



Centre Africain d'études Supérieures en Gestion

**Institut Supérieur de Comptabilité, de
Banque et de Finance
(ISCBF)**

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

**Promotion 23
(2011-2012)**

Mémoire de fin d'étude

THEME

**LE ROLE DE L'AUDIT INTERNE DANS LA
GOUVERNANCE DES SYSTEMES
D'INFORMATION : CAS D'ECOBANK
BURKINA**

Présenté par :

Dirigé par :

Mlle BENEH PRISCA LINDA KABORE

M ALPHA OUSMANE SY

Directeur de l'audit interne de la Banque
Atlantique du Sénégal

Octobre 2012



M0449AUDIT12

2

DEDICACES

- ✓ A nos parents, pour le sacrifice consenti et pour leur soutien et leurs conseils ;
- ✓ A nos frères et sœurs, pour leur présence à nos côtés. Que vous puissiez mieux faire.

CESAG - BIBLIOTHEQUE

REMERCIEMENTS

Nous remercions avant tout le Seigneur pour la santé et le courage qu'il nous a donnés pour entreprendre et achever ce travail.

Nos sincères remerciements vont à l'endroit du corps professoral du CESAG en particulier à :

- ✓ M Yazi Moussa, Directeur de l'Institut Supérieur de Comptabilité de Banque et de Finance (ISCBF), pour la qualité de l'enseignement et pour tous les précieux conseils reçus ;
- ✓ M Alpha Sy, notre directeur de mémoire, qui en dépit de ses nombreuses occupations a accepté de nous guider.

Nous remercions également :

- ✓ M Guiré Marcel, pour nous avoir trouvé le stage ;
- ✓ M Bila Yaméogo, Auditeur Informatique à Ecobank Burkina pour sa contribution inestimable et la mise à disposition des documents ;
- ✓ la Direction de l'audit interne d'Ecobank Burkina en particulier son Directeur M Sidiki Sawadogo, les auditeurs M Somé Ilana, M Kola et Ouattara Lassina pour les conseils et leur contribution à la réalisation de notre travail ;
- ✓ à notre famille et à nos amis pour tout leur soutien et pour leurs prières ;
- ✓ à la 23^{ème} promotion du DESS Audit et Contrôle de Gestion pour le soutien moral, les échanges d'expérience et l'ambiance amicale qui règne toujours entre nous.

Nous témoignons notre reconnaissance à tous ceux et celles qui nous ont apporté leur soutien lors de notre formation.

LISTE DES SIGLES ET ABBREVIATIONS

AFAI : Association Française de l'Audit et du Conseil Informatique

AG : Assemblée Générale

AI : Audit Interne

BACB : Banque Agricole et Commerciale du Burkina

BCEAO : Banque Centrale des Etats de l'Afrique de l'Ouest

CA : Conseil d'Administration

CIGREF : Club Informatique des Grandes Entreprises Françaises

COBIT : Control Objectives for Information and Related Technology

COCO : Criteria of Control Committee

COSO : Committee of Sponsoring Organizations of the Treadway Commission

CRM/GRC : Customer Relationship Management/ Gestion de la Relation Client

DAB : Distributeurs Automatiques de Billets

DM : Direction Métier

DOT : Direction des Opérations et de la Technologie

DSI : Directeur du Système d'Information

EBF : Ecobank Burkina Faso

EDI : Echanges de Documents Informatisés

ERP : Enterprise Resource Planning

ETI : Ecobank Transnational Incorporated

GSI : Gouvernance des Systèmes d'Information

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

IGSI : Institut de la Gouvernance des Systèmes d'Information

IIA : Institute of Internal Auditors

ISACA : Information Systems Audit and Control Association

ITIL : Information Technology Infrastructure Library

PME/PMI : Petites et Moyennes Entreprises/ Petites et Moyennes Industries

SAD : Système d'Aide à la Décision

SI : Système d'Information

SID : Système d'Information pour Dirigeant

SIG : Système d'Information de Gestion

SLA: Service Level Agreement

STT: Système de Traitement des Transactions

TCO: Total Cost of Ownership

TI/IT: Technologie de l'Information/ Information Technology

TPE : Terminaux de Paiement Electronique

UEMOA: Union Economique et Monétaire Ouest Africaine

UPS : United Parcel Service

CESAG - BIBLIOTHEQUE

LISTE DES TABLEAUX ET FIGURES

Liste des tableaux

Tableau 1: Tableau de mesure des indicateurs d'évaluation de l'implication de l'audit interne dans la GSI.....	44
Tableau 2: l'évolution des résultats obtenus par la banque au titre de l'exercice 2011 (Montant en milliers de FCFA)	53
Tableau 3 : la présentation des données du questionnaire d'évaluation de la qualité du système d'information	64

Liste des figures

Figure 1: le modèle d'analyse	42
-------------------------------------	----

CESAG - BIBLIOTHEQUE

LISTE DES ANNEXES

ANNEXE 1 : Structure du cadre de référence COBIT 4	88
ANNEXE 2 : le schéma des outils de la mise en œuvre des bonnes pratiques.....	89
ANNEXE 3: la figure de l'alignement stratégique du système d'information, le modèle d'Henderson et Venkatraman.....	90
ANNEXE 4 : guide d'entretien adressé au chef de division.....	92
ANNEXE 5: guide d'entretien adressé au Directeur de l'Audit Interne	94
ANNEXE 6: questionnaire d'évaluation de la contribution de l'audit interne dans la gouvernance des systèmes d'information	97
ANNEXE 7: Questionnaire adressé aux chefs d'agence	99
ANNEXE 8 : l'organigramme d'Ecobank Burkina (janvier 2011)	100
ANNEXE 9: organigramme de la direction de l'audit interne (janvier 2011).....	101

TABLE DES MATIERES

DEDICACES	i
REMERCIEMENTS	ii
LISTE DES SIGLES ET ABREVIATIONS	iii
LISTE DES TABLEAUX ET FIGURES	v
LISTE DES ANNEXES	vi
TABLE DES MATIERES	vii
INTRODUCTION GENERALE	1
PREMIERE PARTIE : CADRE THEORIQUE	7
INTRODUCTION DE LA PREMIERE PARTIE	8
CHAPITRE 1 : LA GOUVERNANCE DES SYSTEMES D'INFORMATION	9
1.1 Le système d'information.....	9
1.1.1 Les composantes et les acteurs du système d'information.....	9
1.1.1.1 Les composantes du système d'information.....	10
1.1.1.2 Les acteurs du système d'information	11
1.1.2 La qualité des systèmes d'information.....	12
1.1.3 Les TI et avantages concurrentiels.....	14
1.1.3.1 Enterprise Resource Planning (ERP).....	15
1.1.3.2 Customer Relationship Management (CRM).....	16
1.2 La gouvernance des systèmes d'information.....	16
1.2.1 Les référentiels et bonnes pratiques de la gouvernance des systèmes d'information	17
1.2.1.1 Les référentiels COBIT et ITIL.....	17
1.2.1.2 Les outils de la mise en œuvre des bonnes pratiques	24
1.2.2 Les axes stratégiques de la gouvernance des systèmes d'information.....	24
1.2.2.1 L'alignement stratégique.....	24
1.2.2.2 La création de valeur	26
1.2.2.3 La gestion des ressources	26
1.2.2.4 La gestion des risques.....	27
1.2.2.5 La mesure de la performance	27
1.2.3 Gouvernance et gestion des risques	28

CHAPITRE 2 : LE ROLE DE L'AUDIT INTERNE DANS LA GOUVERNANCE DES SYSTEMES D'INFORMATION	29
2.1 L'audit interne	29
2.1.1 Le cadre de référence de l'audit interne.....	29
2.1.1.1 Le code de déontologie.....	30
2.1.1.2 Les normes de l'audit interne	32
2.1.2 Missions et objectifs de l'audit interne	33
2.1.2.1 les missions de l'audit interne	33
2.1.2.2 Les objectifs de l'audit interne	33
2.2 L'audit interne dans le pilotage stratégique du SI.....	35
2.2.1 L'analyse de l'alignement stratégique	36
2.2.2 L'évaluation de la stratégie	37
2.3 L'audit de conformité des systèmes d'information	38
2.3.1 Le référentiel COBIT.....	39
2.3.2 La réglementation bancaire.....	39
2.4 L'audit interne et l'évaluation de la performance	40
3.1 Modèle d'analyse et le tableau de mesure des indicateurs	41
3.1.1 Présentation du modèle d'analyse.....	41
3.1.2 Le tableau de mesure des indicateurs.....	43
3.2 Les outils de collecte des données et la méthodologie d'analyse des données	44
3.2.1 Les outils de collecte des données	45
3.2.1.1 l'analyse documentaire.....	45
3.2.1.2 l'entretien.....	45
3.2.1.3 les questionnaires	45
3.2.1.4 l'observation.....	46
3.2.2 La méthodologie d'analyse des données.....	46
DEUXIEME PARTIE : CADRE PRATIQUE	48
INTRODUCTION DE LA DEUXIEME PARTIE	49
4.1 Missions et objectifs d'Ecobank Burkina.....	51
4.2 Présentation des produits et de l'organisation d'Ecobank Burkina.....	51
4.2.1 Les produits d'Ecobank Burkina.....	51
4.2.2 L'organisation d'Ecobank Burkina et leurs attributions.....	53
4.2.2.1 la direction de la trésorerie	54

4.2.2.2 Corporate Bank.....	54
4.2.2.3 Domestic Bank	54
4.2.2.4 la direction de la gestion des risques	54
4.2.2.5 La direction du contrôle interne	54
4.2.2.6 Le secrétariat général/direction juridique.....	55
4.2.2.7 La direction des ressources humaines	55
4.2.2.8 la direction du contrôle financier.....	55
4.2.2.9 La direction de l'audit interne	55
4.2.2.10 La direction des opérations et technologie	56
CHAPITRE 5 : LA GOUVERNANCE DU SYSTEME D'INFORMATION DE LA BANQUE	57
5.1 Présentation du système d'information et la qualité du système d'information.....	57
5.1.1 Présentation du système d'information.....	58
5.1.1.1 Présentation des applications de FLEXCUBE	58
5.1.1.2 les objectifs et stratégies du SI	59
5.1.1.3 la gestion des ressources.....	60
5.1.1.4 la gestion des incidents.....	61
5.1.2 La qualité du système d'information	62
5.1.2.1 la sécurité du système d'information.....	62
5.1.2.2 les autres critères de la qualité.....	63
5.2 La gouvernance du système d'information d'EBF.....	65
5.2.1 Les acteurs de la gouvernance du système d'information et leurs rôles	65
5.2.2 Le processus de la GSI.....	66
5.2.3 L'application des principes de la GSI.....	67
5.2.3.1 l'alignement stratégique	67
5.2.3.2 La gestion des risques.....	68
5.2.3.3 L'évaluation de la performance.....	69
5.3 Le rôle de l'audit interne dans l'alignement stratégique	70
5.4 L'audit interne et les risques du système d'information.....	70
5.5 Le rôle de l'audit interne dans l'évaluation de la performance	71
CHAPITRE 6 : PRESENTATION-ANALYSE DES RESULTATS ET RECOMMANDATIONS.....	73
6.1 La présentation des résultats.....	73

6.1.1 Le niveau de rattachement hiérarchique	73
6.1.2 La fréquence des réunions avec les acteurs de la GSI	74
6.1.3 Les ressources de l'audit interne	74
6.1.4 Les missions d'audit du SI.....	75
6.1.5 L'évaluation du contrôle interne	75
6.2 L'analyse des résultats.....	76
6.2.1 Les points forts de la GSI.....	76
6.2.2 Les forces de l'implication de l'audit interne dans la GSI.....	76
6.2.2.1 le respect des bonnes pratiques.	76
6.2.2.2 le système de management des risques	77
6.2.2.3 la réalisation des audits d'efficacité	77
6.2.2.4 l'apport de la direction générale.....	77
6.2.3 Les faiblesses de la GSI.....	77
6.2.4 Les faiblesses de l'implication de l'audit interne dans la GSI.....	78
6.2.4.1 L'absence d'audit de management.....	78
6.2.4.2 l'insuffisance des moyens techniques	78
6.2.4.3 les insuffisances dans l'évaluation de la performance du SI.....	78
6.3 Les recommandations.....	79
6.3.1 Recommandations pour la division de la technologie	79
6.3.2 Recommandations pour la direction générale.....	79
6.3.3 Recommandations pour la direction de l'audit interne.....	80
CONCLUSION DE LA DEUXIEME PARTIE.....	82
CONCLUSION GENERALE.....	83
ANNEXES.....	86
BIBLIOGRAPHIE.....	102

INTRODUCTION GENERALE

CESAG
BIBLIOTHEQUE

En Afrique de l'Ouest, comme partout ailleurs dans les économies de marché, les banques jouent un rôle primordial dans le développement de l'économie. Aujourd'hui, le constat est que le secteur bancaire ouest africain en particulier celui de l'Union Economique Monétaire Ouest Africaine (UEMOA) est en plein essor. Il en résulte une rude concurrence qui exige un système bancaire de qualité.

L'Africa Business Market (2011) affirme que selon l'agence de notation Standard & Poors, le secteur bancaire de la zone UEMOA est exposé à des risques et subira une transformation sous l'effet de l'intensification de la concurrence. Cette concurrence exige donc des banques une veille permanente afin de garantir non seulement une amélioration continue des produits et services mais aussi une gestion efficace des risques. Pour ce faire, les banques adoptent des politiques d'amélioration fortes dans le sens de la qualité et/ou de la productivité des facteurs de production en particulier les Technologies de l'Information (TI). Ces politiques permettent de fournir aux différentes parties prenantes de la banque, des informations qui participent à l'élaboration des stratégies d'affaires, à la prise de décision et au contrôle du rendement.

Cependant, le traitement de l'information nécessite la mise en œuvre d'un système dit Système d'Information (SI) qui subit l'influence de l'environnement de l'entreprise et dont la mise en œuvre impacte les coûts, les processus et la valeur ajoutée créée par l'entreprise. Il s'agira donc pour les managers de piloter le système d'information c'est-à-dire d'assurer la Gouvernance des Systèmes d'Information (GSI) pour contribuer à l'atteinte des objectifs de l'entreprise. La banque étant une structure où le système d'information joue un rôle essentiel dans la réalisation des activités, cette dernière doit adopter les bonnes pratiques en matière de système d'information.

Ecobank Burkina Faso (EBF), membre du Groupe Ecobank Transnational Incorporated (ETI), offre à sa clientèle une gamme de produits bancaires et financiers étendue et diversifiée. C'est également une banque qui s'implique fortement dans le financement de la production agricole. Dans la poursuite de sa dynamique commerciale, Ecobank a mené des actions marketing qui lui ont permis de profiter de la fusion absorption de la Banque Agricole et Commerciale du Burkina (BACB). Ces actions marketing lui ont également permis de manifester une plus grande proximité avec sa clientèle et d'améliorer la qualité de ses services. Ecobank Burkina a aussi développé son réseau et consolidé de nouveaux projets

d'infrastructures opérationnelles impliquant donc la modernisation de son système d'information et le renforcement de la gouvernance. Suite à la fusion absorption, Ecobank Burkina a procédé à une migration des deux anciens systèmes d'information bancaires vers un système d'information unique appelé FLEXCUBE.

Selon le rapport annuel 2010 d'Ecobank Burkina paru sur son site, c'est une banque qui veille à l'application conforme des règles de gouvernance institutionnelle par rapport aux standards internationaux d'où l'existence d'un Comité de Gouvernance, d'un Comité de Risque et d'un Comité d'Audit interne. Elle dispose d'une direction de l'audit interne chargée de l'évaluation du contrôle interne et des risques.

Avec le développement de la technologie de l'information et de la communication, les risques sont de plus en plus complexes et l'information de gestion connaît une plus grande exposition. La fiabilité des informations financières et comptables est devenue une préoccupation majeure pour les entreprises, et en particulier pour Ecobank. En effet, avec la migration des deux systèmes bancaires vers un nouveau système en 2010, Ecobank Burkina a connu des perturbations qui ont impacté les opérations bancaires. L'année 2011 a ainsi été marquée par la gestion post-migration et la formation continue du personnel au système bancaire. Les efforts se poursuivent sur l'année 2012 pour maintenir une forte stabilité du système bancaire et assurer une réalisation efficiente des opérations.

Cependant, les préoccupations relatives à la mise en place d'un système stable, sécurisé et fiable, en ligne avec les objectifs commerciaux de la banque ne relèvent pas uniquement de la responsabilité des dirigeants de l'Information Technology (IT). Il ne s'agit plus seulement d'implanter un système d'information mais de faire de la gouvernance du système d'information existant un outil de pilotage et d'amélioration de la performance et de s'assurer de la prise en compte des intérêts des parties prenantes.

Le problème énoncé ci-dessus peut s'expliquer par :

- l'aspect technique des systèmes d'information ;
- la méconnaissance de l'importance de l'intervention de l'audit dans la GSI ;
- le non respect des bonnes pratiques de la GSI.

Avec l'émergence des innovations technologiques, le système d'information est une fonction transversale dans les activités bancaires et des dysfonctionnements peuvent générer des conséquences telles que :

- la production d'informations non pertinentes pour la prise de décision ;
- l'inadéquation entre les décisions opérationnelles et les décisions stratégiques ;
- l'inexistence ou inopportunité et inutilité de certains processus alors que l'audit interne permet d'évaluer la qualité des processus ;
- la non maîtrise des risques du système d'information ;
- le non respect des dispositions légales et réglementaires. Dans l'espace UEMOA, la Commission Bancaire, organisation communautaire du contrôle des banques et établissements financiers, impose à l'audit interne dans sa circulaire N°003-2011/CB/C en son article 2-d une évaluation de la conformité aux lois et règlements.

Les solutions possibles pour y remédier sont entre autres :

- respecter les bonnes pratiques en matière de GSI ;
- former les auditeurs en matière de système d'information ;
- faire intervenir davantage l'audit interne dans la gouvernance des systèmes d'information.

Cette dernière solution s'avère pertinente pour notre étude.

En effet, elle amène l'audit interne à s'assurer de l'adéquation entre système d'information et stratégie, à évaluer les dispositifs de contrôle interne liés à l'efficacité et la sécurité du système d'information.

Pour mieux cerner la problématique de l'étude, nous nous interrogeons sur un certain nombre de questions dont l'une ayant un caractère d'ordre général à savoir :

Quelle est l'efficacité de l'implication de l'audit interne dans la gouvernance des systèmes d'information à Ecobank Burkina?

De façon spécifique, les questions qui peuvent découler de cette question générale sont :

- qu'est ce que la gouvernance des systèmes d'information ?
- quelles sont les applications, les directives et bonnes pratiques en matière de gouvernance des systèmes d'information ?
- comment l'audit interne intervient-il dans la gouvernance des systèmes d'information ?
- comment l'audit interne est-il impliqué dans la gouvernance du système d'information au sein d'Ecobank Burkina ?
- quelles sont les forces et les faiblesses de l'implication de l'audit interne dans la gouvernance du système d'information d'Ecobank Burkina ?
- quelles améliorations apporter à l'implication de l'audit interne en matière de gouvernance du système d'information ?

Telles sont les questions auxquelles nous essayerons d'apporter des réponses à travers l'étude du thème : « le rôle de l'audit interne dans la gouvernance des systèmes d'information » : cas d'Ecobank Burkina (EBF).

Pour mener à bien notre étude, l'objectif général de la recherche sera d'analyser la contribution de l'audit interne à la gouvernance du système d'information à Ecobank Burkina.

De façon spécifique, il s'agit :

- de définir la gouvernance des systèmes d'information ;
- de prendre connaissance des applications, directives et pratiques de la gouvernance des systèmes d'information ;
- d'identifier les différents rôles de l'audit interne dans la gouvernance des systèmes d'information ;
- d'analyser l'implication de l'audit interne dans cette gouvernance au sein d'Ecobank Burkina ;
- d'identifier les points forts et les points faibles de l'apport de l'audit interne dans le processus de gouvernance du système d'information à Ecobank Burkina et faire des recommandations.

Cette étude présente non seulement un intérêt pour Ecobank Burkina mais aussi pour l'auteur que nous sommes.

- Pour Ecobank Burkina

Elle pourrait lui permettre de mieux cerner l'apport de l'audit interne dans la création de valeur ajoutée dans le processus de la gouvernance des systèmes d'information. Elle va aussi permettre de prendre connaissance des forces et faiblesses de l'audit interne dans ce processus et donc de l'impliquer davantage.

- Pour nous-mêmes

Les travaux de recherche qui seront effectués sur ce thème nous permettront de compléter nos connaissances en système d'information et d'acquérir de l'expérience non seulement en audit interne mais aussi en matière de gouvernance des systèmes d'information.

- Pour le CESAG

Le CESAG pourra mettre ce document à la disposition des stagiaires désirant approfondir leurs connaissances en matière d'audit et de gouvernance des systèmes d'information.

Ce mémoire est structuré en deux grandes parties : la première partie sera consacrée d'une part à la revue de la littérature qui abordera les aspects théoriques de la gouvernance des systèmes d'information et l'apport de l'audit interne en la matière et, d'autre part, à l'approche méthodologique de l'étude. La deuxième partie portera sur le cadre pratique de l'étude qui consistera à présenter Ecobank Burkina puis à décrire son processus de gouvernance des systèmes d'information et à présenter et analyser les données qui seront collectées afin de formuler des recommandations.

PREMIERE PARTIE : CADRE THEORIQUE

CESAG
BIBLIOTHEQUE

INTRODUCTION DE LA PREMIERE PARTIE

Aujourd'hui, avec l'évolution concurrentielle de l'entreprise, le développement de l'internet, l'émergence des entreprises numériques et des économies axées sur le savoir et l'information, les technologies de l'information (TI) exercent une influence notable sur la productivité et la rentabilité des entreprises. En effet, ces technologies de l'information sont devenues un outil d'innovation des produits, d'amélioration de la qualité, de réduction de coûts et permettent à l'entreprise d'être agile sur le marché. Aussi, les TI sont sources de changements dans les marchés et leurs structures en particulier dans les marchés bancaires et financiers.

Pour répondre rapidement aux besoins du marché, l'entreprise, en particulier bancaire doit pouvoir capter l'information émanant du marché et faciliter une circulation efficace et rapide de cette information en son sein pour mieux répondre aux besoins de sa clientèle.

Cependant, le système d'information qui peut être une fonction de support doit permettre la maniabilité de l'information reçue du marché afin de la rendre utile non seulement pour l'organisation bancaire mais aussi pour l'ensemble de la clientèle cible. D'après Autissier et al (2008 :48) « le système d'information traite entre autre de l'installation et de l'utilisation de la technologie informatique pour la réalisation des activités d'une organisation ». Les banques dont l'environnement technologique évolue très rapidement doivent bien piloter le système d'information afin d'assurer une synergie entre les TI et les opérations bancaires. L'audit interne, organe de la gouvernance institutionnelle est l'un des outils qui intervient dans le pilotage des systèmes d'information.

