Centre Africain d'Etudes Supérieures en Gestion

CESAG EXECUTIVE
MBA Audit et Contrôle de gestion

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

Promotion 2015 - 2016

Mémoire de fin d'études

THEME

Audit des contrôles généraux informatiques d'une Banque dans le cadre d'une mission de commissariat aux comptes réalisée par le Cabinet Mazars au Sénégal

Présenté par :

M. SYLLA Mohamed

Dirigé par :

M. El Hadji Malick GUEYE
Senior Manager, Département ITAS
Mazars Sénégal

Avril 2019

DEDICACE

"A mes parents, qui m'ont inculqué un esprit de compétitivité, de persévérance et qui m'ont toujours motivé dans mes études. Sans eux, je ne serai, certainement, pas à ce niveau.

- à mes frères et sœurs ;
- à la famille ;
- à tous mes amis.

Merci pour tout !"

REMERCIEMENTS

Nos remerciements vont à l'endroit de :

Mon encadreur, Monsieur El Hadji Malick GUEYE, Senior Manager Responsable du pôle IT Advisory Services au sein du département Consulting de Mazars au Sénégal, pour son encadrement, ses directives, ses remarques constructives, et sa disponibilité.

Ma famille, pour leur soutien indéfectible.

Monsieur Bertin CHABI pour sa collaboration.

Tout le corps professoral et administratif du CESAG, du département CESAG EXECUTIVE, du MBA Audit et Contrôle de gestion pour la qualité et la rigueur de leur travail.

Mes amis de promotion pour ces moments qui resteront à jamais gravés dans ma mémoire.

Tout le personnel du cabinet Mazars au Sénégal pour leurs encouragements continus et leurs aides précieuses.

Et tous les autres.

AVANT-PROPOS

Le CESAG est un Etablissement Public International spécialisé dans la formation, le conseil et la recherche en gestion. Crée en 1985, il s'est rapidement hissé au rang des meilleures écoles de management en Afrique et constitue aujourd'hui une véritable alternative aux grandes écoles de management du Nord. Depuis 1996, le CESAG est placé sous la tutelle de la Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO) pour le compte des Etats de l'Union Economique et Monétaire Ouest Africaine (UEMOA).

A l'occasion de sa réunion du 20 septembre 1996, le conseil des ministres de l'UEMOA a confié à la Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO), la mission de réorganiser le CESAG en vue de favoriser la poursuite et le développement des activités. Depuis lors, le CESAG s'est engagé dans un processus de restructuration et de dynamisation de ses activités pour mieux répondre aux besoins et aux attentes de ses partenaires et clients. L'objectif visé était de doter les pays membres d'une école communautaire capable de former des gestionnaires efficaces tout en tenant compte des réalités de l'environnement africain.

Dirigé par un Directeur Général assisté d'un Secrétaire Général et de Conseillers, le CESAG est doté de deux (2) entités pédagogiques :

- une Direction de la Formation (DF) qui supervise les six (6) écoles spécialisées du CESAG notamment le CESAG EXECUTIVE qui a en son sein le MBA Audit et Contrôle de gestion ;
- une Direction de la Recherche et de la Consultance (DRC) comprenant deux départements.

Celles-ci forment, en étroite collaboration avec les milieux professionnels, des cadres d'entreprises ayant une approche à la fois théorique et pratique des domaines concernés.

Le MBA Audit et Contrôle de gestion qui dure une année est sanctionné par un diplôme. Les managers ont l'obligation d'effectuer des stages pratiques en entreprise qui leur permettent de s'imprégner de l'environnement professionnel.

Pendant ce stage pratique de fin de cycle, le manager a l'obligation de rédiger un mémoire dans lequel, il aura l'occasion de mettre en exergue les aptitudes et qualités acquises pendant son cursus universitaire et professionnel.

.

SIGLES ET ABREVIATIONS

AFAI	:	Association Française d'Audit Informatique
CAC	:	Commissariat aux Comptes
CHAI	:	Comité d'harmonisation de l'audit interne
CISA	:	Certified Information Systems Audito
COBIT	:	Control Objectives for Information and related Technology (Objectifs de contrôle de l'information et des technologies associées)
COSO II	:	Committee Of Sponsoring Organizations of the Treadway Commission
GTAG	:	Global Technology Audit Guide
IFACI	:	Institut Français de l'Audit et du Contrôle Internes
IFACI	:	Institut Français de l'Audit et du Contrôle Internes
ISA	:	International Standards on Auditing
ISACA	:	Information Systems Audit and Control Association
ITAC	:	IT Application Controls (Contrôles généraux applicatifs)
ITGC	:	IT General Controls (Contrôles généraux informatiques)
NIST	:	National Institute of Standards and Technology
SI	:	Système d'information
SIB	:	Système d'information bancaire
TI	:	Technologie de l'information

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ANNEXES

SOMMAIRE

INTRODUCTION GENERALE

Les dernières décennies ont été marquées par l'accessibilité à l'information et à sa place clé dans les organisations. Ces dernières se sont donc lancées dans une politique d'informatisation, et de dématérialisation de leur environnement de travail.

En effet, la forte évolutivité des activités et des métiers a amené les entreprises à développer les systèmes d'information. Ces développements ont été, dans de nombreuses entreprises, un phénomène subi plutôt que volontaire et accompagné. C'est ainsi que M. Lafitte (2003) souligne que « le système d'information est un ensemble complexe, souvent hétérogène car il est constitué d'éléments qui se sont juxtaposés au fil du temps au gré des choix stratégiques, des évolutions technologiques des systèmes informatiques mis en place, du développement de l'organisation elle-même ».

Dans ce contexte, les entreprises s'exposent à de nouveaux risques inhérents à la mise en place de systèmes d'information de plus en plus complexes : coûts financiers de projets informatiques interminables, indisponibilité des systèmes d'information susceptible d'interrompre l'activité de l'entreprise, qualité des données comptables ne garantissant pas la fiabilité des états financiers, mais aussi l'accès à des informations confidentielles et risques de fraudes ou de malversations.

Par conséquent, chaque organisation doit établir un audit de son environnement informatique périodiquement afin de garantir que son système d'information est :

- sécurisé ;
- fiable ;
- pérenne ;
- disponible ;
- efficient.

Au regard de l'application de la norme ISA 315, le Commissaire aux Comptes (CAC) doit spécifiquement prendre connaissance des procédures déployées par l'entreprise dans le cadre de la gestion des risques inhérents à ses systèmes informatiques. Il doit ainsi identifier et évaluer les contrôles généraux mis en œuvre pour maîtriser ces risques afin de garantir la sincérité des états financiers, la validité de la pertinence et de la qualité de l'information financière.

De ce fait, un audit des contrôles généraux informatiques d'une Banque dans le cadre d'une mission de Commissariat aux Comptes réalisée par le cabinet Mazars au Sénégal est nécessaire afin de détecter et de prévenir les risques liés à l'environnement informatique de l'institution financière. La problématique de maitrise des contrôles généraux informatiques de la Banque est résolue à travers le référentiel COBIT (Control Objectives for Information and related Technology) qui est un cadre de référence ainsi qu'un ensemble d'outils jugés indispensables pour assurer la maitrise et le suivi (audit) de la gouvernance du système d'information (SI).

Dans le cadre de notre étude la question fondamentale que l'on pourrait se poser est : quel est l'appréciation du Cabinet Mazars au Sénégal sur le niveau de maîtrise des contrôles généraux informatiques de la Banque ?

Il s'agira spécifiquement de savoir :

- comment le Cabinet Mazars au Sénégal évalue le contrôle interne de l'environnement informatique de la Banque?
- quels sont les contrôles généraux de l'environnement informatique de la Banque évalués par le Cabinet Mazars au Sénégal ?

- quelle est la typologie des risques identifiés par le Cabinet Mazars au Sénégal auxquels s'expose la Banque ?

Pour répondre à toutes ces questions, nous avons décidé d'étudier le thème suivant : « Audit des contrôles généraux informatiques d'une Banque, dans le cadre d'une mission de commissariat aux comptes réalisée par le cabinet Mazars au Sénégal ».

L'objectif principal de cette étude consiste à apprécier les dispositifs de contrôles généraux de l'environnement informatique de la Banque et de pouvoir cerner les risques qui en découlent.

Comme objectifs spécifiques, il s'agira :

- d'identifier, analyser et évaluer des risques généraux informatiques inhérents, prendre connaissance des contrôles relatifs aux sous-thèmes : sécurité physique, sécurité logique, gestion du changement, gestion de l'exploitation, gestion de la sauvegarde et de la continuité d'activité ;
- d'effectuer des tests de contrôles en termes de conception et d'efficacité opérationnelle ;
- d'émettre des recommandations permettant d'améliorer l'environnement informatique.

Cette étude présente plusieurs centres d'intérêts dont :

- Pour l'entreprise :

Cette étude permettra à l'entreprise d'améliorer, de renforcer et de maitriser ses risques.

- Pour le cabinet :

Cette étude permettra d'améliorer son expérience dans l'audit des contrôles généraux informatiques dans le secteur bancaire.

- Pour nous-mêmes :

Cette étude sera pour nous, l'occasion de mettre en application les connaissances théoriques académiques, de nous familiariser aux méthodes utilisées dans ce type de mission par un cabinet d'audit.

- Pour le lecteur :

Ce mémoire est un moyen pour tout lecteur d'avoir une compréhension de l'audit des contrôles généraux informatiques d'une banque.

Ainsi, notre étude est structurée en deux grandes parties :

- une première partie portera sur la revue littérature, le cadre méthodologique et la présentation de l'entité ;
- une deuxième partie dans laquelle sera abordé le cadre pratique de l'audit des contrôles généraux informatiques de la Banque et d'apporter des recommandations pratiques.

PREMIERE PARTIE :

CADRE THEORIQUE ET METHODOLOGIQUE DE L'ETUDE SUR L'AUDIT DES CONTRÔLES GENERAUX INFORMATIQUES D'UNE BANQUE DANS LE CADRE D'UNE MISSION DE COMMISSARIAT AUX COMPTES, ET PRESENTATION DE LA BANQUE

INTRODUCTION DE LA PREMIERE PARTIE

Cette première partie intitulée cadre théorique de l'étude est divisée en deux (2) chapitres. Dans le premier chapitre, nous nous intéressons aux fondements théoriques de l'audit des contrôles généraux informatiques. Ensuite, le deuxième chapitre va porter sur la présentation de la Banque et, celle de la méthodologique de recherche.

CHAPITRE 1 : CADRE THEORIQUE DE L'AUDIT DES CONTRÔLES GENERAUX INFORMATIQUES D'UNE BANQUE DANS LE CADRE D'UNE MISSION DE COMMISSARIAT AUX COMPTES

Ce chapitre nous permettra d'aborder dans un premier temps les concepts liés aux contrôles généraux informatiques. Une présentation de l'approche d'audit sera faite dans un second temps.

1.1. Cadre conceptuel sur l'audit des contrôles généraux informatiques d'une Banque dans le cadre d'une mission de commissariat aux comptes

1.1.1. Définitions

1.1.1.1. Le système d'information

Selon REIX & al. (2011 : 5), le système d'information peut se définir comme « un ensemble organisé de ressources : matériel, logiciel, personnel, données, procédures... permettant d'acquérir, de traiter, de stocker des informations dans et entre des organisations».

Pour la CHAI, le système d'information est l'un des outils qui permet à l'organisation d'atteindre ses objectifs. Il ne se justifie qu'en tant que soutien des processus « métiers », sans lesquels il n'a aucun sens. Il doit donc être aligné avec les objectifs stratégiques de l'organisation. Cet alignement stratégique est fondamental : désormais, un système d'information est un facteur déterminant de la performance (efficacité, efficience, maîtrise des risques) d'une organisation. Inversement, un système d'information inadapté ou mal maîtrisé peut être une source inépuisable de difficultés.

1.1.1.2. Le risque

Selon la norme ISO31000:2009, le risque est la combinaison de la probabilité et des conséquences d'un évènement.

Selon le NIST (National Institute of Standards and Technology), le risque se définit comme suit : « Impact(s) néfaste(s) susceptibles de toucher les opérations (missions, fonctions, image, réputation) ou les actifs d'une organisation, les individus ou d'autres organisations etc. vu le potentiel d'accès, d'utilisation, de divulgation, de perturbation, de modification ou de destruction sans autorisation de l'information et/ou des systèmes d'information. »

Pour que les systèmes d'information atteignent pleinement les objectifs en matière d'avantages, de risques et d'optimisation des ressources, il est essentiel d'évaluer et de contrôler les risques qui pourraient empêcher l'atteinte de ces objectifs.

1.1.1.3. Le contrôle interne

Selon l'IFACI (Institut Français de l'Audit et du Contrôle Internes), le contrôle interne est un dispositif de la société, défini et mis en œuvre sous sa responsabilité. Le COSO (Committee Of Sponsoring Organizations of the Treadway Commission) définit le contrôle interne comme un processus mis en œuvre par la direction générale, le management, et autre personnel d'une organisation, destiné à fournir une assurance raisonnable quant à la réalisation des objectifs entrant dans les catégories suivantes :

- efficacité et optimisation des opérations ;
- fiabilité des informations financières ;
- conformité aux lois et réglementations en vigueur.

Il se compose de cinq composants fortement liés entre eux:

- environnement de contrôle ;
- évaluation des risques ;
- activités de contrôle ;
- information – communication ;
- surveillance.

Il existe des relations directes entre les objectifs (ce que l'entreprise veut atteindre) et les composants (ce dont l'entreprise a besoin pour les atteindre).

Figure 1 ***: COSO II***

SOURCE : Support de formation du CESAG sur le contrôle interne (2015-2016)

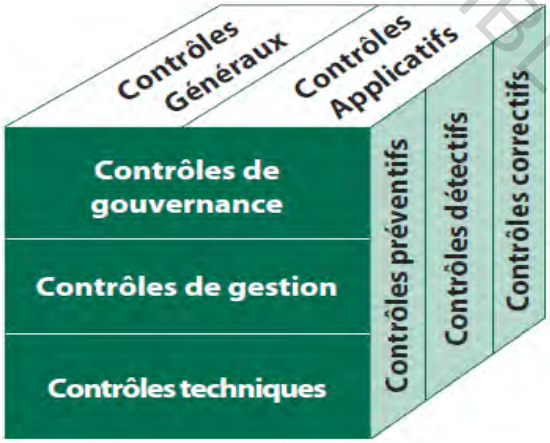
1.1.1.4. Le contrôle interne de l'environnement informatique

L'environnement informatique est un élément essentiel du système d'information et du dispositif de contrôle interne au sein de la Banque, par conséquent il doit être pourvu de son propre dispositif de contrôle interne. Le contrôle interne de l'environnement informatique englobe les processus qui procurent une assurance sur les données et les services informatiques et qui contribuent à contrôler et atténuer les risques découlant de

l'usage des SI par une organisation. Il existe deux types de contrôles informatiques : les contrôles applicatifs et les contrôles généraux.

