intérieur de salles établies à cet effet.

Pour la gestion de la sécurité de l'information d'avec l'extérieur, Ecobank CI utilise des moyens comme désactiver les ports USB, la sensibilisation des partenaires externes et le contrôle des accès. Les contrats faits avec l'extérieur présentent des clauses claires de confidentialité.

5.1.4 Sensibilisation à la sécurité et éducation

Avant tout embauche ou stage, la banque vérifie la véracité des références et la moralité des employés et fait signer des contrats de travail comportant des clauses de confidentialité. Ensuite les différents corps de métier de la banque sont sensibilisés sur l'importance de la sécurité de l'information par des formations obligatoires sur le site d'E-learning du Groupe Ecobank. Même si ces formations ne sont pas régulièrement organisées (soit 2 fois par an), à travers ces dernières, le personnel prend connaissance des dispositifs de sécurité de l'information et des procédures et politiques à cet effet. Il peut par ricochet apprécier leur importance et également savoir comment les mettre en œuvre.

Il faudrait noter que le personnel de Ecobank CI met en œuvre des différentes instructions concernant la sécurité de l'information malgré quelques petites erreurs que nous avons souvent eu à constater. Ces erreurs sont dues quelques fois à de mauvaises manipulations ou traitements des données et ont souvent eu des répercussions sur les missions d'évaluation.

Le personnel de Ecobank CI participe également au maintien de la sécurité de l'information en signalant par une adresse de messagerie définie, tout cas qui pourrait laisser penser à des tentatives de violation du système de sécurité ou des tentatives non autorisées d'accès à l'information. Il participe de plus à la sécurité en se soumettant aux formations thématiques qui sont obligatoires et pilotées par la Direction des Ressources Humaines. Les cas de violation grave de la politique ou des procédures de sécurité de l'information sont traités comme des fautes professionnelles.

5.1.5 Contrôle et conformité

Au sein de Ecobank CI, les directions en charge de la mise en œuvre des contrôles de premier et second niveau sont la Direction des Operations et Technologie et la Direction du Contrôle interne. Ces contrôles concernent la sécurité des réseaux, les outils informatiques, la gestion des privilèges et la protection des informations. En effet ces contrôles sont effectués de façon permanente pour s'assurer du maintien de la sécurité informationnelle.

Pour ce qui est de la sécurité des réseaux et des outils informatiques, des mesures sont prises pour que les accès soient dument authentifiés et que les medias amovibles fassent l'objet d'un contrôle particulier. Tous les ordinateurs connectés au système de la banque sont contrôlables par les responsables TI habilités d'où il y a un suivi permanent de chaque action. Cependant il n'existe aucune procédure édictée pour surveiller l'utilisation du système de la banque et les systèmes d'information ne relèvent d'aucune exigence statutaire, règlementaire ou contractuelle formelle.

Pour ce qui concerne la gestion des accès et la protection des informations, les zones où sont stockés les moyens de traitement de l'information sont protégés par des moyens d'entrée et de sortie selon le périmètre de sécurité pour s'assurer que seules les personnes autorisées y ont accès. Les badges d'accès et les identifiants et mots de passe pour les applications informatiques sont règlementés par la Direction du contrôle interne. Elle attribue les accès après approbation et validation de la Direction Générale. Les accès sont donnés en fonction de l'importance de la tâche à accomplir et de la fonction. Notons que lorsque le contrat de travail d'un employé permanent ou temporaire prend fin, l'accès aux informations lui est immédiatement retiré après saisine du Département des Ressources Humaines.

Il existe aussi à Ecobank CI, des tests de restauration des données et des tests de cryptographie pour protéger et contrôler les informations. Ces informations pour être convenablement classées et conservées, sont dupliquées sur un site secondaire distant qui peut prendre le relais dès que le site primaire est non opérationnel.

Pour s'assurer de leur conformité avec la politique et les normes de sécurité, chaque entité de l'entreprise est sujette à des revues régulières par l'audit interne. Les directions elles-mêmes

engagent des actions pour garantir que toutes les procédures de sécurité, dans le périmètre de leur responsabilité, sont correctement suivies. Mais le plus souvent, ce sont les inspections du contrôle interne et de l'audit interne qui décèlent des défaillances et s'attèlent à ce qu'il y ait un suivi pour correction. Il faut souligner que les recommandations ne sont pas toujours correctement suivies par les opérationnels mais les différents organes de contrôle donnent par des moyens adéquats, l'assurance de la réduction considérable du risque.

5.1.6 Gestion et intervention face à l'incident

Il existe des procédures de gestion des incidents au sein de Ecobank CI. Le personnel est constamment sensibilisé sur les incidents et leur gestion. Ainsi, les incidents de sécurité sont signalés en temps réel et dès leur survenance. Il existe également des procédures et des outils pour signaler les dysfonctionnements des programmes mais elles ne sont pas tout le temps suivies. Toujours est-il que lorsqu'un incident survient, qu'il soit majeur ou mineur, les plans d'intervention et de relance des activités se mettent en marche pour éviter un temps de latence trop long. Notons que ces plans sont régulièrement mis à jour. Les interventions pour la gestion des incidents dépendent de la nature de l'incident (les prestataires pour la gestion du serveur, la compagnie d'électricité pour les pannes de courant, e-Process pour la base de données).

Il existe un comité de technologie qui se tient informé de la gestion des TI chaque trimestre et fait un compte rendu à la Direction Générale. Et pour s'assurer que les incidents ont été gérés au mieux et selon les procédures, il existe un comité d'urgence. Ce comité est composé du DG, de la Direction des Finances, du Responsable de la sécurité, de la Direction de l'audit interne, la Direction du contrôle interne, la Direction des opérations et la Direction des RH. Le comité d'urgence ne se réunit le plus souvent qu'en cas d'incident majeur. Il a donc une approche réactive face aux incidents. Des décisions sont prises et des acteurs sont mandatés pour les exécuter. Ceux-ci tiennent le comité informé de l'évolution de la situation et quand la menace est maîtrisée, un point final permet de remettre en veille ledit comité.

Pour la sauvegarde des informations de son SI bancaire, Ecobank CI dispose de plusieurs sites distants (Ghana, Londres, Paris) lui permettant de toujours fonctionner correctement en cas de défaillance. Il faut aussi noter qu'en CI, il est possible de continuer de travailler indépendamment

du Ghana pendant une journée entière. Notons cependant que la sauvegarde sur les sites secondaires ne concerne que les données du système contenues dans les serveurs (information clients, dossier de crédit, données sur les plateformes de transferts et de transaction etc.). Les informations traitées sur les ordinateurs de bureaux, ordinateurs portables ou autres appareils mobiles, en cas de sinistre grave, sont définitivement perdues.

Voici ainsi décrit le cadre de gestion de la sécurité de l'information au sein de Ecobank CI. La prochaine étape sera de décrire la fonction de l'audit interne et son implication au maintien de la sécurité de l'information avant toute confrontation à la théorie.

5.2 Description de la fonction de l'audit interne et du dispositif de contrôle interne

Nous allons d'abord décrire la fonction d'audit et par la suite, nous prendrons connaissance du dispositif de contrôle interne mis en place par Ecobank CI pour la gestion de la sécurité informationnelle.

5.2.1 La fonction d'audit interne

Pour ce qui est de la pratique de l'audit interne concernant la sécurité de l'information, nous notons que les auditeurs internes ont une connaissance générale mais non suffisante de la norme ISO 27002 (selon les réponses au questionnaire de contrôle destiné à la direction de l'audit interne).

Concernant les missions d'audit interne à cet effet, il y a une seule mission d'audit interne sur la sécurité de l'information qui a eu lieu en 2011. Apres cette date, il n'a été organisé que des missions partielles d'évaluation de la sécurité physique et logique. Ceci est dû au fait qu'après 2011, une centralisation des systèmes sensibles a été effectuée sur la plateforme e-Process à Accra et donc une partie des risques n'est plus du ressort de la filiale. La méthodologie adoptée pour la mission de 2011 a été de deux ordres :

- ✓ l'audit organisationnel : pendant lequel il fallait s'intéresser aux aspects de gestion et d'organisation de la sécurité

- ✓ l'audit technique et physique : il s'agissait ici d'évaluer les mesures de sécurité physique des systèmes et réseaux et celles relative à la sécurité logique des données et ressources.

Les vérifications effectuées lors de la mission d'audit de sécurité de l'information étaient :

- ✓ l'organisation de la structure auditée
- ✓ la mise en place et le bon fonctionnement des outils de sécurité adéquats
- ✓ la formation des agents à l'utilisation et à l'entretien de ces outils
- ✓ le fonctionnement de la stratégie déployée sur les outils des agents
- ✓ les sauvegardes de données et test de restauration
- ✓ le test et la mise à jour du plan de continuité

L'audit interne est chargé de l'évaluation du dispositif de contrôle interne mis en place à tous les niveaux du traitement de l'information. Comme outils utilisés pour réaliser la mission, nous avons la revue documentaire, l'interview, les inspections physiques et la revue des logs. Les logs sont – on peut le dire – des fichiers contenant des enregistrements d'évènements généralement datés et classés par ordre chronologique et générés par des déclencheurs ; ces derniers permettent d'analyser pas à pas l'activité interne du processus et ses interactions avec son environnement.

De façon journalière, seuls les ordinateurs portables et ordinateurs de bureau connectés au réseau de la banque sont vérifiés par le service TI. Notons que la Direction d'audit interne ne dispose pas d'outils ou de logiciels spécialisés d'audit pour inspecter le contenu des fichiers de données (y compris les fichiers de journalisation d'exploitation). Elle ne dispose pas non plus d'outils ou de logiciels spécialisés pour évaluer le contenu de la base de données du système d'exploitation et des fichiers de paramètres d'application (pour détecter les irrégularités dans les réglages des paramètres du système).

Il faut aussi noter le soutien et l'accompagnement que la Direction Générale apporte à la direction de l'audit interne. Cela se démontre par les actions qu'elle engage pour assurer le suivi des procédures de sécurité et les recommandations d'audit. Il faut noter que les recommandations d'audit et les procédures de sécurité ne sont pas toujours suivies par les agents, mais ceci n'empêche pas l'audit interne de jouer pleinement son rôle au sein de la banque.

5.2.2 Le dispositif de contrôle interne en matière de sécurité de l'information

Il faut déjà noter la présence d'un SMSI au sein de Ecobank CI, règlementé au niveau du Groupe ETI. Le SMSI est encadré d'un dispositif de contrôle soumis à tout le personnel de la banque et géré par la Direction du Contrôle interne. C'est cette Direction qui est chargé de veiller au jour le jour à l'application et au respect des mesures sécuritaires établies pour protéger et sauvegarder les informations. Les vérifications effectuées par la direction du contrôle interne couvrent trois principaux types de risques :

- ✓ le risque opérationnel
- ✓ le risque de crédit
- ✓ le risque du marché

Le dispositif de contrôle interne au sein de Ecobank se compose de moyens techniques et physiques.

Pour la sécurité logique, Ecobank CI dispose de pare-feu, d'antivirus, d'un système de cryptographie des données, de la mise en place de codes d'accès pour les applications, de la messagerie web sécurisée (Outlook) pour les échanges de données sensibles, d'un système de filtrage des mails venant de l'extérieur. La banque impose une connexion obligatoire de tous des ordinateurs à son réseau pour un meilleur suivi. Notons également que les ports USB sont verrouillés et sécurisés. La messagerie Outlook offre un cryptage interne et un système d'accusé de réception et de lecture qui permet de s'assurer que le message a été envoyé au bon destinataire et qu'il l'a effectivement reçu et lu. La DCI se charge également des attributions et privilèges aux employés pour les applications du système d'information et autres. En effet des demandes d'habilitations sont émises par les différents corps de métiers existant au sein de la banque au niveau du contrôle interne. Lui, il se charge de vérifier les demandes et d'acheminer les dossiers vers la Direction Générale qui les approuve en apposant sa signature. Ensuite les login et mots de passe sont créés et sont uniques et propres à une seule personne. A la fin du contrat, les privilèges et attributions lui sont immédiatement retirés.