Cette première partie théorique présentera, dans un premier chapitre, la gouvernance des systèmes d'informations afin de mieux cerner les applications et bonnes pratiques de ce concept. Le deuxième chapitre mettra en exergue la relation qui peut exister entre l'audit interne et la gouvernance des systèmes d'information.

Le troisième et dernier chapitre sera consacré à la méthodologie de recherche qui présentera d'une part, le modèle d'analyse et le tableau de mesure des indicateurs et d'autre part, les outils de collecte des données et la méthodologie d'analyse.

CHAPITRE 1 : LA GOUVERNANCE DES SYSTEMES D'INFORMATION

Avec l'accroissement de la concurrence, les décisions stratégiques n'émanent plus d'un décideur unique mais de toutes les parties prenantes de l'entreprise d'où la nouvelle notion de gouvernance d'entreprise qui vise à assurer au mieux les intérêts des parties prenantes. La gouvernance d'entreprise est un ensemble de processus, de réglementations et de lois qui influencent l'administration, la direction et le contrôle de l'entreprise. La gouvernance appliquée au domaine des systèmes d'information qui sont non seulement un outil de coordination en interne mais aussi en amont et en aval de la chaîne de valeur nous amène à introduire la notion de gouvernance des systèmes d'information.

Ce chapitre sera structuré en deux sections : une première section qui permettra de prendre connaissance du système d'information et une deuxième section qui s'intéressera à la gouvernance des systèmes d'information.

1.1 Le système d'information

L'information joue un rôle important dans nos milieux de vie mais encore plus dans l'entreprise qui est confrontée à une exigence croissante des besoins en matière d'information surtout financière. Cette information financière destinée à des tiers tels que les actionnaires, les créanciers, les fournisseurs et autres parties prenantes doit être fiable, pertinente, significative et compréhensible par les utilisateurs afin d'aider leurs prises de décisions. La production de l'information nécessite donc la mise en place d'un système d'information afin de répondre aux caractères qualitatifs de toute information. Quels sont les composantes de ce système et qui sont les acteurs chargés de sa gestion ?

1.1.1 Les composantes et les acteurs du système d'information

Plusieurs auteurs ont apporté une définition au système d'information. Il s'agit entre autre d'Autissier et al (2008 :49), Hémici et al (2007 :162) qui définissent le système d'information comme un « ensemble de dispositifs techniques et organisationnels permettant la mise en place et l'exploitation de la technologie informatique nécessaire aux utilisateurs et à la stratégie de l'entreprise ». Cet ensemble de dispositifs techniques et organisationnels

comprend les hommes (les informaticiens et les utilisateurs), les données (sous forme alphanumériques, de figures, textuelles ou de modèle), les procédures, le matériel, les logiciels (base ou application) et réseaux et permet de transformer des données en produits d'information à travers la saisie, le traitement et le stockage.

Le système d'information se distingue donc du système informatique qui est un ensemble d'éléments physiques et de logiciels permettant d'assurer le traitement automatique de l'information.

Notons que les informations produites peuvent à leur tour constituer des données qui seront traitées pour produire d'autres informations : le système d'information a donc un caractère rétroactif.

Pour Angot (2004 : 20), c'est « un réseau complexe de relation structurée qui a pour objet d'engendrer des flux ordonnés d'informations pertinentes, provenant des sources internes et externes à l'entreprise et destinées à servir de base aux décisions ».

De ces définitions, il ressort que le système d'information comme tout système comprend un ensemble de composantes et d'activités qui permettent de produire et d'exploiter l'information.

1.1.1.1 Les composantes du système d'information

Les principales composantes du système d'information sont :

- les ressources humaines. Il s'agit des informaticiens qui conçoivent et mettent à disposition le système informatisé et des utilisateurs ou clients qui exploitent et utilisent le système ou l'information qu'elle produit ;
- les ressources matérielles. Il s'agit du système informatique qui regroupe l'unité centrale, les dispositifs d'entrée comme le clavier, les dispositifs de sortie comme les imprimantes et les supports physiques de stockage comme les disques magnétiques et optiques ;

- les données qui sont des faits à l'état brut recueillis, saisis, traités pour produire de l'information qui est ensuite stockée et diffusée. Elles peuvent être sous forme alphanumérique, sous forme textuelle ou sous forme de figure organisées soit en base de données (données traitées), soit en base de modèle qui présente des programmes de calcul ou des techniques d'analyse ou encore en base de connaissance ;
- Les logiciels (logiciels de base, des logiciels d'application ou des procédures) et les réseaux de télécommunication (internet, intranet, extranet) ;
- Les moyens techniques.

Certains auteurs comme Rivard et Talbot (2001 :34) distinguent « trois types de systèmes d'information qui correspondent aux trois niveaux hiérarchiques de l'entreprise. Il s'agit du Système de Traitement des Transactions (STT) destiné au niveau opérationnel, du Système d'Information de Gestion (SIG) pour le niveau intermédiaire et du Système d'Information pour Dirigeant (SID) pour le niveau stratégique ». Cependant, des auteurs comme Laudon et al (2010 : 471) et Voyer (2006 :319) ont identifié un quatrième qui est « le Système d'Aide à la Décision (SAD) conçu pour les experts du niveau intermédiaire ».

Ces types de système sont en interrelation car le SIG entre dans le fichier SIG les données provenant du STT qui sont ensuite analysées dans le SIG pour fournir au SAD et au SID des rapports d'analyse. Ces rapports qui sont des données sont introduits dans le SAD et/ou le SID pour être traités et servir à la prise de décision. Le SAD peut également obtenir ses données du STT et fournir aux SID des informations pour la prise de décision.

La gestion des systèmes d'information implique la collaboration d'un certain nombre d'acteurs.

1.1.1.2 Les acteurs du système d'information

Les acteurs impliqués dans la gestion du système d'information sont :

- la Direction des Systèmes d'Information (DSI) responsable du fonctionnement quotidien des systèmes d'information, elle détermine les besoins des utilisateurs et leur apporte son assistance. Au sein de la direction, il est désigné un Maître

d'œuvre qui est chargé de la conception des systèmes d'information, du développement des projets informatiques, de la maintenance des applications et du pilotage des évolutions du système d'information et qui sert d'interface entre la direction et les utilisateurs. Responsable de la performance et de la maîtrise des coûts du système d'information, le DSI doit adapter la stratégie des systèmes d'information à la stratégie globale ;

- les Directions Métiers (DM) qui regroupent l'ensemble des autres directions ne sont pas spécialistes en technologie. Chaque DM désigne un Maître d'Ouvrage (MOA) qui définit ses besoins et ses priorités en système d'information à la DSI.

Ces deux acteurs, avec la Direction Générale doivent être en coordination étroite afin d'assurer une gestion efficace des systèmes d'information.

Selon Autissier et al (2008:10) « pour rester dans la course à la compétitivité, les organisations doivent aligner leur système d'information, véritable colonne vertébrale de l'entreprise, à leurs objectifs business ». Le système d'information est une fonction support qu'il faut optimiser d'où la question de savoir comment le système d'information peut-il apporter une valeur ajoutée et permettre d'être compétitif ? Des facteurs de compétitivité tels que la flexibilité et la qualité qui sont introduites dans toutes les dimensions de la gestion permettent de répondre à cette préoccupation.

1.1.2 La qualité des systèmes d'information

Les TI offrent aujourd'hui aux entreprises de larges possibilités pour obtenir des avantages stratégiques. Les TI qui sont une composante des systèmes d'information jouent un rôle dans l'amélioration des opérations, la qualité des produits et services et la rapidité à répondre aux exigences du marché. Plusieurs entreprises comme Amazon, Dell et Apple's iTunes ont su se différencier de la concurrence grâce à la qualité de leur système d'information.

Un système d'information de qualité fournit des informations :

- accessibles : les utilisateurs doivent pouvoir accéder facilement aux informations qui les concernent et qu'ils utilisent dans leurs activités ;

- sécurisées. L'information ne doit présenter aucun danger ; le risque doit être maîtrisé. Les données du système d'information doivent être sécurisées contre toute modification, destruction, accès ou acquisition non autorisée. La norme ISO 17799 qui est un guide de bonne pratique pour gérer la sécurité d'un système d'information présente trois (3) caractéristiques de sécurité :
 - ✓ la confidentialité qui consiste à rendre l'information disponible qu'aux destinataires. Selon Morley (2008 :205) « la confidentialité comprend la protection des codes et des données et la mémorisation des accès aux personnes autorisées ». Cette mémorisation sous-entend que les manipulations doivent être enregistrées afin d'assurer leur traçabilité;
 - ✓ l'intégrité qui suppose qu'aucune information n'est pas modifiée de manière involontaire;
 - ✓ La disponibilité de l'information.

Aussi, un SI doit être :

- pertinent c'est-à-dire apte à répondre aux attentes des utilisateurs et approprié au contexte des utilisateurs ;
- fiable c'est-à-dire exempté d'erreurs et qui présente une image fidèle;
- flexible. Avec l'instabilité de l'environnement technologique, la DSI doit être réactif c'est-à-dire capable de modifier rapidement le système d'information pour l'adapter aux évolutions de l'environnement. Le système d'information flexible doit être réactif dans le temps, dans la diversité de l'offre, dans la souplesse de la structure, dans la production;
- efficace et efficient. La DSI doit non seulement fournir un système d'information capable de produire des informations utiles mais également utiliser moins de ressources. Pour cela, la DSI doit déterminer avec les utilisateurs leurs besoins et toujours les associer dans les projets de développement du système d'information.

Un système d'information répondant à ces critères de qualité et dont les coûts sont maîtrisés permet à l'entreprise d'obtenir un retour sur investissement (Return On Investissement). Dumont (2007 :2) soutient « qu'un investissement en équipement peut certes, être plus coûteux mais avoir un meilleur rapport coût/valeur et faire gagner de l'argent à

l'entreprise ». En effet, avec les nombreux défis tels que l'exigence de la clientèle et la compétitivité croissante, les entreprises investissent des capitaux importants dans les TI. Cependant, le retour sur investissement de ces valeurs dépendra de l'adéquation des investissements en TI avec les besoins, les objectifs et la stratégie de l'entreprise.

Les TI permettent d'avoir accès à l'information auprès des partenaires d'affaires (clients, fournisseurs et autres créanciers...) ou de diffuser très rapidement l'information grâce aux outils de travail quotidien tels que la vidéo conférence, le courriel, intranet, extranet, les Echanges de Documents Informatisés (EDI)...Cependant l'on se demande comment les TI peuvent-ils contribuer à accroître la part de marché et donc à obtenir un avantage concurrentiel?

1.1.3 Les TI et avantages concurrentiels

Selon Baumard et al (1998 : X) « l'avantage concurrentiel repose sur les TI et sur leur exploitation stratégique ». Les nouvelles sources de l'avantage concurrentiel dépendent des systèmes d'information qui doivent répondre au besoin de collecte, de traitement, de diffusion des informations et au besoin de coordination des processus au sein et entre les entreprises. Cela est possible grâce aux TI (internet, intranet, courriel...) qui accélèrent les flux d'information, suppriment les tâches sans valeur ajoutée, améliore la productivité (en terme de qualité et de quantité), renforcent la coordination des processus.

L'exploitation stratégique consiste pour une entreprise à :

- rechercher les facteurs de concurrence (prix, qualité, marque...) existants dans son secteur ;
- déterminer la manière dont les TI sont utilisés dans le secteur afin de les utiliser et créer de la valeur pour la clientèle. Pour cela, elle doit déceler les points de la chaîne de valeur où le système d'information permet de créer non seulement plus d'avantages pour le client mais aussi plus de profits pour l'entreprise. L'amélioration de la qualité des produits ou services, la rapidité de traitement de l'information, la réactivité face aux besoins des clients sont des sources de création de valeur. Avec l'émergence du commerce électronique, les entreprises améliorent le service à la clientèle ;

- utiliser des TI qui permettent d'améliorer les activités et les processus.

Comme exemple, United Parcel Service (UPS) qui est une importante entreprise de livraison par voie aérienne et terrestre utilise un système automatisé de suivi des colis qui lui permet d'assurer une bonne coordination des processus en interne (réception du colis-suivi de l'expédition-service clientèle). UPS dispose également d'un site web permettant aux clients de vérifier les itinéraires, de calculer les frais d'expéditions, de planifier une expédition, de régler par carte de crédit.

La préoccupation actuelle des entreprises étant d'assurer une amélioration continue du fonctionnement de leur organisation, le système d'information apparaît comme un moyen d'optimisation des processus et de création de valeur pour le client. C'est pourquoi les progiciels de gestion intégrée sont devenus quasiment incontournables.

1.1.3.1 Enterprise Resource Planning (ERP)

ERP est un logiciel qui permet à l'entreprise de gérer ses ressources en interne. De la définition de certains auteurs comme Lumbroso (2007: 10) et Fernandez (2001:57), il ressort que « l'ERP est un progiciel multifonction centralisant les données et qui comporte plusieurs modules correspondant chacun à une fonction de l'entreprise. L'ERP est orienté processus et est transversale. Il assure l'interdépendance entre les processus. A partir de la base de données centralisée, les modules fonctionnels communiquent et échangent ». En effet, un processus entre les produits informationnels du processus qui le précède pour fournir à son tour de l'information au processus suivant. Pour Morley (2008 :46), il s'agit de « construire, en tirant le meilleur parti du progiciel, un système améliorant la performance de l'entreprise ».

Pillet et al (2011 :295) affirment que pour le Conseil sur les Systèmes d'Information, organisme français, « l'ERP permet de garantir l'unicité des informations et procure à l'entreprise des gains de productivités. Il garantit également la traçabilité de l'information et permet de réduire les coûts (réduction du personnel), supprime les tâches redondantes, réduit les erreurs et incohérences (pas de risque de double saisie des mêmes informations dans des systèmes d'information différents) et réduit les temps de traitement ». Pour assurer la circulation des informations entre les services, l'ERP offre des outils comme les groupware et

workflow qui permettent également d'identifier les intervenants concernés, les actions à réaliser et les délais.

1.1.3.2 Customer Relationship Management (CRM)

Tomas (2002: 40) présente le CRM comme « un progiciel qui permet de traiter directement avec le client, que ce soit au niveau de la vente, du marketing ou du service, et que l'on regroupe souvent sous le terme de "front-office" ». C'est un outil qui permet d'identifier et d'analyser les besoins des clients afin de les conquérir, les satisfaire et les fidéliser en proposant de meilleurs services. Avec le progiciel CRM ou Gestion de la Relation Client (GRC) les entreprises peuvent élaborer une base de données de la connaissance client qui leur permet d'identifier les clients, de faire un classement par rapport au degré de fidélité du client, de personnaliser sa relation avec le client. L'utilisation du progiciel CRM permet à une entreprise d'être compétitive dans la mesure où il lui permet d'être à l'écoute du marché et donc d'être réactive pour répondre aux besoins de la clientèle, de renforcer la communication avec la clientèle à travers internet et les sites web.

Le système d'information est désormais essentiel pour la vie des entreprises particulièrement pour les banques qui sont une industrie d'information et où le système d'information constitue un axe stratégique et une compétence clé. Il est donc nécessaire que les acteurs du système d'information mettent en place un ensemble de techniques pour assurer le pilotage de cette fonction. Autrement dit, il s'agit d'assurer la gouvernance des systèmes d'information.

1.2 La gouvernance des systèmes d'information

Le système d'information, levier de création de valeur, est un facteur de production que toute entreprise doit optimiser afin de maximiser ses gains. Il est donc nécessaire de piloter ce système afin de maîtriser les coûts, de veiller à sa sécurité et à la fiabilité des informations. Le pilotage du SI assure également qu'il contribue à la réalisation des objectifs de l'entreprise. La DSI et les DM, en collaboration avec la direction générale, doivent assurer la gouvernance du système d'information.

Une bonne GSI est basée sur la mise en place d'une structure organisationnelle et des processus SI nécessaires, la disponibilité des ressources informatiques et sur la définition des rôles et responsabilités des acteurs. La GSI doit permettre d'assurer la cohérence entre les objectifs et stratégies SI et ceux de l'entreprise et de respecter les critères de l'information tout en maîtrisant les risques.

Cette section présentera deux paragraphes : le premier présentera les référentiels et bonnes pratiques de la gouvernance des systèmes d'information et le deuxième paragraphe traitera des axes stratégiques ou principes de la gouvernance des systèmes d'information.

1.2.1 Les référentiels et bonnes pratiques de la gouvernance des systèmes d'information

De nombreux auteurs ont défini la gouvernance des systèmes d'information. L'Institut de la Gouvernance des Systèmes d'Information (IGSI) (2005 :8), Delmond et al (2008 :135) et Moisand et al (2009 :1) font ressortir que « la gouvernance des systèmes d'information est la mise en œuvre d'un ensemble de bonnes pratiques qui concourent au pilotage efficace à long, moyen et court terme des systèmes d'information ». Elle se fonde sur plusieurs référentiels mais les principaux sont Control Objectives for Information and Related Technology (COBIT) et Information Technology Infrastructure Library (ITIL).

1.2.1.1 Les référentiels COBIT et ITIL

Les référentiels ITIL et COBIT énoncent des bonnes pratiques qui permettent aux acteurs d'assurer une bonne GSI.

1.2.1.1.1 Information Technology Infrastructure Library (ITIL)

ITIL est un référentiel de bonnes pratiques permettant de gérer le système d'information. Il améliore les relations de client fournisseurs entre la DSI et les DM. ITIL comprend deux versions : ITIL V2 et ITIL V3. ITIL V2 présente les bonnes pratiques et l'alignement de l'informatique aux métiers et ITIL V3 qui est la version actualisée d'ITIL V2 pour tenir compte de la gestion des cycles de vie des processus. Cependant, ITIL V2 est le plus utilisé par les entreprises. Les bonnes pratiques énumérées par le référentiel ITIL permettent à la DSI

de fournir aux utilisateurs des prestations informatiques de bonne qualité en adéquation avec les besoins des utilisateurs. Cependant, des services de bonne qualité n'impliquent pas pour autant une non maîtrise des coûts. Selon Dumont (2007 :10) « ITIL est basé sur des principes tels que l'orientation client, l'industrialisation des services, l'optimisation des ressources »

Les bonnes pratiques qui permettent à la DSI d'assurer le soutien des services sont :

- l'existence d'un centre de service ou service desk qui permet aux utilisateurs d'avoir accès à la DSI afin de solliciter des demandes et/ou formuler des réclamations à l'endroit de la DSI. C'est un centre qui apporte non seulement de l'assistance aux utilisateurs et intervient dans la résolution des incidents mais qui sert aussi d'interface entre les utilisateurs et le service informatique. Il constitue un point de contact unique permettant ainsi aux utilisateurs de bénéficier d'une assistance dans de brefs délais. L'absence de ce service peut donc entraîner une perte de temps et un problème de qualité dans la résolution des incidents ;
- la gestion des incidents. Il s'agit pour la DSI de restaurer rapidement le service suite aux incidents annoncés par les utilisateurs. Pour restaurer rapidement, il lui est nécessaire d'hiérarchiser les incidents en fonction de leur importance qui dépend de l'impact sur les processus et de la durée de l'incident. Il s'agit de gérer les incidents de façon prioritaire afin d'assurer un bon suivi de ceux-ci. Lorsqu'un incident ne peut être géré à un niveau donné, il est transféré au niveau supérieur capable de résoudre cet incident. Comme exemple d'incidents, nous avons les pannes de matériels, les dysfonctionnements des applications, le ralentissement du réseau ;
- la gestion des problèmes consiste à rechercher les causes des incidents signalés par les utilisateurs et apporter des actions correctives afin de les éviter dans l'avenir. La gestion des problèmes vise à améliorer la structure du service informatique ;
- la gestion des configurations concerne la gestion des infrastructures (postes de travail, logiciels, matériels...) du système d'information qui sont utilisées dans l'exécution des services. La gestion des configurations requiert l'utilisation d'une base de données qui permet d'identifier l'ensemble des infrastructures ainsi que des composants comme la date d'achat, le fournisseur...cette base de données doit être hautement sécurisée ;

- la gestion des changements s'intéresse aux changements qu'il faut effectuer suite aux évolutions de l'environnement interne (incidents, problèmes) et aux évolutions externes comme celles des TI, celles du marché... il s'agit d'adapter le système d'information aux évolutions de nos environnements afin d'assurer sa continuité ;
- la gestion de la mise en production intervient à la suite de changements effectués. Il s'agit d'assurer la planification, la conception et la production des changements autorisés.

Ces bonnes pratiques peuvent faire l'objet d'une corrélation. En effet, quand un incident survient, le premier responsable est le centre de service. Il détermine l'importance (impact et urgence) de cet incident afin de le hiérarchiser, le transfère au niveau supérieur si toutefois le premier niveau concerné n'arrive pas à le résoudre. Une fois résolu, l'incident peut encore se reproduire et pour éviter cela, le centre de service informe les responsables de la gestion des problèmes pour qu'ils identifient les causes et envisager des solutions. La solution retenue peut modifier l'architecture du système d'information et faire l'objet de changements qui, à son tour va générer une mise en production.

La DSI doit assurer la sécurité du système d'information qui consiste à mettre en place un ensemble de dispositifs (techniques, organisationnels...) ou de mesures afin de minimiser ou d'éviter les risques liés au système d'information. Assurer la gestion de la sécurité du SI repose sur :

- le respect des critères de sécurité évoqués au niveau de la qualité du système d'information dans le chapitre 1 ;
- la mise en place des mesures de sécurité à savoir la sécurité physique des ressources (protection des locaux informatiques, des matériels de traitement, des réseaux, des fichiers de stockage), la sécurité logique (protection des données et programmes) et la sécurité des applications. La sécurité physique concerne la mise en place d'un système de protection contre les incendies, les fuites d'eau et les inondations. C'est aussi l'utilisation des badges pour limiter l'accès aux locaux informatiques. Il s'agit aussi de prévoir un système de récupération des fichiers en cas de panne et de décentraliser le matériel sur des sites différents. Quant à la sécurité logique, elle concerne l'utilisation d'un identifiant et d'un mot de passe propres à chaque

utilisateur. Cette mesure permet de contrôler l'accès à l'information et d'assurer la confidentialité du système d'information.

Toutes ces bonnes pratiques relatives à la gestion des services permettent à la DSI, en particulier le centre de service, de fournir aux utilisateurs un service de qualité et d'assurer la fiabilité du système d'information.

En plus du référentiel ITIL, nous avons le référentiel COBIT qui permet d'assurer le contrôle et l'évaluation de la performance des systèmes d'information.

1.2.1.1.2 Le référentiel COBIT

Le COBIT, développé par Information Systems Audit and Control Association (ISACA) a pour objectif d'assurer l'alignement stratégique, l'efficacité et l'efficience des processus, l'utilisation optimale des ressources et d'assurer la maîtrise des risques, la sécurité et le contrôle du système d'information. Le COBIT a une vocation pratique pour la DSI : c'est un guide qui permet d'implémenter et de gérer le SI. Il permet aussi à la direction générale de mettre en place l'organisation, les processus, de définir les rôles et les responsabilités pour s'assurer que les stratégies et objectifs SI sont alignés à ceux de l'entreprise.