- Les contrôles applicatifs portent sur l'étendue des processus de l'organisation ou ses applications et incluent les contrôles au niveau des entrées, des traitements et des sorties des applications.
- Les contrôles généraux s'appliquent à l'ensemble des composantes, processus et données d'une organisation ou d'un environnement système et sont intégrés dans les processus de la fonction informatique. Elles apportent l'assurance sur la continuité et l'efficacité des contrôles applicatifs sur lesquels le management s'appuie.

Figure 2 ***: Contrôle interne de l'environnement informatique***

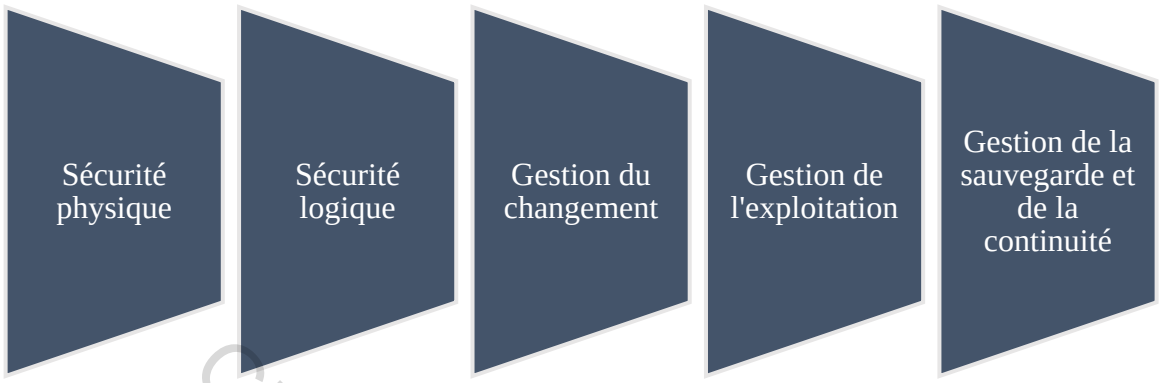


SOURCE : GTA 2 Les risques et les contrôles des systèmes d'information (2010)

1.1.2. Composantes des contrôles généraux informatiques

Les contrôles généraux comprennent tous les contrôles de l'infrastructure informatique nécessaire au fonctionnement des applications. Ces contrôles couvrent les domaines suivants : la sécurité physique, la sécurité logique, la gestion du changement, la gestion de l'exploitation, et la gestion de la sauvegarde et de la continuité d'activité.

Figure 3 ***Composantes des contrôles généraux informatiques***



SOURCE : nous-mêmes

1.1.2.1. La sécurité physique

La sécurité physique porte sur les dispositifs mis en œuvre dans le cadre de l'hébergement des serveurs afin de couvrir les principaux risques suivants :

- pannes matérielles et d'autres équipements critiques (routeurs, firewall, etc.) ;
- indisponibilité prolongée des systèmes ;
- destruction (intentionnelle ou non) des ressources informatiques centrales ;
- vols de composants techniques ;
- actes de vandalisme ou de malveillance ;
- interruption de l'alimentation électrique.

Les objectifs clés de contrôle de ce domaine sont :

- la localisation convenable de la salle informatique ;
- les accès restreints, protégés et contrôlés à la salle informatique ;

- la mise en place de dispositifs de prévention des risques environnementaux (climatisation, alimentation électrique secourue, détection/extinction d'incendie)

1.1.2.2. La sécurité logique

La sécurité logique regroupe les procédures et contrôles concourant à la sécurisation / limitation des accès aux ressources et données afin de couvrir les principaux risques suivants :

- accès non autorisés au système informatique ;
- actions malveillantes ou frauduleuses conduites à partir du système d'information ;
- réalisation d'opérations ou transactions non autorisées ;
- perte de confidentialité et d'intégrité des informations ;
- usurpation d'identité.

Les objectifs clés de contrôle de ce domaine sont :

- la mise en œuvre de techniques de contrôle d'accès / la définition de paramètres de sécurité adéquats ;
- la détermination de règles strictes des droits d'accès aux systèmes (création / révocation, modification) ;
- la validation de la mise à disposition de droits d'accès ;
- la revue régulière des comptes et des habilitations des utilisateurs.

1.1.2.3. La gestion du changement

La gestion des changements regroupe les procédures et contrôles permettant de garantir que les systèmes sont acquis, développés, mis en place et maintenus correctement, dans le

respect des besoins et de la stratégie de la Banque. Elle permet de couvrir les principaux risques suivants :

- le déploiement d'applications qui ne répondent pas aux besoins des utilisateurs ;
- les traitements informatiques et fonctionnalités non fiables ;
- les erreurs dans les états financiers restitués par les systèmes ;
- la régression dans la qualité des fonctionnalités ;
- la mise en place de programmes frauduleux ou malveillants.

Les objectifs clés de contrôle de ce domaine sont :

- l'adéquation du cycle de développement à un processus documenté ;
- la validation et la formalisation des besoins des utilisateurs ;
- la réalisation de tests avant la mise en production ;
- la maitrise des accès aux environnements de production par les développeurs.

1.1.2.4. La gestion de l'exploitation

La gestion de l'exploitation inclut les procédures et contrôles concourant au bon fonctionnement du système d'information dans sa vie courante. Elle permet de couvrir les principaux risques suivants :

- exécution incomplète de traitements informatiques ;
- traitements informatiques exécutés en retard ou dans des délais anormaux ;
- anomalies récurrentes non résolues ;
- pertes de données ou informations rejetées non traitées ;
- intégration de doublons ;
- flux d'interface en échec ;

- interruption de l'activité informatique.

Les objectifs clés de contrôle de ce domaine sont :

- le suivi et la supervision régulière des traitements informatiques sensibles (interfaces, batchs, sauvegardes) ;
- la traçabilité et résolution des incidents / le suivi des actions correctives ;
- les tests périodiques des procédures de continuité d'activité (restauration, plan de reprise, etc.).

1.1.2.5. La gestion de la sauvegarde et de la continuité d'activité

La sauvegarde et la continuité d'activité permet de s'assurer que l'entreprise sera capable de poursuivre son activité, même en cas de sinistre majeur. Elle permet de couvrir les principaux risques suivants :

- perte partielle ou complète de données ;
- incohérence du contenu des sauvegardes avec les besoins de l'entreprise ;
- perte de la traçabilité des incidents de sauvegarde et de la piste d'audit ;
- indisponibilité temporaire ou définitive des systèmes.

Les objectifs clés de contrôle de ce domaine sont :

- la conduite régulière des opérations de sauvegarde
- la réalisation de tests de restauration ou de récupération
- la vérification de la mise en œuvre d'une stratégie de continuité d'activité

1.1.3. Cadre de référence et standards

1.1.3.1. Normes d'audit des systèmes d'information

Selon ISACA, les normes sont des lignes directrices qui encadrent les professionnels de l'audit des TI et de l'assurance des SI. Elles définissent des exigences obligatoires en matière d'audit des SI et de reporting. Elles informent :

- les auditeurs des SI, sur le niveau minimum de performances requis pour satisfaire aux responsabilités stipulées dans le Code d'éthique professionnelle de l'association ;
- les dirigeants d'entreprise et les autres parties concernées, sur les attentes de la profession en matière d'agissements des praticiens ;
- les titulaires de la certification CISA (Certified Information Systems Auditor– Auditeur en SI certifié) sur les exigences de leur charge. Toute incapacité à mettre en œuvre ces normes peut entraîner une enquête sur la conduite du titulaire de la certification par le Conseil d'administration de l'ISACA ou tout autre Comité approprié et, en définitive, des actions disciplinaires.

Pour mener à bien sa mission, l'auditeur doit faire face au choix d'une norme et d'un standard correspondant au domaine audité, puis il définit ses objectifs d'audit avant de décider d'une approche méthodologique.

Dans le souci de bien mener sa mission de manière professionnelle et efficace, l'auditeur doit s'appuyer sur des normes, des standards, des référentiels de bonne pratique ou des méthodes spécifiques à l'audit du système d'information. Nous présenterons ainsi quelques outils adaptés à ce type de mission. Le tableau ci-dessous illustre quelques normes d'audit des SI élaborés par ISACA.

Tableau 1 ***: Les normes d'audit des systèmes d'information***

INTITULE DE LA NORME	DECLARATIONS
	CHARTE D'AUDIT & CONSCIENCE PROFESSIONELLE
Norme d'audit et d'assurance des SI 1001 - Charte d'audit	**1001.1** La fonction d'audit et d'assurance des SI énonce la fonction d'audit de manière appropriée dans une charte d'audit, en indiquant son objet, ses responsabilités et ses pouvoirs. **1001.2** La fonction d'audit et d'assurance des SI obtiendra l'acceptation de la charte d'audit et son approbation à un niveau approprié au sein de l'entreprise.
Norme d'audit et d'assurance des SI 1005 - Conscience professionnelle	**1005.1** Les professionnels de l'audit et de l'assurance des SI feront preuve de conscience professionnelle et, notamment, respecteront les normes professionnelles d'audit en vigueur à la planification, l'exécution et la présentation de rapports sur les résultats des missions.
	PLANIFICATION
Norme d'audit et d'assurance des SI 1201 - Planification de la mission	**1201.1** Les professionnels de l'audit et de l'assurance des SI doivent planifier chaque mission d'audit et d'assurance des SI de manière à prendre en compte : ▪ le ou les objectifs, la portée, le calendrier et les réalisations ▪ le respect des lois applicables et des normes d'audit professionnel ▪ l'utilisation d'une approche fondée sur le risque, lorsque cela se justifie ▪ les questions propres à la mission ▪ les exigences en matière de documentation et de présentation de rapports **1201.2** Les professionnels de l'audit et de l'assurance des SI doivent élaborer et documenter un plan de projet de mission d'audit ou d'assurance des SI qui décrive :

INTITULE DE LA NORME	DECLARATIONS
	▪ nature, objectifs, calendrier et besoins en ressources de la mission ▪ calendrier et portée des procédures d'audit nécessaires pour achever la mission
Norme d'audit et d'assurance des SI 1202 - Évaluation du risque dans la planification	**1202.1** La fonction d'audit et d'assurance des SI doit utiliser une approche d'évaluation du risque et une méthodologie à l'appui appropriées pour élaborer le plan général d'audit des SI et définir les priorités en vue d'une allocation efficace des ressources d'audit des SI. **1202.2** Les professionnels de l'audit et de l'assurance des SI doivent identifier et évaluer les risques pertinents eu égard au domaine examiné lors de la planification de chaque mission. **1202.3** Les professionnels de l'audit et de l'assurance des SI doivent prendre en considération le risque lié à l'objet, le risque d'audit et l'exposition connexe au risque de l'entreprise.
	EXECUTION
Norme d'audit et d'assurance des SI 1203 - Exécution et supervision	**1203.1** Les professionnels de l'audit et de l'assurance des SI doivent mener leurs travaux conformément au plan d'audit des SI approuvé, afin de couvrir les risques identifiés et de respecter le calendrier convenu. **1203.2** Les professionnels de l'audit et de l'assurance des SI doivent assurer la supervision du personnel d'audit des SI dont ils ont la responsabilité, afin d'accomplir les objectifs de l'audit et de respecter les normes d'audit professionnel applicables. **1203.3** Les professionnels de l'audit et de l'assurance des SI ne doivent accepter que les tâches correspondant à leurs connaissances et compétences ou pour lesquelles ils peuvent s'attendre raisonnablement soit à acquérir les compétences correspondantes pendant la mission, soit à bénéficier d'une supervision lors de l'exécution de la tâche. **1203.4** Les professionnels de l'audit et de l'assurance des SI doivent obtenir des éléments probants suffisants et appropriés pour la réalisation des objectifs de l'audit. Les conclusions de l'audit doivent être appuyées par une analyse et une interprétation adéquate de ces éléments probants. **1203.5** Les professionnels de l'audit et de l'assurance des SI doivent documenter le processus d'audit et décrire le

INTITULE DE LA NORME	DECLARATIONS
	travail et les éléments probants de l'audit à l'appui de leurs résultats et conclusions. **1203.6** Les professionnels de l'audit et de l'assurance des SI doivent identifier les résultats et en tirer des conclusions.
	RAPPORT
Norme d'audit et d'assurance des SI 1401 – Rapports	**1401.1** Les professionnels de l'audit et de l'assurance des SI doivent fournir un rapport afin de communiquer les résultats à l'achèvement de la mission, comprenant : ▪ identification de l'entreprise, de ses destinataires pressentis et de toute ▪ restriction relative à son contenu et sa diffusion ▪ la portée, les objectifs de la mission, la période couverte et la nature, ▪ le calendrier et l'étendue des travaux exécutés ▪ les résultats, conclusions et recommandations ▪ toute restriction ou limitation de la portée signalée par le professionnel de l'audit et de l'assurance des SI concernant la mission ▪ la signature, la date et la diffusion conformément aux termes de la charte d'audit ou de la lettre de mission **1401.2** Les professionnels de l'audit et de l'assurance des SI doivent veiller à ce que les conclusions du rapport d'audit soient étayées par des éléments probants suffisants et appropriés.
	SUIVI DES RECOMMANDATIONS
Norme d'audit et d'assurance des SI 1402 - Activités de suivi	**1402.1** Les professionnels de l'audit et de l'assurance des SI doivent effectuer un suivi des informations pertinentes afin de conclure si la direction a planifié/pris les mesures appropriées et ponctuelles pour traiter les résultats de l'audit et les recommandations figurant dans le rapport.

SOURCE : ISACA (2016)

1.1.3.2. Les référentiels d'audit des systèmes d'information

On nommera référentiel du système d'information un ensemble cohérent et outillé de données du système d'information de l'entreprise, partagées par une communauté d'acteurs et possédant les cinq propriétés suivantes :

- **Centralité :** il est reconnu comme la référence sur le sujet qu'il traite ;
- **Stabilité :** ses données changent relativement peu dans le temps ;
- **Qualité :** lui sont associés des processus assurant une certaine maîtrise de la fiabilité des données ;
- **Unité de sens :** ses données ont une homogénéité sur le plan sémantique ;
- **Interopérabilité :** il est techniquement coordonné avec le système d'information, et lui fournit un certain nombre de services.

Il existe de nombreux référentiels méthodologiques généraux, faisant l'objet d'une ample littérature, notamment dans le domaine des SI :

- COBIT (Control Objectives for Information and Relatead Technology) pour la gouvernance des SI ;
- ITIL (Information Technology Infrastructure Library) pour le niveau de service rendu par le SI ;
- CMMI (Capability Maturity Model Integration) pour le développement et la maintenance du SI ;
- ISO/CEI 27001/27002 pour la sécurité de l'information.

1.1.3.2.1. COBIT5 (Control Objectives for Information and Relatead Technology)

COBIT est un cadre de référence qui est né de la collaboration entre l'ITGI et l'ISACA. Il est traduit en français par l'Association Française d'Audit Informatique (AFAI). Pour ainsi dire, COBIT est un intégrateur des bonnes pratiques en TI (Technologie de l'information) et le référentiel général de la gouvernance des systèmes d'information. C'est un référentiel qui se veut complet en essayant de fournir aux entreprises les outils nécessaires leur permettant d'atteindre leurs objectifs en matière de gouvernance et de gestion des SI.