Concernant la sécurité physique, Ecobank CI dispose de gardiens, d'extincteurs, d'un dispositif d'identité magnétique à chaque porte de bureau et des badges d'accès, d'une protection sécurisée

dans le périmètre où se situe le serveur central des bases de données, d'un système d'alarmes, des visuels de signalisation, de caméras de surveillance, de câblages informatiques sécurisés, de plusieurs serveurs distants (pour la continuité d'exploitation), des salles ou entrepôts pour le stockage d'informations et d'outils utiles et sensibles (dossiers comptes clients, dossiers de crédit, matériel de travail). Notons que les informations ne sont pas classées suivant un ordre de priorité particulier mais seulement par catégorie. Les badges d'accès électroniques aux différents offices sont délivrés uniquement par la Direction du Contrôle Interne sous présentation du contrat de travail ou de stage.

La Direction du Contrôle Interne effectue un contrôle journalier de toutes les opérations de l'entreprise pour réajuster les écarts et faire respecter les différentes procédures. Il s'assure que les tâches sont effectivement et convenablement exécutées et que les moyens physiques et techniques mis à disposition sont fonctionnels. L'audit interne se charge de faire un contrôle périodique pour attester du maintien de la sécurité de l'information et de l'efficacité du dispositif de contrôle interne.

Des formations obligatoires sont engagées pour le personnel et des conseils de sécurité sont transmis par courriel régulièrement. C'est également un moyen utilisé par Ecobank CI pour minimiser les risques inhérents à la sécurité de l'information.

Notre prochaine étape est l'essence même de notre étude à savoir le diagnostic critique de la gestion de la sécurité de l'information menée par Ecobank CI. Ce diagnostic nous permettra de confronter la théorie d'avec la pratique et déceler les manquements auxquelles il faudrait remédier.

5.3 Diagnostic critique de la gestion de la sécurité de l'information

L'analyse critique se fera suivant trois étapes : d'abord l'évaluation de la gestion de la sécurité de l'information, ensuite l'évaluation des activités et de la technologie relatif à la sécurité de l'information et enfin la pratique de l'audit interne en matière de sécurité de l'information. L'analyse critique nous permet de comparer la pratique d'avec la théorie en vue de déceler les insuffisances et trouver des solutions adéquates pour le bon fonctionnement de Ecobank CI.

5.3.1 Evaluation de la gestion de la sécurité de l'information

L'évaluation de la gestion de la sécurité de l'information passe par une analyse propre de l'organisation de la sécurité au sein de la banque. Pour évaluer la gestion de la sécurité de l'information, nous procéderons par un examen plus ou moins détaillé de chaque point d'anomalie décelée dans la description du SMSI existant.

5.3.1.1 Absence d'un comité de pilotage de la sécurité de l'information

La première remarque qui ressort de notre évaluation, c'est l'absence d'un comité de pilotage de la sécurité de l'information au niveau des filiales. Cette absence crée un problème dans le processus de gouvernance de la sécurité de l'information. Il est vrai qu'il existe un groupe SECURITY au sein de la maison mère qui se charge d'établir des politiques de sécurité et les pratiques et que des rapports sont transmis par les filiales pour un suivi. Cependant, les risques en l'absence d'un comité de pilotage de la sécurité de l'information au sein des filiales sont de plusieurs ordres. Premièrement les objectifs fixés par la maison mère pour la gestion et le maintien de la sécurité ne sont pas correctement atteints au niveau de tous les corps métiers. On assiste par ricochet à une confusion au niveau des tâches à accomplir et des responsabilités. Ensuite les procédures ne sont pas correctement appliquées parce qu'elles ne sont pas comprises ou entièrement adaptées aux besoins du personnel.

Les risques qui en découlent sont la mauvaise gestion du système, la mauvaise gestion des actifs, le manque de coordination dans les tâches, un manque d'organisation etc. L'absence du comité de pilotage peut entrainer une méconnaissance des réels risques inhérents aux corps métiers. La banque ne pourra pas uniquement compter sur son Risk Manager ou son Responsable de sécurité de l'information ; il est donc d'une importance capitale pour la filiale d'avoir en son sein un comité de pilotage de la sécurité de l'information afin de mieux prendre en compte toutes les difficultés à l'ensemble de l'organisation.

5.3.1.2 Inexistence d'une politique d'appétence pour le risque de sécurité de l'information

Concernant les politiques et procédures, le groupe SECURITY a défini en fonction du besoin de sécurité, une panoplie de politiques utiles pour la bonne organisation et gestion de la sécurité de l'information. Toutes les politiques contenues dans la norme ISO 27001 sont techniquement représentées. A ceux-là s'ajoutent des politiques propres à la banque toujours en fonction de son environnement de travail. Nous constatons néanmoins l'absence d'une politique d'acceptation du risque de gestion. Les risques liés à la sécurité de l'information sont nombreux selon l'ampleur de l'activité bancaire tant à l'intérieur qu'à l'extérieur de la banque. Leur méconnaissance par les employés et les partenaires externes peut créer des erreurs parfois irréparables pour l'entreprise.

Les risques en matière de sécurité de l'information représentent une menace considérable pour les entreprises du fait des possibles pertes et préjudices financiers, perte de services essentiels de réseaux, ou encore perte de confiance des clients et autres atteintes à la réputation qu'ils entraînent. La gestion des risques est l'un des éléments clés de la prévention des fraudes en ligne, vols d'identité, détériorations de sites Web, pertes de données personnelles et autres incidents divers concernant la sécurité de l'information. Faute de cadre solide de gestion des risques, les organisations s'exposent à de nombreux types de cyber-menaces. L'absence de politique de l'acceptation du risque entraine donc des écarts dans les différentes actions à mener étant entendu que les employés n'ont pas réellement connaissance de ce que la banque attend d'eux en matière de gestion des risques de sécurité.

L'analyse de la gestion de la sécurité de l'information nous a permis de faire ressortir des insuffisances au niveau de l'organisation et de la gestion du risque de sécurité.

Notre prochaine étape concerne les activités et technologies de la sécurité de l'information car on ne peut évaluer la gestion organisationnelle de la sécurité de l'information sans évaluer les activités et technologies relatives à la sécurité de l'information.

5.3.2 Evaluation des activités et de la gestion des technologies relatives à la sécurité de l'information

Pareillement à l'évaluation de la gestion organisationnelle de la sécurité de l'information, nous énoncerons point par point les différentes défaillances décelées dans la description du SMSI existant.

5.3.2.1 Inefficience de la gestion de la sécurité de l'information

De l'évaluation des opérations ou activités de sécurité de l'information, nous pouvons noter l'existence d'un service responsable de la sécurité de l'information avec à sa tête un responsable Security, encore appelé Responsable de la sécurité de l'information. Il travaille de concert avec la Division IT, le Contrôle et l'Audit Interne. .

Selon l'organigramme de la structure bancaire, le responsable Security est en staff sous la direction informatique ; ce qui n'est pas de nature à faciliter ses tâches. Il se pose donc le problème d'indépendance de la fonction par rapport au système à évaluer, de temps de réponse aux préoccupations particulières de la filiale et de gestion efficace de la sécurité de l'information. Le responsable Security ne sera pas en mesure de couvrir correctement toutes les zones de sécurité sans l'aide permanente d'un comité de pilotage de la sécurité du système d'information. De plus, chacune des filiales évolue dans un pays différent et donc dans un environnement de travail différent. Par ricochet, les besoins de sécurité et les risques sont également différents.

Le système d'information automatisé se compose d'humains, de matériel informatique et de données diverses. Il est important d'avoir une bonne organisation, impliquer le personnel, appréhender son SI de manière globale. Mais il est aussi nécessaire d'avoir un système informatique sécurisé, car il y a toujours des portes d'entrée qui doivent être protégées.

5.3.2.2. Traçabilité des agents et ouverture du réseau de l'entreprise vers l'extérieur

Nous constatons que chaque utilisateur ayant une activité dans le système s'identifie par un mécanisme clair d'identification (soit un login et un mot de passe). Un journal est

automatiquement généré et fait apparaitre le nom de l'agent qui a passé une opération donnée avec son code d'identification électronique, la date et l'heure de l'enregistrement. Cependant tous ne sont pas parfaitement traçables excepté ceux qui manipulent les informations comptables et données financières (physiques ou numériques). Ce fait pourrait donner l'occasion à un stagiaire ou un employé d'une autre direction de mener des infractions contre la sécurité sans se faire repérer. Même si elles demeurent mineures, on assistera à une atteinte au principe de traçabilité et de non-répudiation.

Aussi le service informatique permet aux ordinateurs portables (délivrés bien entendu par la banque elle-même) d'accéder non seulement aux systèmes d'information mais aussi au réseau internet. Il faut cependant noter que l'accès WEB est restreint par défaut et que les systèmes sensibles sont couverts. Les ordinateurs personnels de même que les informations sensibles contenues dans ses machines ne sont pas totalement exemptent de risques. Ainsi ce fait peut donner lieu à tout type d'infraction. La sécurité du réseau et donc des systèmes d'information est menacée.

5.3.2.3 Périodicité des formations trop longue

Nous savons que le maillon le plus faible au sein d'une entreprise est l'homme. Ainsi il est important de notifier que Ecobank CI, dans le souci d'atteindre effectivement ses objectifs, met en place des formations et des tests en lignes obligatoires pour son personnel. Plus de 80% des employés ont déjà complétés leur formation et cela réduit considérablement le taux d'erreurs et permet aux employés de mieux comprendre l'ampleur de leur tâche et les éléments de sécurité qui s'y rattachent. Si l'aspect humain n'est pas pris en compte, ceci peut entrainer des pertes financières, des pertes d'informations importantes et sensibles.

Ce que nous remarquons par contre au niveau des formations, c'est la périodicité ou la fréquence de celles-ci. En effet, les agents peuvent recevoir seulement une ou deux formations dans l'année. Ce qui est très peu vu l'évolution technologique rapide et l'environnement de mondialisation dans lequel évolue la banque. Il y a par conséquent de nouveaux risques qui surviennent dont le personnel doit prendre connaissance et quels sont les mesures et moyens de sécurité à adopter pour réduire le risque.

5.3.2.4 Méthodologie de classification des informations non optimale

Nous avons remarqué que les informations sont classées seulement par catégorie et non par ordre de priorité particulier. Les informations physiques telles que les dossiers d'ouverture de compte, les dossiers de crédit et autres sont stockés à différents endroits selon la classification personnelle des gestionnaires de ces actifs. Les informations numériques personnelles quant à elles sont stockées sur les ordinateurs de bureaux, les ordinateurs portables et autres appareils mobiles sans balises de sécurité et méthodes de classification particulières.

Nous savons que la protection de l'information commence par la classification de celle-ci selon son degré de sensibilité et son niveau de partage. Une mauvaise classification peut occasionner une mauvaise prise de décisions de la part du management. Il sera difficile pour ce dernier d'apprécier quelles informations sont les plus importantes à prendre en compte. Ce fait peut aussi entrainer la banque vers des horizons risqués qu'elle n'avait pas forcément prévu. La norme ISO 27002 exige que les informations soient classées par ordre de priorité afin de mieux orienter les outils de sécurité pour les données sensibles. Les informations doivent être classées du plus important au moins important et du plus sensible au moins sensible.