COBIT sert de référentiel d'audit du SI. Il permet aux auditeurs d'évaluer la performance et la conformité aux politiques, aux normes et aux procédures. Il permet aussi aux auditeurs non informaticiens d'effectuer avec professionnalisme des missions d'audit du SI.

1.2.1.1.2.1 l'architecture du COBIT

L'architecture de COBIT présente quatre (4) domaines, des ressources technologiques à mettre en œuvre et des exigences en information pour atteindre les objectifs business et ceux de la gouvernance (voir annexe1 page 87). Chaque domaine est réparti en un certain nombre de processus qui présentent des objectifs de contrôle détaillés (318), les responsabilités des acteurs, et des indicateurs de performance. Moisand et al (2009 : 5) affirme que selon le COBIT « la gouvernance du système d'information est constituée de structures et de processus de commandement et de fonctionnement qui conduisent l'informatique de l'entreprise à soutenir les objectifs et les stratégies de l'entreprise, et à lui permettre de les élargir ».

Les quatre domaines sont : Planifier et Organiser (PO), Acquérir et Implémenter (AI), Délivrer et Supporter (DS) puis Surveiller et Evaluer (SE).

- Planifier et Organiser (PO). Le DSI doit élaborer des stratégies à long et moyen terme cohérentes avec celles de l'entreprise et qui permettent de prévoir les ressources afin de répondre aux critères qualité du système d'information. Comme processus, ce domaine en regroupe 10 ;
- Acquérir et Implémenter (AI). Les processus de ce domaine concernent l'identification des solutions informatiques, l'acquisition des applications et infrastructures technologiques, la gestion des changements et les modifications. Ils sont au nombre de 7 et doivent être intégrés aux processus métiers ;
- Délivrer et Supporter (DS). Il comprend 13 processus qui décrivent la gestion du service informatique et le soutien aux utilisateurs et clients. Autrement dit, il concerne l'exploitation, la sécurité, la formation, les plans d'urgence ;
- Surveiller et Evaluer (SE). Il présente 4 processus qui traitent du contrôle et de l'évaluation de la performance, de l'évaluation du contrôle interne, du respect de la conformité réglementaire et de la mise en œuvre de la GSI.

Quant aux ressources technologiques, il s'agit :

- des applications ;
- des données ;
- des infrastructures qui regroupent les installations et la technologie nécessaire pour traiter les données ;
- du personnel nécessaire pour planifier et organiser les ressources, acquérir et implémenter les applications et infrastructures, pour fournir les services et pour contrôler et évaluer le SI.

Pour répondre aux objectifs de l'entreprise, l'information doit respecter 7 critères qui sont :

- l'efficacité ;
- l'efficience ;
- la confidentialité ;
- l'intégrité ;
- la disponibilité ;

- la conformité ;
- la fiabilité.

L'un des axes stratégiques de la GSI étant la mesure de la performance du système d'information, COBIT présente un tableau de bord prospectif appelé IT Scorecard permettant de mesurer cette performance.

Comme la Balance Scorecard, il se décline en quatre perspectives. Selon Autissier et al (2007 :221), chaque perspective a ses propres objectifs avec ses indicateurs qui s'inscrivent dans des schémas de causalité. En effet, il s'agit de déterminer pour chaque perspective, les objectifs prioritaires qui permettront de créer de la valeur, les indicateurs qui permettent de s'assurer que les objectifs sont atteints et d'établir une relation entre les objectifs des différentes perspectives. Assurer la formation des directions métiers en système d'information permettra de maîtriser les processus et donc de réduire les pertes de temps, de mieux satisfaire les clients et de créer de la valeur.

- Perspective financière : de nombreux auteurs comme Berland et al (2010 :110), Autissier et al (2007 :222) affirment que cette perspective « a pour objectif de déterminer les attentes des actionnaires et se traduit par des indicateurs de rentabilité, de marge, de chiffre d'affaire et d'utilisation des actifs ». En matière de système d'information, ce sont les indicateurs mesurant la maîtrise des coûts et le respect du budget, la création de valeur pour les métiers et la maîtrise du risque. Pour mesurer les budgets informatiques, Bohnké (2010 : 77) présente le Total Cost of Ownership ou coût total de possession (TCO) comme étant « un modèle de justification des investissements en IT et d'optimisation des coûts ». le TCO comprend les coûts d'acquisition de biens en TI (acquisition de logiciels, d'ordinateurs, d'infrastructures et réseaux), les coûts cachés comme la maintenance, la formation des utilisateurs et, les coûts d'électricité liés au fonctionnement des machines.
- Perspective client : cette perspective vise, qu'il s'agisse de la stratégie générale de l'entreprise ou de la stratégie du système d'information, à identifier les attentes des clients (clients internes et externes) pour les satisfaire. Il s'agit pour les clients d'évaluer la qualité du service fourni par la DSI afin que celle-ci puisse répondre à

leurs attentes. Les indicateurs sont ceux de la satisfaction client, la flexibilité du SI, la GRC, l'équilibre des prestations par rapport à l'ensemble des métiers.

- Perspective processus vise à identifier et améliorer les processus clés afin de répondre aux attentes des actionnaires et des clients. Cette perspective permet d'assurer la performance opérationnelle. Elle se décline en deux types d'objectifs : la capacité d'innovation et la capacité de production.
- Perspective d'apprentissage relative à l'existence des compétences humaines et méthodologiques et à la pérennité des infrastructures et technologies.

1.2.1.1.2.2 Audit et COBIT

En générale, la conduite d'une mission se déroule en trois phases qui sont : la phase de pré-audit ou de préparation de la mission, la phase d'investigations ou de réalisation de la mission et la phase de formalisation.

Moisand et al (2009:198 ; 199) affirment que selon le COBIT qui est un référentiel d'audit « la phase de pré-audit consiste à :

- établir la lettre de mission ;
- définir le périmètre de l'audit des SI ;
- choisir un cadre de référence de contrôle des SI ou élaborer un référentiel d'audit ;
- dépister les risques ;
- définir le champ d'action et les objectifs détaillés ;
- préparer les dossiers et documents de travail.

Pendant les investigations qui consistent à évaluer le contrôle interne des SI et identifier les risques, il s'agit d'évaluer :

- les domaines, les processus en fonction du périmètre de l'audit. Chaque processus, définis par le COBIT, indique des objectifs de contrôle et des points de contrôle ;
- les ressources technologiques (applications, données, infrastructures, personnes) ;
- les critères de l'information (efficacité, efficience, confidentialité, intégrité, disponibilité, conformité et fiabilité) ».

ITIL et COBIT sont certes, des référentiels qui permettent d'améliorer la gestion du système d'information mais leur mise en œuvre doit être adaptée à la réalité de l'entreprise.

1.2.1.2 Les outils de la mise en œuvre des bonnes pratiques

L'Institut de la Gouvernance de Système d'Information (IGSI) fondé par l'Association Française de l'Audit et du Conseil Informatique (AFAI) et le Club Informatique des Grandes Entreprises Françaises (CIGRIEF) ont identifié 11 vecteurs qui sont des outils permettant l'application des bonnes pratiques en matière de gouvernance des systèmes. Ces 11 vecteurs sont schématisés par une figure présentée en annexe 2 à la page 88.

1.2.2 Les axes stratégiques de la gouvernance des systèmes d'information

Selon le référentiel COBIT, la GSI comprend cinq axes stratégiques qui sont : l'alignement stratégique, la création de valeur, la gestion des ressources, la gestion des risques et la mesure de la performance. Ces axes stratégiques sont des principes de la GSI.

1.2.2.1 L'alignement stratégique

L'alignement stratégique consiste à aligner la stratégie des systèmes d'information à la stratégie de l'entreprise. Comme l'affirme Reix (2004:280) « les TI ne sont plus vues simplement comme une ressource de support mais comme une ressource stratégique capable de conférer, à l'entreprise qui saura les utiliser un avantage concurrentiel véritable ». Partant de là, il est donc fondamental d'adapter la stratégie des systèmes d'information à la stratégie de l'entreprise.

Le DSI doit utiliser ses compétences et connaissances des TI pour en faire un levier de transformation de l'entreprise. Il doit faire comprendre aux DM les potentialités du système d'information. En plus du rôle technique, le DSI doit participer en tant qu'acteur au développement du business et gérer le dialogue avec les DM et la direction générale. Il est donc nécessaire qu'il développe une proximité avec les DM pour connaître les activités de l'entreprise et tenir compte de leurs besoins. Le DSI doit également connaître le marché de l'entreprise et identifier les évolutions qui vont générer des changements dans le système

d'information. Pour aligner la stratégie du système d'information à celle de l'entreprise, le DSI doit être proactif.

Des auteurs comme Reix (2004 :297) et Delmond et al (2008:137) ont proposé dans leur ouvrage « le modèle de l'alignement stratégique selon Henderson et Venkatraman qui permet d'identifier quatre modes d'alignement. C'est un modèle construit à partir de deux axes représentant l'intégration stratégique qui relie les éléments internes et externes de l'entreprise et l'intégration fonctionnelle qui met en cohérence les domaines fonctionnels et les besoins en TI. Chaque type d'alignement indique le principal moteur (celui qui pilote le changement), le pivot (celui qui fait l'objet du changement) et le domaine d'impact » (voir annexe 3 page 89).

L'importance en alignement stratégique c'est la mise en œuvre de la stratégie choisie et la concentration des efforts sur les processus clés selon la stratégie choisie. Sur cette base, pour assurer la performance, l'entreprise quelque soit son mode d'alignement doit bien mettre en œuvre sa stratégie sur des processus clés.

Fimbel (2007 : 16) affirme que selon la communauté scientifique et professionnelle « le modèle d'alignement stratégique de Hendersen et Venkatraman présente des limites car pour les scientifiques il n'intègre ni le temps, ni l'histoire de manière explicite et pour les professionnels, il ignore trois aspects caractérisant les pratiques de l'alignement du système d'information :

- les alignements peuvent se réaliser au travers d'action sur les existants et/ou sur les projets ;
- les volontés et intentions d'alignement du SI ne produiront leurs effets que dans la pertinence et l'intensité des pratiques cohérentes qu'en feront les usages ;
- les différents niveaux de management s'efforceront de limiter le coût et le délai de l'opération de réalignement ».

1.2.2.2 La création de valeur

Le système d'information déployé doit permettre de créer de la valeur pour l'entreprise. Un système d'information en adéquation avec la stratégie de l'entreprise et qui répond aux critères d'accessibilité, de sécurité, d'efficacité et/ou d'efficience permettra d'obtenir une valeur ajoutée dans l'organisation des processus métier. Selon Moisand et al (2009 :8), « l'apport de valeur se concrétise par la maîtrise des processus de fonctionnement en termes d'efficacité et d'efficience ». Bounfour et al (2006 :64) ajoutent que « la création de valeur s'appuie sur des processus maîtrisés de conception, de production, de conduite de projet et sur des processus d'innovation et la mobilisation des parties prenantes ».

Comme précédemment indiqué, le système d'information grâce aux TI est devenu un outil de compétitivité et une bonne exploitation de ce système permet d'obtenir un retour sur investissement et donc de le transformer en centre de profit.

Cependant, il est nécessaire de mesurer ce retour sur investissement pour voir si la valeur créée couvre le coût des investissements en TI car il ne suffit pas d'investir pour développer la compétitivité.

1.2.2.3 La gestion des ressources

Le système d'information comprend plusieurs composantes telles que les ressources humaines et matérielles. Les ressources humaines sont composées des directions métiers (utilisateurs) et de la direction des systèmes d'information (informaticiens). La direction des systèmes d'information doit, recueillir les besoins définis par les utilisateurs pour mettre en place la stratégie du système d'information et définir les infrastructures et processus informatiques nécessaires pour assurer la cohérence avec la stratégie de l'entreprise.

Moisand et al (2009: 8) soulignent que « les ressources pour mesurer l'activité informatique doivent être optimales pour répondre aux exigences des métiers ». En effet, la direction des systèmes d'information doit avoir des informaticiens suffisants en termes de volume, de compétences. Elle doit aussi mener une veille technologique pour assurer à ses informaticiens des formations correspondant aux besoins du moment. Pour Bounfour et al (2006 :61) « la

DSI doit évaluer de façon permanente les performances des compétences de ses collaborateurs par rapport non seulement aux évolutions technologiques mais aussi par rapport aux compétences requises pour dialoguer avec les directions métiers ».

Quant aux ressources matérielles (support et matériel technologique) et aux logiciels et programmes, la DSI doit tenir un plan d'infrastructure qui va lui permettre de suivre les acquisitions, les développements, les changements et la maintenance de ce capital. Ce plan d'infrastructure doit également tenir compte des moyens alloués.

1.2.2.4 La gestion des risques

Un arrêt ou un dysfonctionnement du système d'information peut paralyser le déroulement des activités et dans les entreprises où les processus clés dépendent du système d'information, le dysfonctionnement génère une cessation de l'activité et donc des pertes considérables pour l'entreprise. C'est le cas par exemple des banques, de la bourse, des compagnies aériennes... dont l'activité dépend du système informatique. Ces entreprises doivent tenir compte des risques informatiques et mettre en place un système de prévention, de détection et de traitement du risque. Il s'agit d'assurer la sécurité des locaux et la sécurité logique (sécurité des données) surtout avec l'ouverture de l'entreprise à l'extérieur (échanges avec fournisseurs, clients).

1.2.2.5 La mesure de la performance

Il s'agit d'évaluer et de suivre le niveau de satisfaction des clients internes et externes, les compétences de la DSI, l'efficacité organisationnelle. Les investissements en TI représentent certes des coûts importants mais lorsqu'ils sont maîtrisés et répondent aux besoins de l'entreprise ils lui permettent d'automatiser ses tâches et réduire le temps de travail, de coordonner ses processus, de se rapprocher des fournisseurs et de la clientèle, d'innover... Tous ces facteurs procurent des avantages concurrentiels et améliorent la part de marché relative. Ils contribuent également à l'amélioration de la performance et plusieurs outils tels que le tableau de bord (Balance Scorecard) adapté aux systèmes d'information permettent l'évaluation de la performance.

1.2.3 Gouvernance et gestion des risques

La gestion des risques, comme précédemment mentionnée, est un axe stratégique de la GSI. La GSI relevant de la responsabilité des dirigeants, ces derniers doivent définir clairement l'appétence de l'entreprise pour le risque informatique. Ils doivent communiquer l'appétence pour le risque informatique et mettre en place un plan de gestion qui fait ressortir les rôles et responsabilités des différents acteurs de la gestion des risques.

Les acteurs de la gouvernance doivent également mettre en place des dispositifs de prévention, de détection et de traitement du risque informatique. Une bonne gestion des risques informatiques contribue à la création de valeur ajoutée.

La gouvernance des systèmes d'information est un processus qui, une fois bien mis en œuvre, permet à l'entreprise de faire des progrès importants car elle contribue à la performance globale de l'entreprise. Les solutions d'une bonne GSI reposent sur :

- l'alignement stratégique ;
- l'optimisation des coûts et des ressources informatiques (applications, infrastructures, données, personnes et technologies) ;
- l'évaluation périodique indépendante de la performance et de la conformité aux normes, aux politiques et aux procédures.

Après avoir présenté le système d'information ainsi que les bases de la gouvernance de ce système, il est à présent question de prendre connaissance du rôle de l'audit interne dans la GSI car cette fonction est, comme l'affirme Barbier (1999 :45) « reconnu aujourd'hui comme un bien indispensable ».

CHAPITRE 2 : LE ROLE DE L'AUDIT INTERNE DANS LA GOUVERNANCE DES SYSTEMES D'INFORMATION

La gouvernance des systèmes d'information permettant de créer de la valeur et d'améliorer le fonctionnement des entreprises nécessite de la transparence et une mise en place d'un système de management cohérent avec les stratégies définies par l'entreprise. L'implication des autorités de contrôle telles que l'audit interne peut permettre d'assurer une bonne gouvernance.

Selon l'Institut Français de l'Audit et du Contrôle Interne (IFACI) (2011 :16), les normes internationales pour la pratique professionnelle de l'audit interne de l'Institute of Internal Auditors (IIA) exigent à travers la norme 2110.A2 que l'audit interne évalue si la gouvernance des systèmes d'information de l'organisation soutient la stratégie et les objectifs de l'organisation. Quelle relation peut donc exister entre l'audit interne et les acteurs de la GSI? Nous tenterons de répondre à cette question à travers ce chapitre qui comprendra deux sections : la première section consacrée à l'audit interne permettra de prendre connaissance du cadre de référence et des missions et objectifs de cette fonction et la deuxième section présentera les différents rôles que peut jouer l'audit interne dans la GSI.

2.1 L'audit interne

Avec la complexité des opérations et la délégation des pouvoirs, l'Audit Interne (AI), qui est une activité normée, occupe aujourd'hui une place importante au sein des entreprises car elle offre à la direction générale et aux différentes directions une assurance raisonnable quant à la maîtrise de leurs activités. La fonction d'audit interne est basée sur un cadre de référence et a, comme toutes les autres fonctions, des missions et objectifs à atteindre.

2.1.1 Le cadre de référence de l'audit interne

Dans un souci d'harmoniser la pratique de l'audit interne exercée dans des milieux divergents, les professionnels ont défini un cadre de référence pour la pratique de cette fonction.

L'audit interne est défini de plusieurs manières mais la définition officielle est celle de l'IIA. Selon l'IIA « 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 des 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 ».

Le cadre de référence est constitué d'un code de déontologie et des normes pour la pratique professionnelle qui sont des exigences auxquelles les auditeurs internes doivent se conformer dans l'exercice de leur métier.

2.1.1.1 Le code de déontologie

Le code de déontologie présente aux auditeurs un ensemble de principes fondamentaux et de valeurs à respecter dans l'exercice de la profession.

Selon l'IFACI (2009 :1) « le code de déontologie a pour but de promouvoir une culture de l'éthique au sein de la profession d'audit interne. Compte tenu de la confiance placée en l'audit interne pour donner une assurance objective sur les processus de management des risques, de contrôle et de gouvernement d'entreprise, il était nécessaire que la profession se dote d'un tel code.»

Ces principes fondamentaux et valeurs sont :

- l'intégrité ;

Les auditeurs internes doivent être intègres dans l'accomplissement de leurs missions car, comme l'affirme Peretti (2010 :104) , l'intégrité est « la base de la confiance accordée aux auditeurs ». Pour cela :

- ✓ ils doivent accomplir leurs missions avec honnêteté, diligence et responsabilité ;
- ✓ ils doivent respecter la loi et faire les révélations requises par les lois et les règles de la profession ;

- ✓ ils ne doivent pas sciemment prendre part à des activités illégales ou s'engager dans des actes déshonorants pour la profession d'audit interne ou leur organisation.

- l'objectivité ;

Selon Shick (2007 :9) « l'objectivité permet d'évaluer équitablement tous les éléments pertinents examinés relatifs au domaine audité et de ne pas se laisser influencer dans son jugement ». Les auditeurs internes :

- ✓ ne doivent pas prendre part à des activités ou établir des relations qui pourraient compromettre ou risquer de compromettre le caractère impartial de leur jugement. Ce principe vaut également pour les activités ou relations d'affaires qui pourraient entrer en conflit avec les intérêts de leur organisation ;
- ✓ ne doivent rien accepter qui pourrait compromettre ou risquer de compromettre leur jugement professionnel ;
- ✓ doivent révéler tous les faits matériels dont ils ont connaissance et qui, s'ils n'étaient pas révélés, auraient pour conséquence de fausser le rapport sur les activités examinées ;

- la confidentialité ;

Elle concerne la protection des informations reçues et leurs divulgations. Les auditeurs internes :

- ✓ doivent utiliser avec prudence et protéger les informations recueillies dans le cadre de leurs activités ;
- ✓ ne doivent pas utiliser ces informations pour en tirer un bénéfice personnel, ou d'une manière qui contreviendrait aux dispositions légales ou porterait préjudice aux objectifs éthiques et légitimes de leur organisation ;

- la compétence ;

Les auditeurs internes doivent posséder les connaissances et l'expérience requise pour la réalisation de travaux d'audit. Les auditeurs internes :

- ✓ ne doivent s'engager que dans des travaux pour lesquels ils ont les connaissances, le savoir-faire et l'expérience nécessaires ;

- ✓ doivent réaliser leurs travaux d'audit dans le respect des normes pour la pratique professionnelle de l'audit interne ;
- ✓ doivent toujours s'efforcer d'améliorer leur compétence, l'efficacité et la qualité de leurs travaux.

Selon l'IFACI (2009 :1) « le champ d'application du code de déontologie concerne les personnes et entités qui fournissent des services d'audit ». Ces personnes et entités doivent respecter un ensemble de normes internationales élaborées par L'IIA.

2.1.1.2 Les normes de l'audit interne

Selon l'IIA, les normes internationales pour la pratique professionnelle de l'audit interne ont pour objet de :

- définir les principes fondamentaux de la pratique de l'audit interne ;
- fournir un cadre de référence pour la réalisation et la promotion d'audit interne à valeur ajoutée ;
- établir les critères d'appréciation du fonctionnement de l'audit interne ;
- favoriser l'amélioration des processus organisationnels et des opérations.

Les normes sont composées :

- des normes de qualification représentées par les normes de la série 1000 à 1322 qui font référence à la mission, aux pouvoirs et responsabilités et aux principes d'indépendance et d'objectivité ;
- des normes de fonctionnement référencées par la série des normes 2000 à 2600 qui décrivent l'exercice de l'activité et qui présentent les critères d'évaluation de la performance de l'audit interne.

Les normes présentent également une autre série de normes appelées normes de mise en œuvre qui explicitent les exigences pour les activités d'assurances et de conseils.

Comme l'affirment Lejeune et al (2007: 28), « les normes sont destinées à permettre aux professionnelles d'apprécier concrètement la nature et l'étendue des diligences qu'ils doivent mettre en œuvre dans une situation donnée ».

Après avoir pris connaissance des normes, nous présenterons les missions et objectifs assignés à l'audit interne.

2.1.2 Missions et objectifs de l'audit interne

L'audit interne est une fonction normée qui doit être indépendante et objective dans l'exercice de ses missions. Pour assurer son indépendance, il doit être rattaché au niveau hiérarchique le plus élevé.

2.1.2.1 les missions de l'audit interne

L'audit interne doit effectuer des missions d'assurance et de conseils. Selon l'IFACI (2011 :16), la norme de fonctionnement 2100 de l'IIA stipule que « l'audit interne doit évaluer les processus de gouvernement d'entreprise, de management des risques et de contrôle, et contribuer à leur amélioration sur la base d'une approche systématique et méthodique ». En effet l'AI identifie les points forts et les points faibles pour formuler des recommandations d'amélioration. C'est un outil de contrôle et d'amélioration continue. C'est pourquoi Schick (2007: 5) affirme que « l'audit interne aide à anticiper les problèmes et se place dans une démarche vertueuse d'amélioration continue ». Par ses recommandations, il oriente la prise de décisions de la direction. Il assure aussi le suivi de la mise en œuvre des recommandations qui lui permettra ainsi de contribuer à la création de valeur ajoutée.