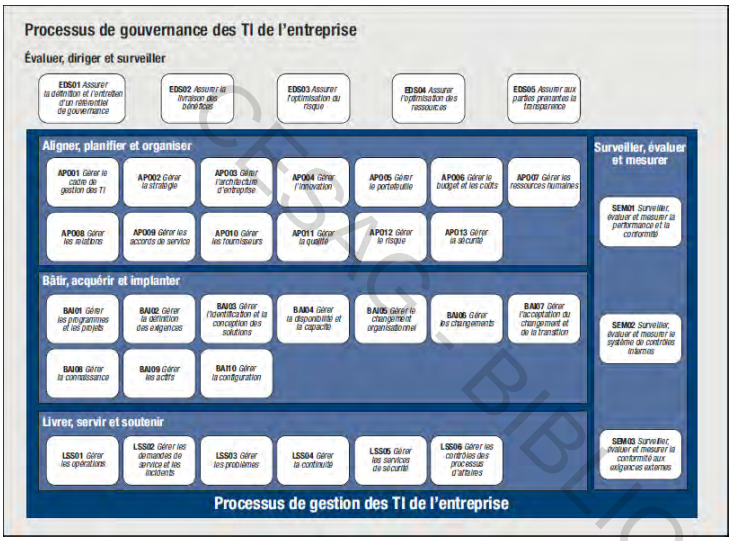
Dans sa cinquième version, il identifie trente-sept (37) processus qui sont un ensemble organisé de pratiques et d'activités permettant d'atteindre des résultats des objectifs généraux liés aux technologies informatiques. Ces différents processus sont regroupés en cinq domaines :

- **Domaine 1 -- évaluer, diriger et surveiller : EDS**. Ce domaine permet de s'assurer du respect des grandes règles de gouvernance. Il comprend cinq (5) processus ;
- **Domaine 2 -- aligner, planifier et organiser : APO.** Comprenant treize (13) processus, ce domaine présente les bases de la gestion de l'informatique ;
- **Domaine 3 -- bâtir, acquérir et implanter : BAI.** Ce domaine comprend dix (10) processus, il a pour but d'améliorer les processus de définition et de mise en place des applications informatiques ;
- **Domaine 4 -- livrer, servir et soutenir : LSS.** Ce domaine comprend six (6) processus. L'objectif est de perfectionner le fonctionnement de l'exploitation informatique ;

- **Domaine 5 -- surveiller, évaluer et mesurer : SEM**. Ce domaine comprend trois (3) processus. Il détaille les bases du contrôle des systèmes d'information dont le contrôle interne.

Le schéma ci-dessous présente de façon résumée les processus de COBIT 5.

*Tableau 2**: Processus de gouvernance de COBIT 5***



SOURCE : COBIT 5 (2012)

1.1.3.2.2. ITIL (Information Technology Infrastructure Library)

ITIL se positionne sur la gestion des services TI. Il a pour objectif de guider, par les bonnes pratiques, les professionnels des SI dans la gestion efficace des ressources et l'obtention de la qualité des services informatiques.

ITIL permet, grâce à une approche par les processus clairement définis et contrôlés, d'améliorer la qualité des SI et de l'assistance aux utilisateurs en créant la fonction centre de services qui centralise et administre l'ensemble de la gestion des systèmes d'information. Les apports pour l'entreprise sont une meilleure traçabilité de l'ensemble des actions de la

DSI. Ces traces servent de base à l'optimisation des processus de services TI pour atteindre un niveau de qualité maximum du point de vue de la satisfaction des clients.

ITIL v3 comporte cinq (5) ouvrages, chacun traitant d'une perspective pour les services informatiques :

- **Domaine 1 -- La stratégie des services :** aborde les aspects de la gestion financière, de la gestion du portefeuille des projets de service ainsi que la gestion des demandes. L'objectif est de garantir que les futurs services soient alignés avec les besoins métiers et créeront une valeur pour l'entreprise ;
- **Domaine 2 -- La conception des services :** ce sont sept (7) processus à mettre en œuvre pour gérer la continuité des services et leurs évolutions. Elle propose un ensemble d'indicateurs pour la mesure de l'alignement de la capacité des services à la demande ;
- **Domaine 3 -- La transition des services :** propose quatre (4) processus pour la gestion des changements, des configurations, du déploiement des services et de la connaissance ;
- **Domaine 4 -- L'exploitation des services :** propose les bonnes pratiques en matière de gestion des niveaux de contrat de services (SLA) ;
- **Domaine 5 -- L'amélioration continue des services :** cet ouvrage traite de la supervision, de l'alignement et de la mise en œuvre du plan d'amélioration des services.

Le schéma ci-dessous représente le cycle de vie des services selon ITIL v3 :

Figure 4 ***: Cycle de vie des services***

SOURCE : ITIL V3(2011)

1.2. Etat des connaissances sur l'approche d'audit des contrôles généraux informatiques d'une Banque dans le cadre d'une mission de commissariat aux comptes

1.2.1. Définitions

1.2.1.1. L'audit légal

Selon L'IFAC (2006 :48) «°une mission d'audit des états financiers a pour objectif de permettre à l'auditeur d'exprimer une opinion selon laquelle les états financiers ont été établis dans tous leurs aspects significatifs, conformément à un référentiel comptable identifié. ». Pour atteindre cet objectif, l'ISA 315 énonce que « l'auditeur doit acquérir une connaissance de l'entité et de son environnement, y compris de son contrôle interne, qui

soit suffisante pour lui permettre d'identifier et d'évaluer le risque les états financiers contiennent des anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs, et de concevoir et de mettre en œuvre des procédures d'audit complémentaires. ».

1.2.1.2. L'audit du système d'information

L'audit des systèmes d'information se définit selon l'ISACA (Information Systems Audit and Control Association) comme un examen formel, une entrevue ou un test permettant de déterminer si :

- les systèmes d'information sont en conformité avec les lois, les règlements, les contrats ou les lignes directrices de l'industrie ;
- les données et les renseignements des SI ont reçu les niveaux de confidentialité, d'intégrité et de disponibilité appropriés ;
- les opérations de SI sont accomplies efficacement et les objectifs d'efficacité sont respectés.

1.2.2. Risques liés au système d'information

Les risques induits par le système d'information sont plus élevés dans le secteur bancaire que pour d'autres secteurs de l'économie en raison d'un double constat.

En premier lieu, les activités bancaires, reposent aujourd'hui dans un environnement informatique de plus en plus complexe intégrant de nombreuses fonctionnalités ayant un impact direct sur les processus opérationnels. En effet, les flux d'information bancaires dématérialisés, automatisés dans des applications informatiques et télématiques sont échangés sur les réseaux (internet, intranet, VPN). De ce fait les valeurs monétaires sont valorisées grâce à système informatique.

En second lieu, le risque systémique est inhérent au système bancaire et financier, du fait des interrelations existant dans ce secteur entre les différentes institutions et les différents marchés. Le risque systémique du secteur financier est d'autant plus dangereux que ses répercussions se diffusent sur l'économie réelle.

Quelques risques majeurs lié au système d'information dans le secteur bancaire :

- L'indisponibilité des SI supportant l'activité affecte la Banque de manière significative. Plus l'activité est dépendante des systèmes informatiques, plus le risque potentiel de pertes financières ou d'atteinte à la réputation de l'entreprise est significatif.
- La divulgation d'informations critiques conduisant selon leur nature et leur criticité à des pertes financières en cas de fraude ou de vol ou encore à des non-conformités légales ou règlementaires.
- Le manque de fiabilité des systèmes d'information conduisant l'entreprise à des pertes directement et indirectement financières. Ces pertes résultent de l'incohérence ou de l'inadaptation des traitements des informations, des travaux de correction nécessaires pour rectifier les anomalies de traitements ou de l'utilisation de processus inefficaces ou dupliqués par les utilisateurs qui ne font pas confiance au SI.
- Des interfaces non maîtrisées entre des systèmes critiques pour l'établissement des états financiers peuvent conduire l'entreprise à des pertes ou à une corruption des données comptables et/ou de gestion. Ces dernières peuvent résulter de problématiques techniques, logicielles ou matérielles liées à une exploitation informatique non fiable, du manque de cohérence des référentiels et/ou des bases

de données entre deux applications, du manque de suivi des transferts de données de la part des équipes d'exploitation et/ou métier.

Assurer la maitrise du dispositif de contrôle interne de l'environnement informatique est impératif dans le secteur bancaire où les manquements constituent l'un des vecteurs possibles de transmission du risque pouvant à la limite créer un risque systémique.

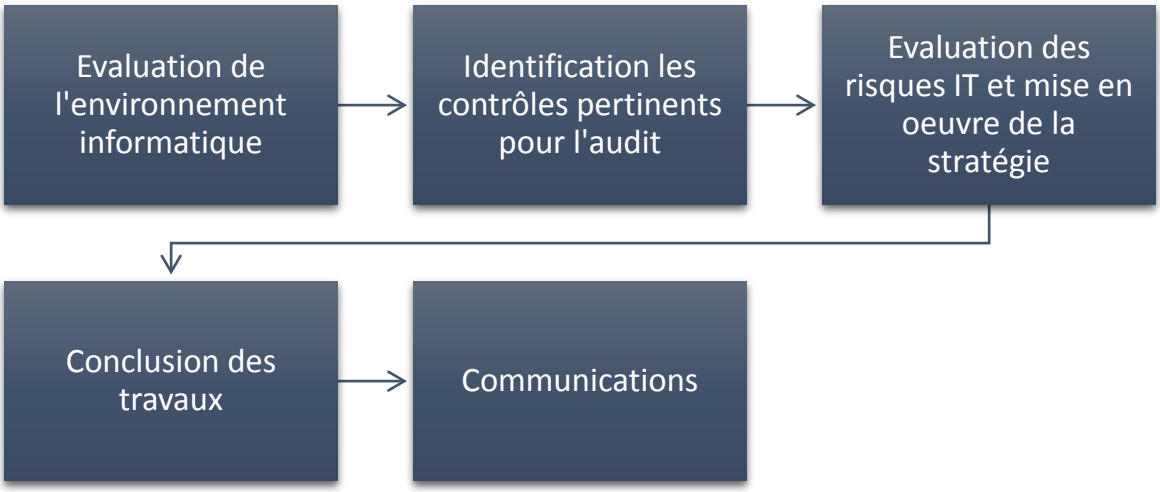
1.2.3. L'audit des contrôles généraux informatiques

L'intégration de l'audit des contrôles généraux informatiques dans l'approche d'audit est un enjeu majeur pour mener à bien la mission de commissariat aux comptes. Effet, lorsqu'une équipe d'audit financier estime qu'un environnement informatique est complexe et qu'un auditeur IT est nécessaire, une réunion est organisée avec ce dernier afin que les deux équipes puissent échanger sur le périmètre d'intervention afin de l'intégrer à la stratégie d'audit.

Après cette réunion, l'auditeur financier doit préparer un cahier des charges validé par l'auditeur IT. Cela garantira que le travail d'audit des contrôles généraux informatiques réalisé répondra aux exigences de l'auditeur financier et garantira une stratégie d'audit intégrée. Il est important que ce cadre de travail définisse les responsabilités relatives des auditeurs financiers et IT.

Dans le cadre de ce processus, l'audit IT doit dérouler l'approche suivante : comprendre l'environnement informatique, identifier les contrôles pertinents pour l'audit, concevoir la stratégie à mettre en œuvre, évaluer les risques informatiques connexes, puis analyser les données, conclure les travaux et communiquer avec l'entreprise auditée.

Figure 5: ***L'approche d'audit des contrôles généraux informatiques***



SOURCE : nous-mêmes

1.2.3.1. Evaluation de l'environnement informatique

L'évaluation de l'environnement informatique consiste en la prise de connaissance du système d'information. Elle passe par les étapes suivantes :

- prendre en compte le secteur, l'activité et l'importance des flux / transactions ;
- décrire les SI utilisés par la Banque, notamment ceux impactant les états financiers et portant sur les cycles – applications les plus sensibles ;
- obtenir la cartographie de l'écosystème applicatif ayant un impact sur les états financiers et sur la description des interfaces de contrôle ;
- réaliser des entretiens avec le DSI / Responsable informatique sur la compréhension de l'organisation de la fonction, des changements intervenus tant au niveau de l'architecture que des applications et la formalisation dans un compte-rendu d'entretien ;
- documenter l'absence de changements sur les SI et obtenir les rapports d'exception générés par le système.

1.2.3.2. Identification les contrôles pertinents pour l'audit

Cette étape consiste à identifier les contrôles automatisés pertinents pour l'audit par Cycle-Application en lien avec les assertions et les rapports issus du SI sur lesquels l'équipe va s'appuyer : documentation de la piste d'audit.

1.2.3.3. Evaluation des risques informatiques et mise en œuvre de la stratégie

Cette étape consiste à mettre en œuvre les diligences nécessaires à la validation des contrôles généraux informatiques sur les applications supportant les contrôles pertinents à l'élaboration des états financiers :

- revue des composantes des contrôles généraux informatiques (sécurité logique, physique, etc.) ;
- utiliser les techniques de contrôle assistées par ordinateur pour améliorer le niveau des tests de validation et des tests relatifs à l'automatisation de systèmes complexes et aux processus de transaction.

1.2.3.4. Conclusions des travaux

Cette étape consiste à documenter le dossier du client par un rapport de synthèse des travaux effectués.

1.2.3.5. Communication

Cette étape consiste à identifier les éléments clés des travaux et conclusions de l'auditeur IT, puis communiquer sur les défaillances de contrôle constatées et sur la qualité de

l'environnement de contrôle à la fois au Management et au comité d'audit (et à défaut au Conseil).

CHAPITRE 2 : CADRE METHODOLOGIQUE DE L'AUDIT DES CONTRÔLES GENERAUX INFORMATIQUES D'UNE BANQUE DANS LE CADRE D'UNE MISSION DE COMMISSARIAT AUX COMPTES ET PRESENTATION DE LA BANQUE

Ce chapitre nous permettra d'aborder dans un premier temps l'approche méthodologique de notre étude. Une présentation de l'entité ayant fait l'objet de notre travail sera faite dans un second temps.

