Centre Africain d'études Supérieures en Gestion

CESAG

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

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

Promotion 22
(2010-2011)

CESAG - BIBLIOTHEQUE

Mémoire de fin d'étude

THEME

EVALUATION DES RISQUES LIES A L'APPLICATION INFORMATIQUE DE GESTION DU CREDIT : CAS DE LA CNCA SENEGAL.

Bibliothèque du CESAG
111776

Présenté par :

M. Papa Makha BEYE

Dirigé par :

M. Alain SAWADOGO
PROFESSEUR ASSOCIE
CESAG

Avril 2012

DEDICACES

Je dédie ce travail

A mon père et ma mère qui se sont occupés de ma tendre enfance, surtout de ma perfection et de mon éducation dès le bas âge. Aucun langage, fut-il sublime, ne peut traduire la gratitude et les sentiments que j'éprouve pour eux.

A mes frères et sœurs.

A mes cousins et cousines.

A mes oncles et tantes.

A mes neveux et nièces.

A mes chers ami(e)s.

A toute la communauté scientifique.

CESAG - BIBLIOTHEQUE

REMERCIEMENTS

Je souhaite témoigner ma profonde gratitude et mes remerciements les plus sincères à mon directeur de mémoire Monsieur SAWADOGO Alain pour ses conseils et le temps qu'il m'a accordé pour la réalisation de ce rapport.

J'adresse également mes remerciements au Directeur du Contrôle Général de la CNCAS et ses plus proches collaborateurs (M. FALL, M. DIOP, M. SECK, M. SY, M. NDIAYE et Mme KANFODI), pour les documents qu'ils m'ont fournis, nécessaires à la rédaction du présent mémoire ; pour l'accueil chaleureux, le soutien indéfectible tout au long de ce stage et les multiples conseils qui m'ont été donnés, enfin, la disponibilité totale dont ils ont fait montre pour répondre à toutes mes attentes.

Mes remerciements vont aussi à l'endroit de Ousmane NDAO et tout le personnel de la CNCAS pour sa disponibilité et sa collaboration.

Enfin, je remercie le corps professoral et administratif du CESAG pour le service rendu, et plus particulièrement Monsieur YAZI Moussa, Directeur de l'Institut Supérieur de la Comptabilité, qui m'a été d'un soutien considérable dans la réalisation du présent mémoire de fin d'études.

CESAG - BIBLIOTHEQUE

LISTE DES SIGLES ET ABREVIATIONS

AFAI	Association Française de l'Audit et du Conseil Informatique
CAJRC	Cellule des Affaires Juridiques, Recouvrements et Contentieux
CI	Contrôle interne
CII	Contrôle interne informatique
CLUSIF	Club de la Sécurité des Systèmes d'Information Français
CNCAS	Caisse Nationale de Crédit Agricole du Sénégal
CNCC	Compagnie Nationale des Commissaires aux Comptes
COBIT	Control Objectives for Information and related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRAMRA	Caisse Régionale d'Assurance Maladie Rhône-Alpes
DCG	Direction du Contrôle Général
DCR	Direction du Crédit et du Réseau
DG	Direction Générale
DOER	Directeur des Opérations, Engagements et Risques
FAR	Feuille d'Analyse des Risques
FERMA	Federation of European Risk Management Associations
IFACI	Institut Français de l'Audit et du Contrôle Internes
IIA	Institute Internal Auditor
ISACA	Information Systems Audit and Control Association
MARION	Méthode d'Analyse de Risques Informatiques Orientée par Niveaux
MEHARI	Méthode Harmonisée d'Analyse des Risques
MEP	Mise en Place
PGI	Progiciel de Gestion Intégrée
POCA	Pratiques d'Organisation Communément Admises
QCI	Questionnaire de Contrôle interne
QPC	Questionnaire de Prise de Connaissance
SDIO	Sous Direction de l'Informatique et Organisation
SG	Secrétaire Général
SI	Système d'information
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TFfA	Tableau des Forces et faiblesses Apparentes

CESAG - BIBLIOTHEQUE

LISTE DES TABLEAUX ET FIGURES

A. Liste des Tableaux

B. Liste des Figures

CESAG - BIBLIOTHÈQUE

LISTE DES ANNEXES

CESAG - BIBLIOTHEQUE

TABLE DES MATIERES

CESAG - BIBLIOTHEQUE

CESAG - BIBLIOTHEQUE

CESAG - BIBLIOTHEQUE

INTRODUCTION GENERALE

CESAG - BIBLIOTHEQUE

L'accès des organisations aux technologies de l'information et de la communication tend à modifier la communication entre les différents acteurs du monde des affaires. Notamment entre l'entreprise et ses clients, le fonctionnement interne de l'entreprise et la relation de l'entreprise avec ses différents partenaires et fournisseurs (BLAIN, 2006 : 03). Ce nouveau modèle suppose l'intégration des principaux processus de l'entreprise et la mise en place d'un système d'information cohérent garantissant l'unicité de l'information et l'accès à celle-ci à partir de toutes les fonctions de l'organisation.

L'efficacité de la gestion bancaire est liée à celle des informations relatives à son exploitation, c'est à dire l'enregistrement des mouvements des différentes opérations de banque et d'exploitation des comptes bancaires. La gestion informatique du crédit demeure encore une préoccupation majeure pour toutes les institutions financières désirant rendre leur organisation et leur gestion plus cohérente et plus performante. Ainsi pour s'adapter aux changements que connaît l'environnement et atteindre leurs objectifs stratégiques, plusieurs banques ont adopté des progiciels bancaires pour assurer la gestion quotidienne de leurs activités.

CESAG - BIBLIOTHEQUE

C'est le cas de la Caisse Nationale de Crédit Agricole du Sénégal (CNCAS). La CNCAS est une banque de la place créée en 1984. En plus des missions traditionnelles de toute banque, elle est connue pour le financement des activités agricoles et des autres activités du secteur primaire. A l'instar des autres institutions financières de la place, la CNCAS exploite, depuis longtemps, un progiciel standard du marché pour assurer ses orientations organisationnelles et stratégiques.

L'utilisation de logiciels standards de gestion du crédit par nos institutions financières africaines ne garantie toujours pas la conformité avec leurs processus métiers et n'est pas exempt de risques. Au delà des risques techniques que sont la confidentialité, l'intégrité et la disponibilité des données ; la gestion informatique du crédit présente, entre autres, les risques opérationnels suivants :

- l'octroi de crédit par un utilisateur non délégataire ;
- le dépassement des habilitations du délégataire ;
- le dépassement de la capacité d'endettement du client.

Ces risques peuvent avoir plusieurs causes dont :

- l'inadaptation du progiciel avec le processus de crédit de la banque ;
- la gestion décentralisée du crédit du fait de la dispersion géographique du réseau d'agences de la banque ;
- le défaut de paramétrage des règles de gestion ;
- la faiblesse du dispositif de prévention des risques ;
- l'insuffisance du contrôle hiérarchique ;
- la négligence de certains opérationnels.

Les consequences qui en découlent sont :

- le non respect de la politique de crédit de la banque ;
- l'anarchie ;
- le défaut de paiement ou la perte de chiffre d'affaire prévisionnel ;
- les fraudes.

CESAG - BIBLIOTHEQUE

Pour une bonne maitrise des risques opérationnels de la gestion informatique du crédit, les solutions envisageables sont, entre autres, les suivantes :

- développer un logiciel sur mesure ;
- veiller au respect des procédures de crédit de la banque ;
- créer un service de Risk management ;
- maîtriser les risques opérationnels liés au progiciel de gestion du crédit en place.

Du fait de l'importance des coûts de développement d'un progiciel sur mesure, la solution retenue est la maîtrise des risques opérationnels du progiciel de crédit déjà acquis.

Au regard de la solution retenue, la question principale de recherche est : quel est le niveau d'efficacité du système de maîtrise des risques opérationnels liés à l'application informatique de gestion du crédit de la CNCAS ?

Pour bien mener notre étude, la question principale interpelle les questions spécifiques suivantes :

- quels sont les risques opérationnels liés au progiciel de gestion du crédit ?
- quels sont les dispositifs mis en œuvre par la CNCAS pour la maîtrise de ces risques ?
- quel est le niveau d'efficacité des contrôles informatiques ?
- quel est le degré de criticité des risques opérationnels liés à l'application de gestion du crédit de la CNCAS ?

Pour répondre à ces questions, nous avons retenu comme thème de recherche : « **Evaluation des risques opérationnels liés à l'application informatique de gestion du crédit : cas de la CNCAS** ».

CESAG - BIBLIOTHEQUE

Notre étude a pour objectif général l'évaluation des risques opérationnels liés à la gestion informatique du crédit. En outre, elle sous-tend aussi les objectifs spécifiques suivants :

- l'identification des risques opérationnels liés à l'application de gestion du crédit de la CNCAS ;
- l'évaluation de l'efficacité du dispositif de maîtrise de ces risques ;
- l'évaluation de la criticité de chaque risque opérationnel identifié ;
- la conception de la matrice des risques liés à la gestion informatique du crédit ;
- la proposition de recommandations pour maîtriser les faiblesses constatées.

Cependant, on notera très tôt que notre étude ne traitera pas l'organisation administrative de la gestion du crédit mais on se limitera tout simplement aux risques émanant du processus informatique de gestion du crédit.

L'intérêt du mémoire se situe à deux niveaux :

a) **Pour l'entreprise** :

Cette étude permettra d'abord à l'entreprise de connaitre le niveau de risques liés à la gestion informatique du crédit en particulier et ensuite d'améliorer ou de mettre en œuvre un dispositif de maitrise des risques liés aux applications informatiques de gestion en général.

b) **Pour nous-mêmes**

Ce travail, nous donnera l'opportunité de mettre en pratique la théorie qu'on a apprise sur la démarche et la méthodologie de l'audit en général et l'évaluation des risques liés aux applications informatiques en particulier.

Notre étude s'articule sur deux grandes parties :

- ✓ Le cadre théorique qui constitue la première partie de ce travail permettra d'abord de mieux cerner la notion de risques et contrôles informatiques (chapitre 1), ensuite la démarche d'évaluation et les méthodes d'analyse des risques applicatifs (chapitre 2) et enfin la méthodologie de l'étude (chapitre 3) ;
- ✓ La deuxième partie, dénommée cadre pratique, sera consacrée à la présentation générale de la CNCAS (chapitre 4) ; à la description du processus et de l'application de gestion du crédit de la CNCAS (chapitre 5) et à l'évaluation des risques opérationnels liés à l'application informatique de gestion du crédit accompagnée de recommandations pour la maitrise de ces risques (chapitre 6).

CESAG - BIBLIOTHEQUE

PREMIERE PARTIE : CADRE THEORIQUE

CESAG - BIBLIOTHEQUE

INTRODUCTION DE LA PREMIERE PARTIE

« C'est la théorie qui décide de ce que nous pouvons observer » Albert Einstein (THUILLIER, 1981). Donc cette première partie théorique va être la lanterne de notre étude. Elle sera consacrée à la revue critique de la littérature en matière d'évaluation des risques en général et celle des risques applicatifs en particulier.

Cette partie va nous permettre d'acquérir une connaissance élargie des aspects techniques de l'évaluation des risques applicatifs. Elle sera aussi le lieu pour nous d'essayer de donner des réponses à la question de recherche et aux questions spécifiques du mémoire.

CESAG - BIBLIOTHEQUE

La première partie de mémoire va être constituée de trois chapitres de synthèse de la littérature sur les thèmes suivants :

- les risques et contrôles informatiques ;
- l'évaluation et les méthodes d'analyse des risques informatiques ;
- les outils de collecte et d'analyse des données.

CHAPITRE I : RISQUES ET CONTRÔLES APPLICATIFS

Introduction

Aujourd'hui et de plus en plus, les entreprises utilisent l'informatique pour gérer leurs différents processus. De ce fait, presque l'ensemble des processus des entreprises repose sur les systèmes d'information informatisés. C'est ce qui amène l'AFAI (2008a : 8) à considérer les systèmes informatiques comme éléments clés des processus des organisations et qu'ils constituent la base des activités de contrôle : c'est la quatrième composante du contrôle interne (CI).

L'utilisation des systèmes informatiques permet de réduire considérablement l'intervention humaine mais accroît aussi les risques liés aux technologies de l'information.

Or, la fiabilité des informations financières et opérationnelles est un des objectifs principaux du CI (RENARD, 2010 : 144). Donc la fiabilité de ces informations passe d'abord nécessairement par la fiabilité des systèmes informatiques qui les produisent. D'où la mise en place de ce que l'on appelle les contrôles informatiques qui constituent des dispositifs de maîtrise des risques informatiques.

CESAG-BIBLIOTHEQUE

1.1. Les risques informatiques

Pour aborder les risques informatiques, nous allons d'abord le définir ensuite donner ses différentes typologies et enfin lister.

1.1.1. Définition du risque informatique

En matière informatique, le risque est définit comme :

- un événement susceptible de compromettre l'atteinte de l'objectif du projet informatique (dérapage de son planning, de son cout) ou l'objectif de l'activité informatique (performance des systèmes, pérennité des outils, sécurité des données) (DESMOULINS, 2009 : 216) ;
- le risque métier associé à l'utilisation, la possession, l'exploitation, l'implication, l'influence et l'adoption de l'informatique dans une organisation (AFAI, 2010 : 12) ;

- l'exploitation de manière fortuite ou délibérée d'une ou plusieurs vulnérabilités du système d'information par une menace interne ou externe (CHARTRES & al, 2002 : 8).

Donc, nous pouvons retenir que le risque informatique dans une entreprise est étroitement lié à la dépendance de cette entreprise par rapport à son système d'information (BALLOY, 2002 : 6) et il peut résulter d'une multitude d'événements : technologiques, commerciaux, environnementaux, règlementaires, humains, etc (DESMOULINS, 2009 : 216-217).

1.1.2. Typologie des risques informatiques

Selon l'Assemblée plénière des sociétés d'assurances dommages (in BALLOY, 2002 : 6), la typologie des risques regroupe trois catégories principales (accidents, erreurs, malveillances), elles-mêmes décomposées en sous-catégories selon la nature du risque.

Selon le GUIDEINFORMATIQUE (2012), on peut répartir les risques informatiques en deux catégories :

- les risques logiques : ils sont d'origine humaine soit lorsque les informaticiens ou les utilisateurs créent eux-mêmes des situations illogiques, voire dangereuses ; soit lors d'attaques externes criminelles (virus et intrusion).

- les risques physiques : ils sont liés à l'environnement du système informatique (accès, bâtiments, fourniture électrique, climatisation...). Les risques physiques qui menacent l'informatique sont essentiellement liés :

  - à l'homme ;
  - les maladresses,
  - les malveillances ;
  - aux bâtiments ;
  - aux sinistres (incendie, inondation…) ;
  - aux avaries d'environnement - climatisation, électricité....

CESAG BIBLIOTHEQUE

Pour l'AFAI & al (2007 : 06), les risques peuvent être scindés en risques internes et risques externes. Les risques internes étant ceux qui prennent leurs sources au sein du périmètre de l'entité (salariés, équipes internes de gestion, processus et organisation de l'entreprise, etc.) et les risques externes ont pour sources l'extérieur de l'entité (partenaires commerciaux, pirates, etc.).

1.1.3. Les différents risques informatiques

Les risques informatiques peuvent être scindés en cinq (5) grandes catégories : ceux liés à la sécurité logique, à l'exploitation des applications, à la maintenance des applications, à la gestion des incidents, au plan de secours.

Par rapport aux risques liés aux applications informatiques, on peut identifier les risques par rapport à la sécurité logique, à l'exploitation des applications, à la maintenance des applications, à la gestion des incidents, au plan de secours, etc.

CESAG - BIBLIOTHEQUE

1.1.3.1. Risques liés à la sécurité logique

La sécurité logique est l'ensemble des sécurités qui tournent autour de la protection des données de l'entreprise, des applications et du système d'information.

Ces risques liés à la sécurité logique peuvent être cités :

- accès non autorisé ;
- absence de confidentialité ;
- altération des données ;
- dépassement des habilitations utilisateurs ;
- attaque logique du réseau ou intrusion ;
- vice caché d'un progiciel.

1.1.3.2. Risques liés à l'exploitation des applications et du système

L'exploitation des applications et du système est l'ensemble des procédures et des moyens mis en œuvre pour la production de l'information par le biais du système informatique.

Ces risques suivants peuvent être dus à l'exploitation des applications et du système :

- indisponibilité du système ;
- absence de traces des opérations des utilisateurs ;
- non continuité de l'exploitation ;
- erreur de saisie ;
- erreur de paramétrage ;
- erreur de transmission ;
- malveillance ;
- carence du personnel ;
- perte de données (sauvegardes et stockage des données) ;
- accident matériel (panne, bug, climatisation, électricité, sinistre…).

1.1.3.3. Risques liés à la maintenance des applications

Les risques suivants peuvent être cités parmi d'autres par rapport à la maintenance des applications :

- carence de prestataires ;
- altération accidentelle des données pendant la maintenance ;
- dégradation involontaire de performances, à l'occasion d'une opération de maintenance.

1.1.3.4. Risques liés à la gestion des incidents

Si on s'inspire de la définition d'un incident de sécurité du système d'information de l'AFAI (2011 : 11), on peut définir un incident informatique comme un événement potentiel ou avéré, indésirable et/ou inattendu, impactant ou présentant une probabilité forte d'impacter le système informatique en termes de disponibilité, d'intégrité, de confidentialité et/ou de preuve.