5.3.2.5 Gestion de la sauvegarde des données sur les ordinateurs et appareils mobiles

Dans notre description du SMSI de Ecobank CI, nous avons pu noter que les plans de sauvegarde sont assez performants. Les serveurs conservent les informations des différents systèmes de la banque et se relaient en cas de panne de l'un d'eux. Ainsi les informations concernant les clients (particuliers ou entreprises) contenues dans les logiciels d'enregistrement et de gestion des bases de données sont sauvegardées. Ceci répond au plan de continuité des activités de la banque pour éviter toute rupture d'informations.

Néanmoins nous pouvons remarquer qu'aucune mesure n'a été prise pour la conservation des données sur les ordinateurs de bureau ou portables et autres appareils mobiles (tablette numérique, téléphone portable, clé USB etc.). Les antispams et antivirus ont uniquement pour rôle la protection des données mais pas leur conservation. Aujourd'hui la menace des formules BYOD (Bring Your Own Device) est très fréquente dans les entreprises. Les managers autorisent

le personnel à venir avec leurs propres appareils mobiles pour effectuer leur travail. Les appareils mobiles sont connectés au réseau de l'entreprise pour faciliter le travail partout où les agents se trouveront. Le plus souvent les terminaux personnels sont des dispositifs Apple[5], Samsung ou BlackBerry. Ces dispositifs présentent des exigences de bandes passantes et des connectivités inconnues du gestionnaire des terminaux et réseaux de l'entreprise. Par conséquent ces dispositifs de travail restent généralement sans sécurité et utilisent les mêmes ressources que les terminaux internes de l'entreprise. En cas de sinistre ou de vol, il n'y a aucun moyen de récupération des données. Les informations perdues peuvent être utilisées à mauvaise escient et cela pourrait porter atteinte à la réputation de la banque.

5.3.2.6 Gestion des badges d'accès et privilèges par la Direction du Contrôle Interne

Un point qui s'avère être une force pour Ecobank CI, c'est que chaque individu en fonction de son poste, a un privilège qui l'autorise à entrer dans les applications du système nécessaire seulement pour son travail. Ceci est une exigence du CobiT. Il insiste sur le fait que les droits et privilèges de chaque utilisateur par rapport aux données et aux systèmes doivent être en phase avec les besoins d'affaires de l'entreprise et que le rôle joué par l'utilisateur doit être parfaitement lié aux besoins du poste qu'il occupe.

En revanche CobiT explique que les droits d'utilisateurs doivent être requis par le service de la gestion des utilisateurs, approuvés par les propriétaires du système et exécutés par le personnel responsable de la sécurité de l'information. Mais le constat que nous faisons, c'est qu'au sein de Ecobank CI, à défaut d'être approuvés par la Direction Générale (et donc les propriétaires du système), chaque droit d'utilisateur est demandé par la Direction à laquelle il appartient et c'est la Direction du contrôle interne qui se charge de l'attribution des droits. Dans ce cas de figure, l'on peut dire que la Direction du contrôle interne de Ecobank CI joue aussi le rôle d'un service responsable de la sécurité de l'information. Si cette tâche n'est pas contrôlée et règlementée, elle pourrait porter atteinte au principe de séparation des tâches incompatibles étant donné qu'il existe déjà un responsable de la sécurité de l'information. Ce fait peut aussi porter atteinte à

[5] Apple: entreprise multinationale qui conçoit et commercialise des produits électroniques grand public

l'objectivité de la Direction du Contrôle Interne qui est supposée garantir la fiabilité et l'efficacité du dispositif de contrôle interne.

5.3.2.7 Approche réactive du comité de gestion des incidents

Un autre point fort est la présence d'un comité de gestion des incidents. Ce comité a pour charge de réfléchir sur les problèmes ou incidents qui surviennent dans le courant des activités de la banque et d'apporter des solutions pertinentes pour les résoudre.

Nous notons cependant que ce comité ne se réunit qu'en cas d'incidents majeurs de sécurité et après leur gestion, il est mis en pause jusqu'à la survenance d'autres incidents. On dira que la gestion des incidents est abordée sur une base réactive. Il ressort donc de ce fait un manque de planification anticipée des différents problèmes (sachant que d'un problème peut découler plusieurs incidents). Ceci peut entrainer une compréhension erronée des problèmes à traiter et l'apport de réponses inadéquates ou tardives aux incidents survenus.

Normalement chaque incident résolu dans le passée devrait permettre avec l'expérience de résoudre le même incident en cas de survenance. Toutefois nous sommes dans une ère nouvelle de mondialisation et de nouvelles technologies. Les risques sont multipliés et les incidents et problèmes sont de plus en plus nombreux. Il est vrai que le management de la technologie est trimestriellement suivi. Néanmoins, gérer les incidents sur base réactive n'est pas toujours efficace surtout que les incidents peuvent être d'ordre divers. Les conséquences qui en découlent peuvent avoir un impact préjudiciable pour la banque et pour ses activités qui dépendent aujourd'hui encore plus des nouvelles technologies de l'information.

A toutes ces insuffisances, l'audit interne doit pouvoir apporter des recommandations pour y palier et ainsi créer de la valeur ajoutée. La prochaine étape nous permettra donc d'analyser l'impact que l'audit interne de Ecobank CI a eu sur son SMSI. Notre analyse s'axera autour de la méthodologie utilisée pour l'évaluation de la sécurité de l'information et de la compétence dont font preuve les auditeurs internes.

5.4 Analyse de l'implication de l'audit interne à la sécurité de l'information

Comme nous l'avons signifié plus haut, la Direction de l'audit interne n'a mené qu'une seule mission de sécurité de l'information qui a eu lieu en 2011. En effet cela peut-être dû au fait que le SMSI de la banque n'existe que depuis peu ou qu'il y a un manque de moyens d'évaluation de la sécurité de l'information ou encore que les compétences et connaissances en matière d'évaluation d'un SMSI sont insuffisantes. Dans cette analyse, nous énoncerons de façon détaillée chaque point qui nous semble être une faiblesse dans l'implication de l'audit interne à la sécurité de l'information.

5.4.1 Les missions d'évaluation de la sécurité de l'information

La première remarque à faire c'est que l'audit de la sécurité de l'information a été effectué une seule fois et en 2011. Cet audit faisait partir du plan de mission de 2011. Sachant que la Cote d'Ivoire a connu une crise due aux élections présidentielles de 2010, cet audit a aussi été surement mené dans le but d'apprécier le fonctionnement du dispositif de contrôle interne. Après 2011, la centralisation des systèmes sensibles s'est faite sur la plateforme e-Process au Ghana. Ainsi les auditeurs internes ont vu leurs tâches être réorientées puisqu'une partie des risques est gérée au Ghana à Accra.

Cependant comme nous l'avons dit plus haut, chaque filiale évolue dans un environnement de travail différent. De 2011 à cette année-ci, Ecobank CI a connu beaucoup d'évènements tels que l'acquisition de nouveaux biens, le changement du système de gestion informatisé des données, l'accroissement de la clientèle, la signature de nouveaux contrats avec des partenaires extérieurs etc. Cette situation a occasionné de nouveaux risques qui devraient faire l'objet de nouveaux audits. Fort heureusement, l'audit interne couvre périodique lors de ses missions les aspects qui touchent la sécurité de l'information. Néanmoins des revues dédiées à la sécurité de l'information devraient être instituées afin de couvrir le maximum des risques qui y sont inhérents.

5.4.2 La méthodologie d'audit du SMSI

Concernant la méthodologie d'audit du SMSI, les auditeurs internes ont opté pour une analyse en 2 étapes : audit organisationnel et l'audit technique et physique. L'audit organisationnel pour vérifier l'organisation de la structure à auditer, la formation du personnel et le fonctionnement de la stratégie déployée sur les outils ; ensuite l'audit technique et physique pour s'assurer de la mise en place et le bon fonctionnement des outils de sécurité, de la sauvegarde des données et de la mise à jour du plan de continuité. Nous notons que la méthodologie utilisée en elle-même est une méthode établie par l'IFACI. Mais ce qui nous importe ici c'est le contenu de la méthode pour évaluer la gestion de la sécurité de l'information.

Le constat que nous faisons est qu'avec la centralisation des systèmes sensibles de Ecobank CI à Accra au Ghana, une grande partie des risques de sécurité ne sont plus du ressort de la filiale. C'est aussi la raison pour laquelle les missions d'évaluation de la sécurité de l'information sont partielles et sommaires. Elles ne sont effectuées que pour s'assurer de l'application des recommandations par les utilisateurs finaux. Les auditeurs internes et externes mènent des revues au niveau du e-Process (le centre commun de technologie de Ecobank) ; ceci dans le but de rassurer le Management sur la sécurité du SI et de préconiser des mesures pour améliorer la gouvernance du SI. L'insuffisance de cette méthode est que l'audit ne se fait que pour un souci de respect de la conformité aux politiques et procédures et non pour une analyse spécifique des systèmes de pilotage ou de gouvernance de la sécurité de l'information en interne (c'est-à-dire au sein de la filiale elle-même).

Les actions bien que conformes aux règles, peuvent ne pas répondent convenablement au besoin de sécurité de l'information et au besoin d'affaires de la banque. L'IFACI explique que l'audit interne ne doit pas restreindre ses tâches aux procédures ou aux activités de contrôle, mais également prendre en compte l'organisation, le pilotage et la surveillance du processus qui se fondent sur une approche par les risques et une diffusion fiable de l'information.

Les normes ISO 27000 permettent d'établir un cadre adéquat pour la gestion des systèmes d'information de l'entreprise et aussi d'implémenter un SMSI qui répond aux besoins et d'obtenir des moyens de l'évaluer. Si nous partons du fait que les filiales dépendent de la maison

mère, il faut aussi savoir que les environnements de travail et de contrôle sont différents. Ainsi la direction de l'audit interne doit donner l'assurance que le SMSI correspond à son environnement de travail.

5.4.3 Les compétences et outils de travail

Concernant la compétence des auditeurs, nous avions remarqué qu'un seul sur les quatre auditeurs internes avait une formation et une certification en matière de système d'information. A travers le questionnaire d'audit interne sur la sécurité de l'information, nous avons noté en moyenne, une méconnaissance des exigences de la norme ISO 27002 pour les systèmes d'information de la banque. Il est vrai que le référentiel de l'audit interne selon l'IIA n'oblige pas les auditeurs à posséder l'expertise d'un auditeur informatique. Néanmoins, nous remarquons que, bien que sachant quel rôle jouer en tant qu'auditeurs internes, la sécurité de l'information ne fait pas souvent partir de leur programme annuel de mission.

Un autre point est le nombre très faible d'auditeurs pour les 48 agences de Ecobank déployées sur le territoire ivoirien. Cette situation favorise que certaines agences ne soient évaluées que chaque 2 ou 3 ans. Ce qui occasionne l'accumulation de risques divers et des pertes financières. Aussi le faible nombre des auditeurs n'offre pas à la Direction de l'audit interne et donc à Ecobank CI une pluralité de spécialités.

A propos des outils de travail, nous constatons que la Direction de l'audit interne ne dispose pas de logiciels d'audit spécialisés utiles pour les tests d'intrusion ou les tests d'appréciation de la vulnérabilité du système de la banque. Ce manque ne permet pas à l'auditeur interne d'inspecter et d'évaluer en intégralité les systèmes informatiques et les risques présents et ceux qui pourraient survenir.

Nous savons à travers la théorie que l'audit de la sécurité de l'information est rendu obligatoire par la clause 6 de la norme ISO 27001 qui précise que des audits doivent être conduits à intervalles planifiés. De plus, l'IFACI précise que le processus de contrôle de l'audit interne doit viser l'ensemble du dispositif de contrôle interne. En matière de système d'information, l'IFACI explique que les auditeurs doivent effectuer des contrôles des technologies de l'information. Ces contrôles viennent en appui de la gestion et de la gouvernance de l'organisation et comportent

des contrôles généraux et des contrôles techniques sur les infrastructures des technologies de l'information dans lesquelles on retrouve les applications, les informations, les installations et les personnes. Pour cela ils doivent posséder une connaissance suffisante des principaux risques et contrôles relatifs aux technologies de l'information, et des techniques d'audit informatisées susceptibles d'être mises en œuvre dans le cadre des travaux qui leur sont confiés.