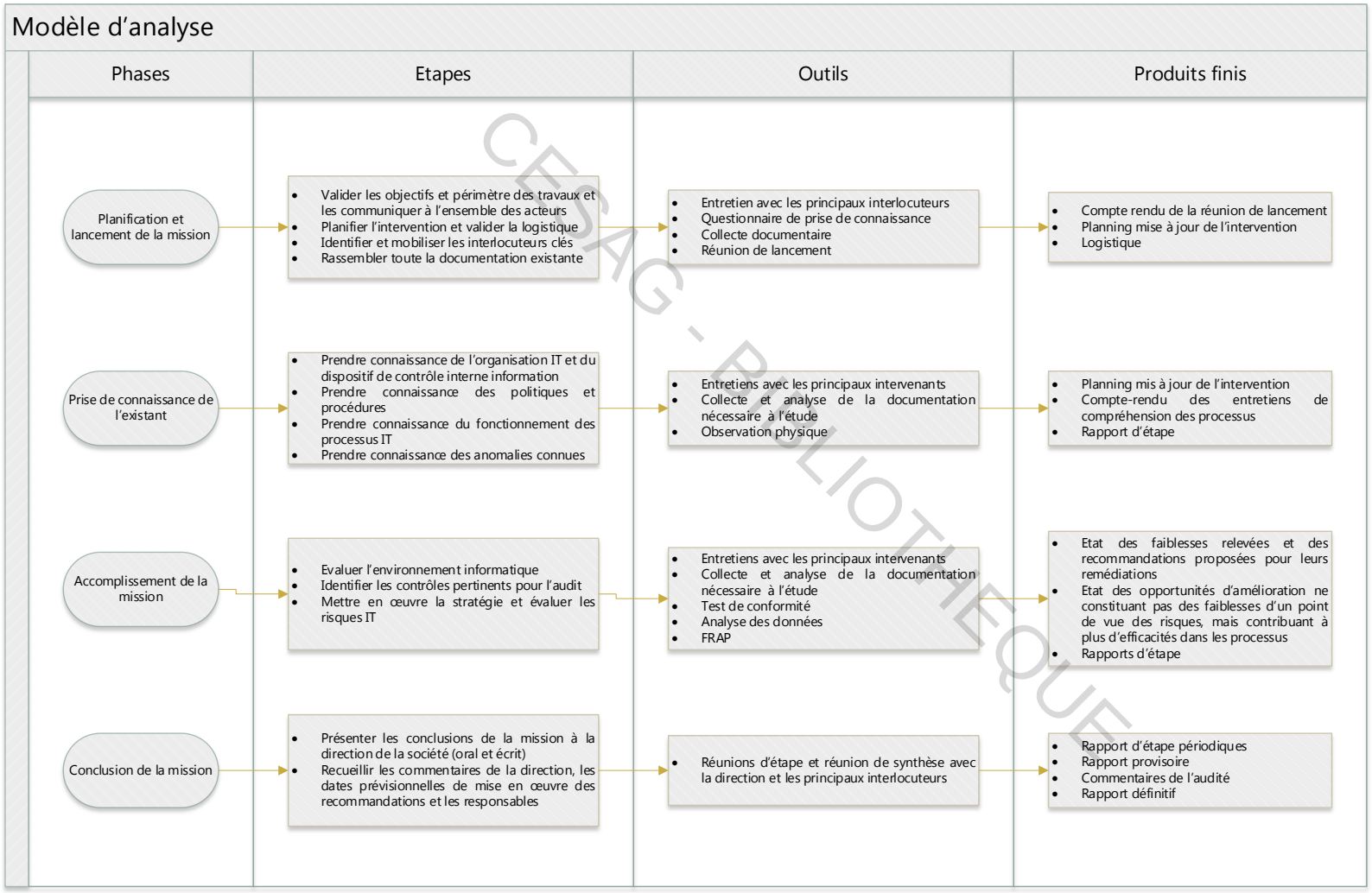
2.1. Méthodologie de l'étude

De l'avis de Zumatwo Some cité par Yekeye (2001 : 19) « la méthodologie est l'ensemble des démarches, approches, réflexions, organisations, hypothèses, susceptibles de permettre d'atteindre un objectif pédagogique ou de recherche à caractère scientifique ou un autre». Cette partie nous permet de préciser et de définir les réflexions méthodologiques qui serviront de support à cette recherche. Nous mettrons ainsi en relief le modèle d'analyse de données et la méthode de collecte des données.

2.1.1. Modèle d'analyse

Notre modèle d'analyse sera axé essentiellement sur trois phases à savoir : la phase de planification et lancement de la mission d'audit, la phase de prise de connaissance de l'existant, la phase d'accomplissement et la phase de conclusion.

*Tableau 3**: Modèle d'analyse***



SOURCE : nous-mêmes

2.1.2. Outils de collecte de l'information

Les outils de collecte de l'information portent sur le « comment » dans la démarche de l'audit. Les outils choisis doivent être pertinents par rapport à la taille de l'échantillon « le qui », au temps disponible pour mener l'audit « le quand » et au type d'information à recueillir (le pourquoi).

Nous avons décidé d'utiliser l'analyse documentaire, l'entretien individuel et l'observation, le questionnaire de prise de connaissance (QPC), et la FRAP (Feuille de Révélation et d'Analyse de Problème).

2.1.2.1. L'analyse documentaire

Elle consiste à consulter et à exploiter les documents que la Banque nous aura fournis. Selon Sylvie Guerrero (2008 : 24), l'analyse documentaire présente l'avantage d'être rapide, de permettre une collecte facile et systématique de l'information. Toutefois, elle ajoute que cet instrument doit être utilisé en complément d'autres outils de collecte pour une meilleure efficacité.

2.1.2.2. Questionnaire de Prise de Connaissance (QPC)

Le Questionnaire de Prise de Connaissance (QPC) intervenant lors de la phase de préparation, permettra de prendre connaissance de la Banque, du système de contrôle interne, des procédures et processus. La prise de connaissance du domaine ou de l'activité à auditer doit être réfléchie et organisée, c'est pourquoi nous allons utiliser un questionnaire dénommé « Questionnaire de Prise de Connaissance » récapitulant les points importants dont la réponse doit être connue si nous voulons avoir une bonne

compréhension du domaine à auditer. C'est un moyen efficace pour organiser la réflexion et les recherches et surtout pour :

- bien définir le champ d'application de sa mission ;
- prévoir en conséquence l'organisation du travail et en particulier en mesurer l'importance ;
- préparer l'élaboration des Questionnaires de Contrôle Interne.

Chaque auditeur construit son QPC en fonction de ses acquis, de ses expériences, de ce qu'il sait et de ce qu'il a besoin d'apprendre. Quelles que soient ses dimensions, il est indispensable à la compréhension du sujet par l'auditeur.

2.1.2.3. L'entretien individuel

Selon AUGER (2008 :68), « la richesse des informations issues de l'entretien est essentiellement liée à la capacité d'écoute et d'empathie de celui qui interroge ».

Il joue un rôle capital dans la réalisation du travail. L'auditeur aborde les thèmes et les points qui lui permettront de compléter ses recherches débutées avec la revue documentaire. Cette méthode bien qu'elle soit longue, permet d'obtenir des informations riches et détaillées de la part de l'audité.

2.1.2.4. L'observation

L'observation est un mode de collecte des données par lequel l'auditeur observe de lui-même, des processus ou des comportements se déroulant dans une organisation, pendant une période de temps délimitée. Avec cet outil de collecte, nous allons observer si les procédures sont respectées comme l'indique le manuel de procédures en vigueur.

2.1.2.5. Test de conformité

Il permet de s'assurer que les dispositifs de contrôle interne et de gestion des risques ont été bien appliqués. En effet, il permet de vérifier si la description du processus est conforme à la réalité et donc de vérifier la piste d'audit. HAMZAOUI (2008 :196) disait que le test de conformité permet de vérifier l'application effective du dispositif décrit lors de l'entretien et de sa conformité à la réalité d'une part et d'autre part que les points forts théoriques fonctionnent de façon permanente tel que prévu dans les procédures.

2.1.2.6. Les FRAP (Feuilles de Révélation et d'Analyse de Problème)

La FRAP est un document normalisé qui s'utilise durant la phase de terrain. Celui-ci aide l'auditeur à conduire et à structurer son raisonnement de façon logique et chronologique. Ainsi, chaque fois que l'auditeur constate un problème ou un dysfonctionnement, il rédige une FRAP.

La finalité de la FRAP est de formuler des recommandations, et servir de base pour la rédaction du rapport.

2.2. Présentation de la Banque auditée

L'objectif est de mettre en exergue la présentation de la Banque auditée, les missions, les activités, ainsi que l'organigramme afin de mieux appréhender leur organisation.

2.2.1. Objectifs

Dans le souci de participer au développement de l'économie de façon rigoureuse et harmonieuse, les dirigeants de la Banque ont mis sur pied une stratégie visant plusieurs objectifs à savoir :

- développer le commerce national et international ;
- diversifier les interventions dans le financement à court, moyen et long terme ;
- participer à l'essor des PME ;
- favoriser les investissements par la mobilisation des ressources nationales et internationales ;
- susciter l'engouement de la clientèle à travers une variété de produits et services ;
- assurer de bonnes conditions de vie et de travail au personnel en vue d'obtenir de meilleurs rendements ;
- promouvoir la croissance, l'amélioration et l'efficacité de ses services bancaires afin de satisfaire au mieux sa clientèle et d'en tirer le profit nécessaire ;
- poursuivre une politique sociale interne attentive à l'amélioration des conditions de travail de son personnel ;
- optimiser la qualité de ses services au moyen d'un développement accru de ses capacités informatiques ;
- avoir un meilleur rayonnement au plan national et s'implanter sur le plan régional en tant que leader ;
- assurer une forte rentabilité en restant toujours sélective au niveau des emplois et des ressources ;
- être plus accessible à travers la création de nouvelles agences ;
- supprimer toutes les barrières monétaires et linguistiques.

2.2.2 Activités

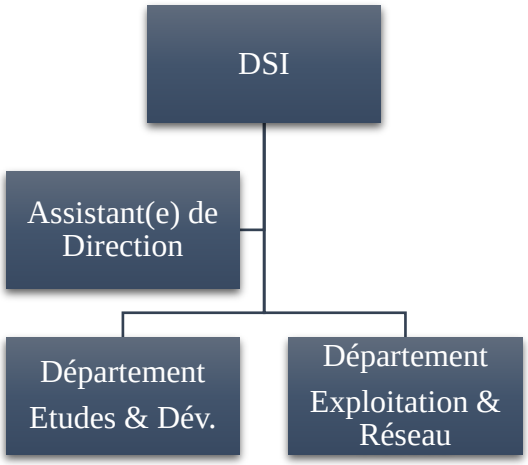
La Banque offre une gamme variée de produits à sa clientèle. On peut notamment citer :

- la tenue de comptes courants, de comptes de dépôt et d'épargne ;
- les opérations de prêt (l'escompte des effets de commerce, les facilités de caisse, les découverts, les crédits de campagne, les crédits immobiliers, etc.) ;
- les opérations de remise documentaire et de crédit documentaire ;
- les crédits par signature sous forme de caution ou d'aval ;
- les opérations de change, d'arbitrage ;
- les transferts de fonds ;
- les remises d'effets et de chèques à l'encaissement ;
- les achats et ventes de chèques de voyage ;
- la gestion de trésorerie et de fonds.

2.2.3. Organigramme de la DSI

L'organigramme de la DSI se présente ainsi :

Figure 6 ***: Organigramme de la DSI de la Banque***



SOURCE : la Banque

On distingue deux (02) pôles : le pôle Etudes et Développements et le pôle Exploitation et Réseau.

Le Directeur coordonne l'activité des différents pôles et participe au Comité de Direction de la Banque.

2.2.3.1. Le département Etudes et Développements

Ce pôle est en charge de l'étude et de la prise en compte des besoins exprimés par les services, de la maintenance des applications informatiques et de la maîtrise d'ouvrage informatique.

Le Chef du département est secondé par deux ingénieurs développeurs.

2.2.3.2. Le département Exploitation et Réseau

Ce pôle est en charge de la maintenance des équipements et applications informatiques, de la sécurité du réseau, de l'assistance hotline aux utilisateurs et des traitements informatiques périodiques.

Le Chef du département est assisté dans ces fonctions par deux (02) pupitreurs chargés des traitements informatiques, et deux techniciens chargés des travaux de réseau et de l'assistance aux utilisateurs.

CONCLUSION DE LA PREMIERE PARTIE

Dans cette première partie, il a été mis en exergue les différents concepts et fondamentaux de l'audit des contrôles généraux informatiques mais aussi, la description organisationnelle de la Banque et celle de la méthodologie de recherche.

Une meilleure connaissance théorique du traitement de notre thème a été faite afin de faire comprendre l'audit du dispositif de contrôle interne de l'environnement informatique et de faciliter la description du modèle d'analyse qui nous permettra de collecter les données, informations nécessaires pour la rédaction du mémoire et en particulier la deuxième partie comme sus énoncé dans le plan.

DEUXIEME PARTIE :

CADRE PRATIQUE DE L'ETUDE SUR L'AUDIT DES CONTRÔLES GENERAUX INFORMATIQUES D'UNE BANQUE DANS LE CADRE D'UNE MISSION DE COMMISSARIAT AUX COMPTES REALISEE PAR LE CABINET MAZARS AU SENEGAL

INTRODUCTION DE LA DEUXIEME PARTIE

Cette deuxième partie intitulée cadre pratique de l'étude est divisée en deux (2) chapitres. Dans le premier chapitre, nous nous intéressons à la conduite de la mission d'audit des contrôles généraux informatiques de la Banque et aux analyses des résultats. Ensuite, le deuxième chapitre sera consacré aux recommandations et suggestions pour l'amélioration du dispositif de contrôle interne de l'environnement informatique de la Banque.

CHAPITRE 3 : CONDUITE DE L'AUDIT DES CONTROLES GENERAUX INFORMATIQUES DE LA BANQUE DANS LE CADRE D'UNE MISSION DE COMMISSARIAT AUX COMPTES REALISEE PAR LE CABINET MAZARS AU SENEGAL

Après avoir présenté la Banque, il nous revient dans ce chapitre de décrire le processus de conduite de la mission d'audit des contrôles généraux de la Banque dans le cadre d'une mission de commissariat aux comptes réalisée par le cabinet Mazars au Sénégal à travers le modèle d'analyse et les outils de collectes décrits dans la section consacrée au cadre méthodologique de l'étude.

3.1. Planification et lancement de la mission

La phase de planification a consisté d'abord au cadrage du périmètre des travaux à couvrir avec les équipes de la Banque et à la fixation du calendrier d'intervention (voir annexe 1) sur ce périmètre dans les locaux de la société. Ensuite les questions de logistique nécessaire à la mission notamment la salle de travail, les badges d'accès à la société, les accès au système d'information bancaire, ont été discutés, et enfin une liste de mande documentaire (voir annexe 2) a été envoyée afin de préparer l'exécution des travaux d'audit.

Une réunion de lancement a eu lieu dans les locaux de la Banque en présence de la Direction des Systèmes d'Information, du Département Risque et Conformité, et de la Direction de l'Audit Interne afin de marquer le démarrage officiel de la mission. Lors de cette réunion, il s'est agi de présenter d'abord les objectifs de la mission, c'est-à-dire évaluer les risques généraux informatiques inhérents au système d'information bancaire à travers la prise de connaissance des contrôles relatifs au périmètre couvert par la mission et

le test des contrôles en termes de conception et d'efficacité opérationnelle. Ensuite l'équipe d'intervention a été présenté et le planning d'entretiens (voir annexe 3) mise à jour. Enfin, un suivi de la réception des documents demandés lors du cadrage a été réalisé. Un compte rendu de la réunion de lancement a été rédigé puis archivé dans le dossier de travail.