Selon Tonye (2011: 28) « l'audit interne est un maillon essentiel du système de gestion des établissements de crédit et sa mission est de s'assurer de la régularité, de la conformité des opérations et de l'efficacité des dispositifs de contrôle interne, et spécifiquement de leur adéquation à la nature de l'ensemble des risques inhérents aux opérations selon une période bien définie ».

L'audit interne a des objectifs qui doivent être définis dans la charte d'audit.

2.1.2.2 Les objectifs de l'audit interne

Pour Bertin (2007: 21) « la mission générale de l'audit interne consiste à vérifier si les objectifs de contrôle interne sont atteints ». Mandzila (2005: 229) abonde dans le même sens

en affirmant que « pour l'audit interne, l'évaluation du contrôle interne est l'objectif essentiel de la mission ». En effet, défini par un certain nombre de référentiels comme le Committee of Sponsoring Organizations of the Treadway Commission (COSO), le Criteria of Control Committee (COCO), le TURNBULL, le contrôle interne présente trois objectifs qui sont :

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

Selon Tsapi (2009 :118) « le COSO définit le contrôle interne comme un processus mis en œuvre par le conseil d'administration, les dirigeants et le personnel d'une organisation, destiné à fournir une assurance raisonnable quant à la réalisation d'objectifs entrant dans la réalisation et l'optimisation des opérations, la fiabilité des informations financières et la conformité aux lois et aux réglementations en vigueur ».

Pour s'assurer que ces objectifs sont atteints, l'audit interne doit donc vérifier la qualité de l'information, évaluer les processus internes et vérifier l'application des instructions, lois et règlements. Le contrôle interne est donc une finalité pour l'audit interne.

Cependant, Angot et al (2004 :123) avancent que « si le système de contrôle interne a été conçu pour répondre aux différents objectifs, il ne donne pas la certitude que les objectifs fixés sont atteints et ce, en raison des limites inhérentes au fonctionnement de toute procédure ».

L'évaluation des processus internes permet à l'auditeur interne de vérifier si les principes du contrôle interne (organisation, intégration, permanence, universalité, indépendance, information, harmonie, prévision et qualité du personnel) sont respectés et d'identifier les risques qui peuvent compromettre l'atteinte des objectifs de l'entreprise.

Avec le progrès rapide des TI, les processus opérationnels sont pour la plupart automatisés d'où la nécessité d'évaluer les dispositifs de contrôle interne des systèmes d'information mis en place surtout en milieu bancaire où l'activité en dépend. L'audit des systèmes d'information est donc un volet important pour l'auditeur interne.

Pour l'AFAI (2008 :6) « le cœur de la démarche de contrôle interne des systèmes d'information est d'assurer un suivi des flux des données d'un processus à un autre, de mettre en place un mécanisme de contrôle d'étape en étape et d'assurer un contrôle des bases de données ».

L'audit interne permet d'exercer un contrôle sur les fonctions de l'entreprise et est perçu d'après Mandzila (2005 :232) « comme un médecin, un sauveur de l'entreprise » mais il doit également faire l'objet d'une évaluation afin d'éviter les dysfonctionnements au sein de cette fonction.

Le chapitre précédent sur la GSI nous a permis d'appréhender les principes de cette gouvernance ainsi que les bonnes pratiques énoncées par les référentiels de la GSI. Parmi ces principes qui sont tous importants, la GSI est surtout basée sur l'alignement stratégique, la gestion des risques et l'évaluation de la performance du SI.

Quelles relations peuvent-ils donc exister entre ces composantes de la GSI et l'audit interne ?

2.2 L'audit interne dans le pilotage stratégique du SI

Le système d'information étant un outil permettant de créer une valeur ajoutée doit être bien piloté afin d'assurer à l'entreprise un avantage concurrentiel. Pour cela, les acteurs de la gouvernance du système d'information doivent s'assurer de la bonne adéquation entre les stratégies du système d'information et celle de l'entreprise à travers l'alignement stratégique. Ils doivent aussi planifier l'évolution du système d'information pour anticiper les changements de l'environnement et garantir sa pérennité.

L'audit interne peut intervenir dans le pilotage stratégique en évaluant la cohérence entre les stratégies du système d'information et la stratégie globale de l'entreprise. Il peut également effectuer un audit stratégique afin d'informer les dirigeants des éventuels dysfonctionnements et risques, et améliorer les prises de décisions du système d'information.

2.2.1 L'analyse de l'alignement stratégique

Les éléments qui entrent dans l'alignement stratégique sont la stratégie en matière de système d'information définie par la DSI, la stratégie définie par la direction générale, les processus internes et l'infrastructure technologique. Pour assurer cet alignement, les différents acteurs doivent collaborer et l'auditeur interne peut intervenir pour assurer l'efficacité de cet alignement.

Le rôle de l'auditeur interne consiste :

- à vérifier d'abord l'existence de stratégie en matière de système d'information ;
- à procéder à l'analyse de cette stratégie si elle est définie afin de s'assurer qu'elle soutient la stratégie globale et que les informations produites permettent de répondre aux besoins des utilisateurs. Pour cela, l'auditeur interne :
 - ✓ analyse les besoins exprimés par les directions métiers afin de s'assurer qu'ils ont été clairement définis par ces derniers et pris en compte par la DSI dans la formulation de leurs objectifs ;
 - ✓ une fois rassuré que les besoins ont été correctement exprimés et pris en compte, il procède à une évaluation des ressources humaines et technologiques, des processus du SI et logiciels déployés pour atteindre les objectifs des SI ;
 - ✓ et analyse la stratégie globale de l'entreprise pour vérifier que les dirigeants ont tenu compte de la stratégie des SI dans la formulation de la stratégie globale.

Si ces différents points de contrôle présentent des défaillances, l'auditeur informe les acteurs de la GSI et définit les responsabilités qui incombent à chacun pour parvenir à l'alignement stratégique.

Selon Bertin (2007 : 295), « l'auditeur ne doit pas seulement évaluer la cohérence des décisions stratégiques de l'entreprise, mais également recenser les modes de décisions et les jeux d'acteurs ayant permis la mise en œuvre de la stratégie ».

Le pilotage stratégique étant une démarche top-down qui permet de définir la stratégie de l'entreprise, l'auditeur interne peut également intervenir pour évaluer la stratégie adoptée par les acteurs de la GSI.

2.2.2 L'évaluation de la stratégie

Le rôle de l'auditeur interne est d'informer la direction générale des forces et faiblesses du management stratégique des systèmes d'information et de faire des recommandations pour l'améliorer. Pour cela, il peut effectuer un audit stratégique. L'audit stratégique permet d'apprécier la manière dont les dirigeants se fixent les objectifs à longs termes et effectuent les choix stratégiques, d'apprécier la cohérence et le maintien des politiques à long terme et, d'évaluer les ressources (humaines, technologiques, financières) et processus organisationnels engagés pour mettre en œuvre les choix stratégiques.

Le but d'une mission d'audit stratégique des systèmes d'information est d'analyser sa situation actuelle ainsi que son environnement externe. Cette analyse permet d'identifier d'une part, les forces et les faiblesses du système actuel et, d'autre part de saisir les opportunités et d'éviter les menaces de l'environnement. L'audit stratégique permet donc, à partir d'un diagnostic, d'analyser les dysfonctionnements et de faire des recommandations. C'est pourquoi, Weill (2011 : 6) affirme que « l'audit stratégique peut aussi être considéré comme un pré diagnostic d'une organisation et qu'il offre à ce titre une approche rapide et économique pour une identification des problèmes de l'entreprise ». Pour Gauzente (2005 : 15, 24) aussi « l'audit stratégique s'attache à analyser les influences de l'environnement d'une part, les couples produit-marché et de la concurrence d'autre part, et enfin les capacités et les limites de l'entreprise. La confrontation des capacités et ressources de l'entreprise à l'environnement permet à cette dernière d'identifier ses points forts mais surtout ses lacunes et ses axes de progrès ».

Pour assurer l'objectivité des auditeurs internes en mission d'audit stratégique, ils doivent dépendre des organes de contrôle comme le conseil d'administration ou le comité d'audit.

Cependant, la réalisation d'une mission d'audit stratégique nécessite de la part de l'auditeur une forte expérience car elle est complexe à mettre en œuvre. Comme le dit Harakat (2011 :388), « c'est un audit qui suppose la mise en œuvre de moyens spécifiques, tant au niveau des hommes et des méthodes de travail que des structures d'évaluation ».

Avec le développement croissant des TI et surtout de l'internet, les systèmes d'information des entreprises sont confrontés à de nombreux risques d'où la mise en place de dispositifs de

contrôle et de management des risques pour garantir la disponibilité, la confidentialité et la sécurité des flux d'information. L'audit interne, qui est outil stratégique, doit selon la norme :

- 2120. A1 « évaluer les risques afférents au gouvernement d'entreprise, aux opérations et aux systèmes d'information de l'organisation au regard des objectifs du contrôle interne » ;
- 2130. A1 « évaluer la pertinence et l'efficacité du dispositif de contrôle choisi pour faire face aux risques relatifs au gouvernement d'entreprise, aux opérations et système d'information ».

Comment l'audit interne peut-il intervenir pour répondre aux exigences de ces normes ? L'objet du point suivant sera d'apporter une réponse à cette question.

2.3 L'audit de conformité des systèmes d'information

Avec la nouvelle organisation des entreprises basée sur l'approche processus, la gestion des processus du système d'information incombe à la DSI. Cependant, avec le développement des TI, la confidentialité des données des entreprises ainsi que la sécurité de leur système d'information sont menacées. La DSI doit donc impliquer l'audit interne dont l'objectif est d'évaluer le contrôle interne mis en place par l'entreprise afin de s'assurer du respect des objectifs.

Les dirigeants ont besoin d'outils qui puissent leur assurer la bonne application des bonnes pratiques en matière de système d'information. Le référentiel COBIT, présenté dans le chapitre 1, est un cadre de référence de la gouvernance des systèmes d'information qui fournit selon les normes de l'ISACA (2004 :1) « un ensemble détaillé de contrôles et de techniques de contrôle destinées aux environnements de gestion des systèmes d'information ». Référentiel de bonnes pratiques, COBIT est destiné aux dirigeants et au DSI mais il peut être également utilisé par les auditeurs pour l'évaluation des dispositifs de contrôle interne.

2.3.1 Le référentiel COBIT

L'audit interne, pour évaluer les dispositifs de contrôle interne du système d'information, peut effectuer un audit de conformité qui a pour objectif de vérifier l'application des bonnes pratiques selon COBIT. L'audit de conformité permet à l'audit interne d'analyser les causes des non respects ainsi que les conséquences ou risques qu'ils peuvent engendrer afin de faire des recommandations. C'est pourquoi Renard et al (2011 :83) affirment que « l'audit de conformité, s'il est bien conduit, permet d'améliorer le contrôle interne ».

Chaque processus, défini par le COBIT, présente des objectifs de contrôle et des points de contrôle. Lors de la phase de prise de connaissance, les objectifs de contrôle peuvent servir à l'élaboration du référentiel d'audit. Pour cela, chaque objectif est présenté de façon détaillée et accompagné de tests à effectuer selon le périmètre de l'audit. Ces tests doivent également être détaillés.

L'évaluation du contrôle interne du SI consiste, à partir d'une approche par les risques, à porter un jugement sur la conformité et les risques liés à l'alignement métier, à l'attribution des rôles et responsabilités, à la séparation des tâches, à l'application des politiques et procédures en matière de gestion des accès, de gestion des infrastructures...

Dans le domaine bancaire, l'auditeur interne va également s'assurer du respect de la réglementation bancaire définie par la commission bancaire de l'UEMOA.

2.3.2 La réglementation bancaire

Le titre II portant organisation du système de contrôle interne de la circulaire N°003-2011/CB/C de la commission bancaire de l'UEMOA stipule en son article 11 que l'auditeur interne vérifie particulièrement, en s'appuyant sur une méthodologie permettant d'identifier les risques significatifs, la conformité des procédures aux dispositions régissant la fiabilité et la sécurité du système d'information.

Lors d'un audit de conformité, l'audit interne doit :

- s'assurer que le SI fournit des informations fiables, accessibles, pertinentes, explicites et conformes à la réglementation ;

- s'assurer de la sécurité du système informatique (sécurité physique, sécurité logique et des applications).

2.4 L'audit interne et l'évaluation de la performance

L'audit interne peut intervenir pour évaluer la pertinence des objectifs et des indicateurs définis dans un IT Scorecard. Il peut également effectuer un audit qualité pour évaluer la qualité du service de la DSI afin de s'assurer de la satisfaction des clients, évaluer la compétence technique et humaine de la DSI ainsi que l'efficacité et l'efficience des processus.

Au vu de ce qui précède, la GSI est un outil de pilotage et vise à mettre à la disposition des organes délibérants, exécutifs et autres parties prenantes des informations fiables, pertinentes et répondant aux exigences de qualité. Pour parvenir à cet objectif, tous les acteurs y compris l'auditeur interne qui est un acteur indépendant doivent jouer pleinement leur rôle. Ayant pour objectif d'améliorer la performance de l'entreprise, sa contribution dans cette gouvernance à travers l'analyse de l'alignement stratégique, l'évaluation du contrôle interne et l'évaluation de la performance SI est l'un des facteurs permettant d'atteindre cet objectif.

CHAPITRE 3 : METHODOLOGIE DE L'ETUDE

Etablir les relations qui existent entre l'audit interne et la gouvernance des systèmes d'information a nécessité au préalable une prise de connaissance théorique de ces deux variables. Pour résoudre notre problème de recherche dans la pratique, il s'avère indispensable de construire une cartographie permettant de formuler les hypothèses et de présenter les outils qui seront utilisés pour collecter les données.

Ce chapitre s'articulera d'abord autour de l'élaboration du modèle d'analyse et du tableau de mesure des indicateurs puis, il présentera les outils de collecte des données et la méthodologie d'analyse.

3.1 Modèle d'analyse et le tableau de mesure des indicateurs

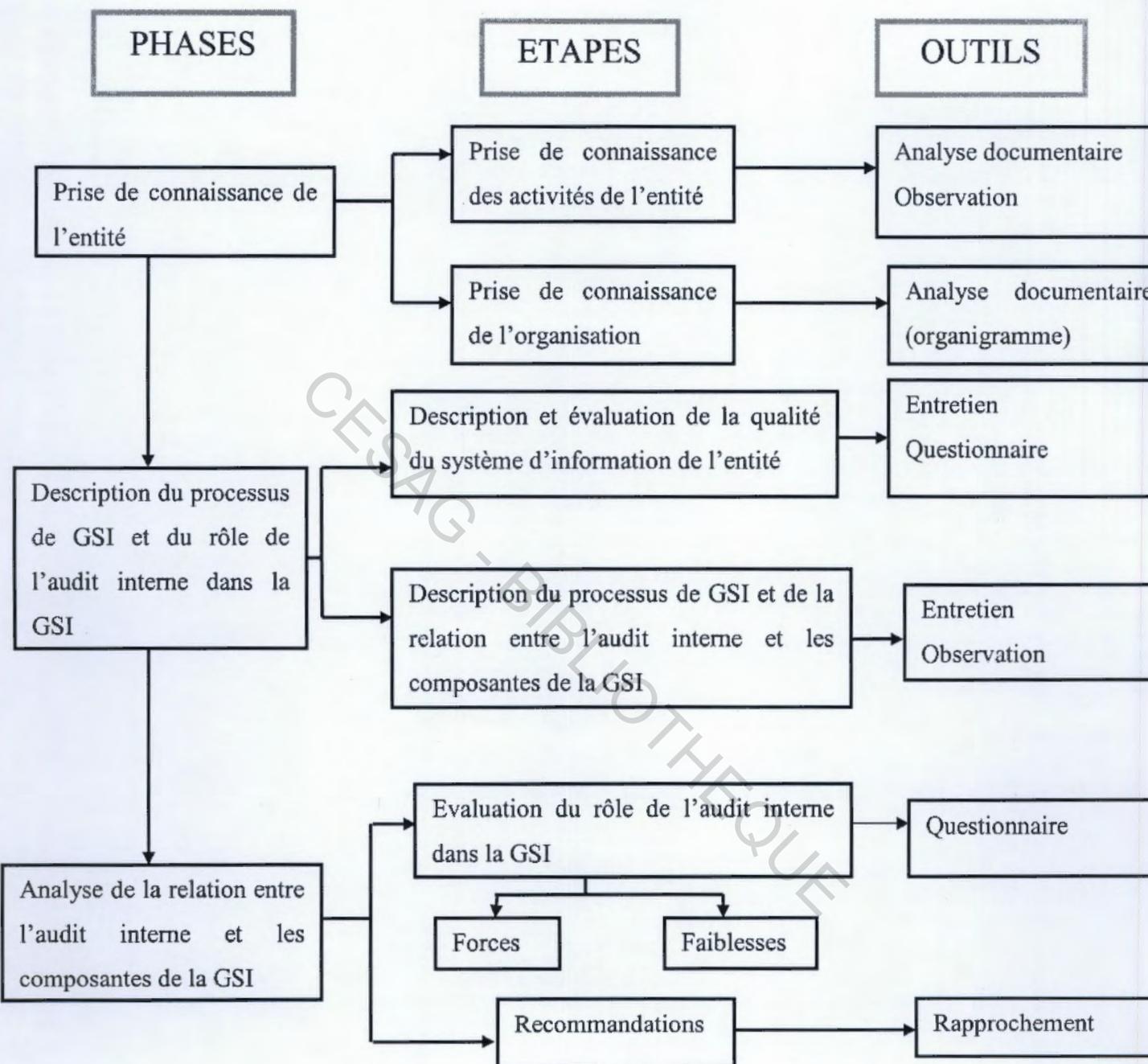
Pour présenter le modèle d'analyse, nous allons construire un schéma qui décrit des phases comprenant chacune plusieurs étapes. A chaque étape correspond un outil permettant de recueillir les données.

A la suite du modèle d'analyse, nous allons présenter un tableau de mesure des indicateurs.

3.1.1 Présentation du modèle d'analyse

Le modèle d'analyse est structuré en trois phases qui sont : la prise de connaissance, la description du SI et de la GSI et l'analyse de la relation entre l'audit interne et la GSI.

Figure 1: le modèle d'analyse



Source : nous même

La première phase du modèle d'analyse comprend deux étapes à savoir la prise de connaissance des activités et de la structure organisationnelle d'Ecobank Burkina.

Dans la deuxième phase structurée en deux étapes, la première étape consiste à présenter le système d'information de la banque et évaluer ce système pour vérifier qu'il répond aux critères qualité. Dans la deuxième étape, nous allons prendre connaissance du processus de GSI au sein d'Ecobank Burkina ainsi que de la relation qui existe entre l'audit interne et cette gouvernance.

La troisième phase de notre étude concerne l'analyse des relations qui existent entre l'audit interne et les composantes de la GSI. Ces relations (l'audit interne analyse l'alignement stratégique, évalue les risques et la performance du système d'information) sont la traduction de nos trois hypothèses liées par la variable indépendante. Dans cette phase qui comprend deux étapes, la première sera consacrée à l'évaluation du rôle de l'audit interne dans la GSI afin d'identifier les forces et les faiblesses. La deuxième et dernière étape consiste à formuler des recommandations.

3.1.2 Le tableau de mesure des indicateurs

Le tableau de mesure des indicateurs présente les indicateurs que nous allons renseigner sur le terrain afin d'appréhender l'implication de l'AI dans la GSI. Les différents éléments du tableau sont:

- les relations de l'AI avec les acteurs de la GSI. Cette variable renseignée par le nombre de réunions auxquelles l'AI a participé permet de cerner le niveau d'implication de l'AI dans le comité de GSI ;
- les missions d'audit afin de renseigner la nature des missions effectuées sur le SI et les types d'audits réalisés ;
- l'évaluation du contrôle interne pour prendre connaissance du type d'approche utilisé lors des audits du SI
- les ressources de l'AI pour savoir si l'audit interne dispose des ressources nécessaires pour jouer son rôle
- La prise en compte des recommandations par la direction générale et le suivi des actions correctives afin de savoir si l'implication de l'AI dans la GSI permet de créer de la valeur ajoutée.

Soit le tableau ci-dessous.

Tableau 1: Tableau de mesure des indicateurs d'évaluation de l'implication de l'audit interne dans la GSI

ELEMENTS	INDICATEURS
Relation de l'AI avec les acteurs chargés de la GSI	Nombre de réunions auxquelles l'AI a participé
Les missions d'audit	Type d'audit réalisé Nombre de missions effectuées sur le SI Nombre de missions programmées Nombre de missions recommandées Nombre de missions inopinées
Evaluation du contrôle interne des SI	Fréquence des contrôles Type d'évaluation
Ressources de l'AI	Nombre d'auditeurs SI Expérience des auditeurs SI Existence d'un manuel de procédure d'audit existence d'une cartographie des risques
Recommandation	Nombre de recommandations mises en œuvre Pertinence des recommandations Existence d'un système de suivi de la mise en œuvre des recommandations

Source : nous même

Pour mieux étayer notre étude, nous allons utiliser les outils précédemment présentés dans le modèle d'analyse puis nous ferons cas de la méthodologie nécessaire à l'analyse des données.

3.2 Les outils de collecte des données et la méthodologie d'analyse des données

Pour obtenir le maximum d'information, il nous a paru nécessaire de diversifier les outils de collecte.

3.2.1 Les outils de collecte des données

Pour recueillir les informations nécessaires, nous ferons des entretiens et administrerons des questionnaires. Nous procéderons également à des observations et à des recherches et analyses documentaires.

3.2.1.1 l'analyse documentaire

Le choix de cet outil a pour objectif d'obtenir les informations nécessaires à la prise de connaissance de l'entité. En effectuant une revue des documents de l'entité tels que les statuts, le manuel de procédure, les rapports d'activité, le manuel d'audit... nous aurons une meilleure compréhension des activités et de la structure organisationnelle de l'entité.

3.2.1.2 l'entretien

Nous élaborerons des guides d'entretien pour effectuer des entretiens directifs avec le chef de division de la technologie et avec le directeur de l'audit interne. Ces entretiens nous permettront de décrire le système d'information et son processus de gouvernance et de cerner le rôle des auditeurs dans la GSI au sein de la banque (voir les guides d'entretien en annexes 4 et 5 pages 90 et 92).

3.2.1.3 les questionnaires

Nous allons administrer en face à face un questionnaire au directeur de l'audit interne pour évaluer la contribution de l'audit interne dans la gouvernance des systèmes d'information. Un questionnaire sera également administré aux quarante chefs d'agence d'Ecobank Burkina pour évaluer la qualité du système d'information (voir annexes 6 et 7 pages 94 et 95). Compte tenu du nombre des agences et de la disponibilité des répondants, ce questionnaire sera administré par voie électronique.