Les risques qui peuvent être liés à la gestion des incidents sont :

- inexistence de procédures formelles de signalement ;
- inexistence de journal des incidents ;
- non priorisation de traitement des incidents.

CESAG - BIBLIOTHEQUE

1.1.3.5. Risques liés au plan de secours

Le plan de secours est défini par MENTHONNEX (1995 : 200) comme « l'ensemble des solutions étudiées par la direction générale de l'entreprise et par la direction informatique pour reprendre l'activité informatique après un sinistre total, dans des conditions qui permettent la survie de l'entreprise ».

Les risques suivants peuvent être liés avec le plan de secours :

- non fonctionnalité du plan de continuité informatique ;
- inexistence de sauvegardes ;
- inexistence de procédures alternatives pour les utilisateurs ;
- non prise en compte des dernières évolutions du système.

Face à ces risques, il existe les contrôles informatiques qui constituent leur dispositif de maîtrise.

CESAG - BIBLIOTHEQUE

1.2. Les contrôles informatiques

« Les contrôles informatiques permettent d'atténuer les risques inhérents à l'usage d'une technologie par une organisation. Il peut s'agir de politiques d'entreprise aussi bien que de leur mise en œuvre en programmes informatiques, de protection des accès physiques à la capacité d'imputer des actions et des transactions aux utilisateurs, de validations automatiques ou encore d'analyse de cohérence pour un grand volume de données » (IIA, 2005 : 1).

Parmi les contrôles des systèmes informatiques, on distingue deux grandes catégories : les contrôles généraux et les contrôles applicatifs.

1.2.1. Les contrôles généraux informatiques

Selon l'IIA (2007 : 2), les contrôles généraux informatiques s'appliquent à tous les composants, processus et données des systèmes d'une organisation, ou d'un environnement de systèmes. Ils ont pour objectif de veiller au développement et à la mise en œuvre appropriés des applications, à l'intégrité des fichiers de programmes et de données, ainsi que des opérations informatiques.

Les contrôles généraux informatiques les plus courants regroupent notamment (IIA, 2005 : 5 ; PROTIVITI, 2004 : 2 ; IIA, 2007, 2) :

- l'organisation générale et la double séparation des fonctions entre informaticiens et non informaticiens d'une part, et entre études et exploitation informatiques, d'autre part. ces notions doivent être dans un organigramme de la direction des systèmes d'information et une description des rôles et responsabilités de ses équipes ;
- les procédures de développement / maintenance ou d'acquisition des logiciels et matériels ;
- les procédures de mise en production des applications et de leurs évolutions ;
- le suivi d'exploitation et de gestion des incidents ;
- les sauvegardes et plan de secours techniques ;
- la gestion du parc informatique (cartographie, inventaire) ;
- les éventuels contrats d'infogérance ;
- la méthodologie de gestion des projets informatiques (développements et infrastructures techniques) ;
- la politique de sécurité de l'information (sécurité des installations, du réseau, des systèmes d'exploitation, des applications et des données) ;
- la gestion de l'acquisition et de la mise en place de systèmes ;
- contrôles sur la gestion des changements dans les programmes ;
- contrôles de sauvegarde et de restauration des systèmes et des données ;
- la continuité d'activité.

CESAG - BIBLIOTHEQUE

Dans les dispositifs de maîtrise des risques informatiques, on retrouve, à coté des contrôles généraux informatiques, les contrôles applicatifs qui sont directement intégrés dans les différentes applications informatiques

1.2.2. Les contrôles applicatifs

Ils contribuent directement au système de contrôle interne. Selon l'AFAI (2008b : 34), ils permettent aux entreprises de garantir la saisie exhaustive, exacte, valide et vérifiable de toutes les transactions commerciales significatives des processus métiers ainsi que le traitement, l'enregistrement et l'édition de ces dernières par le système.

Les contrôles applicatifs peuvent être automatiques ou manuels. Selon la CNCC (2003 : 59) et KPMG (2004 : 37), les contrôles automatiques sont directement intégrés dans les applications et sont effectués de manière automatique dans différents stades de traitement de l'information alors que les contrôles manuels sont effectués par les utilisateurs et viennent compléter les premiers. De ce fait, les contrôles manuels sont essentiellement constitués de contrôles hiérarchiques.

Selon DERRIEN (1992 : 25), un bon contrôle interne implique l'existence de contrôles hiérarchiques sur les opérations. Et pour lui, ce principe a pour conséquence informatique la définition :

- de procédures de validation des opérations par un supérieur hiérarchique dès leur saisie ;
- soit de procédures d'édition d'états de contrôle des opérations de saisies (exhaustif ou par exception), pour analyse *a posteriori* par un supérieur hiérarchique ;
- soit d'une combinaison des deux types de procédures.

Il est important de noter que les contrôles manuels sont le plus souvent en aval. C'est pourquoi THORIN (2000 : 115) fait remarquer que, les contrôles automatiques doivent permettre d'avertir les utilisateurs distraits sur l'importance des erreurs d'entrée et qu'ils soient plus en amont et doivent se poursuivre durant tous le processus de traitement des données pour garantir la fiabilité des informations de sortie.

Les contrôles des applications peuvent être soit préventifs, soit de détection par nature (IFAC, 2009 : 50).

1.2.2.1. Les contrôles préventifs

« La qualité de fonctionnement d'un système d'information suppose une prévention et une protection suffisantes et cohérentes vis-à-vis des risques encourus » (NAAIMA, 2002 : 34). Pour répondre à ce besoin, les développeurs des applications informatiques de gestion ont intégré dans leur conception des contrôles préventifs.

CESAG - BIBLIOTHEQUE

Les contrôles préventifs sont des contrôles a priori, c'est-à-dire effectués avant toute action dans le système (CNCC, 2003 : 59) et destinés à empêcher que des erreurs puissent être faites (KPMG, 2004 : 36).

Ainsi les contrôles de prévention peuvent être classés en deux (2) catégories :

- les contrôles d'accès aux applications ;
- les contrôles de saisie des données.

1.2.2.1.1. Les contrôles d'accès aux applications

Selon l'IFACI (1993 : 6), THORIN (2000 : 89) et la CNCC (Avril 2003 : 60), les contrôles d'accès aux applications informatiques ont pour objectif de garantir la protection des informations et la confidentialité de celles-ci.

Ils sont nécessaires pour :

- garantir les accès interdits à toute personne non autorisée à utiliser l'application ;
- accorder le droit à certains collaborateurs d'utiliser certaines fonctions de l'application ;
- limiter la consultation des données confidentielles à certains utilisateurs autorisés.

CESAG - BIBLIOTHEQUE

En outre, pour DERRIEN (1992, 20) les procédures d'autorisation d'accès aux applications permettent de limiter les risques de manipulations frauduleuses par des utilisateurs.

Les contrôles d'accès aux logiciels peuvent prendre plusieurs formes et sont le plus souvent mis en œuvre par des codes d'identification couplés de mots de passe pour chaque utilisateur. De ce fait donc, chaque personne responsable de la saisie ou de la modification des transactions commerciales peut être identifiée dans le système (AFAI, 2008 : 35).

Selon l'IFACI (1993 : 6), les fonctions d'identification et d'authentification des utilisateurs peuvent être :

- intégrées aux différentes applications ;
- réalisées par un logiciel de contrôle d'accès ;
- assurées par un système de gestion de base de données.

Pour que les contrôles d'accès aux données puissent être efficaces, il faut que les mots de passe ne soient connus que par leur propriétaire et un groupe restreint[1] et les mots de passe doivent être changés fréquemment (LY, 2005 : 128).

Par ailleurs, cette approche des contrôles d'accès est un outil efficace permettant de répondre à l'objectif majeur de contrôle interne qu'est la séparation des tâches (DERRIEN, 1992 : 25 ; IFACI, 1993 : 6 et KHADIR, 2004 : 13). Ce principe de séparation des fonctions est mis en œuvre dans les systèmes applicatifs par ce que l'on appelle gestion des habilitations ou gestion des profils utilisateurs.

Pour KHADIR (2004 : 13), la gestion des habilitations permet d'acquérir un niveau d'assurance raisonnable quant au fait que seuls les utilisateurs autorisés ont accès aux ressources nécessaires à l'accomplissement de leurs tâches et en liaison avec leurs rôles et responsabilités.

CESAG - BIBLIOTHEQUE

1.2.2.1.2. Les contrôles de saisie

Les contrôles de saisie sont conçus pour assurer la fiabilité des données saisies sur les applications. Ils sont le plus souvent intégrés directement dans les systèmes applicatifs.
L'objet de ces contrôles est d'empêcher les erreurs de saisie. « Ils servent essentiellement à vérifier l'intégrité des données saisies dans une application, qu'elles soient saisies directement par les utilisateurs, à distance par un partenaire ou à travers une application Web » (IIA, 2005 : 11).

On peut distinguer deux niveaux de contrôle de saisie des données :

- le contrôle des champs de saisie ;
- le contrôle des ensembles de champs.

a) le contrôle des champs de saisie

Comme son nom l'indique le contrôle des champs de saisie porte seulement sur les caractères spécifiques du champ concerné.

1 Par exemple la hiérarchie directe pour des mesures de sécurité concernant la continuité de l'exploitation

Les contrôles typiques des champs de saisie sont, entre autres, les suivants (AFAI, 2008 : 35-36) :

- masques de saisie compréhensibles et conviviaux avec des contrôles de format de données intégrés (par ex. champs de date, données numériques, champs obligatoires, etc. et liste de valeurs prédéfinies et récurrentes) ;
- contrôle automatique approfondi des valeurs saisies (par ex. dépassements de valeurs limites du champ de saisie, contrôle de plausibilité des contenus du champ de saisie) ;
- affichage des libellés de code complets après saisie du code (par ex. la désignation d'un article s'affiche à la saisie du numéro d'article) ;
- saisie de contrôle (appelée également double saisie, contrôle des 4 yeux) pour les valeurs importantes.

CESAG - BIBLIOTHEQUE

b) le contrôle des ensembles de champs

Selon la CNCC (2003 : 61), ce type de contrôle s'effectue sur un champ en prenant en compte la valeur d'autres champs et vise à vérifier la cohérence d'un ensemble de données élémentaires. L'ensemble considéré peut être :

- un lot d'opérations ;
- un enregistrement d'un fichier ;
- le fichier lui-même.

1.2.2.2. Les contrôles détectifs

Les contrôles détectifs peuvent être regroupés trois (3) catégories :

- les contrôles des traitements ;
- les contrôles des transmissions ;
- les contrôles des sorties.

1.2.2.2.1. Les contrôles des traitements

Selon l'IIA (2007 : 2,19), ces contrôles surveillent les données en cours de traitement et constituent un moyen automatisé de faire en sorte que le traitement soit complet, exact et autorisé. Ils sont conçus pour apporter une assurance raisonnable que le traitement des données s'est déroulé comme prévu, sans omission ni double décompte. Ces contrôles sont :

- les totaux intermédiaires ;
- les rapports des totaux de contrôle ;
- les contrôles des fichiers et des opérateurs, tels que les labels externes et internes ;
- les journaux système des opérations informatiques et les tests de vraisemblance.

Un état de contrôle permet de suivre les traitements et « en cas de rejet d'un mouvement, un enregistrement doit être créé de manière à permettre la surveillance de la correction et du traitement ultérieurs et une des méthodes consiste à utiliser un état trié par date d'ancienneté des mouvements rejetés non encore corrigés » (IFACI, 1993 : 10).

CESAG - BIBLIOTHEQUE

1.2.2.2.2. Les contrôles des transmissions

Il peut arriver une transmission de fichiers entre deux applications différentes ou dans un même système applicatif. Donc pour THORIN (2000 : 89), aucune données ne doit être perdue, ni déformée par la transmission et pour maitriser de cette transmission, il faut pouvoir contrôler selon la CNCC (2003 : 63) que :

- le fichier reçu est le fichier émis par le correspondant ;
- l'émetteur envoie la bonne version du fichier ;
- le contenu du fichier reçu est identique au contenu envoyé.

1.2.2.2.3. Les contrôles des sorties

Ces contrôles portent sur ce qui est fait des données et doivent rapprocher les résultats en sortie avec le résultat escompté, en confrontant les données de sortie aux données entrées comme (IIA, 2007 : 2,19) :

- comparer et rapprocher les totaux de contrôle sortis pendant le traitement, aux totaux de contrôle d'entrée et intermédiaires produits en cours de traitement.
- comparer les rapports de modification générés par l'ordinateur pour les fichiers maîtres, aux documents source originaux afin de vérifier que l'information est correcte.

Conclusion

Ce chapitre a été consacré à l'étude des risques informatiques et aux dispositifs de maitrise de ces derniers qui sont les contrôles informatiques. Ils permettent de garantir la confidentialité, l'intégrité et la disponibilité des données afin d'assurer la fiabilité des informations financières et opérationnelles qui est un des principes fondamentaux du CI.

Ces contrôles informatiques sont constitués de contrôles généraux et de contrôles applicatifs. Les premiers s'appliquent à tous les composants, processus et données des systèmes d'une organisation, ou d'un environnement de systèmes. Alors que les seconds sont intégrés dans les applications et peuvent être automatiques ou manuels. Ils ont pour but la prévention ou la détection des erreurs. Par conséquent, pour être plus efficaces, les contrôles applicatifs doivent être plus préventifs que détectifs et plus automatiques que manuels.

CESAG - BIBLIOTHEQUE

CHAPITRE II : EVALUATION ET MÉTHODES D'ANALYSE DES RISQUES INFORMATIQUES

Introduction

L'évaluation des risques constitue la quatrième composante du modèle COSO 2. Comme nous le rappelle MOREAU (2002 : 01), le risque est, par définition, au cœur de l'entreprise qui évolue en permanence dans un univers de risques, le plus souvent complexe, dynamique et hostile.

Pour le comité de Bâle (1998 : 13), dans la perspective du contrôle interne, l'évaluation des risques doit permettre d'identifier et d'apprécier les facteurs internes et externes pouvant compromettre la réalisation des objectifs opérationnels. Ces risques internes ou externes doivent être évalués (Coopers & LYBRAND, 2000 : 49) pour permettre à l'entreprise d'établir des actions en vue de réduire et de maintenir la menace à un niveau raisonnable et acceptable (CARPENTIER, 2009 : 24).

CESAG - BIBLIOTHEQUE

Selon l'AFAI (2008a : 50), « la multiplication des risques liés au contrôle interne est probablement plus importante en ce qui concerne les systèmes d'information que dans d'autres secteurs de l'organisation ». ANGOT & al (2004 : 265) abordent dans le même sens pour dire que l'intégration des systèmes augmente la complexité et le degré de sophistication de l'environnement informatique ; ce qui peut accroitre le risque et nécessiter une attention particulière.

Ce chapitre est structuré en deux grandes (2) sections : la démarche d'évaluation des risques applicatifs et la présentation de quelques méthodes d'analyse et de gestion des risques informatiques.

2.1. Démarche d'évaluation des risques applicatifs

Il découle de la revue de littérature que la démarche d'évaluation des risques applicatifs se décline comme suit : l'identification des ces risques ; l'évaluation du contrôle interne informatique et la cotation des risques.

2.1.1. Identification des risques

C'est la première étape de toute démarche d'évaluation des risques. Elle vise à identifier l'exposition d'une organisation à l'incertitude (FERMA, 2003 : 6). Car, comme le dit l'AFAI (2008a : 37), parmi toutes les fonctions et tous les processus de l'entreprise, certains supportent des niveaux de risques particulièrement importants alors que d'autres bénéficient de niveaux nettement plus faibles.

Pour PR4M4 (2010 : 13), l'identification des risques est le processus de recherche, de reconnaissance et d'enregistrement des risques.
Cette phase va conditionner la suite de la mission en permettant à l'auditeur de « construire son référentiel, de concevoir son programme et de l'élaborer de façon « modulée », en fonction non seulement des menaces mais également de ce qui a pu être mis en place pour y faire face » (RENARD, 2010 : 233).

CESAG - BIBLIOTHEQUE

En ce qui concerne les risques informatiques, ce processus de recherche des risques peut être défini par les actions suivantes (CARPENTIER, 2009 : 29) :

- identification des actifs (une première bonne pratique est de connaître la liste des matériels et logiciels) utilisés par les services informatiques ;
- identification des menaces et de leurs impacts possibles sur la confidentialité, la disponibilité et l'intégrité de ces actifs.

Selon la FERMA (2003 :15), les techniques d'identification de risque sont entre autres :

- le brainstorming ;
- les questionnaires ;
- les comparaisons sectorielles ; (benchmarking) ;
- l'analyse de scénarios ;
- les ateliers d'appréciation des risques ;
- les enquêtes sur les accidents ;
- l'inspection ;
- HAZOP (Études de Risque et d'Opérabilité).

Cette phase d'identification des risques peut être matérialisée par un tableau des risques avec notamment le nom du risque, sa nature, son impact (exemple faible, moyen, important) et son dispositif de maitrise, etc.

2.1.2. Evaluation des contrôles généraux informatiques

Selon GENEVA (2011), les contrôles généraux comprennent tous les contrôles de l'infrastructure informatique nécessaires au fonctionnement des applications.

L'évaluation de ces contrôles consistera à évaluer les forces et les faiblesses de la fonction informatique par rapport :

- à la séparation des fonctions informatiques ;
- à la sécurité physique de l'infrastructure informatique ;
- à la sécurité logique du réseau et des données ;
- aux procédures de développement et maintenance des logiciels et matériels ;
- aux procédures d'exploitation des applications ;
- à la gestion des incidents informatiques ;
- aux sauvegardes et au plan de continuité de l'activité.