3.2. Prise de connaissance de l'existant

Sur la base des comptes rendus d'entretiens réalisés avec la DSI, et d'une analyse des documents collectés, nous avons eu une meilleure compréhension du fonctionnement de l'organisation actuelle de la fonction IT, du dispositif de contrôle interne de l'environnement informatique, des politiques et procédures applicables. Ensuite nous avons réalisé une cartographie applicative du périmètre de la mission d'audit et enfin les points de contrôle du programme de travail (voir annexe 4) de la mission ont été affinés.

3.3. Phase d'accomplissement

Le chef de mission répartit les sous-thèmes des contrôles généraux du programme de travail à évaluer entre les membres de l'équipe. L'évaluation de chaque composante s'effectue sur la base d'entretien suivant le planning établi lors de la phase de planification, d'analyse des documents collectés, de test de conformité (vérification de la mise en œuvre de procédure, de politique, revue des habilitations, analyse des comptes utilisateurs, revue des tickets de demande d'évolution d'applicatif, etc.). Ensuite, nous rédigeons des comptes rendus de réunion (voir annexe 5) sur les sous-thèmes des contrôles généraux informatiques. Et enfin, nous formalisons dans les FRAP (voir annexe 6), les constats relevés sur les points de contrôle de chaque sous-thème des contrôles généraux informatiques.

A chaque constat est attribué un niveau de risque reflétant l'importance de leur survenance au sein de la Banque et, par conséquent, l'urgence des actions requises dans la mise en œuvre des recommandations qui ont été formulés :

- Elevé – L'institution est exposé à des pertes financières, des dommages à la réputation ou à la perte d'informations. Cela peut avoir des implications sur la réalisation des objectifs stratégiques. La recommandation devrait être prise en compte immédiatement.
- Moyen – Il est nécessaire de renforcer le contrôle interne. Les recommandations devraient être mises en œuvre dans un futur proche.
- Faible – Le dispositif de contrôle interne devrait être renforcé dans ces domaines supplémentaires dès que possible.

3.3.1. Sécurité physique

L'évaluation des points de contrôles de la sécurité physique de la Banque a relevé les insuffisances ci-dessous.

3.3.1.1. Manquements dans la protection des locaux techniques, contre les risques environnementaux

Il est ressorti de notre visite de la salle des serveurs du siège de la Banque, que celle-ci n'est pas suffisamment protégée contre les risques environnementaux. En effet, ce local ne dispose pas des mesures adéquates afin d'éviter tout dommage causé par :

- les risques d'incendie : l'extincteur automatique n'a jamais connu de maintenance depuis son installation le 01/10/2010. De plus, des objets inflammables, tels que des commodes en bois et autres équipements vétustes sont conservés dans la salle,

servant de support aux serveurs et équipements réseaux. Enfin, la porte d'accès et les baies en verre, ne permettront pas de confiner les flammes en cas d'incendie ;

- les inondations : en plus de n'être consultable qu'à l'intérieur du local, l'hygromètre déployé ne renvoie pas d'information fiables. Il n'est donc pas possible de surveiller le niveau d'humidité de la salle, à partir de l'extérieur ;
- les dégagements calorifiques : les deux splits armoires déployés fonctionnent à plein régime, et en même temps afin de maintenir une température ambiante raisonnable. Un fonctionnement en alternance des deux armoires aurait été suffisant n'eut été les perforations notées au niveau de la porte d'accès en verre. En plus de faire baisser le niveau de performance des splits armoires, ces ouvertures ne favorisent pas bon fonctionnement du dispositif anti-incendie en place.

3.3.1.2. Insuffisance du dispositif de vidéosurveillance

Un dispositif de vidéosurveillance a été installé au siège de la Banque. Les enregistrements issus de ce dispositif sont visualisables à partir :

- de la Direction des Ressources Humaines et de l'Administration (DRHA) ;
- des postes du Chargé d'exploitation et de réseau ;
- du Directeur des Opérations et de la Monétique.

Cependant, il a été constaté l'absence d'agents dédiés au contrôle des images de vidéosurveillance en temps réel. De plus, des zones à risques telles que les locaux techniques d'étage ne sont pas couverts. Enfin, la période de stockage des images de vidéosurveillance, actuellement de trente (30) jours est jugée insuffisante.

3.3.1.3. Faiblesses dans la gestion des accès à la salle serveurs

La salle serveurs se trouve dans les locaux de la DSI, au rez-de-chaussée du siège de la Banque. Lors de la visite de la mission dans cette salle, les points de faiblesse suivants ont été relevés :

- ventouse défectueuse de la porte principale d'accès à la DSI ;
- porte d'entrée vitrée de la salle serveurs ;
- absence de détecteur sismique malgré le fait que l'un des murs de la salle serveur soit mitoyen à l'arrière-cour de la Banque ;
- armoires rack maintenues ouvertes en permanence ;
- absence de contrôle de détection en cas de fermeture incomplète des portes de la DSI ou de la salle serveurs ;
- absence de revues inopinées de l'aménagement et des accès à la salle.

3.3.1.4. Emplacement non judicieux et inefficient de la salle serveurs de secours

La salle serveurs de secours de la banque se trouve dans les mêmes locaux que la salle serveurs principale. Un bureau se trouvant au 1er étage du siège, a été aménagé à cet effet il y a un an. Celui-ci, ne répondant pas aux normes d'aménagement des locaux techniques (à l'exception de la climatisation), expose la banque à des risques de sécurité. Nous comprenons, suite aux entretiens, que la Banque projette de déplacer cette salle vers une autre agence. Cependant, aucun échéancier validé de mise en production du nouveau site n'a été soumis à la mission.

3.3.2. Sécurité logique

L'évaluation des points de contrôles de la sécurité logique de la Banque a relevé les manquements ci-dessous.

3.3.2.1. Inexistence de politique de sécurité des systèmes d'informations, d'une charte informatique et d'une procédure de gestion des accès

Il n'existe pas de politique de sécurité des systèmes d'information, de charte informatique et d'une procédure de gestion des accès. A date, ces documents sont formalisés mais pas encore validés et mis en œuvre au sein de la Banque. Un programme de sensibilisation à la sécurité informatique a été initié le 10 Novembre 2016. Dans le cadre de ce programme, des bulletins de sécurité sont diffusés au personnel de la Banque.

3.3.2.2. Absence de revue périodique de la pertinence des habilitations attribuées

Aucune revue des habilitations n'a été opérée. En effet, depuis la mise en place de la matrice des droits dans le cadre de la migration du système d'information bancaire en Janvier 2015, les habilitations sont attribuées au fil de l'eau. La matrice des droits d'accès (habilitations) ne nous permet pas d'avoir les informations sur les droits en lecture, écriture et suppression des fonctions attribuées à chaque rôle. Lors des travaux, la mission a requis attribution d'un compte utilisateur sur l'application bancaire ayant uniquement des accès en lecture seule sur l'application. Nos différents tests effectués avec notre compte utilisateur nous ont permis d'avoir accès en lecture et modification aux modules qui sont incohérents avec notre profil.

Tableau 4 ***: Revue des habilitations du progiciel bancaire***

	Progiciel bancaire module Référentiel			Progiciel bancaire module applicatif		
	Création	Modification	Suppression	Création	Modification	Suppression
Fonctions Tiers	X	X	X			
Personnes physiques	X	X	X			
Affectation des comptes externes	X	X	X			
Création/MAJ modification autorisation de découvert				X	X	X
Validation des modifications des autorisations de découvert				X	X	X
Création d'opération de règlement Banque				X	X	X

SOURCE : nous-mêmes

3.3.2.3. Ecarts notés sur les comptes utilisateurs du domaine et du progiciel bancaire

Il n'existe pas au sein de la Banque de processus de revue périodique des comptes utilisateurs. Aucune revue périodique des comptes utilisateurs n'a été opérée par la Banque depuis la mise en production du nouveau système d'information bancaire. Cette défaillance du dispositif de contrôle interne nous a amené à procéder à une revue des comptes et profils sur le domaine et le progiciel bancaire. Notre revue des comptes de l'Active Directory et du progiciel bancaire a permis d'établir le tableau ci-après : :

Tableau 5 ***: Récapitulatif des écarts notés sur les comptes utilisateurs***

	Active Directory au 24/04/2017	**Progiciel bancaire au 26/04/2017**
Comptes génériques actifs	228	7
Comptes génériques inactifs	7	1
Comptes en doublon actifs	11	4
Comptes à droits d'administrateur	15	4
Comptes présents sur la liste du personnel (*)	209	229
Comptes absents de la liste du personnel (*)	64	126
Comptes présents sur la liste du personnel (*), et inconnus du domaine Active Directory	4	0
Comptes inactifs	51	4
Total	**555**	**407**

SOURCE : nous-mêmes

Nous comprenons lors de nos entretiens que :

- chaque doublon actif dans le progiciel bancaire correspond au compte d'un employé de la Banque lorsqu'il était stagiaire. En effet, le progiciel bancaire ne permet pas de transférer l'intégralité des fonctionnalités appliquées au dossier d'un client initié sous un compte vers un autre. Par conséquent, ces comptes stagiaires demeurent actifs ;
- les cent vingt-cinq (125) comptes du progiciel bancaire non présents dans la liste du personnel correspondent à des intérimaires caissiers qui ne font pas partie du personnel de la Banque.

3.3.2.4. Faiblesse de la stratégie de mot de passe d'accès au domaine et au progiciel bancaire

La mission a procédé à une analyse de la protection des accès aux systèmes, plus précisément de la stratégie de mot de passe mise en œuvre sur le contrôleur de domaine et le progiciel bancaire. Il en est ressorti des défauts de paramétrage pouvant impliquer des accès inappropriés ou frauduleux aux ressources informatiques, des altérations ou saisie de données frauduleuses ou non intentionnelles.

*Tableau 6**: Analyse des stratégies de mot passe Active Directory et du progiciel bancaire***

CRITERES	Bonnes pratiques	Active Directory	Progiciel bancaire
Longueur du mot de passe	8	6	1
Caractères alphabétiques	Oui	Non	Non
Caractères numériques	Oui	Non	Non
Caractères spéciaux exigés	Oui	Non	Non
Délai de réutilisation des mots de passe	3 derniers	10 derniers	Non
Période de validité du mot de passe	90 jours	90 jours	90 jours

Changement du mot de passe à la première connexion	Activé	Activé	Activé
Nombre de tentatives d'identification infructueuses avant désactivation du compte	3	3	5
Temps d'inactivité avant déconnexion automatique	15 min	30 min	30 min

SOURCE : nous-mêmes

Il est à noter que la Banque ne dispose pas de l'accès au paramétrage des mots de passe du progiciel bancaire. A date, la politique de paramétrage des mots de passe est formalisée mais pas encore mise en œuvre.

3.3.2.5. Faiblesse du dispositif de protection antiviral de la Banque

Le verrouillage de l'accès aux paramètres vitaux de l'antivirus Kaspersky Security 10 par l'utilisateur n'est pas effectif. En effet, l'utilisateur non-administrateur de son poste a la possibilité de désactiver le fonctionnement de son antivirus Kaspersky Security 10.

Tableau 7 ***: Analyse des ordinateurs couverts par l'antivirus Kaspersky Security 10***

	Kaspersky Security 10	
Ordinateurs sans antivirus installés	31	9,33%
Ordinateurs dont la date de dernière mise à jour est antérieure à 2017	8	2,40%
Ordinateurs présentant des risques élevés d'infection (au moins 100 virus détectés)	14	4,21%
Total	**332**	100%

SOURCE : nous-mêmes

3.3.3. Gestion du changement

L'évaluation des points de contrôles de la gestion du changement au sein de la Banque a relevé les manquements ci-dessous.

3.3.3.1. Absence de procédure de gestion des changements et évolutions

Il n'existe pas au sein de la Banque une procédure décrivant les dispositifs globaux en place pour la gestion des changements et évolutions. Nous constatons que les changements applicatifs sont pris en charge par les éditeurs tandis que les changements techniques sont gérés par le Département Exploitation et Réseau.

3.3.3.2. Absence de schéma directeur informatique

La Banque ne dispose pas de schéma directeur ou de plan informatique formalisé définissant les grandes orientations ou évolutions à moyen et long terme du système d'information. Nous comprenons que les demandes d'évolution, sur le progiciel bancaire notamment, sont remontées par les utilisateurs au fil de l'eau ou définis en fonction des évolutions légales puis étudiées par le comité de projet pour validation.

3.3.3.3. Absence de critères d'évaluation de l'efficacité dans le cadre de la gestion des changements et évolutions

La Banque est reliée au prestataire du progiciel bancaire dans le cadre d'un contrat de maintenance. Ainsi le prestataire prend en charge toutes les demandes d'évolution et de résolution d'incidents sur le progiciel bancaire. Une interface web a été mise en place par l'éditeur. Ainsi au moyen de cette interface, la Banque déclare toutes ses demandes

d'évolutions et des tickets sont créés avec des numéros de suivi. Trois niveaux de priorité des incidents déclarés existent : Bloquante, Majeure, Normale.

Aucun niveau de priorité ne dispose d'indicateurs définis pour assurer l'efficacité du processus mis en œuvre avec le prestataire et la continuité d'activité. Par ailleurs, ces critères ne sont pas mis en œuvre dans le cadre de la gestion des changements et évolutions techniques.

3.3.4. Gestion de l'exploitation

L'évaluation des points de contrôles de la gestion de l'exploitation au sein de la Banque a relevé les manquements ci-dessous.

3.3.4.1. Absence de procédure de gestion des incidents

Au sein de la Banque, il n'existe pas de procédure décrivant les dispositifs de gestion des incidents techniques et applicatifs. En effet, dans la procédure de clôture de journée, une partie traite des incidents d'exploitation liés à la non-exécution des batchs. Cependant, une procédure de gestion des incidents applicatifs du métier, sur le progiciel bancaire notamment, n'est pas mise en œuvre avec le prestataire en charge de leur gestion. Les dispositifs de gestion des incidents sur les serveurs et les systèmes ne font pas l'objet de documentation.

3.3.4.2. Absence de cartographie des applications du système d'information

Il n'existe pas de cartographie des applications du système d'information de la Banque. Les flux échangés entre les différentes applications et les opérations de contrôle associées ne sont pas consignés dans un document dédié.

3.3.4.3. Absence de traçabilité des incidents

Les incidents d'exploitation rencontrés lors des traitements de fin de journée ne font pas l'objet d'une traçabilité dans un répertoire dédié. En effet, ces incidents sont directement détectés par l'état de déroulement après exécution des batchs. Dans le cas d'incidents bloquants, ils sont relancés par l'exploitant directement. Les incidents non bloquants sont relancés manuellement le lendemain. Toutefois, nous notons que des emails sont envoyés aux responsables pour informer de l'état du déroulement des traitements. Par ailleurs, les incidents métiers sur le progiciel bancaire sont gérés au moyen d'une interface web de ticketing mise en œuvre par le prestataire. Nous notons cependant l'absence d'outil de ticketing propre à la Banque.