3.2.1.4 l'observation

L'observation qui sera participative nous permettra de prendre connaissance des produits et services d'Ecobank Burkina. Cette observation se fera auprès des chargés de clientèle. Aussi, notre séjour au sein de la direction de l'AI permettra de participer aux activités et donc de s'assurer des données collectées pour la description de l'existant.

3.2.2 La méthodologie d'analyse des données

Les données qui seront collectées à partir des entretiens et des questionnaires seront analysées afin d'identifier les forces et les faiblesses du processus de GSI, et de la contribution de l'audit interne dans ce processus. Ces données nous permettront d'affirmer ou d'infirmer les hypothèses.

Le cadre théorique sur le rôle de l'audit interne dans la gouvernance des systèmes d'information nous a permis d'élaborer le modèle d'analyse ci-dessus, de choisir des outils de collecte et d'adopter une méthodologie d'analyse des données afin d'orienter nos recherches sur le terrain.

CONCLUSION DE LA PREMIERE PARTIE

En rappel, dans la première partie, nous avons procédé d'abord à la présentation du SI à travers ses composantes, ses acteurs et les moyens qui permettent aux entreprises d'utiliser le système d'information pour être compétitives et se distinguer de la concurrence. Nous avons aussi pris connaissance de la GSI en présentant les bonnes pratiques et les axes stratégiques.

Ensuite, nous avons présenté le cadre de référence, les missions et les objectifs de l'AI puis nous avons mis en exergue les différents rôles que peut jouer l'AI auprès des acteurs de la GSI.

Enfin, nous avons présenté le modèle d'analyse et les outils de collecte des données qui permettront de mener notre étude sur le terrain.

Il ressort de la revue de la littérature que l'audit interne intervient dans le pilotage stratégique du système d'information en évaluant l'alignement stratégique et en effectuant des audits stratégiques. Aussi, l'AI réalise des audits de conformité pour s'assurer non seulement du respect des procédures et bonnes pratiques et des règlements en vigueur mais aussi pour évaluer les risques liés au système d'information. En sus de ces rôles, l'AI évalue la performance du système d'information.

A partir du modèle d'analyse, nous allons à présent vérifier que l'audit interne d'Ecobank Burkina joue effectivement ces différents rôles présentés dans la revue de la littérature.

DEUXIEME PARTIE : CADRE PRATIQUE

CESAG
BIBLIOTHEQUE

INTRODUCTION DE LA DEUXIEME PARTIE

Face aux mutations technologiques, les entreprises se doivent d'être à l'écoute du marché afin d'utiliser le système d'information qui lui permet d'obtenir le meilleur rendement possible car, le système d'information n'est plus perçu comme un centre de coût mais un centre de profit. En effet, comme mentionné dans la première partie, le système d'information source de création de valeur permet, s'il est bien exploité de se distinguer de la concurrence d'où la nécessité d'en assurer une bonne gouvernance et d'associer des acteurs comme l'audit interne qui joue un rôle primordial au sein de nos entreprises. Autrefois limité à l'aspect comptable et financier, l'audit s'est étendu à tous les domaines de l'entreprise.

Aujourd'hui, les entreprises, en particulier celles de grande taille prennent davantage conscience de la nécessité de recourir à l'audit interne surtout en milieu bancaire où la concurrence est plus accentuée. Pour mieux s'imprégner du rôle de l'AI dans la GSI, nous avons choisi Ecobank Burkina Faso (EBF), filiale du groupe Ecobank Transnational Incorporated (ETI).

Dans cette partie nous aborderons trois chapitres dont le premier sera consacré à la présentation d'EBF. Le deuxième chapitre traitera de la gouvernance du système d'information au sein de la banque. Quant au troisième et dernier chapitre, il sera consacré à la présentation, à l'analyse des résultats et aux recommandations.

CHAPITRE 4 : PRESENTATION D'ECOBANK BURKINA

Ecobank Transnational Incorporated (ETI), holding bancaire, est présente dans 32 pays de l'Afrique. Suite à la grande crise financière des années 1970 connue par l'Afrique de l'ouest et centrale francophone conduisant à la diminution du poids des banques publiques et à la disparition de la plupart des banques de développement, les fondateurs d'ECOBANK ont pris l'initiative de créer en 1985 une institution bancaire régionale privée. Elle offre une large gamme de produits et services aux autorités publiques, institutions financières, entreprises multinationales, organisations internationales, petites, moyennes et micro entreprises et aux particuliers. Ce portefeuille de clients est regroupé en trois catégories : le corporate banking composé des entreprises multinationales, des organisations internationales et ambassades, le domestic banking composé des organisations locales, des petites, moyennes et micro entreprises et des particuliers. Quand aux institutions financières, elles sont regroupées dans le pôle Ecobank capital.

Le groupe ETI dont le siège est à Lomé au Togo est coté sur les bourses du Nigéria, du Ghana et sur la Bourse Régionale des Valeurs Mobilières (BRVM) à Abidjan. Elle avait comme vision de bâtir une banque panafricaine d'envergure mondiale et de contribuer à l'intégration et au développement économique et financier de l'Afrique et aujourd'hui, elle est considérée comme le principal groupe bancaire panafricain. Désirant poursuivre son expansion et pénétrer de nouveaux segments de clientèle pour accroître ses parts de marché, le concept du groupe est « une seule banque où que vous soyez » pour signifier à sa clientèle des offres de services continues et fiables à travers toutes ses filiales.

Ecobank Burkina (EBF), filiale du groupe ETI, a procédé, suite à l'absorption de la Banque Agricole et Commerciale du Burkina (BACB), à une restructuration de son réseau en 2010. L'année 2011 fût marquée par la standardisation du système d'information.

Notre objectif dans ce chapitre est de présenter les missions et objectifs d'EBF, filiale du groupe ETI, puis de faire connaître ses activités et son organisation.

4.1 Missions et objectifs d'Ecobank Burkina

Ecobank Burkina, banque de l'espace UEMOA, dispose d'un réseau large de quarante (40) agences à travers le Burkina Faso.

Ecobank Burkina a ouvert ses portes en 1997, et comme toutes les autres filiales du groupe Ecobank, a pour mission de participer au développement économique du pays et d'assurer un retour sur investissement pour ses actionnaires. EBF mène des activités à caractère social qui vise à assurer le développement durable de l'économie, de la société et de l'environnement du Burkina.

Les objectifs commerciaux de l'année 2012 sont la mobilisation de ressources pour améliorer le volume de dépôts et ainsi assurer plus substantiellement les besoins en financement de l'économie nationale et régionale. C'est ainsi que l'année 2012 est consacrée au client pour accompagner celui-ci avec des services performants et à valeur ajoutée.

4.2 Présentation des produits et de l'organisation d'Ecobank Burkina

Au cours de l'année 2011, EBF a exercé ses activités dans un environnement opérationnel instable marqué par la crise sociopolitique que le pays a connu et par la crise économique et financière internationale. Ses activités s'articulaient autour de la conquête de la clientèle, de l'amélioration du système d'information et de la résolution des dysfonctionnements liés à la qualité du service offert à la clientèle.

4.2.1 Les produits d'Ecobank Burkina

EBF met à la disposition de chaque catégorie de clientèle des produits et services. Ainsi, la clientèle du Corporate Bank bénéficie de :

- solution de marché internationale qui permet aux clients de régler facilement les transactions commerciales (crédit documentaire, caution en douane...);
- d'une gestion de trésorerie (les circuits de paiement et la gestion des encaissements);
- chaîne d'approvisionnement des finances (credit, financement de stock, financement du fonds de roulement);

- des opérations de prêts telles que le financement à court et moyen terme ;
- la banque d'entreprises par internet ;

Le domestic bank offre aux particuliers et aux Petites et Moyennes Entreprises (PME)/ Petites et Moyennes Industries (PMI) :

- des comptes courants ;
- des comptes épargnes ;
- un compte diaspora ;
- des cartes bancaires ;
- des produits électroniques ;
- les transferts de paiement ;
- des comptes d'entreprise ;
- des crédits de commerce ;
- des produits de commerce ;
- une microfinance ;
- une banque par internet.

Ecobank capital ou banque d'investissement met à la disposition de sa clientèle des services de trésorerie, de banque d'investissement et de gestion d'actifs.

Grâce au dévouement de son personnel et au programme de formation initié par la direction générale, EBF a pu améliorer la qualité du service fourni à sa clientèle d'où une amélioration de son rendement au cours de l'année 2011. Cette amélioration de 45,13% par rapport à l'année 2010 lui a permis de conforter sa position sur le marché avec la hausse des principaux indicateurs représentés ci-dessous.

Tableau 2: l'évolution des résultats obtenus par la banque au titre de l'exercice 2011 (Montant en milliers de FCFA)

RUBRIQUES	REALISATION (2011)	REALISATION (2010)	VARIATION (%)
Total des dépôts	275 447 847	214 552 428	28.38
Total bilan	400 794 453	295 605 725	35.58
Produit net bancaire	27 120	19 122	41.83
Résultat net	6 695	4 613	45.13

Source : rapport annuel d'activité 2011

La mise à disposition des produits est soutenue par une organisation solide qui fera l'objet du point suivant.

4.2.2 L'organisation d'Ecobank Burkina et leurs attributions

Selon le rapport d'activité 2011, Ecobank Burkina, société anonyme (SA) possède un capital de 7 495 000 000 FCFA détenu entre des actionnaires nationaux (12.68%) et étrangers (87.32%).

EBF dispose de deux organes décisionnels qui sont le Conseil d'Administration (CA) et l'Assemblée Générale des actionnaires (AG). Le CA, avec à sa tête un président, est chargé de soumettre le programme d'activités et le budget prévisionnel à l'approbation de l'AG, de traduire les orientations de l'AG en plans d'actions. Cet organe est également chargé de la nomination du Directeur Général qui doit assurer la gestion courante de la banque. Il supervise toutes les directions et est épaulé par une assistance de direction.

La banque dispose d'une division de la conformité directement rattachée à la direction générale. Elle a pour mission de vérifier la conformité aux lois et dispositions réglementaires de la commission bancaire de l'UEMOA et de s'assurer du respect des directives et règlements internes en vigueur.

EBF est organisé en deux types de départements : le département commercial et le département support. Le département commercial comprend la direction de la trésorerie, la

direction de la banque des grandes entreprises ou Corporate Bank et la direction de la banque de détail ou Domestic Bank. Quant au département support, il regroupe la direction de la gestion des risques, la direction du contrôle interne, le secrétariat général/direction juridique, la direction des ressources humaines, la direction du contrôle financier, la direction de l'audit interne et la direction des opérations et technologie. L'organigramme d'EBF (voir annexe 8 page 97) permet de visualiser toutes ces différentes directions.

4.2.2.1 la direction de la trésorerie

Elle assure la gestion des correspondants bancaires et intervient sur le marché monétaire et financier. Cette direction est également responsable du suivi quotidien des réserves obligatoires formulées auprès de la Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO).

4.2.2.2 Corporate Bank

Elle est responsable de la gestion des entreprises multinationales, régionales et locales du secteur public.

4.2.2.3 Domestic Bank

C'est une direction qui est responsable de la gestion des particuliers, des PME/PMI, des entreprises locales à travers le réseau des agences de la banque.

4.2.2.4 la direction de la gestion des risques

La direction de la gestion des risques qui comprend la division de l'administration du crédit (CAD), la division Wholesale risk et la division Retail risk. Elle s'assure du respect de la politique de crédit du groupe et est responsable de l'évaluation du risque crédit.

4.2.2.5 La direction du contrôle interne

La direction du contrôle interne assure un contrôle de deuxième niveau et garantit une conformité effective aux dispositions organisationnelles en vigueur.

4.2.2.6 Le secrétariat général/direction juridique

La direction juridique joue le rôle de secrétariat général lors des assemblées et assure aussi le conseil de la banque dans ses diverses branches d'activité.

4.2.2.7 La direction des ressources humaines

Elle est chargée d'élaborer les plans de formation du personnel, les bulletins de paie, d'assurer la gestion de carrière du personnel et de veiller à l'application de la réglementation interne.

4.2.2.8 la direction du contrôle financier

La direction du contrôle financier veille au respect des normes et principes comptables, au respect et règlement des déclarations fiscales. Elle produit les rapports financiers destinés à la direction générale, au groupe, à la BCEAO et aux différents partenaires.

4.2.2.9 La direction de l'audit interne

Cette direction s'assure que les opérationnels effectuent les activités conformément aux procédures définies et que les risques liés aux activités sont maîtrisés. Elle veille à la protection des actifs de la banque et au respect de la réglementation de la commission bancaire. Elle effectue des audits sur les opérations bancaires et assure le suivi des actions correctives. Elle conduit aussi des missions d'investigation et participe aux missions de l'audit interne du groupe.

L'audit interne soumet sa stratégie et son programme d'activité à un comité d'audit. Le comité d'audit se réunit quatre (4) fois par an alors que le minimum de réunions exigé par la commission bancaire est de deux (2) réunions par an.

L'audit interne rend également compte de l'évaluation du contrôle interne à la commission bancaire (voir organigramme de la direction de l'audit interne annexe 9 page 98).

C'est au sein de la direction de l'audit interne que nous avons effectué notre stage.

Pour supporter les métiers de la banque, EBF dispose d'une structure informatique qui permet de remplir cet objectif : la direction des opérations et technologie.

4.2.2.10 La direction des opérations et technologie

La direction des opérations et technologie comprend la division des opérations, la division Ecobank Business Services (EBS) et la division de la technologie.

La division des opérations est subdivisée en quatre services à savoir le Cash Management, le Trade, le transfert et le Trops and Loans. Elle est chargée de la gestion des compenses, des chèques, du commerce international, des transferts et des crédits.

La division EBS s'occupe de la logistique de la banque. Elle est chargée de la gestion du matériel et des fournitures, de la gestion du parc informatique et automobile, de la gestion des frais de missions...

La division de la technologie comprend quatre services qui sont :

- service de sécurité informatique qui veille à la sécurité du système informatique et qui est directement rattaché au chef de division de la technologie ;
- delivery ou le service d'assistance aux utilisateurs qui fournit des prestations de services et assiste les utilisateurs en cas d'arrêt ou de dysfonctionnement du système ;
- le service applications qui s'occupe des applications bancaires ;
- le service des infrastructures chargé de la gestion du réseau et du matériel

Ce chapitre nous a permis de prendre connaissance de Ecobank Burkina, filiale du groupe ETI, à travers son organisation et les attributions de ses différentes directions, ses missions, ses offres de produits et services et ses activités.

Cependant, l'objectif de notre étude étant d'analyser la contribution de l'audit interne à la gouvernance des systèmes d'information, il s'avère nécessaire de prendre connaissance du système d'information d'EBF et de sa gouvernance. D'où la présentation du chapitre suivant.

CHAPITRE 5 : LA GOUVERNANCE DU SYSTEME D'INFORMATION DE LA BANQUE

Le groupe ETI, banque universelle axée sur l'Afrique médiane réalise ses activités à partir d'une plate-forme informatique intégrée exploitée par eProcess, la filiale technologique du groupe. Cette plate-forme a été migrée avec succès sur une application bancaire unique appelée ORACLE FLEXCUBE. Dans un souci de centralisation des activités de suivi et de soutien, le groupe a installé son centre de service partagé et de technologie à Accra.

Cependant, pour assurer la sécurité et la continuité de ses opérations, le groupe a implémenté une plate-forme secondaire à Lagos et une unité de gestion des sinistres informatiques à Lomé.

A sa création en 1997, EBF utilisait un système d'information appelé GLOBUS pour communiquer et effectuer ses opérations et transactions bancaires. Suite à l'absorption de la BACB en 2009 qui utilisait DELTA comme système d'information, EBF a effectué une migration des deux systèmes pour donner lieu à FLEXCUBE système d'information en vigueur depuis le dernier trimestre 2010. Aujourd'hui, EBF est dans une perspective d'amélioration de la qualité de FLEXCUBE.

Ce présent chapitre sera structuré en trois sections. La première section sera consacrée à la présentation et à l'évaluation de la qualité du système d'information. La deuxième section qui traitera de la GSI au sein d'EBF présentera les acteurs de la GSI, son processus ainsi que l'application des principes. La dernière section mettra en exergue les différentes relations entre l'audit interne et les composantes de la GSI.

5.1 Présentation du système d'information et la qualité du système d'information

EBF dispose d'un système d'information automatisé mais aussi d'un système manuel. En effet, notre passage au service de la clientèle nous a permis de constater que EBF utilise un certain nombre d'imprimés tels que les formulaires d'ouverture de compte et d'activation de produits, les accusés de réceptions, les formulaires de demande de services qui permettent de réaliser les opérations y afférentes. Elle utilise également des registres de transmission et réception de courriers, d'ouverture de comptes, de chèques de guichets et de demandes de prêts. Ces registres permettent d'enregistrer et d'assurer la traçabilité des opérations. Le

système informatisé d'EBF se définit par un environnement bancaire flexible compréhensif et universel d'où l'abréviation FLEXCUBE (Flexible Compréhensif Universel Bancaire Environnement).

5.1.1 Présentation du système d'information

Pour assurer la saisie, le traitement et le stockage des données relatives à ses activités, EBF dispose d'un matériel informatique, d'informaticiens et d'un logiciel de base appelé FLEXCUBE qui permet d'effectuer les opérations. La banque dispose également de plusieurs applications telles qu'Omni, Busines Object, Internet Banking, image chèque... Les activités de la banque sont assurées via l'intranet qui lui permet d'échanger en interne mais aussi avec les autres filiales du groupe.

Le logiciel FLEXCUBE est composé:

- d'une application pour les opérations du front office appelée FLEXBRANCH ;
- d'une application pour les opérations du back office appelé HOST.

5.1.1.1 Présentation des applications de FLEXCUBE

Pour assurer la sécurité logique, il a été attribué à chaque agent un identifiant et un mot de passe qui lui sont propres et qui lui permettent d'accéder au système. Lorsqu'il accède au système, FLEXCUBE indique la dernière date de connexion et le nombre de tentatives infructueuses. Il est impossible de saisir des caractères spéciaux dans FLEXCUBE ce qui permet d'assurer une certaine clarté des données.

L'application FLEXBRANCH comprend plusieurs modules relatifs au service clientèle, à la caisse et aux agences. Les modules relatifs au service clientèle permettent aux chargés de clientèle d'effectuer des ouvertures de comptes, des transactions de gestion de fonds et de faire des liaisons entre le nom du client, sa photo et signature. Ils lui permettent aussi d'effectuer des requêtes comptes, clients... Lorsqu'on ajoute un client dans le système, cela nécessite la création du code et du compte client qui sont tous deux générés automatiquement. Lors de la création du compte, il est possible d'effectuer une commande automatique de carte

de retrait et/ou de chéquier. Cette fonction présente un avantage dans la mesure où elle permet de réduire la période de commande de chéquier ou de carte.

Pour accéder à l'application HOST, l'utilisateur peut se servir de FLEXBRANCH ou saisir l'adresse URL destinée à cet effet. Host présente une fonction « autoriser » qui permet d'autoriser les opérations exécutées. Cependant, l'autorisation n'est possible que si elle est faite par un utilisateur autre que celui qui a exécuté l'opération. Le système a donc pris en compte la séparation des tâches (autoriser et exécuter).

Le centre de service partagé et de technologie à Accra au Ghana met à la disposition de toutes les filiales comme EBF :

- un centre informatique ;
- un service de télécommunication centralisé qui permet les échanges entre filiales ;
- intranet, email et vidéo conférence ;
- un Switch électronique et une plate-forme de paiement qui soutiennent une banque de réseau, les services de cartes, les Distributeurs Automatiques de Billets (DAB) et les Terminaux de Paiement Electronique (TPE) ;
- un service contact client et une plate-forme pour ses centres d'appels basés à Abidjan, Lagos et Douala ;
- un service de formation en ligne ;
- des procédés centralisés permettant les traitements de comptes, de crédit et des paiements.

L'entretien avec le chef de la division IT nous a permis de prendre connaissance des objectifs et stratégies du système d'information, de la gestion des ressources, de l'accessibilité et de la sécurité du SI et de la gestion des incidents.

5.1.1.2 les objectifs et stratégies du SI

La division de la technologie de Ecobank Burkina, par ses activités de soutien aux autres directions, est chargée du bon fonctionnement des applications, du matériel informatique et du réseau intranet. Tout comme les autres divisions de la banque, la division de la technologie mène ses activités en vue d'atteindre des objectifs.

Les objectifs du système d'information assignés à la division de la technologie découlent des objectifs du business et du plan stratégique du groupe ETI. L'objectif général du business pour l'année 2012 est d'accroître les volumes d'affaires. C'est pourquoi l'année 2012 est dédiée à la clientèle. Les objectifs du SI qui émanent de cet objectif général sont :

- rendre le système d'information disponible ;
- offrir des nouveaux produits à la clientèle interne et externe.

La division de la technologie a pu mettre en place un nouveau produit pour chaque type de client : Omni Flow pour les clients internes et la banque par internet pour les clients externes. Omni flow a pour but de faciliter l'ouverture des comptes. Quant à la banque par internet, elle permet d'effectuer des demandes de transferts et de virement.

Quant à la disponibilité du SI, cet objectif n'affiche pas un taux de réalisation de 100% en raison des difficultés rencontrées telles que les perturbations de la liaison.

Pour atteindre ses objectifs, la division a élaboré un ensemble de stratégies qui sont :

- la création d'une politique back-up ;
- les investissements en équipement ;
- la mise en place d'une politique de sauvegarde (création d'une deuxième salle machine).

La division de la technologie a défini ses stratégies en fonction des évolutions technologiques et de l'environnement bancaire.

Aussi, pour assurer une bonne gestion des IT, EBF se conforme au référentiel ITIL d'où l'existence d'un centre de service (delivery), d'une gestion des priorités selon l'impact et l'urgence, d'une gestion des infrastructures et des changements.

5.1.1.3 la gestion des ressources

Le groupe ETI a défini un taux d'informaticien selon chaque filiale. Selon ce taux, la filiale EBF a droit à 13 informaticiens. Cependant, la filiale ne dispose qu'un effectif réel de 9 informaticiens centralisés et pour 40 agences. Cet effectif se répartit comme suit :

- 3 agents pour le service « delivery »;

- 3 agents pour le service de gestion des applications ;
- 3 agents pour le service de gestion des infrastructures

Cependant, aucun informaticien n'est affecté au service sécurité informatique. Cette absence de personnel dans ce service s'explique par les retraites anticipées et les affectations qui ont eu lieu en 2010. Cependant, les tâches relatives à ce service sont supportées par le chef de division de la technologie.

Il est prévu 40h de formation par an pour les informaticiens mais ce volume d'heures dépend en réalité du budget, des projets à réaliser et de la disponibilité des formateurs. ITIL étant le référentiel choisi par EBF, ses informaticiens bénéficient généralement de formations sur cet outil.