Il ressort donc de notre diagnostic critique une lacune quant à l'implémentation de la norme ISO 27002 aux systèmes d'information de la banque. Ecobank CI possède bel et bien un SMSI défini mais sa gouvernance de même que la stratégie d'audit utilisée pour son amélioration continue pourraient être perfectionnées. Un SI est dit fiable s'il procure des informations pertinentes et en temps réel à l'entreprise. Par ailleurs les flux d'information qui en découlent, doivent faire l'objet d'un excellent cadre de sécurité de l'information. La prochaine étape sera pour nous l'occasion d'apporter des suggestions aux difficultés qui ressortent de notre évaluation.

CHAPITRE 6 : RECOMMANDATIONS AU SERVICE D'AUDIT INTERNE A LA CONTRIBUTION DE LA SECURITE DE L'INFORMATION

Le but du processus d'audit interne est d'apporter des suggestions d'amélioration, créant ainsi de la valeur ajoutée pour l'entreprise qui en bénéficie. Notre étude portant sur la contribution de l'audit interne à la sécurité de l'information, a révélé que le rôle de l'audit interne dans la sécurité de l'information n'était pas totalement compris et mis en exergue. Notons que l'avenir de l'entreprise dans un environnement automatisé dépend de la force de son système de gestion de la sécurité de l'information. Nous allons premièrement rappeler le diagnostic critique effectué et ensuite nous apporterons des recommandations qui pourront être des lignes directrices pour les prochaines missions d'audit de la sécurité de l'information.

6.1 Constats du diagnostic de gestion de la sécurité de l'information

L'évaluation de la gestion de la sécurité de l'information et du rôle de l'audit interne pour son maintien et son amélioration a révélé différentes insuffisantes.

Premièrement, Ecobank CI, bien qu'ayant en son sein un responsable de la sécurité de l'information, ne possède pas de comité de pilotage de la sécurité de l'information. De par cette absence, il s'est posé le problème de gouvernance et donc d'organisation de la sécurité de l'information au sein de la filiale. Les procédures étant très récentes, il n'est donc pas évident que les objectifs de sécurité définies par la maison mère soient réellement compris et atteints par les opérationnels de Ecobank CI.

Nous avons aussi pu observer qu'au sein de Ecobank CI, la Direction du contrôle interne joue le rôle de responsable de la sécurité de l'information en attribuant sous autorisation de la Direction Générale les badges d'accès et les privilèges aux agents. Le risque qui ressortait si cette tâche n'était pas objectivement effectuée était la dérogation au principe de séparation des tâches. Nous avons pu déceler les problèmes dus à la sauvegarde sur les stations de travail et divers appareils mobiles. En cas de perte d'un appareil ou de sinistre, les informations contenues dans ces machines seront définitivement perdues ou utilisées à d'autres fins. Nous avons également fait

ressortir l'approche réactive du comite de gestion des incidents (encore appelé comité d'urgence) qui fait abstraction de la prévention et qui peut entrainer un retard dans les réponses face aux incidents. Deux autres défaillances ont pu ressortir de notre analyse à savoir la fréquence de formations des agents et l'absence de méthodologie pour la classification des informations.

Ensuite nous avons apprécié l'implication de l'audit interne à la sécurité de l'information. Il en est ressorti que le nombre des missions pour l'évaluation de la sécurité de l'information reste insuffisant malgré le fait qu'une partie des risques est gérée par le site du Ghana.

A travers le tableau récapitulatif ci-après, nous allons, avec les différentes étapes d'audit de la sécurité qui nous ont permis d'effectuer notre diagnostic, apprécier les risques dus aux insuffisances relevées. Chaque constat sera noté d'une mention (élevée, moyen, faible) afin de montrer son criticité au sein de la banque. Le tableau récapitulatif se présente comme suit :

TABLEAU 1 : Tableau récapitulatif des insuffisances relevées et leurs risques respectifs

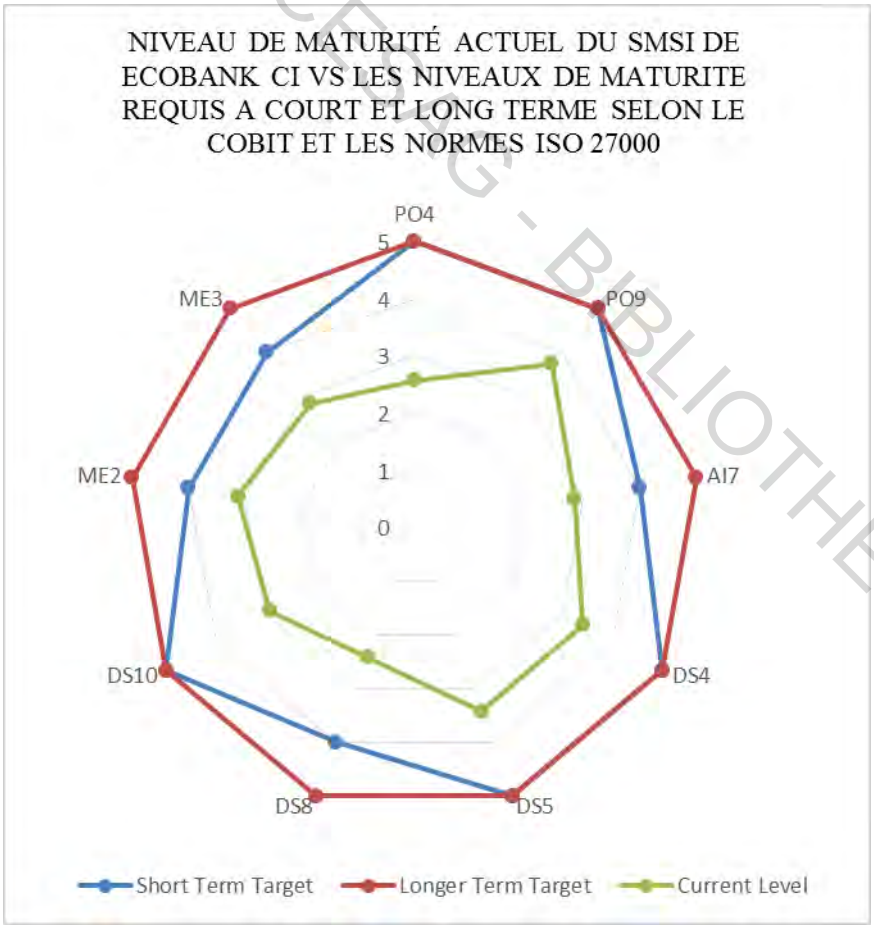
ETAPES D'AUDIT	CONSTATS	RISQUES	MENTION / CRITICITE
Gestion de la sécurité de l'information	- absence d'un comité de pilotage	- inexistence d'une organisation claire de sécurité de l'information	MOYEN
	- politiques et procédures très récentes	- adaptation lente - difficultés à gérer le changement et à impacter la culture de l'entreprise	MOYEN
	- méconnaissance de la politique de risques par les opérationnels	- réalisation de tâches incompatibles - fraudes - mauvaise manipulation de données à répétition - incompréhension dans l'accomplissement des tâches - tolérance d'incidents qui peuvent s'avérer de haute importance pour la banque - disparité des pratiques en matière de risques	ELEVE
Evaluation des opérations de sécurité	- inefficience dans la gestion de la sécurité de l'information	- insuffisance dans la transmission des objectifs de la maison mère en matière de sécurité de l'information - évaluation erronée ou insuffisante des risques de sécurité - mauvaise attribution des responsabilités - méconnaissance des risques inhérents à la sécurité de l'information	ELEVE
	- approche réactive du comité de gestion des incidents	- insuffisance dans la planification des réponses aux incidents - réponses médiates aux incidents - pertes financières	MOYEN
	- Périodicité des formations trop longue	- méconnaissance des risques actuels liés à la sécurité de l'information - méconnaissance des nouvelles technologies de	MOYEN

ETAPES D'AUDIT	CONSTATS	RISQUES	MENTION / CRITICITE
		l'information - pertes financières	
	- inexistence d'une méthodologie formelle de classification des informations	- retard dans les prises de décision - prises de décision erronée - pertes d'informations - transfert d'informations confidentielles ou sensibles aux personnes non autorisées - mauvaise utilisation des informations	MOYEN
Evaluation des technologies de sécurité	- traçabilité des agents et ouverture du réseau de l'entreprise à l'extérieur	- vulnérabilité du réseau - infiltrations des hackers (piratage) - pertes d'informations - pertes financières	FAIBLE
	- gestion de la sauvegarde des données sur les stations de travail et appareils mobiles	- pertes d'informations - fraudes - utilisation des informations à mauvais escient - atteinte à la réputation de la banque	ELEVE

Source : nous-même

Le tableau récapitulatif nous donne d'apprécier les risques qui ressortent du SMSI de Ecobank CI. A travers cette présentation de risques, nous pouvons déduire si le SMSI est vulnérable ou non et si les objectifs de sécurité de la banque sont atteints. Selon notre système de cotation CMMI, les objectifs sont atteints si chacun des 6 éléments clés de la sécurité de l'information élargie aux processus sont au niveau 4. Ce tableau nous permet donc d'évaluer le niveau de maturité du SMSI de Ecobank CI à travers ce graphique ci-après :

Figure 4 : Graphique du niveau de maturité du SMSI de Ecobank CI



LEGENDE

PO4: Organisation et Processus de la sécurité de l'information

PO9 : Evaluation et gestion des risques de sécurité

AI7 : Classification des informations

DS4 : Gestion de la continuité d'exploitation

DS5 : Gestion des technologies de sécurité

DS8 : Gestion des incidents et problèmes

DS10 : Gestion du personnel

Source : Graphique établit par nous-même à partir de la méthode d'évaluation et de calcul CMMI du CobiT

Le calcul et l'évaluation du niveau de maturité du SMSI permet d'apprécier ou se situe la sécurité de l'information par rapport aux exigences de la norme ISO 27000. Nous pouvons constater à

travers ce graphique ci-dessus que le niveau de maturité du SMSI de Ecobank CI (ligne verte) a globalement atteint le critère 3 ; il est bien établit mais présente encore quelques carences. Ce qui signifie que les exigences de la norme ISO 27000 sont plus ou moins respectés avec des insuffisances diverses. Sur neuf (9) éléments de choix pour l'évaluation du SMSI, cinq (5) se retrouvent dans l'intervalle [0 ; 2,99]. Ces éléments critiques sont l'organisation générale de la sécurité de l'information, la classification des informations, le processus de gestion des incidents et problèmes, la gestion du personnel et l'évaluation de la conformité globale aux exigences de la norme et autres exigences du système bancaire.

L'idéal serait d'atteindre le critère 5 mais étant donné qu'aucun système ne peut être assuré absolument, nous avons défini des niveaux à court et long terme selon le CobiT. Le niveau à court terme (critère 4) est le minimal que le SMSI devra accéder pour réduire au mieux ses insuffisances et être par conséquent moins vulnérable. Nous proposerons donc des suggestions pour que le SMSI atteigne le niveau minimum requis. Ces recommandations doivent bien entendu être sujettes à amélioration en fonction de l'évolution et de l'expansion de Ecobank CI.

6.2 Recommandations pour l'amélioration de la sécurité de l'information et l'audit interne au sein de Ecobank Cote d'Ivoire

A travers ce chapitre nous ferons des recommandations pour l'amélioration du SMSI et ensuite des recommandations pour rendre plus opérationnel et accroitre la valeur ajoutée de la Direction d'audit interne en matière de sécurité de l'information. Dans l'étape suivante, nous suggérerons des lignes directrices d'audit qui pourraient être des missions d'audit de la sécurité de l'information.