CESAG - BIBLIOTHEQUE

Après avoir apprécié les contrôles généraux, maintenant il faut étudier, de façon minutieuse, les contrôles notamment leur conception et leur efficacité.

2.1.3. Evaluation des contrôles applicatifs

Les contrôles applicatifs peuvent être évalués à travers la qualité de leur conception et de leur efficacité.

2.1.3.1. Évaluation de la conception des contrôles

Les principaux risques ont été identifiés dans la première étape. Maintenant, l'évaluation de la conception des contrôles, notamment leur positionnement dans le processus métier, permet de savoir s'il y a une adéquation entre les risques identifiés et les dispositifs de contrôles applicatifs mis en place, c'est-à-dire mettre en œuvre les contrôles appropriés pour remédier aux risques identifiés (IIA, 2005 : 20).

Le but de cette étape consiste à atteindre une qualité de contrôle adéquate avec le moins possible de contrôles.

Selon l'AFAI (2008b : 24), une analyse minutieuse de la conception des contrôles permet :

- d'identifier les lacunes, les chevauchements et les doublons en matière de contrôles ;
- d'éviter la réalisation onéreuse de contrôles par les services et, le cas échéant, les tests de fonctionnement des contrôles par l'auditeur en cas de contrôles inappropriés ;
- d'envisager que le même résultat ou un meilleur résultat peut être obtenu avec l'utilisation ou l'adaptation d'autres contrôles, notamment de contrôles déjà établis.

Pour une bonne évaluation de la conception des contrôles, il faut faire, entre autres :

- des interrogations avec les personnes intervenant dans la réalisation des contrôles ;
- des observations physiques d'activités de contrôle ;
- des tests de cheminement par exemple suivre les différents flux d'une donnée dans le système.

CESAG - BIBLIOTHEQUE

A la suite de cette étape, l'auditeur pourra maintenant appréciation l'efficacité des contrôles avec l'étape d'évaluation du fonctionnement des contrôles.

2.1.3.2. Evaluation du fonctionnement des contrôles

C'est le moment de la collecte d'éléments probants par rapport à l'efficacité des contrôles. Selon l'IIA (2007 : 13), cette étape permet à l'auditeur doit déterminer si les contrôles applicatifs fonctionnent efficacement ou si des utilisateurs imaginatifs parviennent à les contourner.

L'évaluation du fonctionnement des contrôles comprend les étapes suivantes (AFAI, 2008b : 28) :

- sélection des contrôles à vérifier, dans la mesure où il n'est pas nécessaire de contrôler l'ensemble des contrôles ;
- choix de la stratégie de test (procédures d'audit orientées processus contre procédures d'audit orientées résultat) ;
- choix de la procédure de test, et notamment de la taille de l'échantillon ;
- réalisation des opérations d'audit orientées processus ou orientées résultat ;

- évaluation des exceptions relevées et de l'importance des erreurs et des faiblesses constatées.

Toute démarche d'évaluation des risques débouche nécessairement sur une estimation qualitative ou quantitative des ces risques : c'est la phase de cotation.

2.1.4. Evaluation et hiérarchisation des risques

Une bonne gestion des risques ne se limite pas à un simple recensement plus ou moins exhaustif des « risques potentiels ou pertinents » mais doit aller au-delà c'est-à-dire une analyse quantitative et/ou qualitative pour pouvoir appréhender et estimer ces différents risques à leurs justes valeurs.

CESAG BIBLIOTHEQUE

Pour GUILLON (2007 : 310), chacun des risques identifiés à l'intérieur des processus lors des étapes précédentes doit faire l'objet d'un traitement : cotation en fréquence et en impact de l'évènement de risque pour pouvoir les hiérarchiser entre eux.

Selon DESMOULINS (2009 : 217) et CLUSIF (2007 : 13), un risque se caractérise par sa gravité ou impact et sa potentialité ou probabilité d'occurrence.

La mesure de ces deux grandeurs se fait à l'aide de ce que l'on appelle échelle de cotation des risques. Ainsi, il existe une pluralité d'échelles de cotation notamment celles à nombre de niveaux pair et celles à nombre de niveaux impair. Mais ce qui compte pour AUBERT & al (2004 : 197), l'échelle choisie doit être compatible avec les objectifs fixés au départ de l'analyse. Cependant, il est important de noter qu'il est préférable d'utiliser une échelle impaire. D'après RENARD (2010 : 316), la conception de cette échelle de cotation est comme suit :

- pour chacune des opérations, nous allons imaginer la situation la plus parfaite susceptible d'être rencontrée. En face de ce cas de figure qui identifie une excellente maîtrise de l'opération on va mettre la cotation un (1) ;
- puis, à l'inverse, nous allons imaginer la pire des situations possibles, c'est à dire le risque maximum possible et on va mettre alors la cotation cinq (5) ;
- entre ces deux extrêmes vont se situer toutes les situations intermédiaires susceptibles d'être rencontrées.

Ainsi la criticité de chaque risque c'est à dire sa note ou son score est obtenu en faisant la multiplication de sa probabilité et de son impact : risque = probabilité x impact. C'est pourquoi, prévenir le risque informatique, c'est soit réduire la gravité et l'impact, soit en réduire la probabilité d'occurrence, soit les deux à la fois (DESMOULINS, 2009 : 217).

2.1.4.1. Evaluation de la probabilité de survenance des risques

Il faut comprendre par probabilité d'occurrence d'un risque la capacité ou la possibilité du risque à se produire dans une situation donnée. Pour déterminer la probabilité d'occurrence des risques, il faut définir les critères d'évaluation et une échelle de cotation. En matière d'évaluation de la probabilité des risques, la méthode qualitative est le plus souvent utilisée plus facile à mettre en œuvre par rapport à la méthode quantitative. Pour se faire on affecte, à chaque qualificatif de la probabilité du risque, un coefficient d'appréciation ou de pondération pour permettre de coter ou de chiffrer les risques.

A titre illustratif, le tableau suivant présente un exemple d'échelle d'évaluation de la probabilité à 4 niveaux.

Tableau 1 : Exemple d'échelle de cotation de la probabilité des risques

Niveau de probabilité	Echelle
1	Improbable
2	Rare
3	Probable
4	Inévitable

Source : CGL consulting (2005 : 1)

2.1.4.2. Evaluation de l'impact des risques

La gravité d'un risque correspond à la gravité des conséquences de la réalisation de cet événement redouté en termes de dégradation des performances, de surcoût et d'augmentation des délais (DESROCHES & al, 2003 : 137). L'évaluation de l'impact des risques est la tentative d'estimation des conséquences des risques si jamais ils se produisaient. Il s'agira

CESAG - BIBLIOTHEQUE

essayer de mesurer les pertes en termes de coût, de délai, d'image, d'efficacité, de compétitivité… Etant difficilement quantifiable, l'impact des risques est évalué de façon qualitative à l'aide d'une échelle de cotation qui sera définit par consensus en essayant d'être le plus objectif possible. Le tableau 2 présente un exemple d'échelle de cotation de l'impact des risques.

Tableau 2 : Exemple échelle de cotation de l'impact des risques

Niveau de gravité	Echelle
1	Faible
2	Moyen
3	Grave
4	Très grave

Source : CGL consulting (2005 : 1)

CESAG - BIBLIOTHEQUE

2.1.4.3. Hiérarchisation des risques

Une fois achevées les évaluations de la probabilité et de l'impact des risques, la hiérarchisation des risques consiste à classer les risques par ordre d'importance décroissante. Le classement des risques se fait à partir de la criticité de chaque risque obtenue en multipliant la note de la probabilité d'occurrence du risque par celle d'impact du risque. La hiérarchisation des risques permet de prioriser les risque pour mieux analyser et de traiter les risques. Elle est présentée sous forme de tableau de synthèse.

2.2. Méthodes d'analyse et de gestion des risques informatiques

Il existe plusieurs développements de méthodes d'analyse et la gestion des risques informatiques. Dans le cadre de ce mémoire, nous allons présentées les trois (3) méthodes les plus connues qui sont MARION, MEHARI et COBIT.

2.2.1. MARION

La méthode d'analyse des risques informatiques orientée par niveaux (MARION) a été conçue par le CLUSIF dans les années 80.

La méthode est basée sur des questionnaires élaborés par le CLUSIF et remis à jour à intervalles réguliers, ces questionnaires prennent en compte 27 indicateurs (facteurs) de sécurité (BALLOY, 2002 : 21), répartis en 6 grands thèmes :

- la sécurité organisationnelle ;
- la sécurité physique ;
- la continuité ;
- l'organisation informatique ;
- la sécurité logique et exploitation ;
- la sécurité des applications.

CESAG - BIBLIOTHEQUE

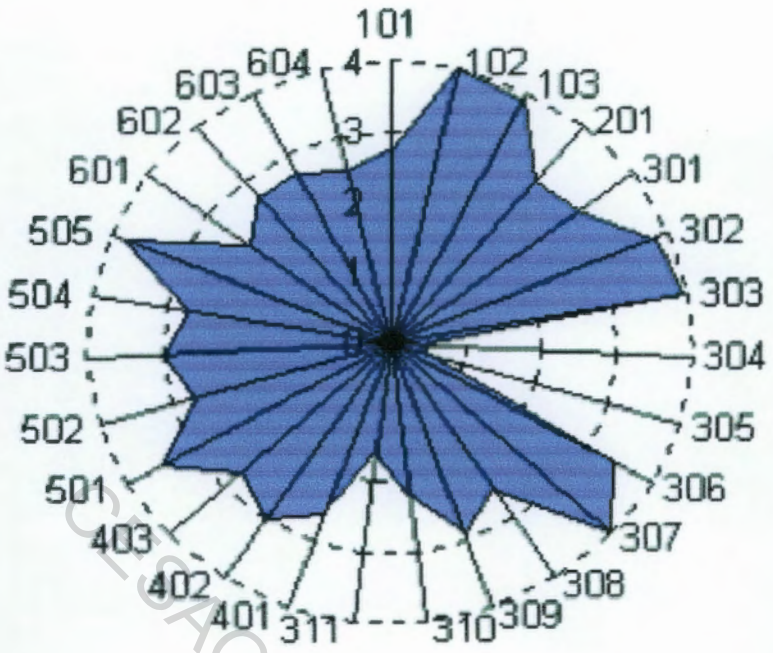
Une note de 0 à 4 est attribuée à chaque thème et la note « 3 » est le niveau à atteindre pour assurer la sécurité jugée correcte.

La méthode MARION se déroule en 4 phases distinctes (CLUSIF, 2006 : 1-5) :

- ✓ *La phase de préparation* : c'est la définition des objectifs de sécurité ainsi que le champ d'action.
- ✓ *La phase d'audit des vulnérabilités* : il s'agira de dérouler les questionnaires de la méthode et de recenser des contraintes propres à l'organisation. Ces questionnaires sont élaborés par CLUSIF et mis à jour périodiquement. Le résultat des questionnaires permet d'obtenir la " rosace " propre à l'entreprise et de juger facilement et rapidement des domaines vulnérables de l'entreprise, la cohérence et l'homogénéité des niveaux de sécurité des différents indicateurs, et donc d'identifier également rapidement les points à améliorer.

Un exemple de rosace MARION d'une entreprise est présenté à la figure 1.

Figure 1: Exemple de rosace MARION



Source : CLUSIF (2006 : 2)

CESAG - BIBLIOTHEQUE

- ✓ *La phase d'analyse des risques* : c'est la phase de l'exploitation des résultats précédents et de classification des risques en Risques Majeurs (RM) et Risques Simples (RS).

  Pour bien mener l'analyse des risques, on découpe le SI en fonctions et en groupes fonctionnels spécifiques, hiérarchisés selon l'impact et la potentialité des risques.

En ce qui concerne l'analyse des risques informatiques, la méthode MARION définit 17 types de menaces (CLUSIF, 2006 : 4) :

- accidents physiques ;
- malveillance physique
- panne du SI ;
- carence de personnel ;
- carence de prestataire ;
- interruption de fonctionnement du réseau ;
- erreur de saisie ;
- erreur de transmission ;

- erreur d'exploitation ;
- erreur de conception / développement ;
- vice caché d'un progiciel ;
- détournement de fonds ;
- détournement de biens ;
- copie illicite de logiciels ;
- indiscrétion / détournement d'information ;
- sabotage immatériel ;
- attaque logique du réseau.

✓ *La phase du plan d'action* : c'est la phase d'analyse et de conception des moyens à mettre en œuvre afin d'atteindre l'objectif de sécurité de la métbode. L'ordonnancement des tâches est fait et on indique le degré d'amélioration à apporter et l'estimation du coût de la mise en conformité.

2.2.2. MEHARI

La méthode harmonisée d'analyse des risques (MEHARI) est la suite de la MARION. Elle est aussi développée par le CLUSIF en 1995 et la dernière mise à jour est lancée en novembre 2010.

MEHARI permet d'évaluer qualitativement et quantitativement les risques informatiques et de porter un jugement sur le niveau de ces risques. A cet effet, la méthode s'appuie sur des outils (critères d'appréciation, méthodes de calcul, etc.) et des bases de connaissances (en particulier pour le diagnostic de la sécurité) qui s'avèrent indispensables en complément du cadre minimum proposé par la norme ISO 27005 (CLUSIF. 2010 : 6).

Les objectifs MEHARI sont décrits, dans le document de la présentation générale de la méthode (CLUSIF, 2010 : 4), comme suit :

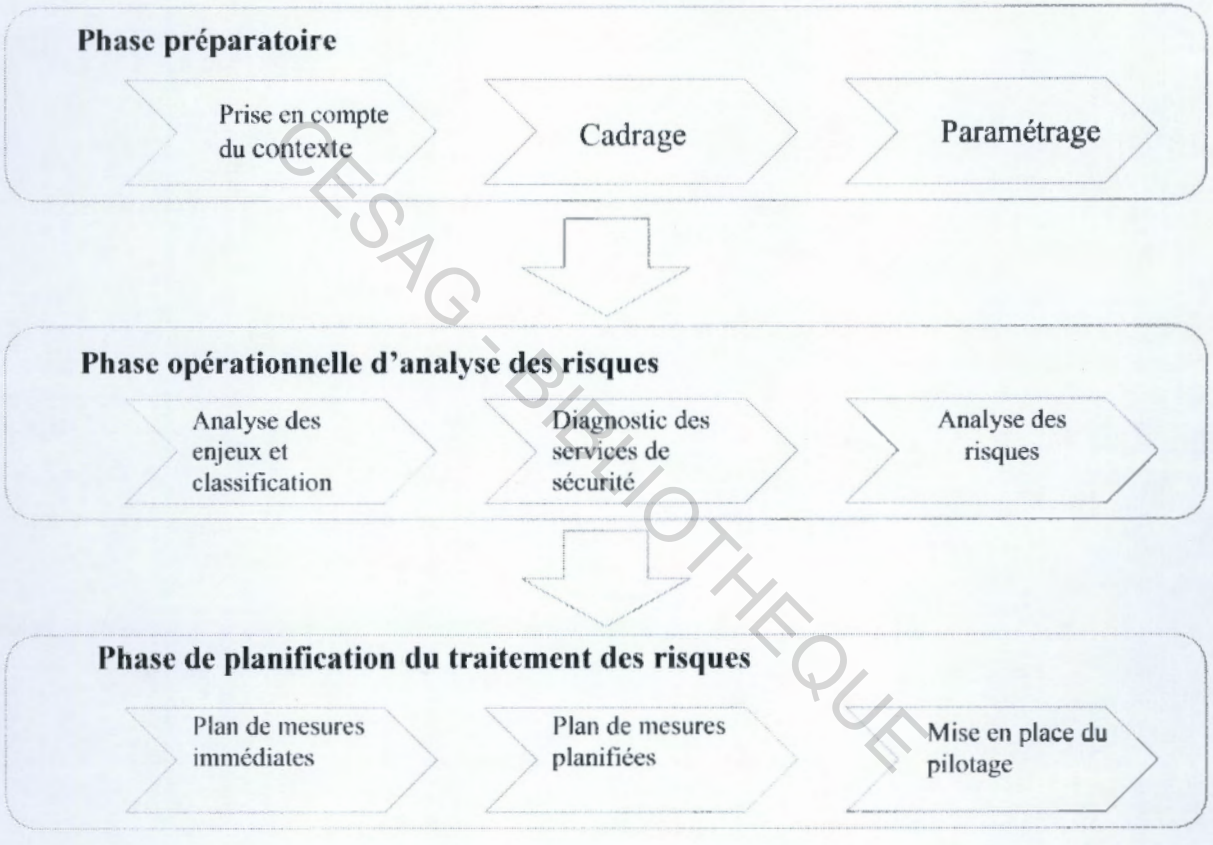
- permettre une analyse directe et individualisée de situations de risques décrites par des scénarios de risques ;
- fournir une gamme complète d'outils adaptée à la gestion à court, moyen et long terme, de la sécurité, quelle que soit la maturité de l'organisme en matière de sécurité et quelques soient les types d'actions envisagées.

CESAG - BIBLIOTHEQUE

Méhari est une démarche complète d'analyse et de traitement des risques en conformité avec la norme ISO/IEC 2700:2005.