3.3.4.4. Utilisation d'un compte générique pour les traitements de fin de journée

Une procédure de clôture de journée existe, dans laquelle est consigné l'ordre d'exécution des modules. Les traitements de fin de journée sur le progiciel bancaire sont gérés par la Direction Exploitation et Réseau (DER) de la Banque. En effet, nous comprenons au cours de nos entretiens que les tâches d'exploitation sont réalisées par les exploitants. La DER dispose de deux exploitants : l'un travaille le matin (entre 7h et 15h) et le second l'après-midi (de 15h à 23h). Nous comprenons par ailleurs que la rotation des horaires de travail s'effectue à une fréquence hebdomadaire. Un calendrier annuel d'intervention de ces deux exploitants n'est pas mis en œuvre et tenu à jour au sein de la DER. En fin de journée, l'exploitant de l'après-midi est en charge de lancer les traitements de clôture. Nous notons que ces traitements sont réalisés au moyen d'un compte générique batch. Le mot de passe de ce compte est détenu uniquement par les exploitants. Après exécution de tous les batchs,

les états de contrôle sont envoyés par les exploitants au moyen d'email aux responsables de la DSI, la DPO, au Directeur Général.

3.3.5. Gestion de la sauvegarde et de la continuité d'activité

L'évaluation des points de contrôles de la gestion de la sauvegarde et de la continuité d'activité au sein de la Banque a relevé les manquements ci-dessous.

3.3.5.1. Absence de procédure de gestion des sauvegardes

Une procédure de gestion des sauvegardes n'a pas été mise en œuvre au sein de la Banque. Néanmoins, deux plans de sauvegarde ont été mis à notre disposition. Nous notons que ces plans ont été établis avec le prestataire en Janvier 2017, et n'ont toujours pas été mis en œuvre. A date de la mission, les processus de sauvegarde en place ne font l'objet d'aucune formalisation.

3.3.5.2. Absence de tests de restauration

Il n'existe pas de tests de restaurations des sauvegardes sur le progiciel bancaire. En effet, de tels tests permettraient de s'assurer de la capacité à reprendre l'activité en cas d'incident majeur. Cependant, nous notons que des restaurations sont régulièrement réalisées pour les bases de données en environnement de test par l'équipe de la DSI afin de valider des scripts mis en œuvre par le prestataire. En outre, nous notons un projet de mise en place d'un plan de restauration des machines virtuelles avec un contractant local . Cependant, aucune documentation n'a été mise en œuvre à date de la mission.

3.3.5.3. Absence de Plan de Continuité et/ou de Reprise des Activités

Un Plan de Continuité et/ou de Reprise d'Activité n'est pas mis en œuvre au sein de la Banque comme recommander par la banque centrale. Cependant, nous notons qu'il y a une budgétisation d'un Plan de Secours Informatique (PSI) dans le plan stratégique 2017 de la Direction Générale. Ce plan stratégique n'a pas été mis à notre disposition. Le tableau de bord de la Direction Projets et Organisation révèle que le Plan de Secours Informatique est prévu pour Décembre 2017.

3.4. Phase de conclusion de la mission

Au total, trente-cinq (35) points de contrôle ont été évalués sur les sous-thèmes des contrôles généraux informatiques. Pour chacun d'eux, le tableau de synthèse ci-dessous présente les axes d'améliorations :

*Tableau 8****: Synthèse des axes d'amélioration des contrôles généraux informatiques de la Banque***

Sous-Thèmes ITGC	Sécurité physique	Sécurité logique	Gestion des changements	Sauvegarde et continuité d'activité	Exploitation informatique	Gestion des services	Total
Nombre de points de contrôle revus	6	11	3	7	6	2	35
Nombre de points de contrôle effectivement mis en œuvre	2	1	1	1	0	2	7
Nombre de points de contrôle non implémentés	4	10	2	6	6	2	28
% des points de contrôles implémentés	33,3%	9%	33,3%	14,29%	0%	100%	20%

SOURCE : nous-mêmes

Nos différentes diligences ont permis de mettre en exergue vingt-neuf (29) constats pour lesquels des recommandations ont été émises. Leurs niveaux des risques sont présentés dans le tableau ci-dessous :

*Tableau 9****: Synthèse de l'évaluation du niveau de risque contrôles généraux informatiques de la Banque***

Sous-themes ITGC	Elevé	Moyen	Faible	Total
Sécurité physique	2	2	0	4
Sécurité logique	6	2	0	8
Gestion des changements	3	2	0	5
Sauvegarde et continuité d'activité	7	1	0	8
Exploitation informatique	4	0	0	4
Total	22	7	0	29

SOURCE : nous-mêmes

Une réunion a été organisée afin de présenter les résultats de la mission, puis le rapport de final et les preuves d'audit (voir annexe 7) ont été fournis à la Direction Générale de la Banque.

CHAPITRE 4 : RECOMMANDATIONS ET SUGGESTIONS ISSUES DE L'AUDIT DES CONTRÔLES GENERAUX INFORMATIQUES DANS LE CADRE D'UNE MISSION DE COMMISSARIAT AUX COMPTES REALISEE PAR LE CABINET MAZARS AU SENEGAL

A l'issue de notre mission d'audit, il est fondamental de formuler des recommandations sur la base des résultats et analyse des FRAP auxquelles nous avons aboutis. Ces recommandations visent à l'amélioration du dispositif de contrôle interne de l'environnement informatique de la Banque.

4.1. Recommandations et suggestions relatives à la sécurité physique

Les constats relevés sur la sécurité physique dans la phase d'accomplissement de la mission ont fait l'objet des recommandations et suggestions suivantes :

4.1.1. Manquements dans la protection des locaux techniques, contre les risques environnementaux

- Mettre en place une politique de protection contre les risques environnementaux et veiller à son respect ;
- Tenir compte de la sécurité physique de la salle serveurs et autres locaux techniques par rapport aux risques environnementaux dans le plan d'audit, et les revues réalisées par le Responsable de la Sécurité du SI ;
- Remplacer l'entrée à la salle serveurs par une porte ignifuge, pour un fonctionnement efficient du dispositif anti-incendie, de la climatisation, mais aussi pour renforcer la sécurité de la salle ;
- S'assurer du bon fonctionnement de l'appareil hydrométrique et mettre en place un écran d'affichage à l'extérieur de la salle ;

- Substituer l'hydrométrique défaillant par un nouveau, de préférence électronique, couplé à un thermomètre avec écran digital visualisable de l'extérieur ;
- Vider la salle de tous les objets inflammables, ou non utilisés ;
- S'assurer que tous les serveurs et équipements télécoms sont mis sous rack.

4.1.2. Insuffisance du dispositif de vidéosurveillance

- Dans la politique de sécurité, tenir compte de la gestion du dispositif de vidéosurveillance ;
- Mettre en place un poste de contrôle de sécurité (PCS) qui permettra à la Banque d'avoir une vue d'ensemble des systèmes de sécurité déployés ;
- Augmenter les capacités de stockage des stations de vidéosurveillance pour une conservation des images sur une période minimale de six (6) mois.

4.1.3. Faiblesses dans la gestion des accès à la salle serveurs

- Elaborer une politique de gestion des accès à la salle serveurs ;
- Faire une revue périodique des accès à la salle ;
- Remplacer les baies vitrées par des murs en dur ;
- Remplacer les portes vitrées par des portes coupe-feu ;
- S'assurer que la porte de la DSI reste verrouillée, ne permettant l'accès qu'aux personnes autorisées ;
- Mettre en place un système d'alarme permettant d'informer le personnel de la Direction en cas de défaut de verrouillage des portes ;
- Installer un détecteur sismique permettant de déceler toute vibration structurelle transmise par la paroi (mur, sol, plafond, porte, etc.) qui fait l'objet d'une tentative d'intrusion.

4.1.4. Emplacement non judicieux et inefficient de la salle serveurs de secours

Sur la base d'un échéancier réaliste et réalisable dans un court terme, finaliser les travaux d'installation du site de secours.

4.2. Recommandations et suggestions relatives à la sécurité logique

Les constats relevés sur la sécurité logique dans la phase d'accomplissement de la mission ont fait l'objet des recommandations et suggestions suivantes :

4.2.1. Inexistence de politique de sécurité des systèmes d'informations, d'une charte informatique et d'une procédure de gestion des accès

- Mettre à jour la politique de sécurité du système d'information en tenant compte des recommandations de la mission, la faire valider par la Direction Générale et sensibiliser les utilisateurs aux dispositifs définis dans la politique ;
- Valider la charte informatique, la faire signer à tous les utilisateurs et systématiser sa signature par les nouveaux arrivants à la remise du matériel informatique ;
- Mettre à jour la procédure de gestion des accès en tenant compte des recommandations de la mission, la faire valider par la Direction Générale et la mettre en œuvre au sein de la Banque ;
- Appuyer la procédure de gestion des accès par un outil de ticketing permettant l'historisation de toutes les demandes de création, modification, désactivation des comptes utilisateurs applicatifs et de l'Active Directory.

4.2.2. Absence de revue périodique de la pertinence des habilitations attribuées

- Formaliser et faire valider par la Direction de la Banque, la matrice des droits d'accès (habilitations) incluant :
  - les fonctions attribuées à chaque rôle ;
  - les droits d'accès (lecture, écriture, suppression) octroyés à chaque fonction en relation avec le rôle adéquat.
- Formaliser et mettre en œuvre dans la procédure de gestion des accès, une revue périodique des habilitations incluant :
  - le contrôle annuel de la justification des rôles attribués au regard des évolutions de l'utilisateur dans l'organisation : nouveau poste, changement de service etc.
  - le contrôle annuel de la justification des fonctions attribuées aux rôles ;
  - le contrôle annuel des droits d'accès (lecture, écriture, suppression) attribuées aux fonctions.
  - élaborer des rapports de ces revues périodiques par la direction de l'audit.

4.2.3. Ecarts notés sur les comptes utilisateurs du domaine et du progiciel bancaire

- Formaliser et mettre en œuvre dans la procédure de gestion des accès, une revue périodique des comptes incluant :
  - le contrôle annuel de présence dans les effectifs ;

- le contrôle trimestriel des comptes multiples, des comptes génériques et administrateurs.

- Elaborer des rapports de ces revues périodiques par la Direction de l'Audit.
- Identifier les comptes d'administration avec les privilèges au sein d'un document formel mis à jour et validé périodiquement par la Direction de l'Audit.

4.2.4. Faiblesse de stratégie de mot de passe d'accès au domaine et au progiciel bancaire

- Faire valider par la Direction Générale et mettre en œuvre la politique de paramétrage des mots de passe au sein de la Banque ;
- Le paramétrage des mots de passe du progiciel bancaire doit pouvoir être effectué par des membres identifiés et formés de la DSI. Il faudra donc un transfert de compétence.

4.2.5. Faiblesse du dispositif de protection antivirale de la Banque

- Rendre impossible à l'utilisateur la désactivation ou modification de la configuration de l'antivirus.
- Elaborer et mettre en œuvre une procédure de supervision de la plateforme de protection antivirale (mise à jour, installation d'antivirus).

4.3. Recommandations et suggestions relatives à la gestion du changement

Les constats relevés sur la gestion du changement dans la phase d'accomplissement de la mission ont fait l'objet des recommandations et suggestions suivantes :

4.3.1. Absence de procédure de gestion des changements et évolutions

- Définir et mettre en œuvre dans une procédure un processus unique pour la gestion des changements et des évolutions applicatifs et techniques de la Banque. Idéalement, appuyer ce processus sur un outil de ticketing permettant l'historisation des changements ;
- Communiquer cette procédure à l'ensemble des collaborateurs concernés (Centre de Compétences, DSI, utilisateurs métiers, correspondants fonctionnels et informatiques) et veiller à sa correcte application.

4.3.2. Absence de schéma directeur informatique

Définir les grandes orientations stratégiques du système d'information, à horizon de 2 à 3 ans, avec les équipes métiers afin de s'assurer de la prise en compte de leurs besoins et des évolutions règlementaires. Pour cela, s'appuyer du plan stratégique de la Banque.

4.3.3. Absence de critères d'évaluation de l'efficacité dans le cadre de la gestion des changements et évolutions

- Convenir avec l'éditeur des délais maximums pour la résolution des incidents suivant leur priorité. Formaliser ces délais dans un contrat de maintenance et définir les pénalités en cas de résolution d'un incident dans des délais inadéquats à sa priorité.
- Mettre en œuvre un comité technologique en charge du suivi de la correcte mise en œuvre des termes du contrat.

- Mettre en œuvre un SLA en interne avec la Direction de l'Exploitation et du Réseau de la Banque dans lequel des critères d'évaluation de l'efficacité opérationnelle seraient définis.

4.4. Recommandations et suggestions relatives à l'exploitation

Les constats relevés sur la gestion de l'exploitation dans la phase d'accomplissement de la mission ont fait l'objet des recommandations et suggestions suivantes :

4.4.1. Absence de procédure de gestion des incidents

Mettre en œuvre une procédure décrivant tous les dispositifs en place pour la gestion des incidents techniques et applicatifs au sein de la Banque.

4.4.2. Absence de cartographie des applications du système d'information

- Mettre en œuvre une cartographie des applications, des interfaces et des flux de données du SI. S'assurer que cette cartographie est revue et mise à jour périodiquement.
- Mettre en œuvre une documentation technique pour chaque flux de données spécifiant au moins les éléments suivants :
    - l'application / système source et cible,
    - la nature des données échangées,
    - la fréquence et le mode de déclenchement du flux de données,
    - les tâches de surveillance en cas d'incident opérationnel

4.4.3. Absence de traçabilité des incidents

Appuyer la procédure de gestion des incidents dont la mise en œuvre a été recommandée plus haut d'un outil de tracking pour la gestion des incidents. Un tel outil permettrait de garder la traçabilité des incidents et d'assurer le suivi par un comité technologique à mettre en place.

4.4.4. Utilisation d'un compte générique pour les traitements de fin de journée

- Attribuer aux exploitants les droits pour l'exécution des traitements de fin de journée à partir de leurs comptes personnels.
- Mettre en œuvre au sein de la Direction Exploitation et Réseau (DER) un planning prévisionnel d'intervention des exploitants et tenir à jour ce planning.

4.5. Recommandations et suggestions relatives à la gestion de la sauvegarde et de la continuité d'activité

Les constats relevés sur la gestion de la sauvegarde et de la continuité d'activité dans la phase d'accomplissement de la mission ont fait l'objet des recommandations et suggestions suivantes :

4.5.1. Absence de procédure de gestion des sauvegardes

Mettre en œuvre au sein de la Banque une procédure de sauvegarde sur bande et de restauration des sauvegardes. Définir dans cette procédure la fréquence des sauvegardes, les matériels utilisés, le stockage, les responsabilités, les modalités de supervision, la planification du déroulement des sauvegardes, les dispositifs de restaurations, l'externalisation des bandes, etc.