6.2.1 Recommandations pour l'amélioration du SMSI de Ecobank CI

Concernant l'amélioration du SMSI, nos recommandations se feront sur toutes les anomalies prises ensemble, que nous avons pu faire ressortir au cours de notre analyse à savoir : celles sur la gestion de la sécurité de l'information et celles relatives aux activités et technologies de la sécurité de l'information.

6.2.1.1 Création d'un comité de pilotage de la sécurité de l'information

La première recommandation que nous ferons, c'est la mise en place d'un cadre de gouvernance de la sécurité de l'information au sein de la filiale. Cela signifie établir un comité de pilotage de la sécurité de l'information dans lequel chaque métier clé de la banque sera représenté par son directeur ou un représentant ayant une haute fonction hiérarchique au sein du corps métier. Ce comité aura pour mission première de représenter la maison mère quant aux objectifs de sécurité qu'elle s'est fixée. Ledit comité devra examiner la stratégie de sécurité et sa mise en place ou son adaptation au sein de la filiale et par rapport à son environnement de travail. Il devra aussi veiller à ce que chaque membre de l'entreprise soutienne l'intégration de ce cadre de sécurité de l'information. Le comité de pilotage aide à réaliser un consensus sur les priorités et les compromis. Il sert également de canal de communication efficace et fournit une base continue pour garantir l'alignement du programme de sécurité sur les objectifs opérationnels.

La mise en place d'un cadre de gouvernance de la sécurité de l'information permet la gestion de la conformité par rapport aux objectifs globaux de sécurité, la gestion des ressources de sécurité et de technologies de l'information et la mesure de la performance. Ce qui offre à la banque une rétroaction sur la valeur et une excellente gestion des risques de sécurité.

La figure ci-après nous présente les grandes lignes du pilotage d'un SMSI :

Figure 5 : Pilotage d'un système de management de la sécurité de l'information

Source : Julien Levrard (2012)

Au plan stratégique et décisionnel comme au niveau fonctionnel et opérationnel, la sécurité de l'information doit fédérer toutes les responsabilités et toutes les compétences de l'entreprise. Le comité de pilotage de la sécurité de l'information aura pour mission de coordonner les différentes actions menées dans le strict respect des normes et règlements établis par la maison mère. A l'intérieur de ce comité selon la norme ISO 27002, chacun des corps métiers clés devra être représenté. Il en est ainsi pour que chaque problème de sécurité soit sujet de réflexion et d'apport de solutions pertinentes pour sa résolution. Ceci définit les responsabilités et oblige chaque responsable de département ou direction à s'atteler et à veiller au respect scrupuleux de chacune des mesures de sécurité prises dans la limite de ses fonctions.

Une bonne gouvernance de la sécurité permet d'obtenir les résultats suivants :

- ✓ un alignement de la sécurité de l'information sur la stratégie commerciale pour appuyer les objectifs de la banque
- ✓ une gestion des risques et une exécution de mesures appropriées pour diminuer les risques et réduire à un niveau acceptable les impacts possibles sur les ressources d'informations
- ✓ l'apport de valeur en optimisant les investissements dans la sécurité pour appuyer les objectifs opérationnels
- ✓ la mesure de la performance pour garantir le respect des objectifs
- ✓ la gestion des ressources utilisées avec efficacité et efficience
- ✓ l'intégration des processus pour garantir leur bon fonctionnement

La mise en place d'un tel comité donne à la banque de s'assurer de la participation et de l'implication de tous les intervenants touchés par les considérations de sécurité. Chaque directeur sera donc responsable et garant du processus de sécurité dans sa direction.

6.2.1.2 Gestion efficace de la sécurité de l'information

Le responsable Security de Ecobank CI ne pourra travailler tout seul sur les méthodes et mesures de gestion de la sécurité de l'information commandées par la maison mère pour les adapter au sein de la banque. C'est aussi la raison pour laquelle il est important d'avoir un comité de pilotage de la sécurité de l'information. Le responsable Security pourra s'appuyer sur ce comité pour être mis au courant des risques éventuels actuels liés à la sécurité de l'information pour chaque métier. Il sera également en mesure d'adapter correctement les politiques et procédures de sécurité à chaque direction concernée afin que chacun prenne part à l'implémentation et l'amélioration du SMSI de la banque.

Ce que nous recommandons en plus, c'est une position hiérarchique élevée pour permettre au responsable Security d'être plus proche des autres directeurs mais aussi de la direction générale. Cela concoure à renforcer la collaboration et permet une gestion efficace et efficiente de la sécurité de l'information.

6.2.1.3 Communication / formation régulière du personnel

Il est important de communiquer ses politiques et procédures afin de mettre au courant le personnel sur la conduite à tenir pour maintenir l'image et la crédibilité de la banque. Les politiques notamment celle du risque (appétence pour le risque) devront leur être communiqué par divers moyens afin que les opérationnels sachent l'importance de leurs actions et la finalité sur le système et les objectifs de l'entreprise.

Ne dit-on pas que le maillon faible de l'entreprise c'est l'homme. Ainsi plus le personnel prend conscience des objectifs de sécurité de l'entreprise, moins le taux d'erreurs est élevé. Par cette considération, la banque rencontrera la motivation et l'implication des agents dans l'amélioration continue du SMSI.

Aussi concernant la périodicité des formations trop longue, nous recommandons des formations régulières (au moins 5 à 6 fois dans l'année) pour les agents de Ecobank CI soit en atelier, sous forme de conférence ou en ligne. Les formations permettent au personnel d'avoir une mise à jour sur les dernières technologies de l'information, les risques liés a à leurs activités, la gestion de la sécurité à tous les niveaux. Ces formations doivent être pratiques suivis de test d'aptitudes obligatoires. Des ateliers pourront être organisés dans les différentes directions pour faire participer le personnel à l'actualisation des procédures, à la bonne gouvernance des technologies de l'information et l'apport de solutions favorables au maintien et à l'amélioration de la gestion de la sécurité de l'information.

La direction du contrôle interne ou de l'audit interne pourra faire une enquête régulière d'évaluation des connaissances pour s'assurer que les agents ont bien assimilé les formations et en comprennent désormais les enjeux. Notons que, lorsque les employés sont actifs et participent à l'amélioration d'un système, ils se sentent plus impliqués et plus respectés au sein de la structure. Ainsi ils sont dévoués et s'attèlent à travailler dans l'intérêt de l'entreprise.

6.2.1.4 Mesures de sauvegarde des données sur les ordinateurs et appareils mobiles et gestion des privilèges

Nous savons que malgré tous les débats et les formations au sujet des pirates et des intrus, les violations de sécurité au sein de l'entreprise restent nombreuses. Les employés peu honorables et mécontents sont une menace constante. Aussi nous pouvons souligner que la négligence souvent est considérable, notamment chez les personnes fréquemment en déplacement qui transportent avec elles des ordinateurs portatifs et des disques amovibles. Les cadres dirigeants et les administrateurs qui bénéficient de droits d'accès pratiquement non contrôlés sont presque impossibles à arrêter. De même, le personnel de livraison, les employés temporaires et même les concierges sont trop souvent autorisés à circuler librement dans les services de l'entreprise.

Ainsi s'il est impossible de garantir une protection totale, il existe tout de même quelques mesures que la banque peut prendre pour réduire les risques. Premièrement, elle peut vérifier la distribution des systèmes et privilèges pour s'assurer que personne ne dispose d'un trop grand contrôle par le biais d'un service de sécurité de l'information. Ensuite, la banque peut répertorier l'emplacement de

stockage des sauvegardes, archives et copies des bases de données utilisées pour les tests et la résolution des logiciels. Ecobank CI peut aussi mettre un place un système de cryptage des enregistrements précis des personnes qui utilisent les appareils informatiques portatifs et veiller à ce que les employés sachent comment protéger leurs appareils et leurs données lorsqu'ils sont en déplacement. Pour la menace des formules BYOD, la banque pourrait se tourner vers des solutions spécialisées créées par des entreprises spécifiques. Elles offrent généralement la possibilité d'obtenir des périphériques mobiles intelligents de réseau pour l'authentification des appareils sur le réseau ou encore l'installation de périphériques mobiles en mode agent – sur chaque appareil mobile – afin de s'assurer que les terminaux connectés disposent des bons logiciels, droits d'accès et paramètres de sécurité avant de les autoriser à se connecter au réseau.

Ce que nous recommandons également pour une meilleure gestion des privilèges et badges d'accès, c'est que cette tache soit attribuée à une direction autre que la direction du contrôle interne. Cela permettra à cette dernière d'avoir un meilleur contrôle sur cette activité et de maintenir son objectivité. Selon que l'indique la norme ISO 27000, cette activité devrait revenir au responsable de la sécurité de l'information pour un meilleur suivi.

6.2.1.5 Classification des informations par valeur et niveau de sensibilité

Concernant la classification des données, la norme ISO 27002 explique que l'information devrait être classée et étiquetée selon un système généralement admis, assurant ainsi un niveau de protection approprié. Comme nous l'avons spécifiée dans le développement du thème 3 de la norme ISO 27002, la classification des information doit être accompagnée de procédures formelles et être exécutée en tenant compte des besoins liés à l'exploitation, de la sensibilité des informations, des restrictions éventuelles et du degré d'impact des évènements nuisibles à leur exploitation. De plus, les actifs technologiques liés à la sécurité de l'information, doivent avoir un propriétaire désigné qui se charge de leur gestion et de l'inventaire régulier. Un actif inactif peut être source de motivation à la fraude ou à des violations des règles de sécurité établies par la banque.

Aucune méthode particulière de classification n'est définie étant donné la diversité des secteurs économiques et l'interprétation variante d'une information d'une entreprise à une autre. Cependant, notre recommandation, c'est que la banque garde en mémoire que, quel que soit la méthode de

classification adoptée, elle doit tenir compte du degré de sensibilité et de criticité et du niveau de partage de ses informations. Les informations doivent être classées et foncièrement protégées pour éviter que celles jugées sensibles et confidentielles soient diffusées en interne comme à l'extérieur aux personnes non autorisées accidentellement ou volontairement.

Dans le cas de la banque qui gère des comptes et dossiers personnels de clients divers et qui est tenue par des exigences légales, négliger le classement des informations peut entrainer non seulement des pertes financières mais aussi peut porter atteinte à son image, sa réputation et sa crédibilité.

Pour protéger et classer une information, il faut la connaître et identifier son niveau de sensibilité et de criticité et sa valeur. Il faut pour cela :

- ✓ lister les données et leur localisation dans les processus et activités ;
- ✓ formaliser une échelle de classification et des règles d'utilisation (à travers une politique de classification et protection des informations) ;
- ✓ qualifier la sensibilité des données au regard des impacts liés à un incident de sécurité ;
- ✓ sensibiliser les utilisateurs à ces impacts et à la nécessité d'appliquer les règles de classification.

Cette démarche suit le modèle PDCA qui oriente l'entreprise de la planification au suivi des actions mis en œuvre pour atteindre les objectifs. Nous précisions que la banque doit veiller à la loyauté de ses employés dans leur engagement au respect de la discrétion et la confidentialité quant aux informations.

6.2.1.6 Sécurité du réseau

Comme nous l'avons signifié dans le diagnostic critique, l'ouverture du réseau à l'extérieur en particulier vers les réseaux sociaux et les messageries web non sécurisées, peut s'avérer nuisible pour le SMSI et les systèmes d'informations de la banque. L'ouverture et l'accès au réseau bancaire doivent être balisés par des portails électroniques forts. Normalement, pour une meilleure gestion de la sécurité de l'information, il est conseillé d'éviter la promenade informatique sur des réseaux

autres que le réseau informatique de l'entreprise ou du moins de veiller à ce que les pare-feu et les logiciels contre les attaques malveillantes soient à jour et parfaitement fonctionnels.