La méthode comprend trois phases décrites dans la version 2 du guide de la démarche MEHARI (CLUSIF, 2011 : 5), conformément au schéma ci-dessous :

Figure 2 : Schéma de la démarche MEHARI



CESAG - BIBLIOTHEQUE

Source : CLUSIF (2011 : 5)

Il est important de noter que MEHARI est une méthode d'analyse et de gestion des risques qui est un ensemble cohérent, complet et autosuffisant. Néanmoins, elle est en évolution continue grâce à la « commission méthodes » du CLUSIF qui cherche toujours à l'améliorer. Elle est distribuée par le CLUSIF sous forme de fichiers téléchargeables. La documentation détaillée de MEHARI 2010 V2 (version 2) mise en ligne en novembre 2010 comporte :

- la présentation des principes fondamentaux et spécifications fonctionnelles de MEHARI ;
- un guide d'utilisation de la démarche ;
- le manuel de référence des services de sécurité ;
- un classeur Excel « base des connaissances ».

2.2.3. COBIT

Le référentiel COBIT est un modèle développé, mis au point et fourni par l'ISACA. Il permet de contrôler les objectifs et de manager les processus des technologies de l'information et s'inscrit ainsi dans une logique de contrôle et d'audit (BLANCHIN & al, Juin 2009 : 24).

CESAG - BIBLIOTHEQUE

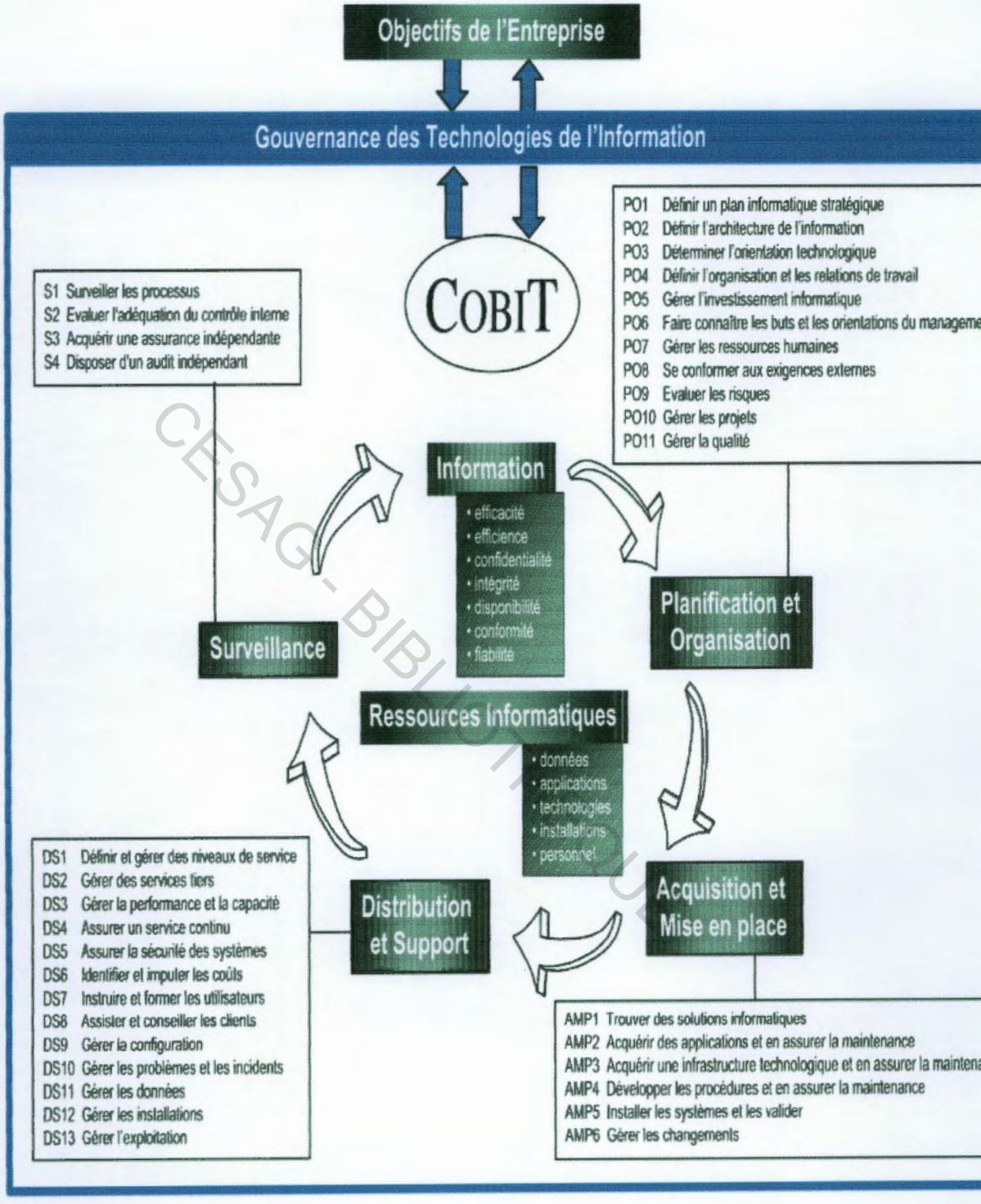
Le COBIT est reconnu comme étant le « socle de la gouvernance des SI » car il permet de comprendre et de gérer les risques en alignant les objectifs et les besoins des métiers aux objectifs informatiques et définit ce qui doit être mesuré et comment le faire.

Selon le document de présentation du CobIT V4.1 dans le site web de l'AFAI (www.afai.fr), l'orientation processus de CobiT est illustrée par un modèle de processus qui subdivise l'informatique en 34 processus et donne ainsi une vision complète de l'activité informatique. Ces différents processus informatiques sont répartis entre les quatre domaines de responsabilités que sont :

- planifier ;
- mettre en place ;
- faire fonctionner
- et surveiller.

Le modèle COBIT est illustré par la figure 3 ci-dessous :

Figure 3 : Le modèle de référence CobIT



CESAG - BIBLIOTHEQUE

Source : GARSOUX (2005 : 5)

La figure permet de voir les 34 processus informatiques de COBIT et leur découpage en quatre (4) domaines.

Conclusion

Ce chapitre constitue une partie essentielle de la revue littéraire car il a été pour nous l'occasion d'avoir une meilleure connaissance sur les types de risques informatiques, la démarche d'évaluation de ces derniers et leurs méthodes d'analyse.
Il nous permettra de mieux définir le modèle d'analyse de notre étude dans le chapitre suivant, la méthodologie de l'étude.

CESAG - BIBLIOTHEQUE

CHAPITRE III : METHODOLOGIE DE L'ETUDE

Introduction

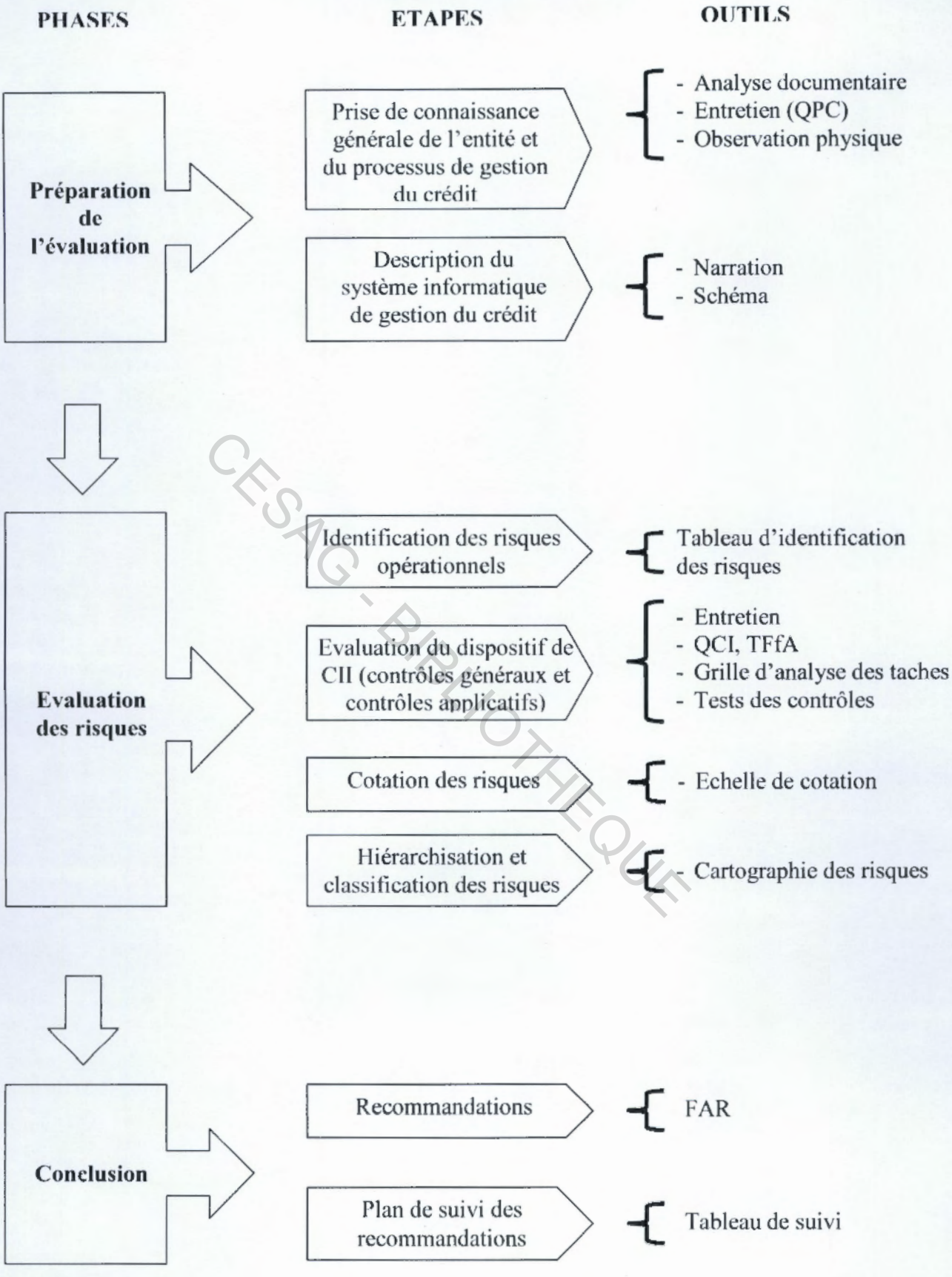
Le présent chapitre aura pour objet de présenter la méthodologie de recherche. Celle-ci est conçue autour d'un ensemble de méthodes et d'outils nous permettant de mettre en œuvre et de prendre en compte tous les points de notre recherche documentaire.
Cette méthodologie est déroulée à travers le modèle d'analyse, les techniques de collecte des données et les outils d'analyse de ces données.

CESAG - BIBLIOTHEQUE

3.1. Le modèle d'analyse

A la lumière de notre revue de littérature et en s'inspirant à de multiples démarches et bonnes pratiques en matière d'évaluation des risques et d'audit des applications, nous avons retenu comme modèle d'analyse le schéma ci dessous pour le déroulement de notre mission d'évaluation des risques informatiques liés à l'application de gestion du crédit. Notre démarche se décline en trois (3) phases principales avec les différentes étapes et outils pour chaque phase. Il est présenté à la figure 4 ci-dessous.

Figure 4 : Modèle d'analyse



CESAG - BIBLIOTHEQUE

Source : Nous mêmes

Notre modèle d'analyse est basé sur l'approche par les risques. Il permet :

- de découper le processus en activités ou tâches ;
- d'identifier les risques liés à chaque tâche ;
- d'identifier les dispositifs ou moyens de maîtrise des ces risques ;
- d'évaluer l'efficacité de ces contrôlés ;
- de coter les risques ;
- d'hiérarchiser les risques entre eux ;
- proposer des recommandations.

3.2. Les outils et techniques de collecte des données

Ils nous permettent de documenter l'étude en collectant les informations nécessaires au déroulement de la démarche. Pour cela, nous avons utilisé l'entretien, le questionnaire de prise de connaissance (QPC), l'observation, analyse documentaire.

CESAG - BIBLIOTHEQUE

3.2.1. Le QPC

Comme son nom l'indique, le QPC permet d'avoir une bonne compréhension du domaine à étudier en répondant aux questions essentielles que l'auditeur se pose. Pour RENARD (2010 : 228), il permet d'organiser la réflexion et les recherches et est indispensable :

- pour bien définir le champ d'application de sa mission ;
- pour prévoir en conséquence l'organisation du travail et en particulier en mesurer l'importance ;
- pour préparer l'élaboration des questionnaires de contrôle interne (QCI).

Dans notre étude, nous avons utilisé le QPC (annexe 1 page 88) afin de prendre connaissance la fonction informatique et le processus de gestion du crédit lors des entretiens avec le responsable de l'informatique de la CNCAS et des deux chefs d'agence rencontrés. Il nous a ainsi permis de faire la présentation de la fonction informatique dans le chapitre IV et la description du processus de gestion du crédit dans le chapitre V.

3.2.2. Analyse documentaire

Elle nous a permis de consulter plusieurs documents essentiels à la compréhension du fonctionnement de la société et de ses différentes activités. Dans le cadre de notre étude, nous avons consulté :

- l'organigramme de la banque ;
- le manuel des procédures (bancaires, audit, informatiques et de crédit) ;
- les rapports du Contrôle général sur les réalisations des crédits.

3.2.3. Entretien

Selon HENRY & al. (2001 : 89), un entretien réussi doit suivre un plan ordonné, se dérouler dans un climat d'écoute et amener des éléments de réponse concrète aux questions suivantes : Qui fait Quoi ? Comment ? Dans quels délais ? Avec quels outils et supports ?

Lors de notre étude, nous avons fait trois en entretiens avec deux chefs d'agence et le responsable de l'informatique.

CESAG - BIBLIOTHEQUE

3.2.4. Observation physique

Un audit sans observation n'est pas un bon audit. L'auditeur doit observer lui-même pour s'assurer de ce qu'on lui a dit, de ce qu'il croit et de ce qui est. Nous avons observé le montage d'un dossier de crédit, le processus de mise en place d'un crédit dans le logiciel Delta Bank et nous avons fait la visite des salles renfermant les installations informatiques.
Selon RENARD (2010 : 351), la pratique de l'observation physique exige trois conditions :

- elle ne doit pas être clandestine
- elle ne doit pas être ponctuelle
- elle doit être validée sauf le cas où elle est elle-même une validation.

Dans le cadre de notre étude, il a servi à faire le rapprochement entre les procédures écrites de crédit et de l'informatique et la pratique de ces dernières.

3.3. Les outils d'analyse des données

Pour notre étude, nous avons retenu le questionnaire de contrôle interne (QCI), la grille d'analyse des tâches et le tableau d'identification des risques.

3.3.1. QCI

« Les QCI ont pour objectifs de guider l'auditeur dans son travail d'analyse afin de lui permettre en toute objectivité, de détecter les dysfonctionnements, et d'en discerner les causes réelles » (ROUFF, 2001 : 15).

Selon MADERS & al (2006 : 57), le QCI a pour objet de « passer à la moulinette » un domaine pour en déterminer les forces et les faiblesses apparentes. En effet, les réponses « oui » correspondent à des forces apparentes tandis que les réponses « non » sont des faiblesses apparentes. La confirmation de ces conclusions provisoires est obtenue par la réalisation de tests de conformité ou de permanence.

Dans notre démarche d'évaluation des risques, les QCI ont été conçus de manière à poser les bonnes questions pour identifier les dispositifs de contrôle ou de maitrise des risques inhérents et opérationnels.

CESAG - BIBLIOTHEQUE

3.3.2. Grille d'analyse des taches

La grille de séparation des tâches décrit et décèle les éventuels cumuls de fonctions incompatibles afin d'y remédier (OBERT, 2004 : 77). Pour SCHICK & al (2010 : 188), toute organisation doit veiller à la séparation des responsabilités incompatibles telles que « détention /manipulation », « enregistrement » et « approbation /décision » qui l'expose à un risque majeur au niveau de ses actifs si des collusions s'instaurent entre les acteurs.

Elle est utilisée dans notre étude pour appréhender la séparation des tâches de la fonction informatique de la CNCAS.

3.3.3. Tableau d'identification des risques

Selon RENARD (2010 : 239-240), le tableau des risques ou tableau d'identification des risques est parfois nommé tableau des forces et faiblesses apparentes. L'identification se fera d'abord en découpant l'activité objet de l'audit en tâches élémentaires ensuite en associant à

chaque tâche les différents risques susceptibles de se produire et enfin en recensant de la mise en place les bonnes pratiques par rapport à la maitrise des ces risques. En fonction du degré d'affinement de l'analyse, le tableau comportera de 3 à 8 colonnes.

Il peut être considéré comme le point de départ du QCI et permet à l'auditeur de définir son programme de contrôle.

Conclusion

Dans ce chapitre de méthodologie de l'étude nous avons présenté les outils de collecte et d'analyse des données que nous allons utiliser sur le terrain. Nous avons aussi élaboré le modèle d'analyse de l'étude que nous avons retenu à la suite de la revue littéraire. Ce modèle d'analyse est élaborée avec la technique d'approche par les risques et nous a permis de définir les variables dépendantes et indépendantes de notre démarche d'analyse.

CESAG - BIBLIOTHEQUE

CONCLUSION PREMIERE PARTIE

Le cadre théorique de ce mémoire nous permis de consolider notre base de connaissance en matière d'évaluation des risques plus précisément celle des risques informatiques.

En résumé, nous pouvons retenir de la première partie de cette étude que l'efficacité du système de maitrise des risques applicatifs nécessite que :

- les contrôles hybrides ou entièrement manuels soient remplacés, dans la mesure du possible, par des contrôles automatiques ;
- les contrôles en aval, c'est-à-dire détectifs, soient remplacés, quand cela est possible, par des contrôles en amont, autrement dit préventifs.