Notons que la division de la technologie dispose d'un plan d'infrastructure qui lui permet de faire un suivi comptable des équipements.

Il ressort de l'entretien que la division de la technologie n'effectue pas des enquêtes de satisfaction clientèle. Cependant, suite à une formation sur le tableau de bord, il a été recommandé d'élaborer, chaque trimestre, un questionnaire de satisfaction pour la clientèle interne mais qui n'est pas encore porté à sa connaissance.

5.1.1.4 la gestion des incidents

La division de la technologie a mis en place une politique de gestion des incidents. Cette politique consiste à enregistrer sur un logiciel appelé Remedy l'ensemble des incidents qui surviennent. Lorsque le centre de service delivery reçoit une demande de gestion d'un incident et qu'il ne peut le résoudre dans un intervalle de temps de cinq (5) à quinze (15) minutes, l'incident est transféré au niveau du service de gestion des applications ou des infrastructures qui ont un temps de réponse de trois (3) à quatre (4) heures. Au-delà de ce temps, si l'incident n'est toujours pas résolu, il est alors transféré au niveau supérieur à Accra. La gestion des incidents se fait selon la procédure d'escalade.

Lorsque le centre de service reçoit simultanément deux (02) ou plusieurs demandes de gestion des incidents ceux-ci sont traités selon la disponibilité des informaticiens. Ainsi, quand le

nombre d'informaticiens présents est suffisant, les incidents sont gérés simultanément. Dans le cas contraire, les incidents sont gérés selon leur priorité en tenant compte de l'impact de l'incident sur l'activité et sur la chaîne et de l'urgence (durée de l'incident).

5.1.2 La qualité du système d'information

L'application bancaire étant au cœur de ses opérations, la banque a mis en place un ensemble de dispositif permettant d'assurer la sécurité du système. Pour s'assurer de la qualité du système, la division de la technologie a défini des accords de service ou Service Level Agreement (SLA) avec la clientèle interne.

5.1.2.1 la sécurité du système d'information

La sécurité du SI étant l'un des critères de la qualité du système d'information, EBF a défini une politique de gestion des accès permettant de veiller à la sécurité du SI. La gestion des accès comprend les accès aux données (sécurité logique) et les accès aux locaux informatiques (sécurité physique).

Pour assurer une bonne gestion de la sécurité logique des données, il a été défini pour chaque utilisateur, un identifiant et un mot de passe personnalisés. Pour accéder à FLEXCUBE, l'utilisateur doit renseigner l'identifiant et le mot de passe. L'identifiant et le mot de passe sont fonction du profil et des tâches de l'utilisateur ce qui permet d'assurer l'intégrité des données.

Pour disposer d'un identifiant et d'un mot de passe, l'utilisateur doit renseigner une fiche de création du profil qui est ensuite soumise au supérieur hiérarchique pour approbation du profil. Après approbation, la fiche est transférée aux ressources humaines pour recueillir l'autorisation de création. Le contrôle interne, responsable de la gestion des profils effectue un « dual contrôle » avant d'attribuer l'identifiant et le mot de passe qui comprend des caractères alpha numériques et qui est très restrictif.

Pour accéder au système, l'utilisateur a droit à trois essais pour saisir le mot de passe correct. A la suite du 3^{ème} essai, si le mot de passe saisi est incorrect, le système se verrouille et c'est

au contrôle interne d'effectuer des vérifications pour s'assurer qu'il s'agit de l'utilisateur approprié avant de procéder au déverrouillage. Le déverrouillage se fait également en dual.

Cette forme permet de protéger les données contre toute modification, tous accès non autorisés et toutes destructions. Elle permet aussi de mémoriser les accès aux personnes autorisées, d'enregistrer les manipulations et de s'assurer de la confidentialité des données. L'enregistrement des manipulations permet d'assurer la traçabilité des données.

EBF dispose d'un système de traçabilité des manipulations. Il s'agit d'un fichier log permettant de visualiser un champ à une heure précise et à une date donnée.

Pour garantir la sécurité des transferts effectués sur internet banking qui est une application destinée à la clientèle externe, le client doit renseigner l'identifiant et le mot de passe mais aussi une image de sécurité choisie et enregistrée depuis sa première connexion.

La banque a également mis en place un ensemble de dispositifs qui permet de mieux gérer la sécurité physique des locaux. Il s'agit des vidéos de surveillance, d'anti intrusions, de deux salles machines pour assurer le système de back-up. Une salle machine est située au siège d'EBF et la deuxième salle dans une autre agence de Ouagadougou.

Pour accéder à la salle machine au siège, il a été mis à la disposition des personnes habilitées à y accéder des badges. Quant à l'accès à la deuxième salle, le dispositif comprend le code et le registre manuel à remplir.

5.1.2.2 les autres critères de la qualité

Pour apprécier la qualité des applications bancaires, la division de la technologie a défini avec chaque direction (client interne) des contrats de niveaux de service encore appelé Service Level Agreement (SLA). Les SLA définissent les niveaux de performance attendus de la division de la technologie par rapport aux différentes prestations fournies à la direction concernée. Ces niveaux de performance sont formalisés sous forme d'indicateurs.

A la fin d'une période donnée, généralement le trimestre, les deux parties font la synthèse pour voir si les indicateurs ont été respectés. Lorsque la direction concernée s'aperçoit du non respect du contrat elle peut attirer l'attention de la division avant même la période d'évaluation.

Pour avoir un aperçu des critères qualité du système d'information, nous avons administré un questionnaire au front office mais plus particulièrement aux chefs d'agences qui sont responsable de la gestion de la relation avec la clientèle externe. Les résultats du questionnaire sont consignés dans le tableau ci-dessous :

Tableau 3 : la présentation des données du questionnaire d'évaluation de la qualité du système d'information

Les critères qualités	Le nombre de répondants	Oui	Non
Confidentialité des données	40	100%	-
Accessibilité et disponibilité des données	40	-	100%
Pertinence	40	100%	-
Fiabilité	40	80%	20%
Rapidité	40	-	100%
Souplesse	40	50%	50%

Source : nous même

Nous avons pu administrer par voie électronique un questionnaire à chaque agence soit un total de 40 questionnaires administrés et nous avons obtenu un taux de participation de 100%.

Il ressort des résultats obtenus que 100% des agences pensent que le système est pertinent et permet de garantir la confidentialité des données.

Cependant, toutes les agences (100%) pensent que le système est lent et inaccessible et que les données sont indisponibles.

80% des agences pensent que le système est fiable et 20% pensent qu'il n'est pas exempté d'erreurs. Aussi, 50% des agences trouvent le système d'information souple.

L'analyse de ces résultats nous amène à dire que la qualité du système d'information est à améliorer. Pour les chefs d'agences, directement en contact avec la clientèle externe, les arrêts et dysfonctionnements de FLEXCUBE sont fréquents et leurs sont préjudiciables alors qu'ils

doivent assurer la satisfaction de celle-ci. Ces arrêts et dysfonctionnements sont dus à l'irrégularité de la connexion et à l'éloignement de la plateforme technologique.

5.2 La gouvernance du système d'information d'EBF

EBF a défini un ensemble de politiques afin de diriger et contrôler le SI pour atteindre les objectifs à court et moyen terme fixés.

5.2.1 Les acteurs de la gouvernance du système d'information et leurs rôles

Ces politiques sont conduites par un ensemble d'acteurs qui sont la division de la technologie relevant de la direction des opérations et de la technologie, le comité de technologie et eProcess responsable de la gestion de la technologie du groupe.

eProcess, installé à Accra au Ghana élabore la politique technologique du groupe en fonction de sa politique business et décline le processus de mise en œuvre aux différentes filiales.

La division de la technologie a pour rôle d'élaborer un budget technologique et un plan d'action qu'il soumet au comité de technologie. Elle assure l'assistance aux utilisateurs et est chargée de la maintenance du matériel informatique et de la gestion des incidents et des problèmes.

Le comité de technologie est composé :

- du directeur général ou de son représentant ;
- du directeur des opérations et de la technologie ;
- du chef de la division de la technologie ;
- du chef de la division des opérations ;
- du directeur du contrôle interne ;
- du directeur marketing.

Ce comité a pour rôle de valider les projets et programmes d'activités de la division de la technologie.

5.2.2 Le processus de la GSI

Ecobank Burkina étant une filiale du groupe ETI, les politiques de la gouvernance du système d'information sont formulées par la direction des opérations et de la technologie et par l'e-process du groupe en fonction de la stratégie business. Une fois validées par le comité de technologie du groupe, ces politiques sont ensuite déclinées au niveau des filiales en actions précises appelées initiatives que les divisions des filiales doivent exécuter et renseigner chaque semaine.

Le comité de technologie de la filiale se réunit chaque trimestre pour prendre connaissance de l'évolution de la qualité du système d'information, des difficultés en termes de ressources technologiques et humaines et pour s'assurer qu'il soutient les objectifs business. Ce comité prend des décisions d'amélioration du système d'information pour qu'il réponde au mieux aux attentes du business.

La division de la technologie élabore le budget et le soumet au supérieur hiérarchique pour validation. Ce budget est ensuite soumis à la direction des opérations et technologie du groupe pour également être validé. Après validation, le budget fait l'objet d'une révision au cours du premier semestre afin de l'adapter à la situation actuelle. Cependant, toute exécution de dépenses d'investissement doit être préalablement autorisée par eProcess.

La dépendance de la filiale au groupe ne permet pas d'évaluer exactement le retour sur investissement. La filiale se limite qu'aux investissements en matériel informatique et en aménagement des salles machines. Les investissements en logiciel, réseau, en application relèvent de la responsabilité de la société mère.

EBF, dans le management de son système d'information, fait face à des risques d'indisponibilité du système et des données dus aux attaques de virus, à la faiblesse de la liaison avec Accra. Elle est aussi exposée à des risques de non qualité des données et des risques de non adaptabilité aux objectifs business. Cependant, pour palier à ces risques, la banque à mis en place des systèmes de prévention tels que :

- le système de monitoring permettant d'assurer une maintenance préventive pour éviter les risques d'indisponibilité ;
- le système de contrôle d'accès, de sauvegarde, de protection contre les intrusions ;

- la vérification périodique de la base de données afin de lutter contre le risque de non qualité des données ;
- la conception d'un plan stratégique et la présence du comité de technologie afin de s'assurer de la cohérence et du suivi du respect du planning des projets.

Les recommandations formulées par l'audit interne lors de ses passages constituent des moyens de traitement des risques informatiques.

Ecobank Burkina applique une gouvernance du système d'information découlant surtout de la hiérarchie du groupe.

5.2.3 L'application des principes de la GSI

En rappel, dans le chapitre 1 de la première partie, nous avons présenté les différents axes de la GSI qui sont : l'alignement stratégique, la création de valeur, la gestion des risques, la gestion des ressources et la mesure de la performance. Ceux-ci sont encore qualifiés de principes ou de piliers de la GSI. A présent, il s'agira de prendre connaissance de l'application de quelque uns de ces principes au sein d'EBF.

5.2.3.1 l'alignement stratégique

EBF étant une filiale du groupe Ecobank, ses objectifs sont fixés par le groupe. La direction générale effectue une retraite de stratégie et décline aux différentes directions des objectifs spécifiques qu'ils doivent atteindre. En fonction des objectifs fixés par la direction générale, la division de la technologie élabore son plan stratégique sur 3ans et le budget permettant de soutenir le dit plan.

Ce plan stratégique est soumis au comité de technologie qui s'assure de la compréhension et de l'intégration des objectifs et stratégies du business dans ceux de l'IT. La division de la technologie définit par la suite les infrastructures IT à mettre en place pour accompagner la stratégie IT. Cependant, le budget de ces infrastructures doit être adopté par le comité de technologie du groupe avant d'être réalisé.

5.2.3.2 La gestion des risques

L'environnement bancaire étant hautement informatisé, le système d'information est un patrimoine important qui est exposé à des risques.

Ecobank Burkina, pour assurer la gestion des risques de son système d'information, a défini des niveaux de sécurité, des précautions et des contres mesures. Ces derniers permettent d'assurer la sécurité des actifs informationnels, la sécurité des infrastructures matérielles et logiciels et la sécurité des locaux informatiques.

EBF est confronté à des risques liés au système d'information. Ces risques sont essentiellement d'ordre opérationnel. Comme risques opérationnels, il s'agit des risques d'erreurs ou de manipulations humaines et des risques juridiques. Les risques d'erreurs sont liés à l'exécution des opérations bancaires comme les opérations de caisse, les informations sur la clientèle, l'octroi de crédit et la gestion des cartes de crédit. Les risques juridiques sont essentiellement la non préservation de la confidentialité des données de la clientèle.

Ces risques opérationnels peuvent aussi prendre la forme de risques de réputation qui impactent négativement sur l'image de la banque.

Pour palier ces risques qui affectent la sécurité des actifs informationnels et assurer la sauvegarde, la confidentialité et la fiabilité des données, les mécanismes de précaution utilisés par EBF sont :

- le système de contrôle d'accès logique ;
- le système de protection des données (cryptage et anti-virus) ;
- désactivation de lecteurs des supports amovible ;
- le système d'autocontrôle qui permet de s'assurer de la bonne exécution des opérations ;
- le système d'autorisation double: toute opération exécutée par un agent doit être autorisée par un supérieur ;
- l'utilisation des codes pour les cartes de crédits ;
- la vérification de l'identité des clients et des signatures;
- existence d'un logiciel appelé Remedy pour l'enregistrement des incidents;

- les plans de continuité d'activité et de reprise après sinistre.

Pour veiller sur la sécurité des infrastructures et logiciels, le service de sécurité informatique effectue des maintenances, assure le marquage du matériel et la mise à jour des logiciels anti-virus et veille au bon fonctionnement de la climatisation.

Quant à la sécurité des locaux informatiques, le service de sécurité informatique a mis en place :

- un système de badge qui permet d'assurer l'autorisation d'accès aux locaux informatiques qu'aux personnes habilitées ;
- un système d'anti intrusion ;
- un registre permettant d'indiquer les entrées et sorties dans la salle machine;
- un système de détection automatique d'incendie ;
- des vidéos de surveillance.

Il veille également à la disponibilité des serveurs.

Pour préserver la sécurité des supports physiques (dossiers d'ouverture de comptes, d'octroi de crédit, les dossiers de garanties, les chèques...) ; EBF dispose de salles d'archivage dont la gestion des accès se fait selon un registre utilisé pour enregistrer les entrées et sorties des salles.

5.2.3.3 L'évaluation de la performance

Les contrats de niveau convenus de service (SLA) entre chaque direction métier et la division de la technologie permettent d'évaluer le respect des indicateurs définis dans les contrats.

L'évaluation de la performance du système d'information repose sur un certain nombre d'indicateurs tels que :

- le taux de disponibilité des équipements et des ressources humaines ;
- le taux de résolution des incidents ;
- le taux de disponibilité des systèmes applicatifs.

La division de la technologie a conçu un questionnaire de satisfaction de la clientèle pour évaluer la qualité du système d'information. Ce questionnaire dont la conception est inachevée sera administré aux directions de la banque chaque trimestre.

Les entretiens réalisés auprès du directeur de l'audit interne et du chef de la division de la technologie nous ont permis d'identifier les différentes relations qui existent entre l'audit interne et les composantes de la GSI.

5.3 Le rôle de l'audit interne dans l'alignement stratégique

L'audit interne évalue l'adéquation de la stratégie IT avec la stratégie business. Cette évaluation consiste à :

- s'assurer de l'existence d'une stratégie IT sur le court terme (un an) ;
- effectuer une revue des ressources à mobiliser pour assurer cette adéquation et faire connaître à la direction générale la nécessité ou non des ressources ;
- s'assurer de la tenue des réunions du comité de technologie.

Lorsque l'audit interne identifie des défaillances, elle informe la direction générale et les dirigeants IT puis situe les responsabilités et les invitent à prendre les dispositions nécessaires à l'amélioration de l'alignement stratégique. Cependant, l'audit interne se limite à l'évaluation de l'alignement stratégique. Elle ne réalise pas d'audit sur le management du système d'information.

5.4 L'audit interne et les risques du système d'information

L'audit interne intervient pour évaluer les risques liés au système d'information. La direction de l'audit interne effectue des missions d'audit de conformité et d'efficacité afin de vérifier le respect des procédures, des règlements, des réglementations en vigueur et de s'assurer que ces procédures permettent la réalisation et l'optimisation des opérations.

A partir de la cartographie des risques, elle programme ses missions d'audit du système d'information en fonction des processus qui présentent un fort potentiel de risque élevé. L'audit du système d'information peut donc porter sur les applications, le réseau, la sécurité, la banque électronique, les cartes bancaires...

Pour effectuer les audits de conformité du système d'information, l'audit interne s'appuie sur la réglementation interne de la banque telle que le guide des opérations, les directives de la direction générale, les notes de services et les mémos. L'audit interne s'appuie également sur la réglementation de la commission bancaire de l'UMOA. Lorsque des anomalies sont décelées lors de l'audit de conformité, l'audit interne se réfère aux bonnes pratiques en matière de GSI particulièrement au COBIT afin de formuler des recommandations.

Lors de ses missions sur le système d'information, l'audit interne utilise une approche par les risques et :

- évalue l'efficacité de l'organisation mise en place afin de s'assurer de la séparation des tâches, de la délégation des pouvoirs et responsabilité et de la disponibilité des ressources humaines;
- s'assure de l'existence de procédures IT;
- vérifie la bonne application des procédures IT;
- évalue l'efficacité des procédures en fonction des risques qu'elles peuvent présenter.

5.5 Le rôle de l'audit interne dans l'évaluation de la performance

L'objet de l'audit interne n'est pas d'évaluer la performance du système d'information mais d'évaluer les SLA afin de s'assurer du niveau de la qualité des prestations fournies par la division de la technologie. L'audit interne vérifie que les indicateurs définis dans les SLA sont mesurables, atteignables et pertinents.

La direction de l'audit interne joue un rôle de conseil auprès des acteurs de la gouvernance du système d'information. Elle s'assure que les directives de la direction générale sont appliquées et attire l'attention de la direction générale sur les dysfonctionnements et anomalies constatées lors de ses missions d'audit. Pour assurer son rôle dans la gouvernance du système d'information, l'audit interne s'appuie sur des référentiels internes et externes tels que le guide des opérations et les règlements de la commission bancaire.

Notre passage à Ecobank Burkina nous a permis, à travers les outils de collecte des données comme les entretiens et l'analyse documentaire de comprendre non seulement l'organisation,

et les activités de la banque mais aussi son mécanisme de GSI. EBF doit renforcer son dispositif de sécurité physique mis en place et améliorer l'accessibilité et la rapidité du SI.

Il ressort également dans ce chapitre que la direction de l'audit interne joue effectivement un rôle dans l'alignement stratégique et dans l'évaluation des risques du SI. Cependant, elle joue un rôle moindre dans l'évaluation de la performance du SI.

Dans le chapitre suivant, il s'agira de présenter et d'analyser les données collectées sur l'évaluation de l'efficacité du rôle de l'audit interne dans la GSI afin d'identifier les forces et les faiblesses et formuler des recommandations.

CESAG - BIBLIOTHEQUE

CHAPITRE 6 : PRESENTATION-ANALYSE DES RESULTATS ET RECOMMANDATIONS

Les entretiens réalisés auprès des principaux acteurs (directeur de l'audit interne et chef de la division technologie) nous ont permis de cerner la contribution de l'audit interne dans la GSI au sein d'EBF. Pour répondre à notre question de recherche qui consiste à évaluer l'efficacité de l'implication de l'audit interne dans la GSI au sein d'Ecobank Burkina, nous avons aussi administré un questionnaire au directeur de l'audit interne. Les données de ce questionnaire nous ont permis de renseigner les indicateurs du tableau de mesure sur l'évaluation de l'implication de l'audit interne dans la GSI.

L'analyse des résultats sera basée sur les informations collectées au cours des entretiens ainsi que sur les données issues du questionnaire.

Dans ce chapitre, nous allons d'abord procéder à la présentation des résultats puis nous les analyserons. L'analyse de ces relations permettra de faire un rapprochement avec les bonnes pratiques et de formuler des recommandations.

6.1 La présentation des résultats

La présentation des résultats consiste à renseigner les indicateurs issus du questionnaire administré au directeur de l'audit interne. Ces indicateurs sont :

- le niveau de rattachement hiérarchique ;
- fréquence des réunions avec les acteurs de la GSI ;
- les ressources de l'audit interne ;
- les missions d'audit du SI
- l'évaluation du contrôle interne.

6.1.1 Le niveau de rattachement hiérarchique

L'audit interne est rattaché à la direction générale et rend compte fonctionnellement au comité d'audit de la filiale et à la direction de l'audit interne du groupe. Elle rend aussi compte au comité d'audit du groupe. Ceci lui garantit son indépendance et lui confère une autorité

facilitant l'exécution de ses missions d'audit. La direction générale approuve les recommandations formulées par l'audit interne en fonction de la disponibilité des ressources à mettre en œuvre. Lorsqu'elle approuve une recommandation, elle veille à sa mise en œuvre auprès des audités.

6.1.2 La fréquence des réunions avec les acteurs de la GSI

L'audit interne prenait part aux réunions trimestrielles du comité de technologie organisées par la direction générale mais avec la nouvelle organisation et dans le souci d'assurer l'indépendance de l'audit interne, cette dernière ne participe plus à ces réunions. En effet, la nouvelle organisation distingue depuis 2011 la direction de l'audit interne de celle du contrôle interne. Ce sont les directions du contrôle financier et du contrôle interne qui prennent part à ces réunions.

6.1.3 Les ressources de l'audit interne

Le questionnaire adressé à la direction de l'audit interne fait ressortir que cette direction chargée de l'évaluation des politiques, des règlements et procédures de l'entreprise a un effectif de 5 auditeurs proportionnel de 1% à l'effectif de la filiale (485 en fin 2010).

Cet effectif est composé de :

- deux (2) auditeurs informaticiens ;
- deux (2) auditeurs comptables et financiers ;
- directeur de l'audit interne.

L'audit interne dispose de moyens humains expérimentés, d'une charte d'audit qui fait ressortir les pouvoirs, les responsabilités et les missions et d'une cartographie des risques. Cependant, elle ne dispose pas encore d'un manuel de procédure car il est en phase d'élaboration.

L'audit interne dispose également d'un plan d'audit et son plan pluriannuel est triennal.

6.1.4 Les missions d'audit du SI

L'audit interne n'effectue pas de missions recommandées ni de missions inopinées sur le système d'information. Le nombre de missions programmées sur le SI varie entre 4 et 5 missions par an.

Avec la migration du système d'information bancaire en fin 2010, l'audit interne a réalisé en 2011 des missions d'audit sur l'évaluation de l'adéquation du nouvel environnement d'exploitation avec les activités et objectifs de la banque. Il a aussi effectué des missions sur la sécurité des actifs informatiques, sur la gestion des accès et sur la banque électronique.