Un réseau vulnérable ouvre aux pirates informatiques l'accès à tout type d'informations ou données électroniques de l'entreprise. Ces informations peuvent aisément être modifiées, supprimées ou transférées vers d'autres réseaux ou bases de données. D'où, il est important d'avoir des anti-virus, des anti-phishing, des anti-spyware, des programmes anti-spam et des pare-feu sur chaque machine du réseau informatique. Il faudrait aussi s'assurer que ce sont les mêmes logiciels authentiques (sous licence) qui sont installées sur les ordinateurs car les logiciels piratés sont vulnérables aux menaces de sécurité. Ces logiciels et leurs correctifs devront être constamment mis à jour afin de s'assurer que la banque dispose des dernières versions des logiciels.

Aujourd'hui les anti-virus et les pare-feu ne représentent qu'un aspect minime de la sécurité informatique. Par conséquent, chaque agent de l'entreprise doit être responsable de la sécurité et doit veiller à son maintien et son amélioration. Il y va de la survie de la banque et de l'atteinte effective et efficace des objectifs. Pour s'assurer de la responsabilité de chaque agent, il serait intéressant de tenir des registres des activités de l'utilisateur. Il est important de le faire lorsque le réseau est constamment connecté à internet.

6.2.1.7 Intervention du comité de gestion des incidents de sécurité

La gestion des incidents est très importante dans le maintien de la sécurité de l'information et l'atténuation des impacts dus aux risques de sécurité survenus. Un incident aussi petit soit-il peut être préjudiciable pour la banque. Il est donc de mise de recadrer le rôle du comite de gestion des incidents selon la norme ISO 27002 afin de prendre en compte tous les contours nécessaires à une gestion efficace des incidents de sécurité.

Ce que nous recommandons, c'est un comité de gestion des incidents en interne disponible et en activité qu'il y ait ou non un incident quelconque. Aucune des tâches de ce comité ne doit pas se faire sur une base réactive. Il serait intéressant qu'une planification anticipée des incidents soit faite. ISACA propose même qu'il soit défini une classification claire des incidents de sécurité par ordre de priorité et d'importance et aussi des ébauches de réponses qui seront communiquées aux agents correspondants pour qu'ils sachent comment s'y prendre lorsque l'incident surviendra.

Chacune des réponses devra être testée pour s'assurer qu'elle répond bien à l'objectif qui est de réparer ou de réduire l'impact de l'incident.

En s'appuyant sur des incidents de sécurité récents, une entreprise peut prévoir et anticiper les problèmes potentiels. Ainsi, si une entreprise prend le temps de traiter les incidents de sécurité de manière pondérée et rationnelle et d'en déterminer les raisons sous-jacentes, il lui sera plus facile de se protéger d'incidents similaires à l'avenir et elle pourra traiter ces problèmes plus rapidement. La planification anticipée exige la participation des différents groupes opérationnels et doit faire appel à des conseillers et à des services en technologie de la sécurité chargés de surveiller les menaces les plus récentes et de transmettre l'information recueillie. Elle donne l'occasion de développer un ensemble clair de stratégies et de procédures à même de gérer les menaces ou les incidents de sécurité. On pourrait donc parler de gestion proactive des incidents de sécurité de l'information.

La gestion proactive des risques de sécurité présente de nombreux avantages par rapport à l'approche réactive. Plutôt que d'attendre que les problèmes se présentent avant d'y répondre, le principe de cette approche est de minimiser la possibilité qu'ils se produisent dès le départ. Pour protéger ses ressources importantes, Ecobank CI doit mettre en place des contrôles visant à réduire les risques d'exploitation des vulnérabilités par des programmes ou des personnes malveillants ou par un usage accidentel. Bien entendu, les entreprises ne doivent pas complètement renoncer à l'approche réactive. En effet, bien qu'une approche proactive efficace permette de diminuer considérablement les risques d'incidents de sécurité, il est peu probable que ces derniers disparaissent complètement. Par conséquent, il est fondamental que les entreprises continuent d'améliorer leurs processus de réponse aux incidents tout en développant des approches proactives sur le long terme.

Toutes ces mesures et bonnes pratiques relevées dans les normes ISO 27000 permettent à la banque de garantir une meilleure gestion de la sécurité de ses systèmes d'informations. Afin de donner l'assurance que les mesures de sécurité de l'information mises en place fonctionnent correctement, la Direction de l'audit interne doit avoir les compétences, les connaissances et les outils nécessaires pour les évaluations diverses. Notre prochaine étape nous donne l'occasion de faire des recommandations d'amélioration des prestations de l'audit interne en matière de sécurité de l'information.

6.2.2 Recommandations pour le perfectionnement de l'audit interne en matière de sécurité de l'information

L'audit interne, de par sa définition, aide l'entreprise à atteindre ses objectifs en évaluant ses processus de management des risques, de contrôle et de gouvernance. C'est un organe de contrôle, conseiller de la Haute Direction, qui aide au management et qui est créateur de valeur ajoutée. Il doit pour cela posséder les meilleures méthodes et outils de travail afin de mener à bien ses missions d'audit.

Pour la sécurité de l'information, les audits doivent se faire de façon régulière. Au moins une fois l'an, les bonnes pratiques voudraient que l'audit interne évalue la gestion de la sécurité de l'information au niveau de la banque toute entière de même que les opérations et les technologies de sécurité. L'évaluation permettra de s'assurer que la stratégie TI est toujours rigoureusement alignée à la stratégie globale d'affaires établie par la banque. Aussi une évaluation des risques de sécurité constante et régulière en collaboration avec le RSI et le RM est importante voire obligatoire pour mieux établir un plan d'audit pertinent.

Aucune agence ni entité de la banque ne doit rester incontrôlée pendant plus d'un an au maximum. Nous recommandons pour cela l'augmentation du nombre des auditeurs internes et aussi l'augmentation des audits de sécurité de l'information. Il serait encore plus intéressant que la Direction de l'audit interne regorge de plusieurs spécialités. Pour cela une formation continue des auditeurs est recommandée de même qu'une auto-évaluation de leurs compétences et aptitudes. Les auditeurs qui ont plus de compétences en matière de sécurité de l'information pourraient formés ceux qui en ont moins (création d'un centre de partage et de réflexion) afin d'accroitre le potentiel de l'audit interne et de réduire les couts de la banque dus aux recours fréquents vers l'extérieur.

L'IFACI recommande aux auditeurs internes d'avoir des connaissances et des compétences suffisantes pour conduire à bien leurs missions d'audit. Nous suggérons donc pour l'évaluation de la sécurité de l'information que chaque auditeur interne ait une connaissance des normes ISO 27000 actualisées, du référentiel CobiT et autres bonnes pratiques en matière de sécurité des systèmes d'information. Avec ces connaissances, la Direction de l'audit interne sera à mesure de fournir des recommandations pertinentes pour l'amélioration de la gestion de la sécurité de l'information.

Concernant la méthodologie d'audit, nous recommandons que l'audit interne s'imprègne de la méthode d'évaluation élaborée par ISACA. Les différentes étapes de l'audit interne passent par 3 phases : phase de planification, phase de réalisation et phase de conclusion matérialisée par un rapport final d'audit. La phase de planification doit déjà prendre en compte les 3 niveaux réunis en 2 qu'ISACA propose à savoir : évaluation de la gestion de la sécurité de l'information et l'évaluation des opérations et des technologies de sécurité de l'information. L'évaluation générale de la sécurité de l'information pourra être effectuée au moins une fois par an pour ne pas perdre un seul aspect de sécurité qui pourrait s'avérer préjudiciable pour la banque. De plus, il faudrait aux auditeurs internes des outils ou logiciels d'audit spécialisés pour effectuer les tests de contrôle conformément aux recommandations de l'IFACI quant à l'évaluation des technologies de l'information.

Cette méthode permet de se rendre compte de la stratégie de sécurité de l'information et de son alignement d'avec la stratégie globale de l'entreprise. Evaluer ces différents aspects de sécurité de l'information cités dans les pages 96 et 97, au moins une fois dans l'année permet de s'assurer que les objectifs de sécurité définis par la maison mère sont atteints avec efficience et efficacité. L'assurance sera également donnée quant au bon fonctionnement du SMSI et de sa conformité avec les règlementations et exigences établies par Ecobank et aussi par le secteur bancaire.

L'auditeur interne doit constamment se former avec d'acquérir des connaissances nouvelles sur les TI, les systèmes d'information, la gestion des SMSI et autres sujets susceptibles de l'aider dans l'accomplissement de ses tâches périodiques et dans l'apport pour la création de valeur.

Conclusion de la deuxième partie

L'exemple de Ecobank CI nous a permis de constater et d'apporter un jugement sur la pratique de la sécurité de l'information au sein même de ladite banque. De notre diagnostic, nous avons remarqué quelques anomalies susceptibles de compromettre le SMSI de la banque et donc l'intégrité, la confidentialité et la disponibilité des informations. De la théorie, ont découlé des bonnes pratiques qui nous ont permis de faire des recommandations afin que Ecobank CI évite ou réduise considérablement tous les risques inhérents de sécurité qui pourraient survenir.

Nous avons également apprécié le rôle de la Direction de l'audit interne dans la sécurité de l'information à travers la méthodologie et le contenu du travail effectué. Nous avons pu noter que l'audit interne s'attèle tant bien que mal à jouer son rôle pour rassurer au mieux la Direction Générale quant à l'efficacité et l'efficience de la sécurité de l'information. Tout ceci en dépit du fait qu'une partie des risques est gérée par le Groupe à cause de la centralisation des systèmes. Cependant les missions à cet effet sont insuffisantes et les aptitudes sont à améliorer. Nous avons fait des recommandations qui, nous l'espérons, aideront la Direction de l'audit interne à redéfinir sa méthodologie d'audit de la sécurité et à être un véritable contributeur à la sécurité de l'information.

CONCLUSION GENERALE

Au regard de la théorie et de la pratique que la notion de sécurité de l'information a pris de l'ampleur dans ce monde actuel de nouvelles technologies. Compte tenu des risques énormes encourus par la vulnérabilité des systèmes, par la maladresse ou l'insouciance du personnel, par des dégâts physiques et autres, les entreprises ont jugé dorénavant primordial de se munir de moyens divers pour protéger leurs actifs informationnels. Doucende (2009 :3) dans son avant-propos, affirme que la sécurité des systèmes informatiques et plus globalement des systèmes d'information (SI) a été considérée pendant très longtemps par les entreprises comme un aspect de second plan. Peu à peu, une prise de conscience amène la sécurité des SI devant la scène. La raison principale est liée à la multitude d'incidents et plus grave, aux sinistres qui provoquent de lourdes pertes pour l'entreprise.

Aussi, Longeon et Archimbaud (1999 :10) pouvaient le dire, l'on ne protège bien que ce à quoi on tient, c'est-à-dire ce à quoi on associe « une valeur ». La trilogie confidentialité, intégrité, disponibilité, détermine la valeur d'une information. La sécurité des systèmes d'information (SSI) a pour but de garantir la valeur des informations qu'on utilise. Si cette garantie n'est plus assurée, on dira que le système d'information a été altéré. Ainsi la sécurité de l'information est aujourd'hui appliquée à différents secteurs d'activités économiques. Les banques, en particulier, considèrent ardemment la sûreté de leurs systèmes d'information car il y va de leur crédibilité quant à eux-mêmes, leurs clients et l'ensemble du système bancaire.