CESAG - BIBLIOTHEQUE

DEUXIEME PARTIE : CADRE PRATIQUE

CESAG - BIBLIOTHEQUE

INTRODUCTION DE LA DEUXIEME PARTIE

Avec la prolifération des institutions financières, la concurrence est devenue rude et pour survivre elles ont besoin d'être de plus en plus performantes. Cette performance passe en grande partie par la maitrise du risque de crédit bancaire qui a été toujours une préoccupation majeure pour les établissements bancaires car le crédit est le produit bancaire qui finance principalement ces derniers. Mais au delà de la maitrise du risque de crédit bancaire, il ne faut pas oublier la maîtrise des risques opérationnels du crédit notamment ceux liés au traitement informatique de gestion du crédit. C'est ce que nous tenterons examiner dans cette deuxième partie.

Le cadre pratique de l'évaluation des risques liés au processus informatique de gestion du crédit de la CNCAS comporte trois (03) chapitres :

- la présentation de la CNCAS ;
- la description du processus de crédit de la CNCAS et de son traitement informatique ;
- l'évaluation des risques opérationnels liés à l'application de gestion du crédit de la CNCAS.

CESAG - BIBLIOTHEQUE

CHAPITRE IV : PRESENTATION GENERALE DE LA CNCAS

Introduction

La Caisse Nationale de Crédit Agricole du Sénégal (CNCAS) est une banque de la place particulière par rapport autres du fait de l'importance qu'elle accorde au financement des activités agricoles et des autres activités du secteur primaire.

Ce chapitre est consacré à la présentation de la CNCAS et constitue pour notre étude la phase de prise de connaissance générale de l'entité qui se fera avec son historique, sa mission et ses objectifs, ses activités, sa structure organisationnelle et ses partenaires.

CESAG - BIBLIOTHEQUE

4.1. Historique

La genèse de la CNCAS remonte de très longtemps notamment avec l'échec de l'Office National pour le Crédit Agricole et le Développement (ONCAD) dans sa mission d'approvisionnement du monde rural en intrants et matériels agricoles.

L'Etat, soucieux de redynamiser le secteur primaire, forma en 1983 un comité chargé d'étudier la réforme du crédit agricole, de même que la réforme du système d'encadrement du monde rural ; la création de la Caisse Nationale de Crédit Agricole du Sénégal (CNCAS) fut alors décidée lors du conseil des ministres du 26 mai 1983.

La CNCAS a été créée en avril 1984 sous forme de société anonyme et a démarré ses activités en mars 1985. Elle a été constituée avec un capital social de 2,3 milliards FCFA réparti entre l'Etat, les privés nationaux et internationaux. Ce capital social a connu une augmentation et est maintenant de 5,5 milliards de francs CFA.

La CNCAS a démarré avec une agence à Dakar en mars 1985 et s'est inscrite sur la liste des banques en juin 1985. Depuis lors, la banque s'est développée et s'agrandit. Elle dispose d'un réseau de 24 agences et bureaux sur le territoire national et l'ouverture prochaine de 03 autres au courant de l'année 2012.

4.2. Mission et objectifs

Depuis sa création, la CNCAS a pour mission principale le financement des activités agricoles et des autres activités du secteur primaire (pêche, élevage, artisanat).

Entes autres, la banque a pour objectifs principaux :

- la collecte de l'épargne ;
- la couverture de toute la gamme des besoins de financement du monde rural par la prise en compte des différentes phases (production, commercialisation, transformation etc.) ; et des différentes filières (riz, arachide, coton, etc.) ;
- la décentralisation du crédit pour promouvoir les activités économiques en milieu rural, urbain et périurbain en étant en relation directe avec ces derniers.

CESAG - BIBLIOTHEQUE

4.3. Activités

La CNCAS intervient dans tous les secteurs d'activités bancaires et pour toute catégorie de clientèle. Comme toute banque commerciale, la CNCAS exerce deux activités principales notamment la distribution de crédit et la collecte de l'épargne. Cependant, compte tenu de sa spécificité de banque du monde rural, un accent particulier est mis sur le financement du secteur primaire.

Les différents types de la CNCAS sont présentés dans le tableau suivant :

Tableau 3 : Types de crédit à la CNCAS

Types de crédit	Bénéficiaire
➢ Les crédits de campagne pour financer la commercialisation des grands produits agricoles (arachide, coton, riz)	- Entreprises agricoles - Groupements de producteurs ruraux - Particuliers secteur agricole
➢ Les crédits à court terme pour financer : • le secteur primaire en termes d'intrants et d'équipements ; • les équipements, l'immobilier, les fêtes nationales et rentrées scolaires	- entreprises agricoles, groupements de producteurs ruraux, éleveurs, pêcheurs - les entreprises commerciales, les commerçants, les salariés privés, les fonctionnaires, les particuliers et les retraités de la fonction publique
➢ Les crédits à moyen et long terme	- Professionnels, entreprises, les commerçants, etc.
➢ Les découverts	- Salariés ; entreprises ; commerçants ; etc.

Source : Nous-mêmes à partir du site web de la CNCAS (rubrique crédits)

CESAG - BIBLIOTHEQUE

Pour la collecte de l'épargne, la CNCAS offre les différents comptes bancaires suivants :

- des livrets d'épargne et de crédit ;
- des comptes à terme pour les dépôts à terme (DAT).

En dehors de ces deux activités principales citées précédemment, la banque opère aussi dans le service de transfert rapide d'argent en partenariat avec *MoneyGram, Western union, Ria et Wari*.

La CNCAS permet à ses clients de gérer leurs comptes par carnet de chèques et à distance avec la mise en place d'un site web et d'un service de gestion des comptes par téléphones (AGRICALL).

4.4. Structure organisationnelle

Nous allons nous intéressé à sa ses organes de gestion et ses différentes directions.

4.4.1. Les organes de gérance de la banque

La CNCAS est une institution fluide qui définit de façon précise le rôle de chaque organe. Elle a à sa tête un Conseil d'Administration qui délègue des pouvoirs de décisions et d'exécution à un Directeur Général.

La gérance de la banque est composée du conseil d'administration (C.A) et de la direction générale (D.G).

CESAG - BIBLIOTHEQUE

4.4.1.1. Le Conseil d'Administration

Le CA est composé de 12 membres choisis parmi les actionnaires les plus importants. La prépondérance de la part de l'Etat dans le capital social lui confère la présidence du conseil d'administration. Il se réunit tous les ans en session ordinaire pour le bilan. Cependant, il peut arriver que des sessions se tiennent pour statuer sur les dossiers de crédit assez importants. Un comité restreint de 5 administrateurs, appelé comité de prêt ou de crédit est constitué au niveau du Conseil d'Administration. Ce comité peut arrêter avec diligence un certain nombre de décisions. Le Conseil d'Administration nomme, en dehors de ses membres, un Directeur Général chargé de la gestion quotidienne de la société.

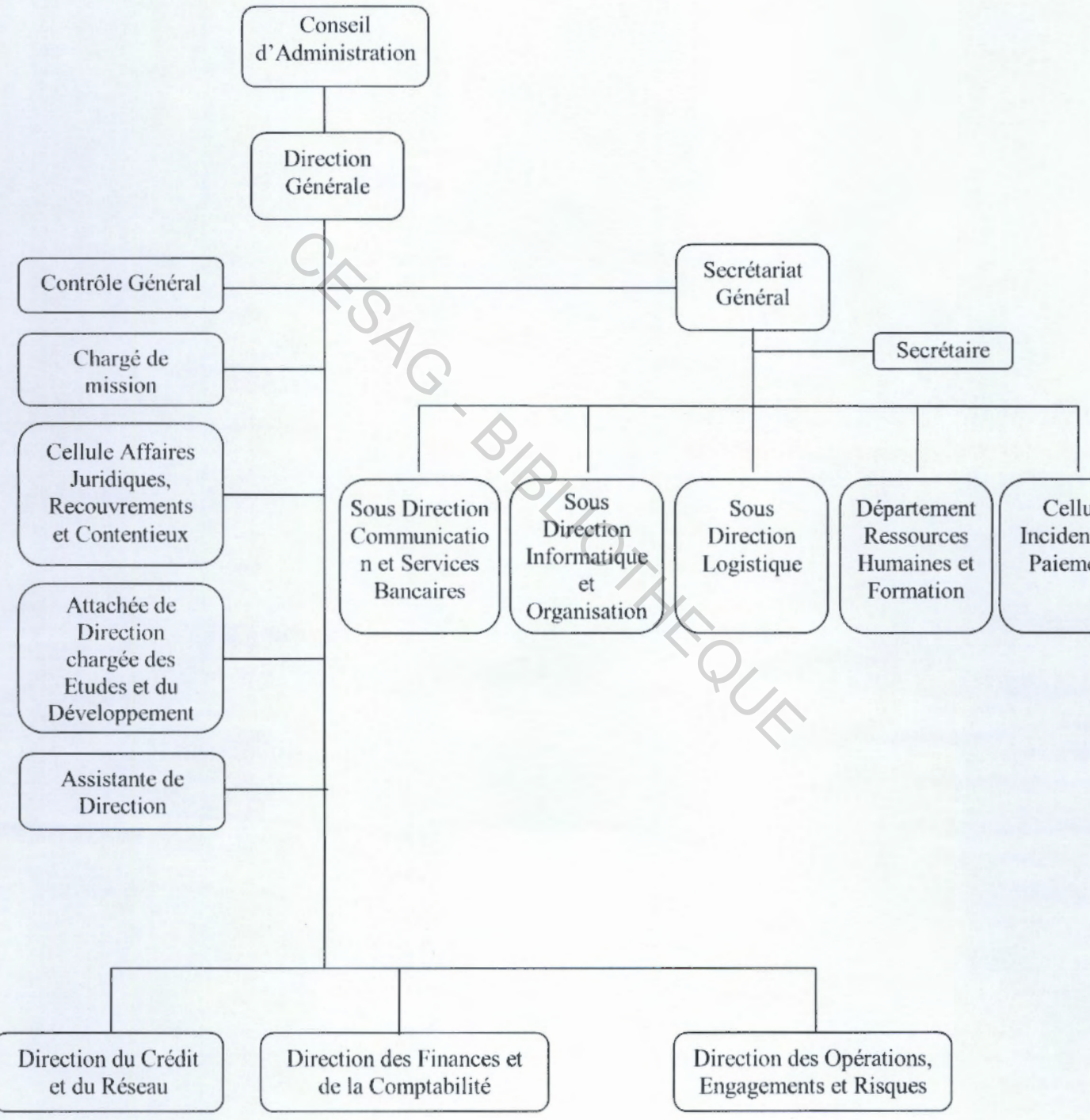
4.4.1.2. La Direction Générale

La Direction générale (DG) est l'organe de gestion et de contrôle. Le Directeur Général fait autorité sur toutes les hiérarchies ; il dispose de pouvoirs pour agir au nom de la société. Il s'appuie sur un conseiller technique. Il délègue certains de ses pouvoirs par la mise en place d'autres directions.

4.4.2. Les différentes directions de la CNCAS

La DG a mis en place des directions par métier, des cellules, des chargés de mission et un secrétariat général (voir organigramme ci-dessous).

Figure 5 : Organigramme de la CNCAS



CESAG - BIBLIOTHEQUE

Source : CNCAS (2012)

L'organigramme nous permet d'appréhender la structure générale de la CNCAS avec ses différentes composantes. Nous allons en présenter deux (02) : la direction du contrôle général et la sous direction de l'informatique et de l'Organisation.

4.4.2.1. La direction du contrôle général

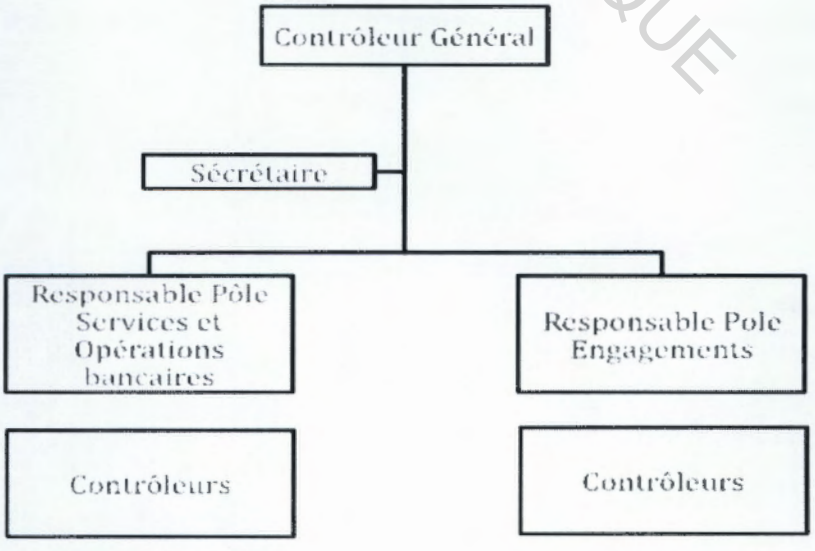
Le contrôle général de la CNCAS joue le rôle d'animateur de la fonction de contrôle interne. Il est chargé de veiller en permanence à l'efficacité et à la cohérence du système de contrôle de la banque. Il dispose d'une indépendance fonctionnelle et jouit de prérogatives étendues quant au champ de ses interventions. Il a comme mission d'assurer les objectifs du CI que sont :

- la sauvegarde de son patrimoine ;
- l'exactitude et la fiabilité de l'information comptable ;
- l'optimisation des processus et des activités ;
- la conformité aux lois et règlements en vigueur.

Le contrôle général de la banque est organisé en deux pôles (figure 6) : le pôle des engagements et celui des opérations bancaires facilitant ainsi la mise en place d'un dispositif favorable au développement de la polyvalence des équipes.

CESAG - BIBLIOTHEQUE

Figure 6 : Organigramme de la Direction du Contrôle général



Source : CNCAS (2012)

Le contrôle général a pour mission d'assurer la sauvegarde du patrimoine de l'institution en veillant à ce que les procédures et la règlementation soient scrupuleusement respectées par les agents d'exécution et par les différents responsables hiérarchiques. Ses différents contrôles portent sur :

- le dispositif de sécurité
- les engagements
- les opérations
- les processus administratifs et financiers
- la fonction informatique

La Direction du contrôle général de la CNCAS se doit de donner une assurance raisonnable à la DG sur degré de maîtrise des risques en assistant et accompagnant les autres départements dans l'exécution efficace de leurs tâches. Elle joue aussi le rôle d'arbitre entre les clients et la banque pour le traitement des réclamations.

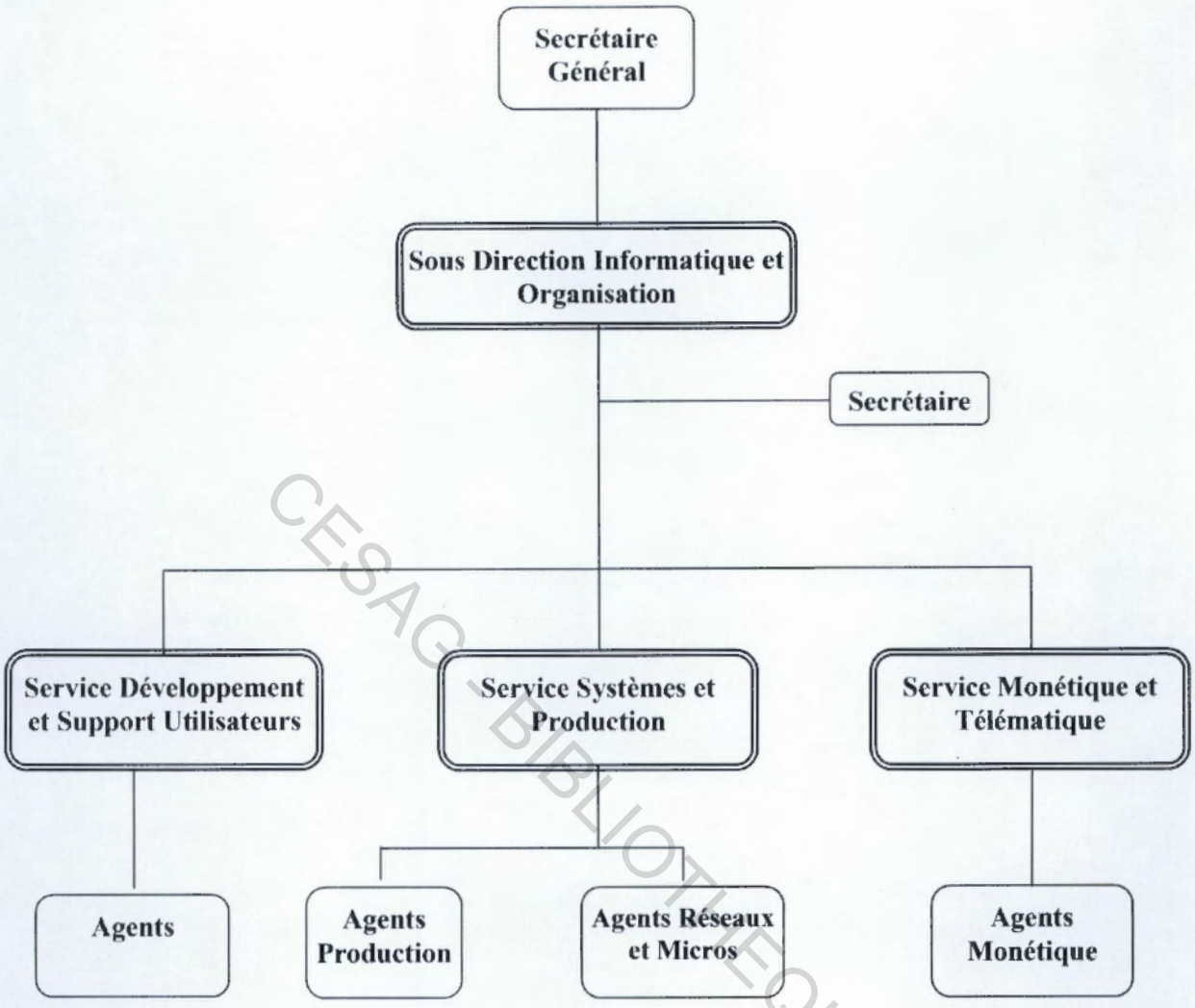
CESAG - BIBLIOTHEQUE

4.4.2.2. La sous direction de l'informatique et de l'organisation

La fonction informatique de la CNCAS est chargée de mettre à la disposition de la banque un système d'information efficace et fiable pour répondre aux besoins stratégiques de l'établissement. Elle met en œuvre la politique en matière de système d'information et assure la veille technologique.