4.5.2. Absence de tests de restauration

- Mettre en œuvre une cartographie des applications, des interfaces et des flux de données du SI. S'assurer que cette cartographie est revue et mise à jour périodiquement.
- Mettre en œuvre une documentation technique pour chaque flux de données spécifiant au moins les éléments suivants:
    - l'application / système source et cible,
    - la nature des données échangées,
    - la fréquence et le mode de déclenchement du flux de données,
    - les tâches de surveillance en cas d'incident opérationnel

4.5.3. Absence de Plan de Continuité et/ou de Reprise des Activités

- Poursuivre le projet de mise en œuvre du Plan de Secours Informatique dans le cadre d'un projet globale de mise en place d'un système de continuité d'activité couvrant les modalités techniques, humaines et logistiques.
- Réaliser une analyse quant aux besoins en termes de reprise d'activité de façon globale au sein de la Banque, en particulier en termes de délai maximum d'interruption autorisé et de pertes maximales de données acceptables. Cet exercice devra être réalisé en collaboration avec les directions métiers, par domaine de données.

CONCLUSION DE LA DEUXIEME PARTIE

Grâce au modèle d'analyse présenté dans la première partie, nous avons déroulé aisément la mission d'audit des contrôles généraux informatiques de la Banque. Ainsi, au terme de cette mission, il en est ressorti des points à consolider ainsi que des points faiblesses à améliorer.

Après avoir analysé les problèmes constatés, nous avons émis des recommandations dont la mise en œuvre permettra d'améliorer et optimiser le dispositif de contrôle interne de l'environnement informatique de la Banque.

CONCLUSION GENERALE

Notre étude a été développée en deux (02) parties : la première consacrée à la revue de la littérature nous a permis d'appréhender les contrôles généraux informatiques et l'intégration de l'audit de ces contrôles dans l'approche d'audit globale. Ensuite, le modèle d'analyse nous a permis de mettre en œuvre la partie pratique à partir d'une prise de connaissance de la Banque, puis l'évaluation du dispositif de contrôle interne de l'environnement informatique. Ainsi, pour atteindre les différents objectifs que nous nous sommes fixés au départ, nous avons pu :

- identifier, analyser et évaluer des risques généraux informatiques inhérents, prendre connaissance des contrôles relatifs aux thèmes : la sécurité physique, la sécurité logique, la gestion du changement, la gestion de l'exploitation, la gestion de la sauvegarde et de la continuité d'activité ;
- effectuer des tests de contrôles en termes de conception et d'efficacité opérationnelle ;
- faire des recommandations permettant d'améliorer le dispositif de contrôle interne de l'environnement informatique.

Suite à cette démarche, et les faiblesses majeures identifiées nous sommes amenés à émettre des réserves quant à la fiabilité du système d'information en ce qui a trait à la production d'informations financières à partir du progiciel bancaire.

Les faiblesses ci-après nécessiteraient la mise en œuvre de plans d'actions visant à améliorer le niveau de contrôle interne lié au SI. En effet, les risques concernent principalement les manquements liés à la sécurité logique du système d'information bancaire, la sauvegarde et continuité d'activité, et l'exploitation informatique. Nous notons qu'au moment de réalisation de la mission le déploiement du nouveau système d'information bancaire était en cours de finalisation avec l'intégrateur.

Au terme de notre étude, nous espérons avoir apporté une piste de solutions, aussi modeste soit-elle, aux problèmes relevés sur le dispositif de contrôle interne de l'environnement informatique de la Banque. La prise en compte des recommandations qui ont été formulées permettra à l'entreprise d'améliorer le dispositif de contrôle interne de l'environnement informatique de la Banque. Une fois les contrôles généraux informatiques maîtrisés, il serait approprié d'évaluer le niveau de maîtrise des contrôles applicatifs de la Banque.

ANNEXES

Annexe 1 : Calendrier d'intervention

CALENDRIER (*)

LUN	MAR	MER	JEU	VEN	SAM	DIM
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Travaux sur site

Séance de restitution

Annexe 2 : Demande documentaire

#	Documents de base	Date de la demande
1	Organigramme de la Direction des Systèmes d'Information	21/03/2017
2	Accords de niveaux de service entre la DSI et les utilisateurs dans l'utilisation du SIB	21/03/2017
3	Contrat et accords de niveaux de service entre la BHS et l'éditeur du progiciel bancaire	21/03/2017
4	Politique de sécurité informatique	21/03/2017
5	Schéma directeur informatique comprendra les évolutions majeures prévus ou déjà réalisées (Roadmap)	21/03/2017
6	Présentation et/ou compte-rendu des comités de pilotage	21/03/2017
7	Procédure de gestion des évolutions	21/03/2017
8	Extraction de l'ensemble des demandes d'évolution formulées après la mise en production du SIB	21/03/2017
9	Procédure de gestion des incidents liés au SI	21/03/2017
10	Extraction des incidents de la plateforme datant du déploiement du SIB	21/03/2017
11	Procédure de sauvegarde et de restauration des données du SIB	21/03/2017
12	Plan de continuité d'activité (PCA) et plan de reprise d'activité (PRA)	21/03/2017
13	Plan de secours informatique (PSI)	21/03/2017
14	Procédure de gestion des comptes utilisateurs et habilitations, y compris employés temporaires et accès à distance	21/03/2017
15	Procédure d'administration des rôles et/ou profils	21/03/2017
16	Matrice des habilitations du SIB	21/03/2017
17	Liste exhaustive des comptes créés dans le système, leurs habilitations et dates de dernière connexion	21/03/2017
18	Extraction des paramètres généraux de sécurité du SIB	21/03/2017

#	Documents de base	Date de la demande
1	Méthodologie et organisation associée au projet de migration du SIB	21/03/2017
2	Manuel utilisateurs	21/03/2017
3	Rapport d'installation du serveur	21/03/2017
4	Données de reprise	21/03/2017
5	Rapports d'analyse des besoins	21/03/2017
6	Planning complet du projet	21/03/2017
7	Stratégie de migration	21/03/2017
8	Stratégie de recette et PV associés	21/03/2017
9	Plan de bascule et plan de retour arrière	21/03/2017
10	PV de mise en production	21/03/2017
11	Documentation de retour sur expérience	21/03/2017
12	Matrice de suivi des risques	21/03/2017
13	Documentation (présentations, et compte-rendu) relative aux comités de pilotage	21/03/2017
14	Supports de formation	21/03/2017
15	Stratégie de formation (planning, recensement des populations, supports, etc.)	21/03/2017
16	Résultats de l'enquête de satisfaction des utilisateurs sur le progiciel	21/03/2017
17	Cahier des charges élaboré	21/03/2017
18	PVs de dépouillement des réponses à l'appel d'offre, et autres documents ayant conduit au choix de l'éditeur	21/03/2017
19	Tableau de bord de suivi des requêtes avec BFI	05/04/2017

Annexe 3: Planning d'entretiens

PLANNING D'ENTRETIENS

1. Présentation de l'environnement informatique
2. Projet de migration du Système d'Information Bancaire
3. Système de Gestion de la Sécurité de l'Information
4. Présentation du progiciel bancaire

DATE	CRENEAUX HORAIRES	INTERLOCUTEURS
Mercredi 05 Avril	14H30-16H	*A discuter*
Mercredi 05 Avril	16H-17H30	*A discuter*
Jeudi 06 Avril	11H-12H30	*A discuter*
Jeudi 06 Avril	14H30-16H	*A discuter*
Jeudi 06 Avril	16H-17H30	*A discuter*
Vendredi 07 Avril	09H-10H30	*A discuter*
Vendredi 07 Avril	11H-12H30	*A discuter*

Annexe 4 : Programme de travail sur la sécurité logique

Contrôle objectif	Risques abordés	Essais d'efficacité de conception	Test d'efficacité opérationnelle
Politiques et procédures	La sécurité informatique est documentée par: - une politique de sécurité informatique. - une charte de l'utilisateur informatique, que les employés doivent déclarer formellement reconnaître. Les programmes de sensibilisation à la sécurité informatique et la formation sont menés au sein de l'entreprise.	*- L'accès non autorisé aux ressources informatiques,* *- Utilisation inappropriée des ressources informatiques.*	Recueillir la politique de sécurité informatique et la charte des utilisateurs informatiques. Vérifiez que les deux documents sont périodiquement revus et à jour. Vérifier qu'un processus disciplinaire en cas de violation de la politique de sécurité informatique et de la charte utilisateur de l'informatique est défini et suivi. Vérifier si les lois et règlements spécifiques à un pays sont respectés. Recueillir la stratégie de formation pour vérifier la couverture de la sécurité informatique.
Gestion des identités	La gestion des accès aux ressources informatiques (création, modification et désactivation des droits d'accès et / ou comptes d'utilisateurs) fait l'objet d'un processus formalisé et consigné. Les demandes de droits d'accès et / ou de comptes d'utilisateurs sont formellement approuvées avant d'être traitées.	*- Accès inapproprié ou frauduleux aux ressources informatiques,* *- altération ou saisie de données frauduleuses ou non intentionnelles.*	Recueillir le compte utilisateur et la procédure de gestion des droits d'accès. Vérifiez que ce document décrit au moins les éléments suivants: - la description des processus de création, de modification et de désactivation des droits d'accès et / ou des comptes d'utilisateurs, y compris les super utilisateurs, qui devraient être couverts par un processus spécifique, - les rôles et les responsabilités au sein de ces processus.

Contrôle objectif	Risques abordés	Essais d'efficacité de conception	Test d'efficacité opérationnelle
Gestion des identités	«Les comptes d'utilisateurs sont uniques et nominatifs. Les comptes privilégiés sont réservés au personnel autorisé. Ces comptes sont distincts des comptes principaux des utilisateurs correspondants. "	*- Accès inapproprié ou frauduleux aux ressources informatiques,* *- Altération ou saisie de données frauduleuses ou non intentionnelles,* *- Perte de la piste d'audit / des journaux des actions des utilisateurs.*	Vérifiez que la politique de sécurité informatique spécifie les règles relatives à la gestion des identités (comptes nominatifs, utilisation de comptes secondaires à des fins administratives, interdiction des comptes génériques, etc.).
Gestion des identités	En collaboration avec les départements d'affaires, les comptes d'utilisateurs sont régulièrement revus afin de vérifier: - que l'existence des comptes est valable compte tenu de la liste du personnel (comptes actifs / inactifs), - les droits d'accès accordés aux comptes d'utilisateurs sont cohérents avec les fonctions de l'employé au sein de l'organisation.	*- Accès inapproprié ou frauduleux aux ressources informatiques,* *- altération ou saisie de données frauduleuses ou non intentionnelles.*	Vérifiez que la procédure de gestion des droits d'accès et des comptes d'utilisateurs spécifie l'examen périodique des comptes d'utilisateur.

Contrôle objectif	Risques abordés	Essais d'efficacité de conception	Test d'efficacité opérationnelle
Sécurité d'accès	Les paramètres de sécurité relatifs aux mots de passe sont conformes aux meilleures pratiques.	*- Accès inapproprié ou frauduleux aux ressources informatiques,* *- altération ou saisie de données frauduleuses ou non intentionnelles.*	Vérifiez que la stratégie de sécurité informatique spécifie les règles et les contraintes de sécurité sur les mots de passe. Vérifiez que ces règles sont conformes aux meilleures pratiques.
Sécurité d'accès	Par nature, les comptes de service ne sont pas expirés. Pour couvrir les risques inhérents à ces comptes, les actions suivantes sont appliquées: - l'organisation de campagnes périodiques de renouvellement de mot de passe, - la désactivation de la possibilité de se connecter en utilisant le compte (" logon interactif ").	*- Accès inapproprié ou frauduleux aux ressources informatiques,* *- Altération ou saisie de données frauduleuses ou non intentionnelles,* *- Perte de la piste d'audit / des journaux des actions des utilisateurs.*	Vérifiez que la politique de sécurité informatique spécifie le processus de gestion des comptes de service. Vérifiez si des contraintes de complexité sont appliquées aux mots de passe de ces comptes. Vérifiez si les paramètres de mot de passe par défaut de l'administrateur ont été modifiés (système d'application, réseau et base de données).
Séparation des tâches	Les principes de la séparation des tâches sont documentés dans une matrice et sont mis en œuvre dans les systèmes. La matrice de séparation des tâches est périodiquement revue dans l'ordre suivant:	*Altération ou saisie de données frauduleuses ou non intentionnelles.*	Obtenir et analyser les matrices de ségrégation des tâches définies par l'entreprise, couvrant à la fois l'informatique et les secteurs d'activité.

Contrôle objectif	Risques abordés	Essais d'efficacité de conception	Test d'efficacité opérationnelle
	- pour assurer le respect des meilleures pratiques, - d'évaluer l'alignement de ces principes sur la réalité opérationnelle de l'entreprise.		
Séparation des tâches	La séparation des tâches est assurée dans le cadre du processus de gestion de l'accès des utilisateurs: aucun utilisateur ne peut traiter seul le processus de gestion des accès des utilisateurs: demander, approuver et mettre en œuvre les droits d'accès.	*- Accès inapproprié ou frauduleux aux ressources informatiques,* *- Altération ou saisie de données frauduleuses ou non intentionnelles,* *- Perte de la piste d'audit / des journaux des actions des utilisateurs.*	Vérifiez que la procédure de gestion du compte utilisateur et des droits d'accès spécifie la séparation des tâches dans le processus pour les utilisateurs informatiques et les utilisateurs professionnels.
Sécurité Internet	Le système d'information (postes de travail, serveurs, etc.) est suffisamment protégé contre les menaces virales.	- Altération des données ou vol, - Indisponibilité du système d'information.	Identifier les systèmes antispam et antivirus en usage au sein de l'entreprise. Vérifiez qu'un processus de surveillance de l'antivirus est en place.

Contrôle objectif	Risques abordés	Essais d'efficacité de conception	Test d'efficacité opérationnelle
Sécurité Internet	Les points d'entrée du réseau de la société sont protégés contre les menaces externes (Firewall, IPS, IDS, etc.) et les ports USB sont bloqués ou sécurisés.	*- Altération des données ou vol,* *- Indisponibilité du système d'information.*	Identifier les outils mis en œuvre afin de protéger le SI contre les attaques extérieures. Vérifiez notamment que les messages et les fichiers joints sont décontaminés et qu'un logiciel anti-spam est installé. Identifier les outils mis en œuvre pour gérer l'accès externe ou distant (pour les employés) au réseau d'entreprise via une connexion sécurisée (TOKEN, VPN, HTTPS, etc.). Vérifiez que les composants du réseau tels que la segmentation de réseau sont implémentés. Vérifiez si les fentes USB sont bloquées ou sécurisées. Obtenir et analyser la procédure de gestion des règles et des paramètres de pare-feu et de proxy. Vérifiez qu'il spécifie: - le processus de gestion des règles de pare-feu (implémentation, maintenance, etc.), - le processus de gestion des exceptions par procuration.
Sécurité Internet	Les utilisateurs n'administrent pas eux-mêmes leurs postes de travail et ne peuvent donc pas installer de logiciels non autorisés.	*- Utilisation inappropriée des ressources informatiques,* *- altération des données ou vol,* *- Non-conformité aux conditions d'utilisation du logiciel IS '.*	Lors d'une entrevue, demandez-vous si l'utilisateur dispose de droits d'administration sur son poste de travail. En outre, identifier les outils mis en œuvre afin de contrôler le logiciel installé sur les postes de travail.