Et pour les aider dans l'amélioration de leur système de management de la sécurité de l'information, la fonction audit interne joue le rôle d'évaluateur et de conseiller de bonnes pratiques. Cependant l'ère de mondialisation sans cesse changeant et la complexité des systèmes ont rendu la tâche de l'audit interne relativement difficile. Cela nécessite plus de connaissance et un long cycle d'adaptation qui ne rencontrent pas la plupart du temps l'adhésion des auditeurs internes. Ce fait a occasionné que l'on se pose la question de savoir comment l'audit interne contribue au maintien et à l'amélioration continue du SMSI dans le milieu bancaire.

L'exemple de Ecobank CI nous a permis d'apprécier la gestion de la sécurité de l'information telle qu'elle est comprise par une banque. Nous savons qu'aucun système quel, qu'il soit, n'est à 100%

assurer de façon absolue contre les divers menaces ou risques qui sont de plus en plus multiples dans cette ère régie par les technologies nouvelles de l'information. Ainsi nous avons décelé quelques insuffisances qui ont fait l'objet d'analyse critique. Ces insuffisances étaient, entre autres, contenues dans la gestion globale de la sécurité de l'information (aspect humain, organisationnel et technologique) et dans le rôle de l'audit interne relatif à l'amélioration continue de cette sécurité.

Nous proposons ainsi des recommandations pertinentes pour palier au mieux aux carences et ainsi contribuer tant bien que mal à la gestion de la sécurité de l'information au sein de Ecobank CI. Nous avons aussi recommandé une reconsidération de la méthodologie d'audit de la sécurité de l'information pour les auditeurs internes en conseillant la méthodologie d'audit d'ISACA parce qu'elle encadre davantage tous les contours de la sécurité de l'information.

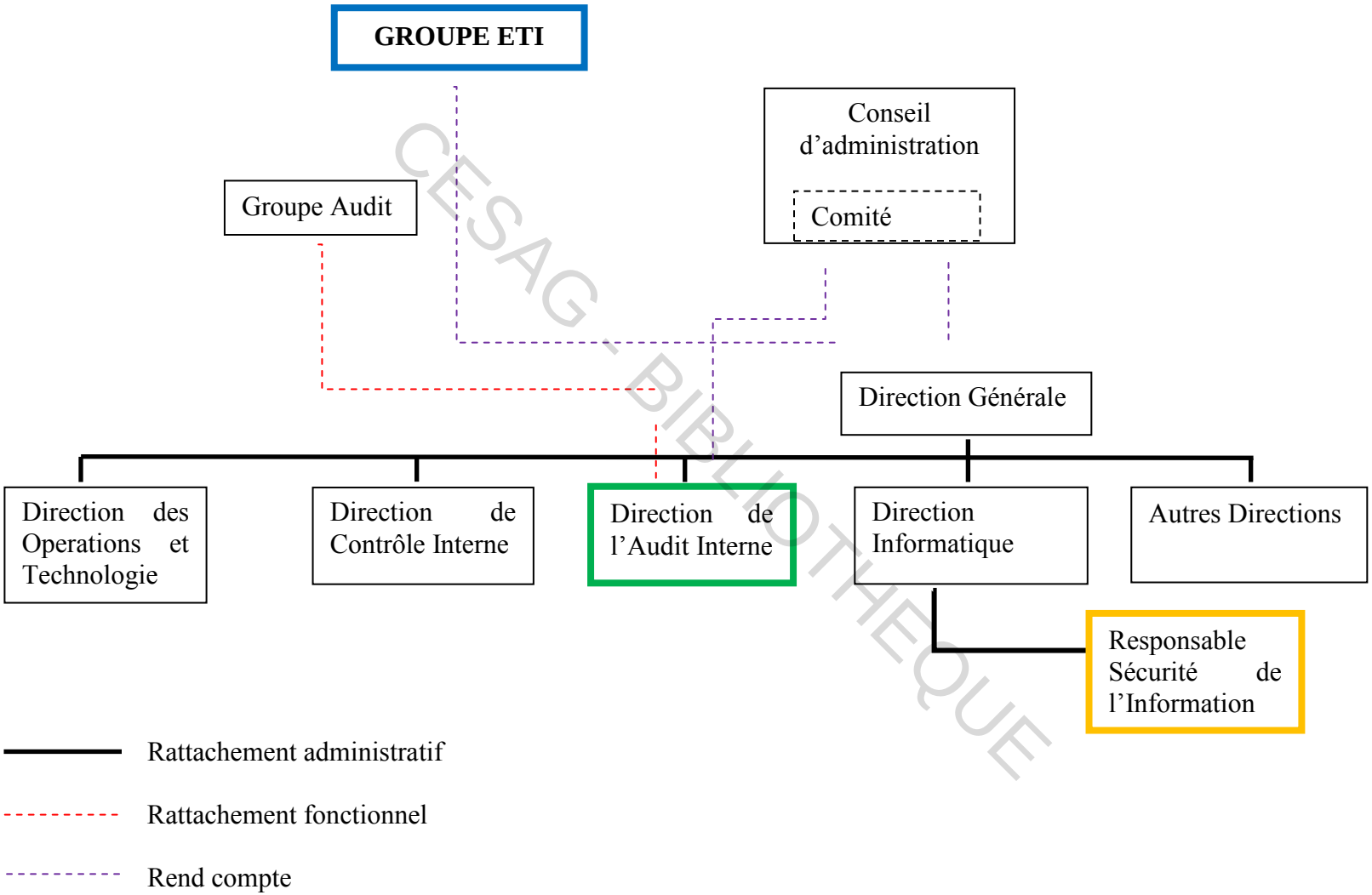
En effet, la méthodologie d'audit préconisée par ISACA permet d'apprécier plus en profondeur la gestion de la sécurité de l'information en passant par son organisation jusqu'à ses activités et sa technologie. L'audit de la sécurité de l'information doit être un processus. Il doit permettre de s'assurer que les SI maintiennent la confidentialité, l'intégrité et la disponibilité des données et des systèmes et que ces derniers fournissent des renseignements pertinents et fiables. ISACA insiste sur le fait que l'audit de la sécurité de l'information doit donner l'assurance que les SI possèdent des contrôles internes qui offrent une assurance raisonnable que les objectifs opérationnels, d'entreprise et de contrôle seront atteints et que les évènements indésirables seront évités ou détectés et corrigés rapidement.

Ainsi la sécurité de l'information est importante pour une banque comme pour toute autre entreprise qui souhaite pérenniser son activité et son image de marque dans le monde des affaires actuel. Elle doit être du ressort de chaque acteur de l'entreprise quelque soit son poste hiérarchique. Aussi les auditeurs internes doivent être vigilants et toujours en alerte afin d'orienter au mieux la gestion de la sécurité de l'information et de favoriser l'atteinte effective et efficace des objectifs de l'entreprise. Assurément, les systèmes d'informations ne pourront pas être totalement protégés compte tenu de l'évolution constante de l'informatique. Ce qui est donc considérable à faire est de s'atteler à réduire au maximum les risques qui pourraient survenir et ainsi préserver les différents systèmes d'informations.

En alignant stratégiquement le SMSI aux exigences de la norme ISO 27000 et aux objectifs et buts généraux de l'entreprise, Ecobank CI aura l'avantage sur les autres banques et une forte crédibilité devant les tiers. De ce fait, cette banque panafricaine indépendante pourra prétendre au titre de certifié en sécurité de l'information et rehausser son image de marque à travers l'Afrique et par ailleurs le monde entier.

ANNEXES

ANNEXE N^{0} 1 : ORGANIGRAMME DE ECOBANK COTE D'IVOIRE



ANNEXE N°2 : QUESTIONNAIRE DE PRISE DE CONNAISSANCE DU SMSI

Cochez oui ou non aux questions suivantes et apportez des explications à celles qui en requièrent.

Thème n°1: Engagement et soutien de la haute direction

1) Comment la haute direction s'implique-t-elle dans la gestion de la sécurité de l'information ?

   ……

   ……

2) Quelles sont les actions déjà menées ?

   ……

   ……

3) Etablit-elle un mandat pour des auditeurs SI spécialisés ou transmet-elle le pouvoir de surveillance à l'audit interne ? ……..

Thème n°2: Politique et procédures

4) Existe-t-il une politique de sécurité de l'information au sein de la banque ? Oui ☐ Non ☐
5) La politique de sécurité est-elle approuvée par la haute direction ? Oui ☐ Non ☐
6) Est-elle régulièrement mise à jour ? Oui ☐ Non ☐
7) Existe-t-il des manuels de procédures régissant la sécurité de l'information ? Oui ☐ Non ☐
8) Ces procédures sont-elles constamment mises à jour ? Oui ☐ Non ☐
9) Ces manuels concernent quel(s) aspect(s) de la sécurité de l'information ?

   ……..

   ...

10) La politique et les procédures sont-elles mise en œuvre ? Oui ☐ Non ☐
11) Qui est le garant de l'exécution de la politique et des procédures de sécurité de l'information ?

    ……

    ……

Thème n°3: Organisation

12) Existe-t-il un comité de gestion de la sécurité de l'information ? Oui ☐ Non ☐
13) De qui se compose-t-il ?

……

……

14) Est-ce que le comité a une implication forte et assure la promotion de la sécurité de l'information par des moyens adéquats ? Oui ☐ Non ☐
15) Si oui, quels sont ces moyens ?

……

……

16) Au sein du comité, qui est le garant principal du maintien de la sécurité de l'information ?

……

17) Le garant de la sécurité de l'information a-t-il des objectifs clairs et mesurables ? Oui ☐ Non ☐
18) Quels sont ces objectifs?

……

19) Le dispositif de contrôle interne est-il aligné aux objectifs de sécurité de l'information définis par la banque ? Oui ☐ Non ☐
20) L'audit interne est-il impliqué dans le bon fonctionnement du système de sécurité de l'information ? Oui ☐ Non ☐
21) Est-ce que la mise en application de la politique de sécurité de l'information est auditée de façon indépendante ? Oui ☐ Non ☐
22) Comment est gérée la sécurité de l'information d'avec l'extérieur ?

……

……

……

Thème n°4: Sensibilisation à la sécurité et éducation

23) Les différents corps de métier de la banque sont-ils sensibilisés sur l'importance de la sécurité de l'information ? Oui ☐ Non ☐

24) Par quels moyens le sont-ils ?

……

……

……

25) Connaissent-ils les dispositifs de sécurité et leur importance ? Oui ☐ Non ☐

26) Le personnel a-t-il connaissance des procédures et politique de sécurité de l'information ? Oui ☐ Non ☐

27) A-t-il connaissance des risques liés à la sécurité de l'information? Oui ☐ on ☐

28) Le personnel met-il en œuvre les procédures ? Oui ☐ Non ☐

29) Définir un taux approximatif d'erreurs sur 3ans : ……..

30) Quels sont les apports du personnel en matière de sécurité de l'information ?

……

……

……

31) Les contrats de travail ou de stage contiennent ils des clauses de confidentialité ? Oui ☐ Non ☐

32) Est-ce que la banque vérifie et contrôle la véracité des références et la moralité des employés permanents et temporaires ? Oui ☐ Non ☐

33) En cas de violation de la politique de sécurité de la banque et de non-respect des procédures de sécurité de l'information, est-il prévu des sanctions disciplinaires ? Oui ☐ Non ☐

Thème n°5: Contrôle et conformité

34) Existe-t-il des périmètres de sécurité pour protéger les zones où se situent les moyens de traitement de l'information ? Oui ☐ Non ☐

35) Est-ce que ces zones de sécurité sont protégées par des moyens de contrôle d'entrée et de sortie permettant d'assurer que seuls le personnel et les visiteurs autorisés peuvent y accéder ? Oui ☐ Non ☐

36) Les contrôles permanents sont-ils effectués pour s'assurer du maintien de la sécurité des informations ? Oui ☐ Non ☐

37) Qui garantit ces contrôles?

……..