La fonction informatique est rattachée au secrétariat général et a un statut de sous direction. Elle porte le nom de sous direction de l'informatique et Organisation (SDIO). La SDIO est organisée en trois (3) services (voir figure 7).

Figure 7 : Organigramme de la SDIO



CESAG - BIBLIOTHEQUE

Source : CNCAS (2012)

Le service systèmes et production : il est chargé de la gestion des systèmes, de la sécurité (physique et logique), des réseaux de télécommunications (internet et téléphonie) et des équipements et de leurs maintenances. Il assure aussi la disponibilité des données en temps réel. En résumé, ce service est l'outil de production et d'exploitation de l'informatique. Il a comme différents attributs :

- l'administration et l'exploitation des serveurs ;
- l'administration de la base de données ;
- l'administration du réseau informatique et de téléphonie ;
- la gestion de la sécurité logique des données et de la sécurité physique des installations ;

- les sauvegardes et leurs stockages ;
- l'exploitation des applications ;
- le transfert des données ;
- le contrôle de la salle des machines ;
- la planification de la maintenance des applications et équipements informatiques ;
- le suivi des contrats de maintenance ;
- la gestion du parc informatique de la banque.

Le service développements et support utilisateur : il est chargé de tout ce qui est travaux informatiques et il assure aussi la formation et le support aux utilisateurs. Les tâches associées à son rôle sont :

- intégration et/ou développement d'applications informatiques ;
- mettre à jour les applications ;
- diffusion des logiciels ;
- donner une assistance technique aux utilisateurs ;
- développer des requêtes ;
- documenter les applications ;
- rédiger les guides utilisateurs ;
- former les utilisateurs ;
- gérer les mots de passe.

Le service monétique et télématique : ses attributions principales sont :

- assurer la gestion des moyens de paiement électronique (cartes bancaires et GAB) ;
- assurer les services de la banque à distance dénommés Agrinet qui gère la plateforme de la banque en ligne et Agricall serveur vocal permettant de consulter son compte et de s'informer des derniers mouvements par téléphone.

4.5. Partenaires

La CNCAS entretient des relations, entre autres, avec des institutions de micro-finances, des projets, des ONG, des sociétés de transfert rapide d'argent, des agences nationales, des privés tels que :

CESAG - BIBLIOTHEQUE

- le projet d'organisation et de gestion villageoises (POGV) ;
- le projet d'intensification et de modernisation de l'agriculture (PIMA) ;
- l'union des mutuelles ;
- MoneyGram ;
- Western Union ;
- Ria ;
- Wari ;
- APIX ;
- EDK Oil ;
- Etc.

Conclusion

Ce chapitre nous a permis de faire la connaissance de la CNCAS notamment avec la présentation de son historique, ses missions et objectifs, ses activités, sa structure organisationnelle et ses partenaires. Après cette prise de connaissance de la banque, nous abordons dans le chapitre suivant la présentation de l'environnement informatique et la description du processus de gestion du crédit.

CESAG BIBLIOTHEQUE

CHAPITRE V : DESCRIPTION DU PROCESSUS DE CREDIT ET DE L'APPLICATION DE GESTION DU CREDIT DE LA CNCAS

Introduction

Ce chapitre est l'occasion pour nous de prendre connaissance du processus de crédit de la CNCAS et sa mise en œuvre dans le progiciel bancaire. La connaissance de ce processus est primordiale dans car elle permet de bien définir le champ de l'étude et de bien identifier les risques. Ce chapitre s'articule autour de trois (03) sections : description du processus de crédit de la CNCAS ; la présentation du progiciel bancaire et la mise en œuvre des crédits dans l'application informatique.

CESAG-BIBLIOTHEQUE

5.1. Description du processus d'octroi de crédit de la CNCAS

Pour mieux comprendre le traitement du crédit à la CNCAS, nous allons d'abord décrire les types de crédit ensuite le processus de crédit et enfin sa mise en œuvre dans le progiciel bancaire.

5.1.1. Les types de crédit de la CNCAS

La CNCAS offre deux types de crédit qui sont les crédits amortissables et les découverts. Les crédits de la CNCAS peuvent être scindés en trois (3) groupes quelque soit le type de crédit (crédit amortissable ou découvert). Ce sont :

- les crédits subdélégués : les crédits (amortissables et découverts) subdélégués sont ceux destinés aux fonctionnaires de l'Etat (salariés et retraités de la fonction publique âgés de moins de 65 ans pendant toute la période de validité du dossier) éligibles à la grille de délégation de pouvoirs de la CNCAS en matière de crédit et de dépassements, aux corps émergents et aux salariés du secteur privé suivant une liste de sociétés homologuées. Les niveaux de pouvoirs des subdélégataires sont déterminés pour les différentes instances de décision de la banque. Pour les découverts la durée maximale est de douze (12) mois ; le montant limite est égal au tiers du salaire domicilié.
- les crédits délégués : les crédits (amortissables et découverts) délégués sont ceux destinés aux fonctionnaires de l'Etat (salariés et retraités de la fonction publique âgés

de moins de 65 ans pendant toute la période de validité du dossier) éligibles à la grille de délégation de pouvoirs de la CNCAS en matière de crédit et de dépassements, aux corps émergents et aux salariés du secteur privé suivant une liste de sociétés homologuées. Les niveaux de pouvoirs sont déterminés pour le Directeur du Crédit et du Réseau (DCR) et le Directeur Adjoint au Crédit et au Réseau (DACR).

- les crédits non délégués : il s'agit de tous les crédits (amortissables et découverts) de la compétence du Directeur Général c'est à dire les crédits de clients particuliers (non salariés, crédits agricoles) et les crédits qui dépassent les pouvoirs du DCR. Ils peuvent être aussi des crédits de la compétence du comité de direction et du conseil d'administration.

5.1.2. Processus d'octroi de crédit de la CNCAS

Le processus de crédit de la CNCAS comporte les deux (2) grandes phases suivantes :

5.1.2.1. La phase de l'instruction du dossier

Le chef de d'unité (agence ou bureau) impute la demande de prêt à l'agent instructeur (agent de crédit) qui s'assure que le dossier est complet et procède à l'analyse et à la constitution du dossier par la saisie dans le Système d'Information (Delta-Bank) puis édite le tableau d'amortissement. Ensuite, il matérialise son avis sur le dossier en inscrivant sur la fiche synoptique ses appréciations du dossier. Après, il le transmet au chef d'unité pour prise de décision selon les pouvoirs alloués.

5.1.2.2. La phase prise de décision

A la réception du dossier, le chef d'unité effectue un contrôle de deuxième niveau, au besoin, il demande des informations complémentaires à l'agent instructeur, si tout est conforme, il prend une décision (défavorable ou favorable avec durée et montant accordés) qu'il matérialise sur la fiche synoptique. Si la demande de crédit dépasse ses pouvoirs il la transmet à un autre fondé de pouvoir qui peut la prendre en charge et celui fera les mêmes contrôles que le chef d'unité pour la prise de décision.

Dans le cas d'un rejet, le chef d'unité ou le fondé de pouvoir habilité saisit la décision de banque (défavorable pour cas) dans Delta-Bank, puis retourne le dossier à l'agent instructeur.

CESAG - BIBLIOTHEQUE

Celui-ci notifie au client la décision de la banque par rapport à sa demande puis classe le dossier.

Si la demande est accordée, l'agent instructeur notifie au client la décision de la banque par rapport à sa demande. Dans le cas où le client accepte les conditions du crédit, il lui fait signer le tableau d'amortissement en deux exemplaires puis lui remet un exemplaire. L'agent instructeur saisit dans Delta-Bank la décision du client et la garantie si nécessaire puis transmet le dossier au fondé de pouvoir compétent pour validation.

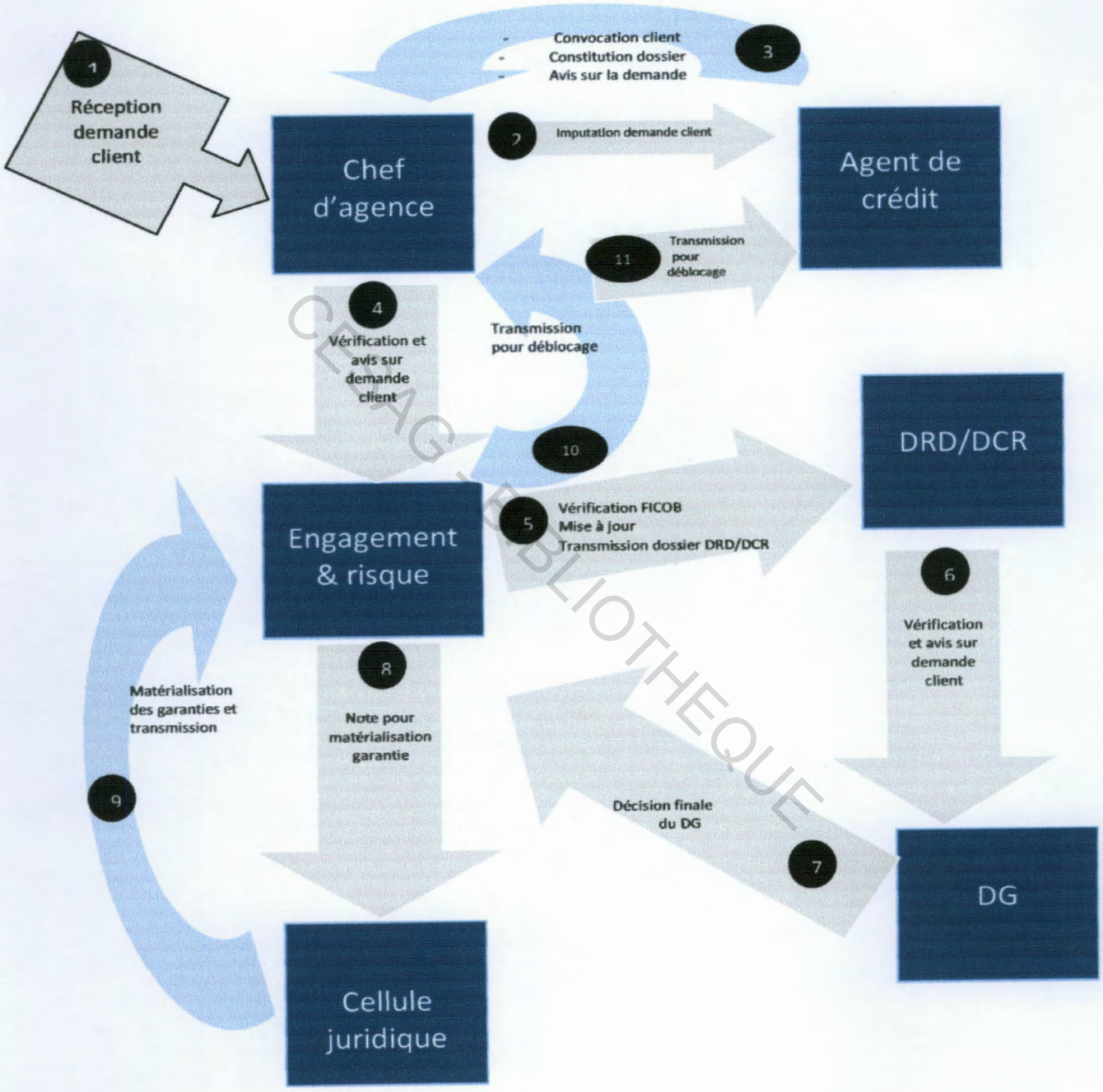
Le fondé de pouvoir effectue un contrôle de conformité puis si tout est conforme, il valide le dossier dans Delta-Bank (montant, durée, type de garantie si nécessaire) et appose sur la fiche le cachet personnalisé «dossier conforme» ensuite classe le dossier.

CESAG - BIBLIOTHEQUE

5.1.2.3. Schéma descriptif du circuit de crédit

Tout le circuit du crédit peut être résumé par la figure suivante qui prend en compte toutes les formes de crédit.

Figure 8 : Schéma description du circuit des dossiers de crédit de la CNCAS



CESAG BIBLIOTHEQUE

Source : CNCAS (2012)

La deuxième section du chapitre est consacrée à la présentation du progiciel bancaire.

5.2. Présentation du progiciel bancaire Delta-Bank

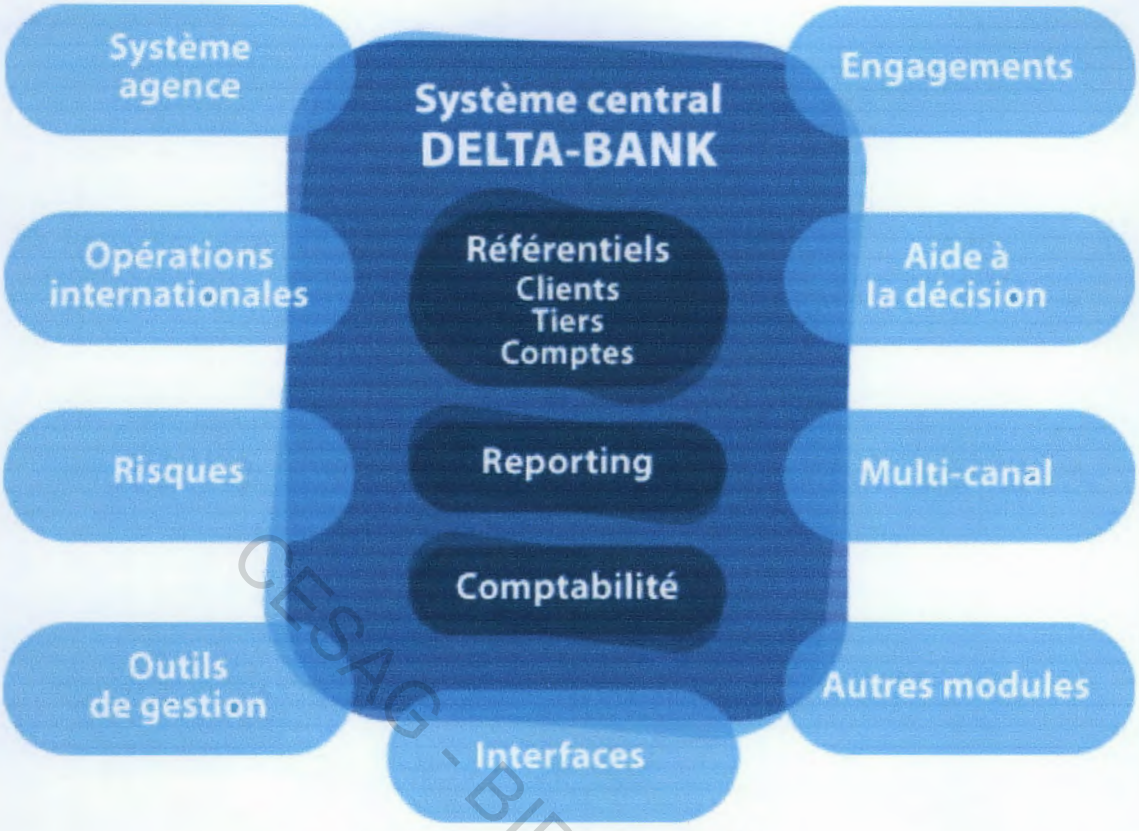
Pour prendre en charge toute l'activité opérationnelle de la banque, la CNCAS s'est dotée d'un progiciel bancaire dénommé *Delta-Bank* (version 9) du fournisseur DELTA INFORMATIQUE. Le Groupe Delta Informatique est une société de services et d'ingénierie en informatique créée en 1980 qui s'est imposée comme le leader des éditeurs de progiciels de gestion intégrée (PGI) pour les grands groupes internationaux présents en Afrique (DeltaInformatique, 2009 : 2).

5.2.1. Architecture du progiciel

DELTA Bank est un PGI des opérations bancaires du guichet au siège. Il est multi plates-formes, totalement sécurisé (cryptage et accès sécurisés), orienté utilisateur (facile d'utilisation), totalement paramétrable, multi devises, multi pays et fonctionne en temps réel. Delta-Bank est une solution conçue avec une architecture 100% modulaire et intégrée autour d'un référentiel unique. Il offre une large gamme d'applications couvrant l'ensemble des métiers d'une banque universelle et dispose d'une architecture évolutive qui permet une implémentation progressive (DeltaInformatique, 2005). La figure 9 ci-dessous nous permet d'apprécier son architecture.