Dans le planning des missions 2012, le nombre de missions planifiées est de 5 et concerne :

- la revue des plans de continuité d'activité et de reprise ;
- la revue des actifs informationnels : données, infrastructures d'exploitation et service réseaux ;
- la revue des applications bancaires et des processus bancaires ;
- la revue des e-banking ;
- la revue de la gestion des accès des applications, des sites physiques.

La durée moyenne d'une mission est de 2 semaines.

6.1.5 L'évaluation du contrôle interne

L'audit interne effectue des missions de conformité et d'efficacité pour vérifier le respect des politiques, des règlements, des procédures et pour s'assurer que les risques sont couverts et que les performances sont atteintes. Le plan d'audit découlant de la cartographie des risques, lors de ses missions, l'audit interne se base sur l'approche par les risques pour évaluer le contrôle interne.

L'auditeur informatique était chargé de la gestion et du contrôle des profils des agents de la banque mais avec la séparation de la direction de l'audit de celle du contrôle interne, c'est la direction du contrôle interne qui en est responsable. Aussi, la division de la technologie a défini des profils pour le système informatique et le réseau Swift qui sont périodiquement suivis et mis à jour par le contrôle interne.

6.2 L'analyse des résultats

L'analyse des résultats va porter sur les forces et les faiblesses de la GSI ainsi que ceux de la contribution de l'audit interne dans cette gouvernance.

6.2.1 Les points forts de la GSI

L'existence du comité de technologie est un atout pour EBF car il contribue à l'amélioration de la GSI. En effet, il se réunit chaque trimestre pour évaluer la qualité du système d'information et veille au respect des principes de la GSI.

Aussi, la division de la technologie d'EBF assure une gestion des services conformément aux référentiels ITIL et COBIT. La formalisation des SLA présente un atout car ils permettent à la division de la technologie de veiller à l'amélioration de la qualité du SI.

6.2.2 Les forces de l'implication de l'audit interne dans la GSI

Les résultats issus de l'évaluation de l'implication de l'audit interne dans la GSI ont permis d'identifier des points forts qui sont : le respect des bonnes pratiques, le système de management des risques, la réalisation d'audit d'efficacité et l'appui de la direction générale.

6.2.2.1 le respect des bonnes pratiques.

L'existence d'un comité d'audit au sein de la filiale contribue à renforcer la relation entre le CA et l'audit interne. Ce comité permet aussi d'assurer l'indépendance des auditeurs.

Comme le préconise la norme 1312 de l'IIA, la direction de l'audit interne est périodiquement évaluée par la direction de l'audit interne du groupe et par la commission bancaire de l'UEMOA. Ces évaluations externes permettent d'effectuer une revue qualité des activités de l'audit interne.

L'audit interne s'appuie sur la réglementation de la commission bancaire de l'UEMOA pour vérifier la conformité avec les dispositions légales réglementaires. Aussi, elle a mis en place un système de suivi de la mise en œuvre des recommandations.

6.2.2.2 le système de management des risques

L'utilisation de la cartographie des risques permet d'orienter l'audit interne sur les zones du SI à fort potentiel de risque. Lors des missions d'audit, l'évaluation du contrôle interne est basée sur une approche par les risques. Ceci permet à l'audit interne de contribuer à l'efficacité du processus de management des risques et du contrôle interne.

6.2.2.3 la réalisation des audits d'efficacité

L'audit interne ne vérifie pas uniquement la bonne application des procédures, de la réglementation et des législations en vigueur en matière de système d'information. Elle effectue aussi des audits d'efficacité afin de s'assurer que les procédures et dispositifs de contrôle interne sont opportuns et permettent d'atteindre les objectifs SI.

6.2.2.4 l'apport de la direction générale

La direction générale met à la disposition de l'audit interne les moyens financiers nécessaires à la réalisation de son programme d'activités. Elle veille également auprès des audités à la mise en œuvre des recommandations formulées par la direction de l'audit interne.

6.2.3 Les faiblesses de la GSI

Comme faiblesses, nous pouvons mentionner :

- l'absence d'évaluation de la satisfaction de la clientèle externe. La division de la technologie établit les SLA qu'avec sa clientèle interne alors qu'elle fournit des services automatisés tels que la banque par internet, les produits électroniques, les transferts de paiement...L'observation nous a permis de constater des plaintes formulées par des clients externes pour des dommages causés par le dysfonctionnement des DAB et de l'e-banking ;
- l'inexistence de Maitre d'Ouvrage pour servir d'interface entre les directions métiers et la division de la technologie ;
- l'absence d'un IT Scorecard. Ce tableau de bord prospectif permet de formuler des indicateurs de rentabilité, de satisfaction de la clientèle, d'amélioration des processus et de compétences humaines.

6.2.4 Les faiblesses de l'implication de l'audit interne dans la GSI

Lors de notre étude, nous avons constaté quelques insuffisances de l'implication de l'audit interne dans la GSI au sein d'EBF.

6.2.4.1 L'absence d'audit de management

L'un des rôles de l'audit interne dans la GSI est d'effectuer des audits stratégiques afin d'analyser les choix stratégiques, la cohérence des politiques à long terme et d'évaluer les ressources et processus mis en œuvre. C'est un audit qui permet de contribuer à l'amélioration du management stratégique. L'entretien avec la direction de l'AI a permis de mentionner l'absence de ce type d'audit.

6.2.4.2 l'insuffisance des moyens techniques

L'audit interne d'EBF dispose d'une charte d'audit, d'une cartographie des risques mais ne dispose pas encore de manuel de procédure car il est toujours en phase d'élaboration. Aussi, nous avons pu noter l'absence de manuel d'audit.

Cette formalisation insuffisante de procédure ne permet pas à l'audit interne de disposer de référentiel aussi bien pour ses missions d'audit financier que celles du SI.

6.2.4.3 les insuffisances dans l'évaluation de la performance du SI

L'audit interne évalue les SLA mais n'évalue pas la pertinence des objectifs et des indicateurs de l'IT Scorecard en raison de son inexistence. Nous notons aussi l'absence d'audit qualité du SI alors qu'il permet d'évaluer la qualité du service fourni par la division de la technologie ainsi que l'efficacité et l'efficience des processus du SI.

L'identification des forces et faiblesses de l'intervention de l'audit interne dans la gouvernance du système d'information nous permet de faire des propositions visant à corriger les insuffisances constatées afin de contribuer à l'émergence d'un audit interne à forte valeur ajoutée.

6.3 Les recommandations

Les propositions d'actions sont formulées à l'endroit du chef de la division technologie qui est un acteur essentiel de la gouvernance du système d'information, de la direction générale et de l'audit interne qui exécute des missions de conseils.

6.3.1 Recommandations pour la division de la technologie

La division de la technologie a conçu un questionnaire d'enquête de la satisfaction de la clientèle qui n'a pas encore été administré aux clients internes. Elle devra améliorer ce questionnaire en incluant les indicateurs d'assistance bureautique (délai et taux de résolution des incidents, la prise en compte des demandes d'assistance). Des indicateurs d'accessibilité et de disponibilité des infrastructures et de l'architecture du SI peuvent être inclus car l'inaccessibilité et l'indisponibilité du système peut freiner la réalisation et l'optimisation des opérations.

La division de la technologie peut également élaborer un questionnaire de satisfaction à administrer à sa clientèle externe afin de recueillir son niveau de satisfaction par rapport à la qualité du système ainsi que leurs attentes.

Nous proposons également à la division de la technologie la mise en place d'une cellule de veille technologique qui sera chargée de suivre les évolutions technologique du marché.

6.3.2 Recommandations pour la direction générale

Nous proposons à la direction générale de collaborer davantage avec la division technologie pour mieux assurer l'alignement stratégique.

Aussi, la direction peut désigner dans chaque direction métier, un Maître d'Ouvrage (MOA) chargé d'élaborer le cahier de charge (définition des besoins de l'activité en terme d'informatique) et formaliser les forces et faiblesses des applications informatiques qu'ils utilisent. Il sera l'interface entre les utilisateurs et la division de la technologie

Nous suggérons également de mettre à la disposition de la division de la technologie des ressources humaines suffisantes pour être en conformité avec les bonnes pratiques qui préconisent un informaticien pour 15 utilisateurs et pour couvrir le besoin en ressources humaine du service de sécurité informatique.

Certes, l'effectif de la direction de l'audit interne respecte le taux proportionnel à l'effectif total des agents fixé par le groupe mais avec le développement de la banque et l'automatisation des activités, les risques sont de plus en plus présents et il s'avère nécessaire de doter cette direction de ressources humaines supplémentaires.

En plus des ressources humaines, la direction générale doit également envisager l'acquisition de la fibre optique qui permettra d'améliorer la disponibilité et la rapidité de l'application bancaire FLEXCUBE.

6.3.3 Recommandations pour la direction de l'audit interne

Nous suggérons à la direction de l'audit interne de veiller à la formalisation du manuel de procédure qui est un outil indispensable pour les audits de conformités, à la formalisation du manuel d'audit afin de doter les auditeurs débutants d'instruments de formation.

Nous préconisons également d'effectuer des audits stratégiques afin d'évaluer les stratégies mises en place et contribuer davantage à l'amélioration de l'alignement stratégique.

L'audit interne peut également recommander à la division de la technologie l'élaboration d'un IT Scorecard afin de pouvoir évaluer la pertinence des indicateurs. Il doit effectuer des audits qualité pour l'évaluation de la performance du système d'information.

Nous proposons à l'audit interne de recommander au contrôle interne la mise en place d'un système de badge électronique et d'un dispositif anti-inondation afin d'assurer une meilleure gestion des accès dans les salles d'archivage et de machine puis pour assurer la sécurité environnementale des salles machines. Le contrôle interne doit également veiller à la mise en place et/ou l'activation des vidéos au sein d'EBF et des DAB/GAB.

L'étude du rôle de l'audit interne dans la GSI nous a permis de décrire le fonctionnement de ses différentes composantes au sein d'EBF et de mettre en exergue les relations qui existent entre l'audit interne et chacune de ses variables. Le rapprochement avec le référentiel COBIT nous a permis de faire ressortir les forces et les faiblesses de l'intervention de l'audit interne dans la GSI et de formuler des recommandations à l'endroit de l'audit interne mais aussi de la direction générale et de la division de la technologie.

CESAG - BIBLIOTHEQUE

CONCLUSION DE LA DEUXIEME PARTIE

Dans le domaine bancaire tout comme en entreprise, l'information est à la fois la source et le véhicule des décisions de gestion. L'étude du rôle de l'audit interne dans la gouvernance du système d'information d'Ecobank Burkina nous a permis de prendre connaissance de l'organisation de la banque et de ses activités. Elle nous a également permis de décrire le processus de GSI et d'analyser les relations qui existent entre l'audit interne et chaque composante de cette gouvernance.

En rappel, nous avons comme objectif d'analyser les différentes relations de l'audit interne dans la GSI d'Ecobank Burkina et de mettre en exergue les forces et les faiblesses de ces relations. L'utilisation des différents outils nous ont permis d'effectuer cette analyse et d'identifier les points forts et les points faibles. Les forces qui ressortent de cette analyse sont entre autre le respect des bonnes pratiques, le système de management des risques et la réalisation d'audit d'efficacité. Comme faiblesses, nous pouvons mentionner l'absence de manuel de procédure et de manuel d'audit, la non réalisation d'audits stratégiques et de qualité du système d'information.

L'identification des forces et faiblesses a permis de formuler des recommandations à l'endroit de l'audit interne, de la division de la technologie qui est un acteur primordiale de la GSI et à de la direction générale chargée de la formulation des stratégies. Les recommandations formulées à l'endroit de la direction de l'audit interne, une fois mise en œuvre permettront d'améliorer sa contribuer à la GSI.

CONCLUSION GENERALE

CESAG - BIBLIOTHEQUE

Avec les évolutions technologiques, le système d'information est devenu le quatrième facteur de production des entreprises en particulier des banques dont l'activité est fortement automatisée. La gestion des flux informationnels occupe une place considérable dans le pilotage des activités bancaires d'où la nécessité d'optimiser le système d'information.

Le problème précédemment posé était de faire de la gouvernance du système d'information un outil de pilotage et d'amélioration des performances. Pour palier à ce problème, nous avons proposé de faire intervenir l'audit interne dans la gouvernance du système d'information car il peut être un outil de création de valeur et d'amélioration de la performance.

Pour mener l'étude sur le rôle de l'audit interne dans la GSI, nous avons pris connaissance des aspects théoriques et des relations qui existent entre ces deux variables. Il est ressorti de ces aspects théoriques que l'audit interne peut effectivement contribuer à faire de la GSI un outil de pilotage car il apporte des conseils pour assurer et améliorer l'alignement stratégique. Il effectue des missions d'audit de conformité du système d'information afin de s'assurer non seulement du respect des procédures, des dispositions légales et règlements en vigueur et évalue les risques liés au système d'information. Aussi, l'audit interne contribue à l'amélioration de la performance du système d'information car il évalue la pertinence des indicateurs et réalise des missions d'audit qualité.

A partir de la revue de la littérature, nous avons formulé des hypothèses traduites par le modèle d'analyse et élaboré des outils afin de vérifier ces hypothèses sur le terrain. Ces hypothèses étaient au nombre de trois à savoir :

- l'audit interne analyse l'alignement stratégique ;
- l'audit interne évalue les risques du système d'information ;
- l'audit interne évalue la performance du système d'information.

L'étude du cas pratique a porté sur Ecobank Burkina. Les données issues de l'analyse documentaire, des entretiens et questionnaires ont permis de prendre connaissance des activités et de l'organisation de la banque et de vérifier si nos hypothèses étaient confirmées ou infirmées.

En effet, au sein d'Ecobank Burkina, la direction de l'audit interne évalue l'adéquation de la stratégie IT avec la stratégie business et apporte des conseils pour améliorer cette adéquation ;

il effectue des missions de conformité et d'efficacité du système d'information. Ces missions concernent les applications, le réseau, la sécurité des données et des locaux, la banque électronique...Cependant, l'objet de l'audit interne d'Ecobank Burkina n'est pas d'évaluer la performance du système d'information. Il évalue uniquement les contrats de niveau de service définis entre la division de la technologie et les différentes directions pour s'assurer que les indicateurs des contrats sont mesurables, réalisables et pertinents.

Seules les deux premières hypothèses à savoir l'audit interne analyse l'alignement stratégique et l'audit interne évalue les risques du système d'information sont confirmées. L'hypothèse selon laquelle l'audit interne évalue la performance du système d'information est quant à elle infirmée.

L'audit interne d'Ecobank Burkina pourrait donc mieux contribuer à la gouvernance du système d'information en évaluant la pertinence des indicateurs de l'IT Scorecard dont nous avons suggéré la mise en œuvre et en réalisant des audits qualité.

L'étude du thème sur le rôle de l'audit interne dans la gouvernance des systèmes d'information nous a permis d'acquérir des connaissances en matière de système d'information tant sur le plan théorique que pratique. Elle permet également à l'audit interne d'Ecobank Burkina, à partir de nos recommandations une fois prise en considération, de contribuer davantage à la GSI et de faire de cette gouvernance un outil de pilotage. Toutefois, notre étude présente certaines limites liées à l'obtention des informations en raison de la confidentialité des données, de l'inaccessibilité à la direction générale et aux applications bancaires. Nous n'avons également pas pu prendre part aux missions d'audit du système d'information lors de notre passage à Ecobank Burkina.

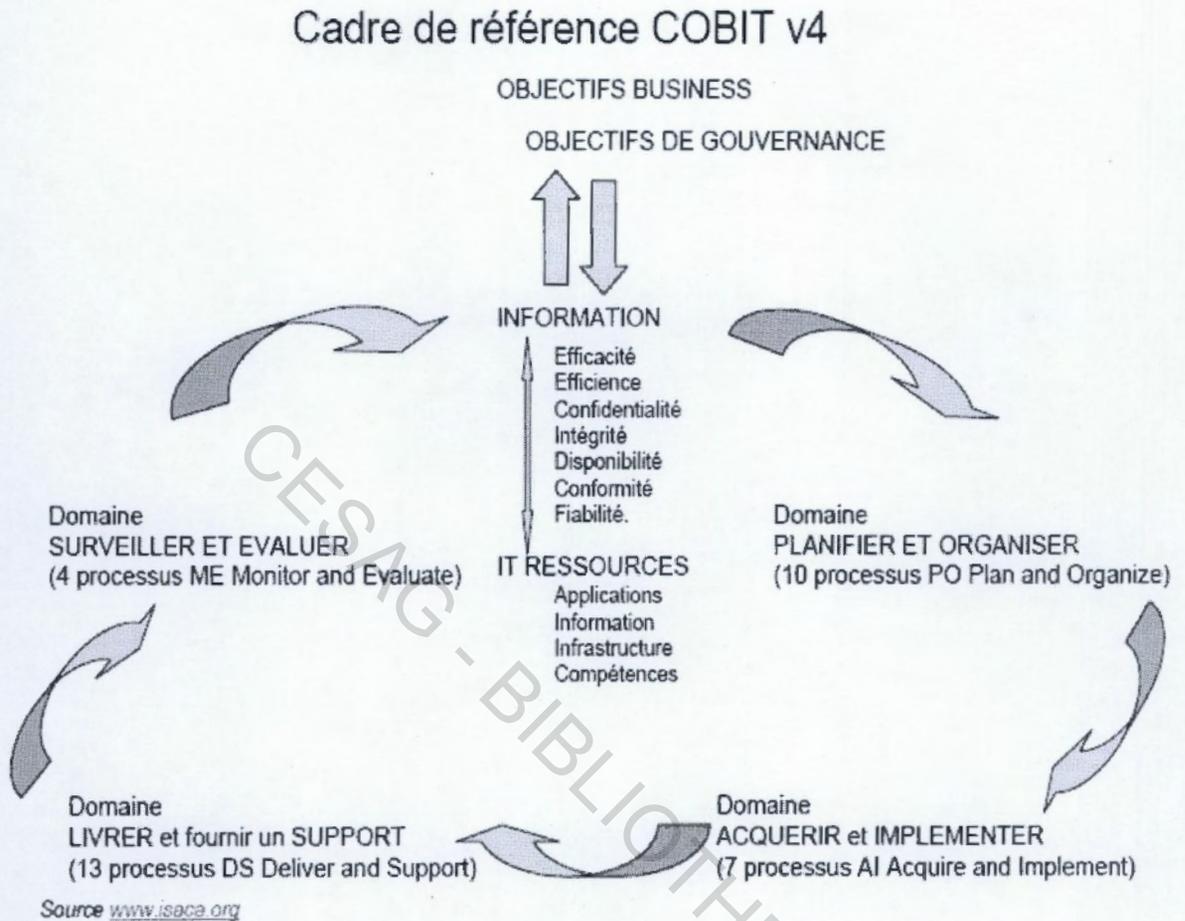
Nous ne pouvons épuiser tous les aspects concernant l'audit et la gouvernance des systèmes d'information, nous ouvrons seulement la voie à d'autres chercheurs qui pourront compléter notre travail sur ce thème.

Avec la migration récente du système d'information d'Ecobank Burkina, nos recherches futures s'articuleront autour de l'audit de la gestion des comptes clients dans le nouveau système d'information d'Ecobank Burkina.

ANNEXES

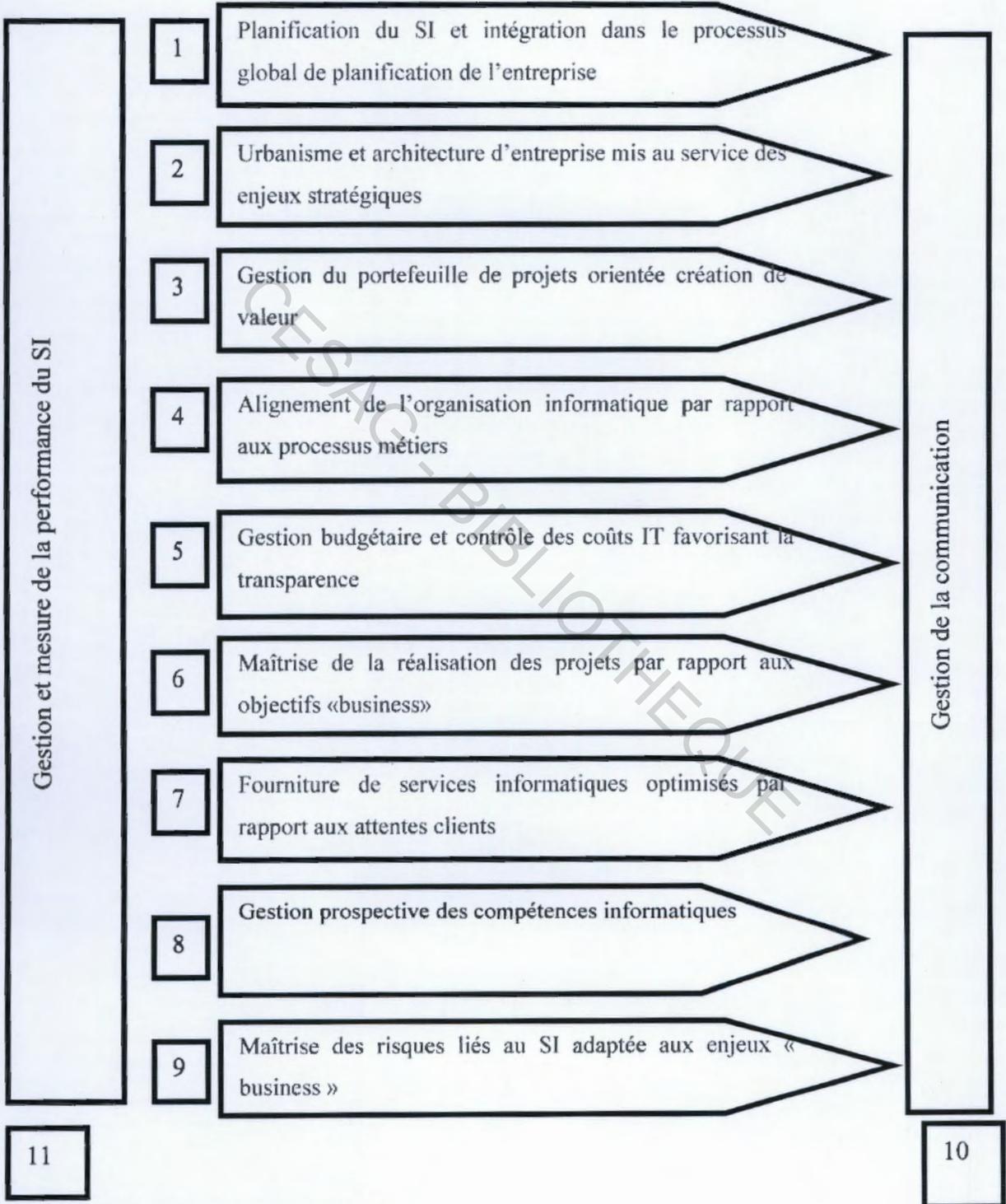
CESAG - BIBLIOTHEQUE

ANNEXE 1 : Structure du cadre de référence COBIT 4



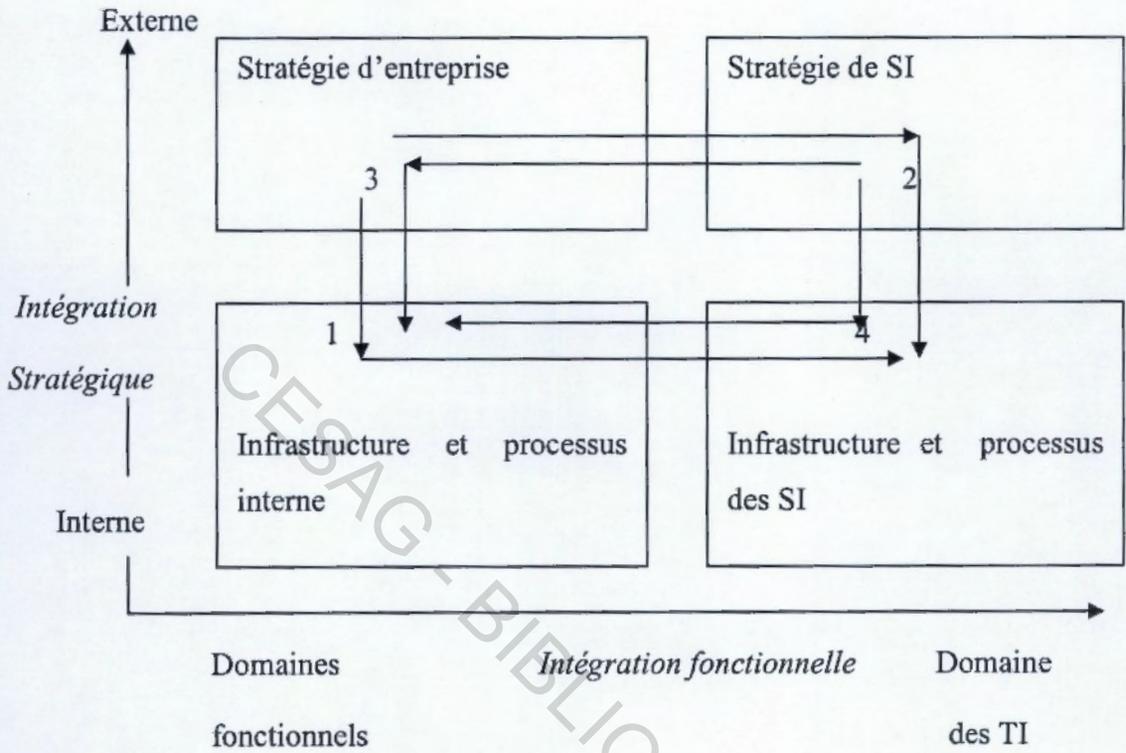
Source : Bergerot Dominique (2007: 12)

ANNEXE 2 : le schéma des outils de la mise en œuvre des bonnes pratiques



Source : Leignel Jean-Louis (2011:7)

ANNEXE 3: la figure de l'alignement stratégique du système d'information, le modèle d'Henderson et Venkatraman



Source : Delmond (2008 :137)

ANNEXE 4 : guide d'entretien adressé au chef de division

Dans le cadre des travaux de notre mémoire sur le rôle de l'audit interne dans la gouvernance des systèmes d'information, nous souhaitons par le canal de ce guide d'entretien, obtenir des informations auprès de vos services habilités.