38) Existe-t-il des contrôles permettant d'établir ou de maintenir la sécurité des réseaux ?
Oui ☐ Non ☐

39) Les medias informatiques amovibles tels que les clés USB, les disquettes, les CD, les bandes etc. font-ils l'objet d'un contrôle particulier ? Oui ☐ Non ☐

40) Est-ce que la gestion des privilèges fait l'objet de contrôles particuliers ? Oui ☐ Non ☐

41) Est-ce que seuls les utilisateurs dument autorisés peuvent accéder aux services en réseaux ?
Oui ☐ Non ☐

42) Est-ce que les accès sont dument authentifiés ? Oui ☐ Non ☐

43) Combien de temps faut-il pour retirer ou supprimer l'accès d'un employé temporaire ou non après son mandat de travail ?

……..

44) Tous les ordinateurs de la banque sont-ils connectés à un système commun de réseau facilement contrôlable par le responsable TI ? Oui ☐ Non ☐

45) Existe-t-il des tests pour protéger et contrôler les données ? Oui ☐ Non ☐

46) Si oui, lesquels?

……

……

……

47) Existe-t-il des techniques de cryptographie pour protéger l'information ? Oui ☐ Non ☐

48) Les informations sont-elles convenablement conservées et classées ? comment et par quels moyens ?

……

……

49) Existe-t-il des procédures pour surveiller l'utilisation du système ? Oui ☐ Non ☐

50) Est-ce que toutes les exigences statutaires, règlementaires et contractuelles dont relèvent les systèmes d'information, sont explicitement définies et documentées ? Oui ☐ Non ☐

51) Est-ce que le système de sécurité de l'information et les systèmes d'information sont contrôlés régulièrement pour vérifier leur conformité avec la politique et les normes de sécurité ? Oui ☐ Non ☐

52) Est-ce que les directions engagent des actions pour s'assurer que toutes les procédures de sécurité, dans leur périmètre de responsabilité, sont correctement suivies ? Oui ☐ Non ☐

53) Est-ce que toutes les entités de la banque sont sujettes à des revues régulières par l'audit interne ? Oui ☐ Non ☐

Thème n°6: Gestion et intervention face à l'incident

54) Existe-t-il des procédures de gestion des incidents ? Oui ☐ Non ☐
55) Est-ce que les incidents de sécurité sont signalés en temps réel et à travers de bons canaux dès leur survenance ? Oui ☐ Non ☐
56) Existe-t-il des procédures pour signaler les dysfonctionnements des programmes et sont-elles suivies ? Oui ☐ Non ☐
57) Existe-t-il des plans de relance des activités après la survenance d'un incident majeur ? Oui ☐ Non ☐
58) Ces plans sont-ils régulièrement mis à jour ? Oui ☐ Non ☐
59) Le personnel est-il sensibilisé sur la gestion des incidents ? Oui ☐ Non ☐

ANNEXE N°3: QUESTIONNAIRE D'EVALUATION / DIRECTION D'AUDIT INTERNE

Cochez oui ou non aux questions suivantes et apportez des explications à celles qui en requièrent.

Nom et Prénoms :

Poste :

1) Etes-vous à ECOBANK CI depuis plus de 3 ans ? Oui ☐ Non ☐
2) Connaissez-vous la norme ISO 17799 ? Oui ☐ Non ☐
3) Si oui, de quoi parle-t-elle ? ……..
4) Pour vous, qu'est-ce qu'une information ?
   ……...
5) Qu'entendez-vous par « sécurité de l'information » ?
   ……
   ……
6) Quels sont les objectifs de la banque en matière de sécurité de l'information ?
   ……
   ……
7) Existe-il une politique de sécurité de l'information ou de sécurité des systèmes d'informations au sein de la banque ? Oui ☐ Non ☐
8) Existe-il un document formel à ce sujet ? Oui ☐ Non ☐
9) Est-ce que la politique de sécurité est régulièrement révisée ? Oui ☐ Non ☐
10) Cette politique a-t-elle subit des changements depuis sa parution ? Oui ☐ Non ☐
11) Qui est charge du maintien et du respect des procédures et politiques de sécurité de l'information au sein de la banque ? …….
12) Avez-vous déjà effectue des missions d'audit de la sécurité de l'information ? Oui ☐ Non ☐
13) L'audit de la sécurité de l'information fait-il partir de votre planning annuel de missions ? Oui ☐ Non ☐

14) Combien de temps mettez-vous entre 2 missions d'audit de la sécurité de l'information ? ……

15) Avez-vous une méthodologie d'audit de la sécurité de l'information ?
Oui ☐ Non ☐

16) Les étapes de votre méthodologie d'audit de la sécurité de l'information comprennent elles ?
L'audit organisationnel l'audit physique l'audit organisationnel et physique l'audit technique l'audit organisationnel et technique l'audit technique et physique

17) Est-ce que les audits sont planifies et réalisés en s'entourant de la sécurité nécessaire pour protéger le fonctionnement des systèmes opérationnelles ? Oui ☐ Non ☐

18) Avez-vous décelez des faiblesses qui ont suscité une quelconque révision ou mise à jour de la politique de sécurité? Oui ☐ Non ☐

19) Les systèmes d'information de la banque sont-ils contrôlés régulièrement afin de vérifier leur conformité avec la politique et les normes de sécurité? Oui ☐ Non ☐

20) Est-il évident de trouver des pistes d'audit adéquates pour mener à bien les missions d'audit de la sécurité de l'information ? Oui ☐ Non ☐

21) Avez-vous des connaissances et compétences en matière de technologies de l'information ?
Oui ☐ Non ☐

22) Donnez-moi un outil d'audit de base de données ? ……..

23) Quels outils utilisez-vous lors d'un audit de sécurité de l'information ? ……

24) Existe-t-il des logiciels d'audit relatif à la sécurité de l'information au sein de la banque ?
Oui ☐ Non ☐

25) Si oui, ces logiciels génèrent ils des rapports réguliers sur les évènements afférents à la sécurité de l'information ? Oui ☐ Non ☐

26) Ces rapports sont-ils protégés? Oui ☐ Non ☐

27) Vos recommandations sont-ils toujours suivis ? Oui ☐ Non ☐

28) Vos recommandations sont-ils promptement et clairement suivis ? Oui ☐ Non ☐

29) La direction engage-t-elle des actions pour assurer le suivi des procédures de sécurité et les recommandations d'audit ? Oui ☐ Non ☐

30) Existe-il un comité d'audit au sein de la banque? Oui ☐ Non ☐

31) A qui rendez-vous directement des comptes lors de vos missions d'audit ?

Directeur General ☐

Conseil d'administration / comité d'audit ☐

Commission bancaire ☐

32) Sur une échelle de 1 à 10, combien noterez-vous le système de gestion de la sécurité de l'information de Ecobank CI ? ……..

33) En quelques mots, que vérifiez-vous lors d'une mission d'audit de la sécurité de l'information ?

……

……

……

34) Selon vous, quel est l'apport de l'audit interne au maintien et à l'amélioration continue de la sécurité de l'information ?

……

……

……

……

BIBLIOGRAPHIE

Livres

1) BERTIN Elisabeth (2007), *Audit Interne : Enjeux et pratiques à l'international*, éditions Eyrolles, Paris, 320 pages

2) CNCC-IRE-CSOEC (2012*), la norme internationale d'audit ISA 315, identification et évaluation des risques d'anomalies significatives par la connaissance de l'entité et de son environnement*, 49 pages

3) Conception de la structure Espace numérique Entreprise (2010), *La sécurité des systèmes d'information, Le guide à l'usage pratique des dirigeants*, 44 pages

4) CLUSIF (2003), *ISO 17799 :2000, une présentation générale*, CLUSIF, Paris, 16 pages

5) DEBROCK Aurélien et GOURDIN Eric (2009), *La sécurisation de l'information dans le Système d'Information*, Mémoire de recherche, Paris, 65 pages

6) DEYRIEUX André (2004), L*e système d'information, nouvel outil de stratégie, Direction d'entreprise et DSI*, éditions Maxima, Paris, 185 pages

7) DI SCALA Robert Michel (2005), *L'essentiel en informatique et programmation*, éditions Berti, Alger, 1017 pages

8) DOUCENDE Bruno (2004-2009), Livre Blanc du Groupe 4, *Sécurité des systèmes d'information*, Synertic Conseil, 4IM SAS, 31 pages

9) GHERNAOUTI-HELIE Solange (2000), *Sécurité Internet, Stratégies et Technologies*, éditions Dunod, 288 pages

10) IFACI (2013), *Cadre de référence international des pratiques professionnelles de l'audit interne*, IIA, France, 238 pages

11) IFACI (1993), *Audit et contrôle des Systèmes d'Information Module 8 : Sécurité*, Paris, 124 pages

12) ISACA (2010), *information Security Management Audit/ Assurance Program,* ISACA, USA, 38 pages

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

14) LACOLARE Vincent (2010), *Pratiquer l'audit à valeur ajoutée*, éditions Afnor, Paris, 188 pages

15) La Commission Bancaire Européenne (1996), *livre blanc sur la sécurité des systèmes d'information dans les établissements de crédit*, France, 344 pages

16) Le comité de Bale pour le contrôle bancaire (1998), *cadre pour le système de contrôle interne dans les organisations bancaires,* la banque des règlements internationaux, 33 pages

17) Le comité de Bale pour le contrôle bancaire (2012), *principes fondamentaux pour un contrôle bancaire efficace,* la banque des règlements internationaux, 83 pages

18) LONGEON Robert et ARCHIMBAUD Jean-Luc (1999), *Le guide de la sécurité des systèmes d'informations à l'usage des directeurs*, CRNS, 94 pages

19) MOISAND Dominique et GARNIER DE LABAREYRE Fabrice (2009), *CobiT, pour une meilleure gouvernance des systèmes d'information*, éditions Eyrolles, Paris, 258 pages

20) PIPKIN L. Donald (2000), *Information security, protecting the global enterprise*, editions Prentice Hall, 364 pages

21) RENARD Jacques (2003), *l'Audit Interne, ce qui fait débat*, éditions Maxima, Paris, 267 pages

22) RENARD Jacques (2010), *Théorie et pratique de l'Audit Interne*, 7eme Edition, éditions Eyrolles, Paris, 463 pages

23) VILLALONGA Christophe (2011), *Le guide du parfait auditeur interne*, Editions Lexitis, France, 124 pages

Autres documents

24) Banque Européenne d'investissement (2007), *charte d'audit interne*, 4 pages

25) Gouvernement du QUEBEC (2009), *Politique concernant la sécurité de l'information*, version 1.1, Québec, 27 pages

26) The Institute of Internal Auditors (2012), *A l'écoute de la profession : Perspectives 2012,* The IIA'S Audit executive center, Floride, 14 pages

Webographie

27) Différentes facettes de la sécurité de l'information, http://foad.refer.org/IMG/pdf/D312_Chapitre-1.pdf

28) La norme ISO 27001, http://fr.wikipedia.org/wiki/ISO/CEI 27001

29) Les caractéristiques de l'information, http://www.formaplace.org/elearning/S53-1/co/S53-1-2-Caract_qualites_%26_fonctions_info.html

30) Définition de la sécurité des systèmes d'information http://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_des_syst%C3%A8mes_d'information

31) Mémoire sur la contribution de l'audit interne à la performance financière http://www.memoireonline.com/10/09/2847/m_Contribution-de-laudit-interne-a-la-performance-financiere-des-entreprises-cas-des-b0.html

32) Informations sur Ecobank CI, http://news.abidjan.net/h/451898.html

33) Informations sur Ecobank CI, http://www.ecobank.com/group/aboutus.aspx?hl=fr

34) Audit comme mesure de sécurité, http://www.ssi-conseil.com

35) Le modèle PDCA, http://asiq.org/documents/conferences/2013/ASIQ-201302.pdf