Annexe 5 : Compte rendu de réunion sur la sécurité logique

MAZARS
Département Consulting
ITAS

PV d'Entretien

Compte Rendu de Reunion

Tenue le 12/04/2017 à 16H00

ETAIENT PRESENTS :

- M. [redacted] Consultant IT (MAZARS)
- M. Mohamed Sylla, Consultant IT (MAZARS)
- M. [redacted] DSI (BANQUE)
- M. [redacted] Directeur de l'Exploitation (BANQUE)

ORDRE DU JOUR :

- Entretien sur la sécurité logique

POINTS DISCUTES :

Sécurité logique

- Gestion des identités
- Sécurité des accès
- Sécurité internet

La gestion des identités de l'Active Directory est assurée par M. XXXX (Directeur de l'exploitation) et celle de progiciel bancaire par M. XXXX (DSI)

La procédure de gestion des identités n'a pas été formalisée. Le processus décrit au cours des entretiens se présentent comme suit :

L'entité émet une demande de création d un nouvel utilisateur de progiciel bancaire et/ou Active Directory avec en copie la direction de l audit, la direction des ressources humaines, et la direction générale à l adresse suivante habilitations@Banque.sn.

L'identifiant de l'utilisateur progiciel bancaire est défini à partir de son matricule dans l'entreprise tandis que l'identifiant de la session Windows est défini à partir du nom et prénom dans l'Active Directory. Notons que si le nouvel utilisateur de progiciel bancaire est un stagiaire, le DSI lui attribue un matricule.

Confidentiel – Propriété de Mazars Sénégal

MAZARS
Département Consulting
ITAS

PV d'Entretien

Une fois l'utilisateur créé et ses habilitations attribuées, une note est envoyée à celui-ci avec l'identifiant et le mot de passe. Lors de la première connexion, le système (Progiciel bancaire / Active Directory) impose à l'utilisateur le changement de mot de passe.

La stratégie de paramétrage du mot de passe de la session Windows est définie dans l'Active Directory tandis que le mot de passe de Progiciel bancaire n'a pas de stratégie de paramétrage. En effet, sur Progiciel bancaire, la seule contrainte est la taille du mot de passe, au minimum 4 caractères.

En outre, les demandes suivantes sont aussi envoyer à l'adresse [illegible]

- changement de poste;
- changement d'agence;
- réinitialisation d'un mot de passe;
- attribution de nouvelle habilitation.

L'attribution de nouvelle habilitation, le changement de poste, la sortie d'un collaborateur de l'entreprise ne font l'état d'une procédure formalisée. En effet, l'information parvient parfois par email aux gestionnaires des identités mais en très souvent de manière informelle (de mémoire, suite à une conversation, etc…)

Quelquefois, il est procédé à un toilettage des utilisateurs sur une base informelle, c'est-à-dire :

- la suppression des utilisateurs qui ne font plus partir du personnel de la Banque
- la mise à jour de la matrice des droits de Progiciel par chaque entité (notons que chaque entité met à jour les droits à octroyer ou pas à certains profils)
- la suppression des comptes inactifs

L'antivirus Kaspersky est déployé sur les postes de la Banque.

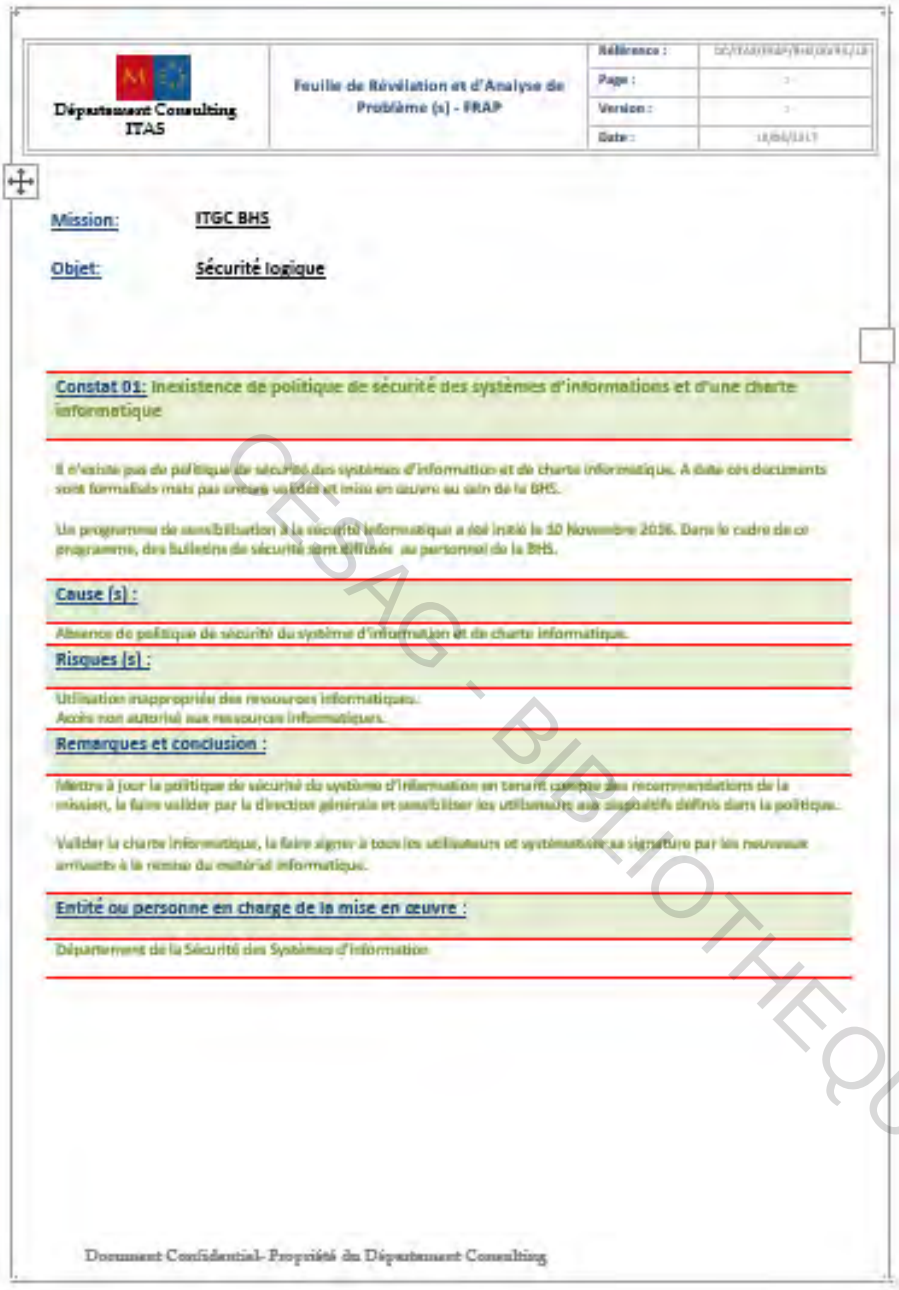
RETOUR SUR LES ACTIONS ISSUES DES REUNIONS PRECEDENTES :

ACTION POINT	RESPONSABLE(S)	STATUS
•		
•		

DECISIONS :

Confidentiel – Propriété de Mazars Groupe

Annexe 6 : FRAP Sécurité logique



Département Consulting ITAS	Feuille de Révélation et d'Analyse de Problème (s) - FRAP	Référence :	
		Page :	
		Version :	
		Date :	

Mission: ITGC BHS

Objet: Sécurité logique

Constat 01: Inexistence de politique de sécurité des systèmes d'informations et d'une charte informatique

Il n'existe pas de politique de sécurité des systèmes d'information et de charte informatique. A date ces documents sont formalisés mais pas encore validés et mise en œuvre au sein de la BHS.

Un programme de sensibilisation à la sécurité informatique a été initié le 10 Novembre 2016. Dans le cadre de ce programme, des bulletins de sécurité sont diffusés au personnel de la BHS.

Cause (s) :

Absence de politique de sécurité du système d'information et de charte informatique.

Risques (s) :

Utilisation inappropriée des ressources informatiques.
Accès non autorisé aux ressources informatiques.

Remarques et conclusion :

Mettre à jour la politique de sécurité du système d'information en tenant compte des recommandations de la mission, la faire valider par la direction générale et sensibiliser les utilisateurs aux aspects définis dans la politique.

Valider la charte informatique, la faire signer à tous les utilisateurs et systématiser sa signature par les nouveaux arrivants à la remise du matériel informatique.

Entité ou personne en charge de la mise en œuvre :

Département de la Sécurité des Systèmes d'Information

Document Confidentiel- Propriété du Département Consulting

Annexe 7 : Preuves d'audit

MAZARS

LISTE DES PREUVES D'AUDIT

Date : 02/05/2017

	Documents de base	Disponib	Fourni	Date de deman	Date de transmissio	Nom du document	Commentaires de la Banque
1	Organigramme de la Direction des Systèmes d'Information	Oui	Oui	21/03/2017	06/04/2017	Organigramme de la DSI	
2	Accords de niveaux de service entre la DSI et les utilisateurs dans l'utilisation du SIB	NON	Non	21/03/2017			
3	Contrat et accords de niveaux de service entre la BHS et l'éditeur du progiciel bancaire	Oui	Oui	21/03/2017	06/04/2017	Contrats et accords de service BHS-BFI	
4	Politique de sécurité informatique	NON	OUI	21/03/2017	14/04/2017	version à date de la politique de sécurité du système c	C'est en cours d'élaboration, fait partie des objectifs 2017 de DPO/RSSI
5	Schéma directeur informatique comprendra les évolutions majeures prévus ou déjà réalisées (Roadmap	NON	Non	21/03/2017			Evolutions du SI incluses dans le document des objectifs 2017 de DSI et DPO
6	Présentation et/ou compte-rendu des comités de pilotage	Oui	Oui	21/03/2017	06/04/2017	- Compte -rendu des comités de pilotage	
7	Procédure de gestion des évolutions	Oui	Oui	21/03/2017	06/04/2017	Procédure de gestion des évolutions et incidents	
8	Extraction de l'ensemble des demandes d'évolution formulées après la mise en production du SIB	Oui	Oui	21/03/2017	06/04/2017	Extraction incifents et évolutions Carthago	
9	Procédure de gestion des incidents liés au SI	Oui	Oui	21/03/2017	06/04/2017	Procédure de gestion des évolutions et incidents	
10	Extraction des incidents de la plateforme datant du déploiement du SIB	Oui	Oui	21/03/2017	06/04/2017	Extraction incifents et évolutions Carthago	
11	Procédure de sauvegarde et de restauration des données du SIB	Oui	Oui	21/03/2017	06/04/2017	Procédure de sauvegarde	
12	Plan de continuité d'activité (PCA) et plan de reprise d'activité (PRA)	NON	Non	21/03/2017			Fait partie des objectifs 2017, budget prévu
13	Plan de secours informatique (PSI)	NON	Non	21/03/2017		Projet de mise en œuvre au cours de l'année 2017	
14	Procédure de gestion des comptes utilisateurs et habilitations, y compris employés temporaires et accès à distance		Non	21/03/2017			
15	Procédure d'administration des rôles et/ou profils		Non	21/03/2017			
16	Matrice des habilitations du SIB	Oui	Oui	21/03/2017	06/04/2017	Matrice des droits	
17	Liste exhaustive des comptes créés dans le système, leurs habilitations et dates de dernière connexion		Non	21/03/2017			

BIBLIOGRAPHIE

OUVRAGES

1. ACPR (2018), *Le risque informatique* , Banque de France, 48 pages
2. ANGOT Hugues (2004), *système d'Information de l'entreprise,* 4eme Edition, De Boeck Supérieur, Bruxelles, 193 pages.
3. BOUNFOUR Ahmed, GEORGES Epinette (2006), *Valeur et performance des SI: Une nouvelle approche du capital immatériel de l'entreprise,* DUNOS, Paris, 244 pages.
4. CHAI (2014), *Guide d'audit des systèmes d'information*, CHAI, Paris, 112 pages.
5. COBIT 5, ISACA, 98 pages
6. Commission bancaire (1996), *livre blanc sur la sécurité des systèmes d'information dans les établissements de crédit*, Commission bancaire, 344 pages
7. Compagnie régionale des commissaires aux comptes (2017), *audit informatique : tous concernés ! 10 fiches pratiques pour réussir*, Paris, 39 pages.
8. DEYRIEUX André (2003), *le système d'information : nouvel outil de stratégie,* Editions, MAXIMA, Paris, 185 pages.
9. DUMONT Christian (2011) *ITIL Pour un service informatique optimal*, Eyrolles, Paris, 378 pages.
10. GUERRERO Sylvie (2008) , *les outils de l'audit social*, Edition Dunod.
11. HAMZAOUI Mohamed (2008), *Gestion des risques d'entreprise et contrôle interne,* Etude (broché).
12. IFACI (2014), *Cadre de Référence International des Pratiques professionnelles de l'Audit Interne*, Edition IFACI, Paris, 254 pages.
13. IIA (2010), *Global Technology Audit Guide (GTAG) 1 et 2 : Les risques et les contrôles des systèmes d'information*,2ème édition, 40 pages.
14. IIA (2008), *Global Technology Audit Guide (GTAG) 11: Developping the IT Audit Plan*, IIA, Altamonte Springs, 34 pages.
15. Lafitte M. (2003), *Les grands projets de systèmes d'information dans les établissements bancaires*, Revue Banque Edition
16. LAUDON Kenneth, LAUDON Jane, FIMBEL Eric, COSTA Serge, CANEVET- LEHOUX Sophie (2013), *Management des systèmes d'information*, 13e Edition, PEARSON, Paris, 666 pages.

17. O'BRIEN James A., MARION Guy (1995), *les systèmes d'information de gestion,* De Boeck Université, Montréal, 768 pages.*Results*, Harvard Business Review Press, Boston, 269 pages.

Autres documents

1. Manuel de Préparation CISA, 26 Edition, ISACA. 2016
2. Mémoire « le système d'information bancaire », Faculté des Sciences Juridiques, Economiques et Sociales, Université Sidi Mouhamed Ben Abdellah de FES, 41 pages.
3. Support de cours de Master audit des systèmes d'information 2011-2012 (Paris Dauphine).
4. Support de cours de MBA audit des systèmes d'information 2015-2016 (CESAG).
5. Support de cours de MBA cartographie des risques (CESAG).

TABLE DE MATIERE