CESAG - BIBLIOTHEQUE

Figure 9 : Architecture du progiciel Delta Bank version 9



Source : DeltaInformatique (2005)

CESAG - BIBLIOTHEQUE

5.2.2. La sécurité du progiciel

DELTA-BANK assure un niveau de sécurité tel que requis par les banques actuelles :

- accès par code utilisateur et mot de passe crypté à durée de vie contrôlée ;
- contrôle des tentatives d'accès (nombre paramétré, enregistrement dans le journal) ;
- personnalisation des menus permettant un contrôle très fin des accès par site et par utilisateur ;
- contrôle des actions (création, suppression, saisie simple, validation,...) ;
- contrôle des données visibles et accessibles par utilisateur (comptes, clients) ;
- enregistrement des modifications de données sensibles (tables, références, comptes, clients) avec image avant et image après ;
- enregistrement de tout accès (début, fin de programme) et de tout message d'erreur ;
- journaux détaillés d'activité par utilisateur ;
- procédure de forçage de transactions non validées avec recyclage pour les transactions de back office ;

- calcul automatique des conditions (dates de valeurs, montants de commissions, etc.) avec contrôle des modifications et des forçages par niveau d'habilitation :
- génération automatique des écritures comptables ;
- piste d'audit comptable permettant et garantissant le caractère chronologique inaltérable avec enregistrement de l'ensemble des informations (utilisateur, date, heure, compte client concerné, etc.) ; l'extraction de l'ensemble des écritures sur un compte pour un intervalle de dates ; la reconstitution de la pièce comptable à partir d'une écriture sur un compte (toutes les écritures générées dans une opération).

La sécurité du progiciel bancaire est renforcée par la gestion des habilitations.

5.2.3. La gestion des habilitations par Delta Bank

CESAG - BIBLIOTHEQUE

La gestion efficace des habilitations et des autorisations est mise en œuvre à l'aide des profils utilisateur regroupés en trois (3) grands types :

- le profil « *Gestionnaire* » *ou* « *Décisionnaire* » : ce sont les utilisateurs qui prennent les décisions, qui valident ou ignorent certaines opérations avec la précision, pour chaque décisionnaire, du montant de forçage de provision, du montant maximum de forçage des escomptes, du plafond maximum des découverts ;
- le profil « *métier de la banque* » : en fonction du profil, l'utilisateur peut faire certaines transactions et d'autres lui sont interdites ;
- et le profil « *stagiaires* » ou « *consultation* » : uniquement pour des consultations et/ou éditions dont les dates de début et de fin sont précisée pour les stagiaires.

Ces trois grands types de profil utilisateur sont scindés en plusieurs profils plus fins selon les métiers de la banque :

- profil caissier ;
- profil directeur (opérations, affaires juridiques, crédit et du réseau) ;
- profil chef agence ;
- profil chargé de clientèle ;
- profil agent de crédit ;
- profil chef de caisse ;

- profil guichetier/agent des opérations ;
- profil chef comptable ;
- profil comptable ;
- profil stagiaire ;
- profil contrôleur ;
- profil opérations/étranger ;
- profil consultation.

Après avoir décrit le processus d'octroi de crédits, nous allons décrire sa mise en œuvre sur Delta-Bank.

CESAG - BIBLIOTHEQUE

5.3. Mise en œuvre des crédits avec Delta-Bank

C'est dans le module « engagements » avec le sous module « prêt » que se matérialise la mise en place des crédits bancaires.

L'observation physique du traitement des crédits a porté sur les crédits dits subdélégués et délégués c'est à dire de la compétence des chefs d'agence, du DACR et du DCR. Elle nous a permis de constater que la mise en place des crédits avec Delta-Bank peut être scindée en quatre (04) étapes :

- instruction du dossier : c'est la constitution du dossier sur Delta-Bank par la saisie des informations de la demande de crédit. Un numéro de dossier est attribué de façon automatique par le système. Ensuite, l'utilisateur renseigne les champs n° compte client, type de crédit, taux d'intérêt, montant demandé, choisit le mode d'amortissement et la durée puis édite le tableau d'amortissement pour le comparer à la quotité cessible. Il répète cette opération jusqu'à avoir un montant des échéances convenable avec la quotité cessible mais rien ne l'empêche de continuer à une étape suivante ;

- saisie de la décision de banque : après analyse nécessaire, le fondé de pouvoir (l'agent habilité) prend une décision c'est à dire l'accord ou le rejet et la matérialise dans delta-bank (rejet ou accord). Si c'est d'un accord, il renseigne la durée et le montant accordés, le type de garantie si nécessaire, date de la première échéance, assurance décès ;

- saisie de la décision du client (accord ou abandon) : dans le cas d'un accord de la demande du client, l'agent instruction notifie au client les termes du prêt et matérialise la décision du client (accord ou abandon) dans Delta-Bank puis classe le dossier ;

- validation du dossier : Si le client est d'accord sur les termes du prêt, la personne habilitée procède à la validation ou la mise en place du crédit sur le compte du client. Il valide définitivement les étapes précédentes qui va permettre de créditer le compte du client.

Conclusion

CESAG - BIBLIOTHEQUE

Ce chapitre nous a permis d'avoir une meilleure connaissance :

- du processus de traitement des crédits ;
- du progiciel bancaire qui permet la gestion quotidienne de l'activité bancaire ;
- et la mise en œuvre des crédits dans l'application.

A suite de cela, nous pourrons aborder aisément l'évaluation des risques opérationnels liés à l'application informatique de gestion du crédit de la CNCAS dans le chapitre suivant.

CHAPITRE VI : EVALUATION DES RISQUES OPERATIONNELS LIES A L'APPLICATION DE GESTION DU CREDIT DE LA CNCAS

Introduction

Ce chapitre sera l'aboutissement de tous les travaux de recherche et de collecte d'informations qui précèdent. C'est le lieu de dérouler notre démarche en matière d'évaluation des risques. Il s'agira de mettre en œuvre le reste de notre modèle d'analyse. Ce chapitre est structuré comme suit :

- identification des risques opérationnels liés à l'application de gestion du crédit de la CNCAS ;
- évaluation du dispositif de contrôle interne informatique notamment les contrôles généraux informatique et les contrôles applicatifs ;
- évaluation de la probabilité et de l'impact des risques opérationnels identifiés ;
- hiérarchisation et classification des risques ;
- formulation de recommandations pour traiter ces risques et proposition d'un plan de suivi de ces recommandations.

CESAG - BIBLIOTHEQUE

6.1. Identification des risques opérationnels liés à l'application de gestion du crédit

Dans cette section, nous allons identifier les différents risques opérationnels liés à l'application informatique de gestion du crédit de la CNCAS en décomposant ce processus en tâches élémentaires. Cette décomposition du processus est faite sur la base du manuel des procédures de crédit et sur la base de l'observation physique de la pratique informatique de gestion du crédit. Elle nous permettra de mieux identifier les différents risques liés à chaque tâches ou activité du processus. L'identification des risques est formalisée avec l'aide d'un tableau constitué de quatre (04) colonnes. La première colonne permet d'identifier et de lister toutes les phases du processus ; la deuxième permet de lister les tâches clés ou « objets auditables » de la phase ; la troisième d'identifier le(s) risque(s) attaché(s) à chaque tâche et la dernière permet de décrire ou de définir le risque.

La gestion du crédit dans le progiciel bancaire peut être résumée en deux grandes phases que sont l'instruction du dossier et la mise en place (MEP) du crédit.

6.1.1. Identification des risques liés à la phase de l'instruction du dossier de crédit

La phase de l'instruction du dossier comporte la constitution dossier avec la saisie des informations de la demande de crédit et l'édition du tableau d'amortissement du crédit.

Tableau 4 : Tableau d'identification des risques liés à l'instruction du dossier

Phase du processus	Tâches / activités clés de la phase	Risques opérationnels	Définition du risque
Instruction du dossier de crédit	attribution du numéro de dossier	R1. existence de doublon de dossier	C'est le risque que deux dossiers aient le même numéro
	choix du type de crédit	R2. choix d'un crédit pour un client qui n'a pas le profil requis	C'est de choisir un type de crédit qui n'est pas éligible pour ce client
	choix du taux d'intérêt	R3. choix d'un taux d'intérêt différent de celui du type de crédit	C'est de choisir un taux d'intérêt qui n'est pas celui du type de crédit
	édition du tableau d'amortissement	R4. dépassement de la quotité cessible pour les salariés	C'est à dire les échéances dépassent la quotité cessible du salarié
		R5. dépassement du taux d'endettement pour les entreprises	Le montant du crédit dépasse la capacité d'endettement de l'entreprise

CESAG BIBLIOTHEQUE

Source : Nous-mêmes à partir de l'observation physique d'une MEP de crédit

6.1.2. Identification des risques liés à la phase de mise en place du crédit

La phase de MEP du crédit comprend la saisie de la décision de banque (rejet ou accord, montant accordé, durée du crédit, nombre d'échéances, le taux d'intérêt, date de la première échéance) et le type de la garantie si nécessaire.

Tableau 5 : Tableau d'identification des risques liés à la mise en place du crédit

Phase du processus	Tâches / activités clés de la phase	Risques opérationnels	Définition du risque
Mise en place du crédit (MEP)	saisie de la décision de banque	R6. MEP de crédit pour un salarié d'une société non homologuée par un agent non habilité	C'est la mise en place de crédit par un utilisateur non compétent pour ce type de crédit
		R7. validation d'un crédit par un utilisateur non délégataire	C'est à dire un utilisateur ne faisant pas de la liste des délégataires valide un crédit
		R8. octroi d'un crédit salarié avant la domiciliation du salaire	C'est le fait d'octroyer un crédit avant le premier virement du salaire
		R9. altération du taux d'intérêt choisi pour valider le dossier	C'est le fait de modifier frauduleusement le taux qui a permis d'accorder le crédit
		R10. altération du montant autorisé	Modification frauduleuse du montant du crédit
		R11. altération de la durée de crédit autorisée	Modification frauduleuse de la durée du crédit
		R12. dépassement des habilitations par rapport au montant	Valider un crédit dont le montant dépasse notre délégation de pouvoirs
		R13. dépassement des habilitations par rapport à la durée	Valider un crédit dont la durée dépasse notre délégation de pouvoirs
		R14. validation d'un dossier rejeté	C'est le fait de valider un dossier dont l'avis est défavorable
		R15. octroi de crédit à un client qui dépasse la limite d'âge par un agent non habilité (pour les retraités)	Pour les retraités dépassant l'âge limite c'est le DG ou son intérim qui doit autoriser le crédit
	Saisie de la garantie du crédit	R16. non saisie de la garantie (si nécessaire) avant validation	Ce le fait de ne pas prendre de garantie pour un crédit le nécessitant

CESAG - BIBLIOTHEQUE

Source : Nous-mêmes à partir de l'observation physique d'une MEP de crédit

Après l'identification des risques, l'étape suivante est l'évaluation du dispositif de contrôle interne informatique afin de pouvoir coter chaque risque identifié.

6.2. Evaluation du dispositif de contrôle interne informatique

Le dispositif de contrôle interne comprend les contrôles généraux et les contrôles applicatifs décrits dans le chapitre I. Le fondement d'évaluer d'abord les contrôles généraux informatiques réside dans le fait que la fiabilité des contrôles applicatifs dépend avant tout de celle de l'environnement informatique.

6.2.1. Evaluation des contrôles généraux informatiques

L'évaluation des contrôles généraux informatiques nous permettra d'apprécier les moyens mis en œuvre afin de garantir la confidentialité, l'intégrité, la disponibilité des données et la continuité de l'exploitation. Ainsi nous allons dégager un aperçu global sur les forces et faiblesses des contrôles généraux et établir la grille de séparation des fonctions informatiques.

CESAG - BIBLIOTHEQUE

6.2.1.1. Evaluation des forces et faiblesses des contrôles généraux

Le QCI (annexe 2 page 90) est élaboré à partir d'une check-list de questions relatives aux bonnes pratiques en matière de contrôles informatiques. Il nous a permis d'élaborer le tableau des forces et faiblesses apparentes (TFfA) des contrôles généraux informatiques de la CNCAS. Comme son nom l'indique, le TFfA est un tableau synthétique sur la prise en compte ou non des risques informatiques d'ordre macroscopiques avant d'entamer les risques informatiques spécifiques au processus étudié. Les résultats du questionnaire sont exploités avec l'aide d'un tableau présenté en annexe 5 page 100.

Ce tableau permet d'avoir une évaluation préliminaire et nous laisse présager les forces et faiblesses du CI. La colonne constat nous permet de le faire en constatant l'existence ou non des POCA/indicateurs (Pratiques d'Organisation Communément Admises) pour gérer le risque. La réponse « oui » permet de tirer une première conclusion qui est une force de conception des contrôles. Cette dernière ne doit pas souffrir d'une faiblesse d'application pour rester en définitive une force de CI. La réponse « non » est une faiblesse de conception et doit être corrigée.

Il ressort de l'analyse du TFfA, entre autres, les forces de contrôles généraux informatiques de la CNCAS suivantes :

- l'existence d'un manuel des procédures informatiques ;

- la maîtrise de la sécurité physique liée à l'accès aux locaux, à la prévention d'incidents électriques et d'incendie ;
- la maitrise de la sécurité logique du système et des données informatiques notamment leur intégrité, leur confidentialité et leur traçabilité ;
- la maîtrise de l'exploitation des applications et du système notamment l'exhaustivité des traitements, la disponibilité du système et des données, la continuité de l'exploitation ;
- l'existence d'une politique de maintenance des systèmes et applications.

Cependant, certaines faiblesses de contrôles généraux ont été relevées :

- rattachement hiérarchique insuffisant de la fonction informatique ;
- le manuel des procédures ne traite pas des procédures de développement d'applications ;
- l'inexistence d'un site de secours et de stockage hors site ;
- l'inexistence d'un dispositif permettant de limiter les dégâts des eaux alors que les locaux de l'infrastructure informatique se trouvent au rez-de-chaussée.

L'étude de la séparation des fonctions informatique a fait l'objet d'un traitement à part.

CESAG - BIBLIOTHEQUE

6.2.1.2. Evaluation de la séparation des fonctions informatiques

Elle nous a permis de comprendre la répartition des responsabilités entre les différents acteurs dans la réalisation des tâches habituelles de la fonction informatique. L'évaluation de la séparation des fonctions informatique de la CNCAS est faite grâce à la grille d'analyse des tâches présentée en annexe 3 page 94. L'exploitation de cet outil montre que la fonction informatique de la CNCAS maitrise plus ou moins le principe de séparation des fonctions. Cependant il y a lieu noter :

- un chevauchement des fonctions entre le sous-directeur de l'informatique et le secrétaire général en ce qui concerne l'administration de la fonction informatique ;
- l'existence de postes vacants non remplacés ce qui peut creuser davantage le manque de personnel informatique déjà constaté et entrainer forcément le cumul de fonctions incompatibles.

6.2.2. Evaluation des contrôles applicatifs

Il s'agit de faire le test de conformité des contrôles applicatifs pour évaluer leur efficacité. Pour cela, nous avons besoin de définir une procédure d'échantillonnage et d'une échelle d'appréciation de qualité des contrôles.

6.2.2.1. Procédure d'échantillonnage et taille de l'échantillon

La base de l'échantillonnage est l'octroi de crédits enregistrés de toutes les agences de la CNCAS dans le progiciel Delta-Bank pour la période du 1er Octobre au 31 Décembre 2011. Nous avons procédé à l'extraction des données par la voie de requêtes avec le logiciel BusinessObjects sous le format d'un classeur Excel qui se présente comme suit :

CESAG - BIBLIOTHEQUE

Tableau 6 : Fichier Excel d'extraction des données de Delta-Bank

n° d'ordre	Agence	N° Compte	Prénom	Nom	N° Dossier	Date Mise en place	Gestionnaire	Profil client	Montant	taux Intérêt	Date 1ere Echéance	Date Dernière Échéance	Montant Echéance	Nombre Echéance	Type de Crédit	Libellé Type Crédit	Nom Utilisateur
1																	
2																	
3																	
4																	
5																	
5																	
7																	
8																	
9																	
10																	
11																	
12																	
…																	
…																	
…																	
n																	

CESAG - BIBLIOTHEQUE

Source : CNCAS (2012)

A partir de ce fichier Excel, nous effectuons ensuite des filtres selon les informations dont nous avons besoin pour faire les tests par rapport à un risque donné. Par exemple, nous avons fait des filtres par rapport :

- aux types de crédit ;
- aux profils des clients ;
- aux taux d'intérêt, etc.

Vu le nombre de crédits octroyés pendant la période de base de l'étude, nous avons retenu la taille de l'échantillon à 20% de la population à étudier pour chaque risque. Les échantillons ont été constitués, après les filtres nécessaires, de façon aléatoire en utilisant la fonction ALEA.ENTRE.BORNES ( ) sauf pour le risque de doublon de dossier pour lequel il fallait vérifier la séquence numérique des dossiers de crédit de l'échantillon.