I-Stratégie et objectifs du SI

1. Quels sont les objectifs et stratégies en matière de système d'information?
2. Comment les stratégies ont-elles été définies?
 - a) en fonction de l'environnement bancaire et des évolutions technologiques?
 - b) selon les besoins des utilisateurs?
 - c) autres
3. EBF se conforme-t-il à un cadre de référence pour maîtriser les TI?
Si oui lequel

II- Gestion des ressources

1. La DSI dispose-t-elle de ressources humaines suffisantes pour faire face aux besoins des utilisateurs?
2. Les informaticiens bénéficient-ils de formations permanentes?
3. La DSI dispose-t-elle d'un plan d'infrastructure ?
4. La DSI effectue-t-elle des enquêtes de satisfaction de la clientèle interne?

III- Accessibilité

1. Existe-t-il une politique de contrôle des accès
2. Avez-vous enregistré des incidents dus aux accès non autorisés
3. Si oui, quel est le nombre actuel de ces incidents dus aux accès non autorisés

IV- Sécurité

1. L'information est-elle disponible qu'aux seuls destinataires?
2. Existe-t-il un système de traçabilité des manipulations?
3. Existe-t-il un dispositif de gestion de la sécurité physique et environnementale?
4. Existe-t-il des plans de secours?

5. Le serveur de données, le serveur d'application et le serveur de messagerie sont-ils séparés?
6. Existe-t-il un plan de continuité?

V- Gestion des incidents

1. Avez-vous enregistré des incidents dus aux TI?
si oui, quel est la nature et le nombre actuel de ces incidents
2. Si vous recevez deux demandes de services émanant d'un responsable et d'un agent relatives respectivement à un problème hardware et à problème de dysfonctionnement du système, quelle sera votre réaction?
3. Quelle est le temps de réponse moyen aux demandes de services relatifs aux incidents?

VI- Gouvernance du Système d'Information (GSI)

1. Qu'en est-il de la GSI au sein D'EBF? Nous décliner les grandes lignes.
2. Qui sont les acteurs et quels sont les rôles et les responsabilités?
3. La banque dispose-t-elle de référentiels de bonnes pratiques? Si oui lesquels?
4. L'audit interne contribue t-il à la GSI? Si oui, quel est son rôle?
5. Les objectifs et stratégies SI sont-il toujours en cohérence avec ceux de l'entreprise?
Pouvez-vous nous fournir une évidence ?
6. Quels sont les risques informatiques auxquels vous faites face?
7. Existe t-il un système de prévention, de détection et de traitement de ces risques?
8. Mettez vous en œuvre les pratiques de la GSI?
9. Elaborez-vous un plan stratégique des SI ?
10. Quels sont les FCS relatifs à la qualité des prestations de service de l'informatique?
 - a) la disponibilité des infrastructures
 - b) la clarté du SI
 - c)accessibilité et intégrité de la base de donnée
 - d) la sécurité logique et la sécurité des locaux
11. Utilisez-vous un IT scorecard? Si oui, quels sont les indicateurs de mesure de la performance du SI?

ANNEXE 5: guide d'entretien adressé au Directeur de l'Audit Interne

Dans le cadre des travaux de notre mémoire de fin d'étude sur le rôle de l'audit interne dans la gouvernance des systèmes d'information, il s'avère nécessaire pour nous de nous entretenir avec vous car étant au cœur de notre étude. Cet entretien portera sur l'organisation de votre direction et sur les différents rôles que vous jouez dans cette gouvernance ce qui nous permettra de faire un rapprochement avec les bonnes pratiques.

I- Organisation et fonctionnement de l'audit interne

1. Quel est le niveau de rattachement hiérarchique de l'audit interne ?
2. Quelles sont vos relations avec le comité d'audit, le conseil d'administration et la direction générale ?
3. Ce niveau assure-t-il l'indépendance des auditeurs?
4. Quels sont les missions et objectifs de l'audit interne ?
5. Quel est l'effectif de l'audit interne ?
6. Les auditeurs sont-ils spécialisés? Si oui quels sont les différents domaines?
7. Quel est le champ d'application de l'audit interne?
8. Disposez-vous d'un plan d'audit?
9. Avez-vous un planning des missions?
10. Quels sont les types de missions effectués?

II-Rôles de l'audit interne dans la GSI

1. L'audit interne s'intéresse-t-il à la GSI? Si oui, quelle est sa relation avec les acteurs de la GSI?
2. L'audit interne s'appuie-t-il à un cadre de référence pour jouer son rôle dans cette gouvernance? Si oui, quel est ce cadre?
3. L'audit interne se conforme-t-il à la norme 2110 A2 de l'IIA qui stipule que l'audit interne doit évaluer si la GSI soutient la stratégie et les objectifs de l'organisation?
4. Si oui, quelles sont les diligences mises en œuvre?
5. Les auditeurs internes se réfèrent-ils aux normes d'audit du système d'information de l'ISACA? Si oui, à quelles normes se réfèrent-ils lors d'un audit du système d'information

6. L'audit interne joue-t-il un rôle dans l'alignement stratégique? Évalue-t-il le plan stratégique du système d'information?
7. Comment intervient-il dans l'évaluation de l'alignement stratégique et du plan stratégique
8. Est-il prévu dans le planning des missions d'effectuer des missions d'audit du système d'information? Si oui, quelle est la nature de ces missions? Sont-elles prévues par fonction informatique?
9. Effectuez-vous des audits de conformité sur le système d'information? Si oui, la vérification de la conformité se fait-elle par rapport au COBIT?
10. Utilisez-vous le guide d'audit des SI qui permet une bonne utilisation du COBIT?
11. Si non, quelles sont les diligences mises en œuvre lors d'un audit de conformité?
12. L'audit interne s'assure-t-il également du respect de la réglementation bancaire définie par la commission bancaire de l'UEMOA sur l'audit des SI?
13. Quel type d'approche utilisez-vous lors d'un audit SI ?
14. Quels sont les différents types de risques liés au système d'information?
15. L'audit interne évalue-t-il la performance du SI? Si oui, comment procède-t-il?

ANNEXE 6: questionnaire d'évaluation de la contribution de l'audit interne dans la gouvernance des systèmes d'information

Dans le cadre des travaux de notre mémoire sur le rôle de l'audit interne dans la gouvernance des systèmes d'information, nous souhaitons par le canal de ce guide d'entretien, obtenir des informations auprès de vos services habilités.

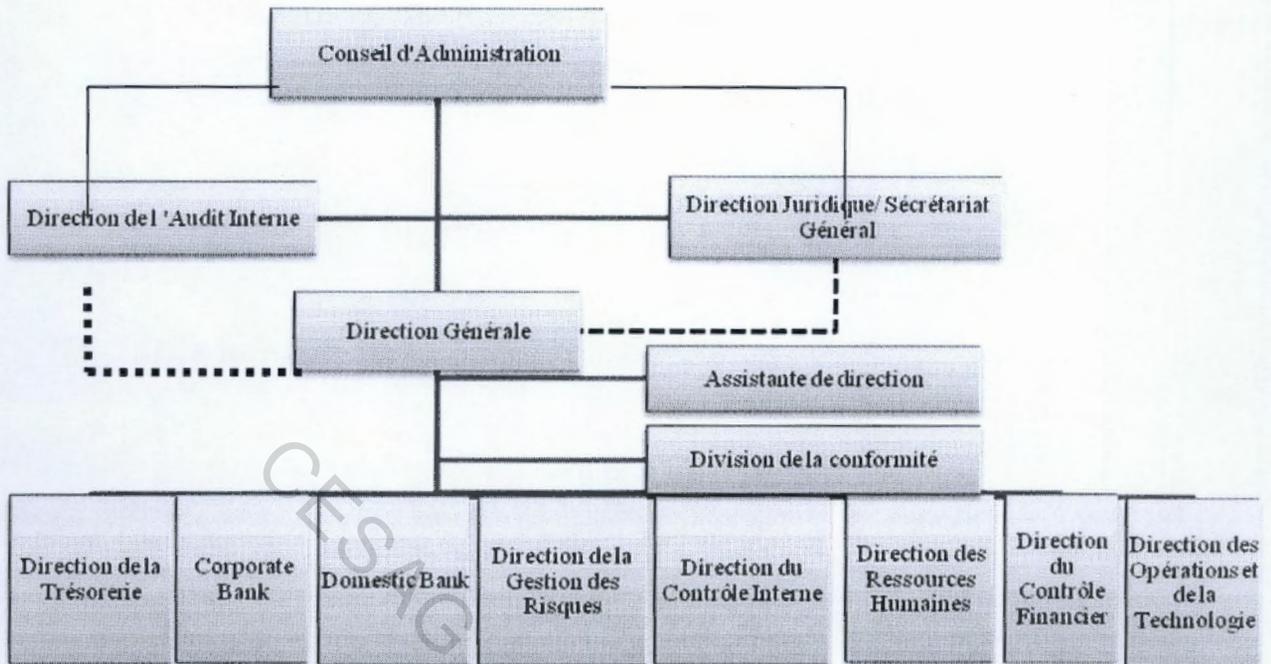
	OUI	NON
Relation de l'audit interne avec les acteurs de la GSI		
Existe-t-il une relation entre l'audit interne et les acteurs de la GSI ? Si oui, quel est le nombre de réunions auxquelles l'audit interne a participé ?	X	
Les missions d'audits du SI		
1- Effectuez-vous plusieurs types d'audit (audit des applications, sécurité, audit réseau, audit projet...) sur le système d'information? Si oui, lesquels et quel est le type et le nombre de missions figurant sur le planning des missions ?	X	
2- Figure-t-il sur le planning des missions recommandées et des missions inopinées sur le SI ?		X
Ressources de l'audit interne		
1- Disposez-vous d'auditeurs SI ? Si oui combien sont-ils	X	
2- Quelle est l'expérience des auditeurs SI		
3- L'audit interne dispose-t-il d'un manuel de procédure		X
4- L'audit interne dispose-t-il d'une cartographie des risques ? si oui, quels sont les risques liés au système d'information ?	X	
Recommandations		
1- La direction générale approuve-t-elle toujours les recommandations ?		X
2- La direction générale veille-t-elle à la mise en œuvre des recommandations ? si oui, quelle est la proportion des recommandations mises en œuvre ?	X	
3- Existe-t-il un système de suivi de la mise en œuvre des plans d'actions ?	X	

ANNEXE 7: Questionnaire adressé aux chefs d'agence

Dans le cadre des travaux de notre mémoire qui porte sur le rôle de l'audit interne dans la gouvernance des systèmes d'information, nous sollicitons un peu de votre temps pour renseigner ce questionnaire qui nous permettra d'avoir une connaissance plus approfondie du système d'information.

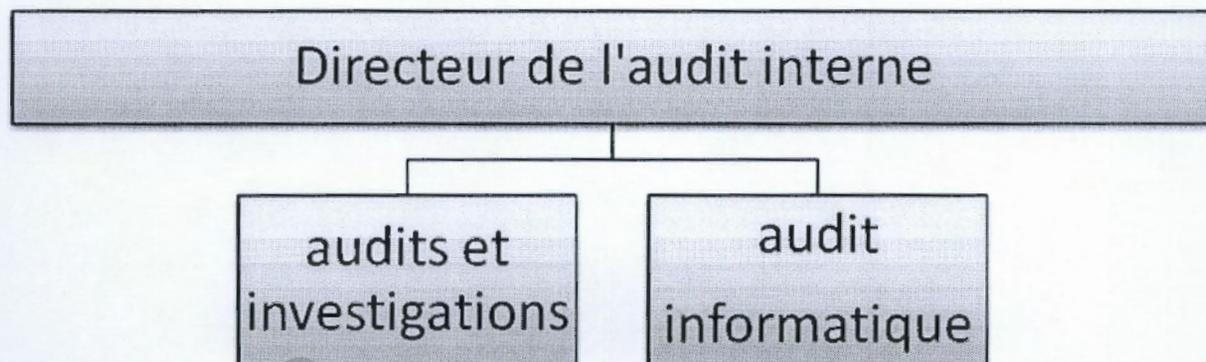
	OUI	NON
confidentialité des données		
Les mots de passe et l'identifiant permettent-ils d'assurer la confidentialité de vos données?		
accessibilité et disponibilité des données		
La connexion est-elle permanente? Si non, connaissez-vous régulièrement des pannes ou arrêts ou dysfonctionnement de FLEXCUBE? Ces pannes/arrêts/dysfonctionnement sont-ils: a) fréquents b) périodiques ces pannes vous sont-elles préjudiciables? Le système est-il disponible pendant les plages horaires de service?		
gestion des incidents		
La Direction des Opérations et de la Technologie (DOT) prend-t-elle toujours en compte vos demandes d'assistance? La DOT répond-t-elle à vos demandes de service liés aux incidents? Si oui, réagit-elle dans a) l'immédiat b) des jours après c) à préciser		
pertinence et fiabilité		
FLEXCUBE répond-t-il à vos attentes? est-il exempté d'erreurs? La gestion des accès (système d'authentification, sécurité des locaux informatique et interconnexion avec le réseau interne) garantit-elle la fiabilité des informations produites		

ANNEXE 8 : l'organigramme d'Ecobank Burkina (janvier 2011)



Source : direction des ressources humaines d'Ecobank Burkina

ANNEXE 9: organigramme de la direction de l'audit interne (janvier 2011)



Source : direction de l'audit interne d'Ecobank Burkina

CESAG - BIBLIOTHEQUE

BIBLIOGRAPHIE

CESAG BIBLIOTHEQUE

I-Ouvrages

1. AFAI (2008), *contrôle interne et système d'information*, 2^{ème} édition, Paris, 55 pages.
2. Angot Hugues (2004), *système d'information de l'entreprise*, 4^{ème} édition, Les Editions de Boeck Université, Bruxelles, 197 pages.
3. Angot Hugues, Ischer Christian (2004), *audit comptable, audit informatique*, Editions de Boeck université, Bruxelles, 301 pages.
4. Autissier David, Delaye Valérie (2008), *mesurer la performance du système d'information*, Editions d'Organisation, Paris, 214 pages.
5. Autissier David, Lourdier Fabienne, Bensebaa Faouzi (2007), *l'atlas du management*, Editions d'Organisation, paris, 479 pages.
6. Barbier Etienne (1999), *mieux piloter et mieux utiliser l'audit*, Maxima, Paris, 132 pages.
7. Baumard Philippe, Benvenuti Jean-André (1998), *compétitivité et systèmes d'information*, Dunod, Paris, 245 pages.
8. Berland Nicolas, Simon François-Xavier (2010), *le contrôle de gestion en mouvement*, Editions d'organisation, paris, 291 pages.
9. Bernard Frédéric, Salviac Eric (2009), *fonction achat : contrôle interne et gestion des risques*, Maxima, Paris, 298 pages.
10. Bertin Elizabeth (2007), *audit interne : enjeux et pratiques à l'international*, Editions Eyrolles, Paris, 320 pages.
11. Bohnké Sabine (2010), *moderniser son système d'information*, Editions Eyrolles, Paris, 283 pages.
12. Bounfour Ahmed, Georges Epinette, *valeur et performance des systèmes d'information*, Dunod, paris, 2006, 258 pages.
13. Delmond Marie Hélène, Petit Yves, Gautier Jean-Michel (2008), *management des systèmes d'information*, 2^{ème} édition, Dunod, Paris, 256 pages
14. Dumont Christian (2007) ° *ITIL, pour un service informatique optimal*, 2^{ème} édition, Eyrolles, Paris, 377 pages
15. Fernandez Alain (2001), *le bon usage des technologies expliqué au manager*, Editions d'Organisation, Paris, 342 pages.
16. Fimbel Eric (2007), *l'alignement stratégique*, Editions Pearson, paris, 370 pages
17. Gauzente Claire (2005), *alerte marketing*, Editions de Boeck université, Bruxelles, 161 pages

18. Harakat Mohamed (2011), les finances publiques et les impératifs de la performance, l'Harmattan, Paris, 456 pages.
19. Hemici Farouk, Hénot Christophe (2007), contrôle de gestion, Les Editions Bréal, Paris, 177 pages.
20. IFACI (2007), le dispositif de contrôle interne, 70 pages.
21. IFACI (2009), les normes professionnelles de l'audit interne, 28 pages
22. IFACI (2011), révision des normes professionnelles de l'audit interne, 29 pages.
23. Laudon Kenneth, Laudon Jane, Fimbel Eric, Costa Serge (2010), management des systèmes d'information, 11ème édition, Editions Pearson, paris, 630 pages.
24. Lejeune Gérard et Emmerich Jean Pierre (2007), audit et commissariat aux comptes, Editions Gualino, Paris, 329 pages.
25. Lumbroso Maurice (2007), Microsoft Navision : développez pour l'ERP, Editions Eni, 463 pages.
26. Mandzila Eustache Ebondo (2005), la gouvernance de l'entreprise : une approche par l'audit et le contrôle interne, l'Harmattan, 2005, 349 pages.
27. Moisand Dominique et Garnier De Labareyre Fabrice (2009), pour une meilleure gouvernance des systèmes d'information, Editions Eyrolles, paris, 258 pages.
28. Morley Chantal (2008), management d'un projet système d'information, 6ème édition, Dunod, Paris, 482 pages.
29. Peretti Jean Marie (2010), tous vertueux : pour une performance durable des organisations, Editions d'Organisation, Paris, 285 pages.
30. Pierre Voyer (2006), tableaux de bord de gestion et indicateurs de performance, 2ème édition, Presse de l'Université du Québec, Québec, 446 pages.
31. Pillet Maurice, Martin-Bonnefous Chantal, Courtois Alain (2011), gestion de la production : les fondamentaux et les bonnes pratiques, 5ème édition, Editions d'Organisation, paris, 467 pages.
32. Reix Robert (2004), système d'information et management des organisations, Editions Vuibert, Paris, 486 pages.
33. Renard Jacques et Nussbaumer Sophie (2011), audit interne et contrôle de gestion, Editions d'Organisation, paris, 233 pages.
34. Rivard Suzanne et Talbot Jean (2001), développement des systèmes d'information, 3ème édition, Presse de l'Université du Québec, Québec, 718 pages.
35. Shick Pierre (2007), mémento d'audit interne, Editions Dunod, Paris, 217 pages.

36. Tomas Jean-Louis (2002), ERP et progiciels de gestion intégrés : sélection, déploiement et utilisation opérationnelle, 2ème édition, Dunod, paris, 308 pages.
37. Tonye Arlette (2011), épargnant d'Afrique, inquiétez vous, l'Harmattan, Paris, 256 pages.
38. Tsapi Victor (2009), implications économiques, comptables et fiscales dans le système OHADA, l'Harmattan, Paris, 251 pages.
39. Weill Michel (2011), l'audit stratégique : qualité et efficacité des organisations, AFNOR, 248 pages.

II -Sources internet

40. Leignel Jean-Louis (2011), tutorial, gouvernance du système d'information, www.youscribe.com/catalogue/tous/ressources-professionnelles/informatique/tutorial-gouvernance-du-systeme-d-information-412783.
41. Africa business (2011), le secteur bancaire de l'UEMOA, www.africabusinessmarket.com/actualite/article-895-2-348.html
42. Bergerot Dominique (2007), les outils de la gouvernance, www.adeli.org/webfm_send/417
43. Institut de la gouvernance des systèmes d'information (2005), la place de la gouvernance du système d'information dans la gouvernance générale de l'entreprise, www.cigref.typepad.fr/itgifrance/files/place_gouvernance_SI_dans_gouvernance_generale.pdf.
44. ISACA (2004), les normes d'audit du système d'information, www.isaca.org/Knowledge-Center/.../Standards-IT-French-S1.pdf.