CESAG - BIBLIOTHEQUE

6.2.2.2. Définition de l'échelle de cotation des contrôles

Pour l'appréciation de l'efficacité des contrôles applicatifs, nous avons défini, avec notre maître de stage, l'échelle ci-dessous :

Tableau 7 : Grille de cotation de la qualité du contrôle

Qualité du contrôle	Cote	Commentaires
Très élevée	5	Le succès du contrôle est compris entre 80 et 100%
Elevée	4	Le succès du contrôle est compris entre 60 et 80%
Moyenne	3	Le succès du contrôle est compris entre 40 et 60%
Insuffisante	3	Le succès du contrôle est compris entre 20 et 40%
Médiocre	1	Le succès du contrôle est compris entre 0 et 20%

Source : Nous-mêmes à partir de JIMENEZ & al (2008 : 238)

La procédure d'échantillonnage et les critères d'appréciation des contrôles étant définis, nous pouvons maintenant procéder aux tests d'évaluation de l'efficacité des contrôles applicatifs.

6.2.2.3. Evaluation de l'efficacité des contrôles

Elle permet de déterminer si les contrôles applicatifs fonctionnent efficacement ou si les utilisateurs imaginatifs parviennent à les contourner. L'évaluation de l'efficacité des contrôles est faite à l'aide d'un tableau dénommé tableau d'évaluation de l'efficacité des contrôles (annexe 6 page 103).

Ce tableau comporte quatre (05) colonnes que sont :

- risques opérationnels : cette colonne permet de lister les risques opérationnels identifiés dans le processus informatique de gestion du crédit ;
- activités ou contrôles limitant le risque : c'est le recensement ou l'identification des activités ou contrôles mis en place pour la maitrise du risque identifié ;
- tests pour éléments probants : cette colonne nous permet de définir les tests pour l'obtention d'éléments probants sur le succès ou non de dispositif de maitrise des risques décrit dans la colonne précédente ;
- résultats du test : c'est la présentation des résultats des tests définis précédemment ;
- évaluation de la qualité du contrôle : c'est l'appréciation de la qualité des contrôles applicatifs après les tests d'efficacité effectués.

La synthèse de l'évaluation de l'efficacité des contrôles est présentée avec le tableau de synthèse suivant :

CESAG - BIBLIOTHEQUE

Tableau 8 : Tableau de synthèse de l'évaluation de l'efficacité des contrôles applicatifs

Risques opérationnels	Activités et contrôles limitant le risque	Evaluation des contrôles	
		Qualité	cote
R1. existence de doublon de dossier	attribution automatique des numéros de dossier	Très élevée	5
R2. choix d'un crédit pour un client qui n'a pas le profil requis	les lignes de crédit sont paramétrées selon le type de client	Insuffisante	2
R3. choix d'un taux d'intérêt différent de celui du type de crédit	le taux est paramétré dans le système selon le type de crédit choisi	Moyenne	3
R4. dépassement de la quotité cessible pour les salariés	l'utilisateur édite le tableau d'amortissement et fait le rapprochement entre échéances et quotité cessible	Insuffisante	2
R5. dépassement du taux d'endettement pour les entreprises	contrôles utilisateur : analyse financière	Moyenne	3
R6. MEP de crédit pour un salarié d'une société non homologuée par un agent non habilité	contrôle utilisateur : vérifier la société du salarié sur la liste des sociétés homologuées	Insuffisante	2
R7. validation d'un crédit par un utilisateur non délégataire	profil et habilitations des utilisateurs	Elevée	4
R8. octroi d'un crédit salarié avant la domiciliation du salaire	en plus du certificat de domiciliation, l'utilisateur doit vérifier le virement du salaire dans le compte du client	Elevée	4
R9. altération du taux d'intérêt choisi pour valider le dossier	le champ du taux est grisé	Elevée	4
R10. altération du montant autorisé	Séparation des fonctions entre l'agent instructeur et le décisionnaire : le dernier nommé saisit directement la décision de banque dans le système et mentionne le montant autorisé sur la fiche synoptique du dossier qui est transmis à l'agent instructeur	Elevée	4

CESAG - BIBLIOTHEQUE

R11. altération de la durée de crédit autorisée	Séparation des fonctions entre l'agent instructeur et le décisionnaire : le dernier nommé saisit directement la décision de banque dans le système et mentionne la durée autorisée sur la fiche synoptique du dossier qui est transmis à l'agent instructeur	Elevée	4
R12. dépassement des habilitations par rapport au montant	profil et habilitations des utilisateurs	Moyenne	3
R13. dépassement des habilitations par rapport à la durée	Idem	Moyenne	3
R14. validation d'un dossier rejeté	En cas de rejet, le décisionnaire le saisit dans le système et l'inscrit dans le dossier puis le transmet à l'agent instructeur	Très Elevée	5
R15. octroi de crédit à un client qui dépasse la limite d'âge par un agent non habilité (pour les retraités)	Contrôle utilisateur (manuel) : l'utilisateur vérifie l'âge du client de profil « retraité » à l'aide de sa CNI	Moyenne	3
R16. non saisie de la garantie (si nécessaire) avant validation	L'instructeur du dossier saisit la garantie et le délégataire vérifie la conformité avant de valider le crédit dans le système	Moyenne	3

Source : Nous-mêmes

CESAG - BIBLIOTHEQUE

Ces risques opérationnels identifiés vont faire l'objet de cotation dans la section suivante.

6.3. Cotation des risques opérationnels liés à l'application de gestion du crédit

La cotation des risques représente l'étape cruciale pour hiérarchiser les risques entre eux. Chaque risque opérationnel identifié fera l'objet d'une cotation en termes de probabilité et d'impact à l'aide de ce que l'on appelle échelle de cotation des risques.

6.3.1. Evaluation de la probabilité de survenance des risques

Pour déterminer la probabilité d'occurrence des risques, nous avons utilisé une évaluation qualitative plus facile à mettre en œuvre par rapport à l'évaluation quantitative. Dans ce cas de figure, la probabilité dépend étroitement de la qualité du CI. Autrement dit plus la qualité du

CI est élevée plus la probabilité de réalisation du risque est faible c'est à dire, les deux grandeurs évoluent en sens inverse. Pour cela, il faut définir une échelle de cotation de la probabilité et une grille de correspondance entre qualité du contrôle et probabilité de survenance des risques.

Tableau 9 : Grille de cotation de la probabilité de survenance des risques

Probabilité	Cote	Commentaires
Très rare	1	La survenance du risque est presque nulle
Rare	2	La survenance du risque est rare
Probable	3	La survenance du risque est relativement fréquente
Fréquente	4	La survenance du risque est fréquente
Très fréquente	5	La survenance du risque est presque certaine

Source : Nous-mêmes à partir de CRAMRA (2004 : 19)

Nous avons défini la grille de correspondance qualité du contrôle et probabilité de survenance des risques suivante :

Tableau 10 : Grille de correspondance entre la qualité du contrôle et la probabilité des risques

Evaluation du contrôle		Evaluation de la probabilité des risques	
Qualité	Cote	Probabilité	Cote
Très élevée	5	Très rare	1
Elevée	4	Rare	2
Moyenne	3	Probable	3
Insuffisante	2	Fréquente	4
Médioere	1	Très fréquente	5

Source : Nous-mêmes à partir de YAZI (2011 : 82)

Cette grille nous permet d'évaluer aisément la probabilité d'occurrence des risques opérationnels liés à l'application de gestion du crédit de la CNCAS.

CESAG - BIBLIOTHEQUE

Tableau 11 : Tableau de l'évaluation de la probabilité de survenance des risques opérationnels liés à l'application de gestion du crédit

Risques opérationnels	Evaluation des contrôles		Evaluation de la probabilité	
	Qualité	Cote	Probabilité	cote
R1. existence de doublon de dossier	Très élevée	5	Très rare	1
R2. choix d'un crédit pour un client qui n'a pas le profil requis	Insuffisante	2	Fréquente	4
R3. choix d'un taux d'intérêt différent de celui du type de crédit	Moyenne	3	Probable	3
R4. dépassement de la quotité cessible pour les salariés	Insuffisante	2	Fréquente	4
R5. dépassement du taux d'endettement pour les entreprises	Moyenne	3	Probable	3
R6. MEP de crédit pour un salarié d'une société non homologuée par un agent non habilité	Insuffisante	2	Fréquente	4
R7. validation d'un crédit par un utilisateur non délégataire	Elevée	4	Rare	2
R8. octroi d'un crédit salarié avant la domiciliation du salaire	Elevée	4	Rare	2
R9. altération du taux d'intérêt choisi pour valider le dossier	Elevée	4	Rare	2
R10. altération du montant autorisé	Elevée	4	Rare	2
R11. altération de la durée de crédit autorisée	Elevée	4	Rare	2
R12. dépassement des habilitations par rapport au montant	Moyenne	3	Probable	3
R13. dépassement des habilitations par rapport à la durée	Moyenne	3	Probable	3
R14. validation d'un dossier rejeté	Très Elevée	5	Fréquente	1
R15. octroi de crédit à un client qui dépasse la limite d'âge par un agent non habilité (pour les retraités)	Moyenne	3	Probable	3
R16. non saisie de la garantie (si nécessaire) avant validation	Moyenne	3	Probable	3

Source : Nous-mêmes

Toujours dans le cadre de la cotation des risques opérationnels identifiés, nous allons maintenant évaluer l'impact ou la gravité des risques.

CESAG - BIBLIOTHEQUE

6.3.2. Évaluation de l'impact des risques

L'évaluation de l'impact des risques est la tentative d'estimation des conséquences des risques si jamais ils se produisaient. Il s'agira essayer de mesurer les pertes en termes de coût, de délai, d'image, d'efficacité, de compétitivité… Etant difficilement quantifiable, l'impact des risques sera évalué, comme la probabilité des risques, de façon qualitative avec l'aide d'une échelle de cotation qui sera définit par consensus en essayant d'être le plus objectif possible.

Tableau 12 : Grille de cotation de l'impact du risque

Impact	Cote	Description des conséquences du risque
Très faible	1	Les conséquences du risque sont négligeables et peuvent être corrigées rapidement
Faible	2	Les effets du risque sont acceptables
Moyen	3	La gravité du risque n'est pas négligeable et mérite des actions limitatives
Grave	4	Les conséquences sont graves, les actions nécessaires doivent être prises
Très grave	5	Les effets du risque sont très graves et le risque mérite des actions immédiates pour réduire sa survenance

Source : Nous-mêmes à partir de CGL consulting (2005 : 1)

Nous allons présenter l'évaluation de l'impact des risques à l'aide du tableau suivant. Ce tableau comporte une colonne des risques identifiés, une colonne de la qualification de l'impact des risques, une colonne pour coter les conséquences des risques et une dernière colonne observations pour justifier l'évaluation de l'impact du risque correspondant.

CESAG - BIBLIOTHEQUE

Tableau 13 : Tableau d'évaluation de l'impact des risques

Risques identifiés	Evaluation impact	Cotation	Observations
R1. existence de doublon de dossier	Très faible	1	Le risque peut être corrigé rapidement
R2. choix d'un crédit pour un client qui n'a pas le profil requis	Grave	4	Cela peut créer des pertes financières et l'anarchie
R3. choix d'un taux d'intérêt différent de celui du type de crédit	Très grave	5	Cela peut créer des pertes financières, l'anarchie, des plaintes de la part du client, des pertes d'image et de compétitivité
R4. dépassement de la quotité cessible pour les salariés	Moyen	3	Le risque peut créer des plaintes du client pour le rallongement de la durée du crédit ou des litiges avec l'inspection du travail
R5. dépassement du taux d'endettement pour les entreprises	Grave	4	Il peut créer le rallongement du crédit, des défauts de paiement, des pertes de chiffre d'affaires prévisionnel
R6. MEP de crédit pour un salarié d'une société non homologuée par un agent non habilité	Moyen	3	Il peut créer le rallongement du crédit, des défauts de paiement, des pertes de chiffre d'affaires prévisionnel.
R7. validation d'un crédit par un utilisateur non délégataire	Très grave	5	Cela crée une porte ouverte à toutes dérives possibles.
R8. octroi d'un crédit salarié avant la domiciliation du salaire	Moyen	3	Cela peut créer des pertes financières.
R9. altération du taux d'intérêt choisi pour valider le dossier	Très grave	5	Les conséquences sont des fraudes et des pertes financières.
R10. altération du montant autorisé	Très grave	5	Les conséquences sont des fraudes et des pertes financières.
R11. altération de la durée de crédit autorisée	Grave	4	Les conséquences sont des fraudes et des pertes de chiffre d'affaires prévisionnel.
R12. dépassement des habilitations par rapport au montant	Très grave	5	Cela peut installer l'anarchie, le favoritisme et même des fraudes
R13. dépassement des habilitations par rapport à la durée	Grave	4	Cela peut installer l'anarchie et le favoritisme.
R14. validation d'un dossier rejeté	Très grave	5	Possibilité de toutes les dérives (fraudes, l'anarchie, favoritisme…)
R15. octroi de crédit à un client qui dépasse la limite d'âge par un agent non habilité (pour les retraités)	Grave	4	Il peut en découler des défauts ou retards de paiements et des pertes financières ou de chiffre d'affaires prévisionnel
R16. non saisie de la garantie (si nécessaire) avant validation	Très grave	5	Possibilité de défauts de paiements et donc des pertes financières.

Source : Nous mêmes

CESAG - BIBLIOTHEQUE

Après avoir fini avec les étapes de l'évaluation de la probabilité et de l'impact des risques, nous allons les hiérarchiser entre eux et les formaliser avec la cartographie ou matrice des risques.

6.3.3. Hiérarchisation et cartographie des risques

La hiérarchisation des risques consiste à classer les risques par ordre décroissant selon leur criticité. Le tableau ci-dessous fait office de synthèse de la cotation et de la hiérarchisation des risques.

Tableau 14 : Tableau de synthèse et de cotation des risques identifiés

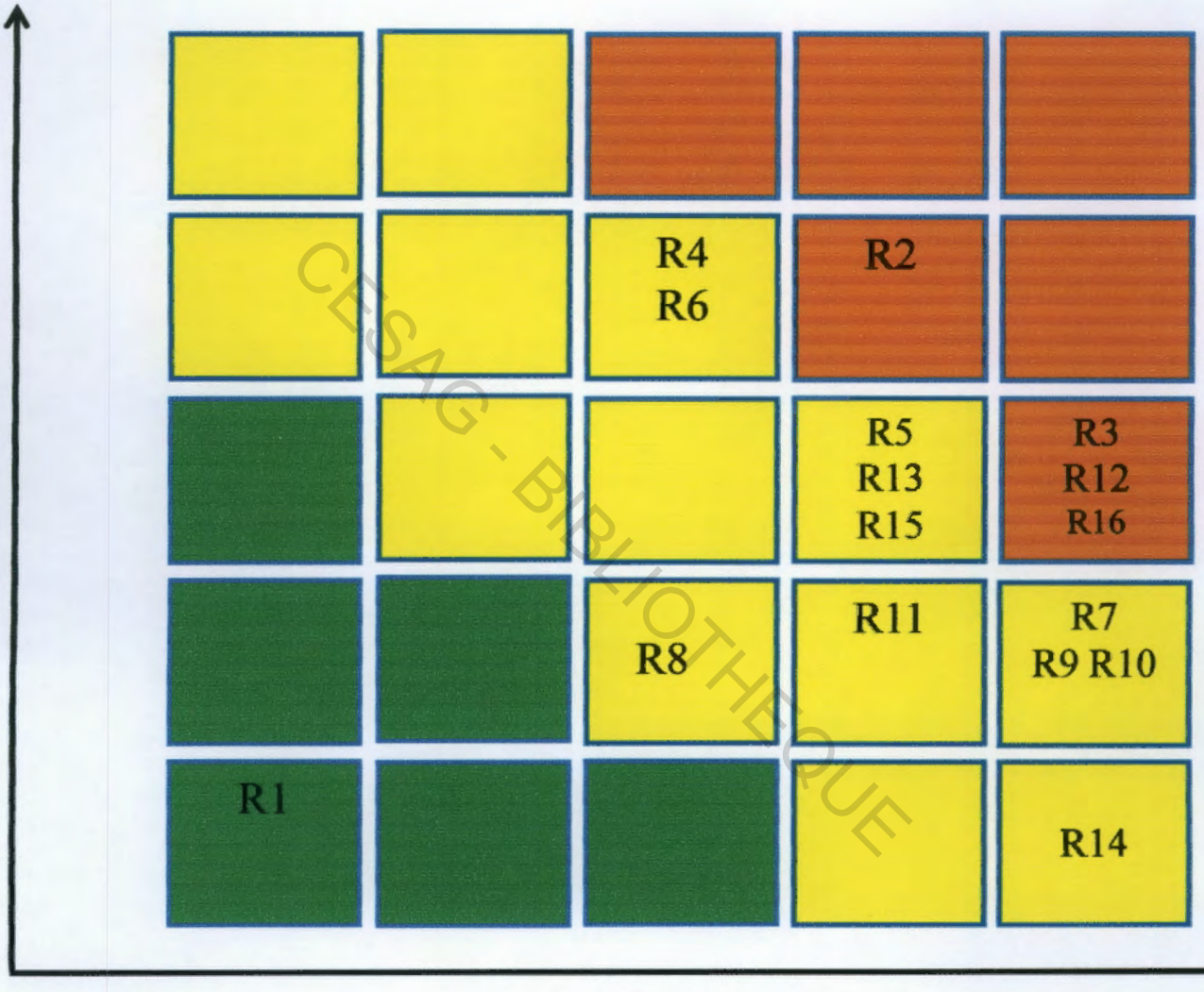
Risques identifiés	Evaluation probabilité	Evaluation impact	Criticité des risques
R2. choix d'un crédit pour un client qui n'a pas le profil requis	4	4	16
R16. non saisie de la garantie (si nécessaire) avant validation	3	5	15
R3. choix d'un taux d'intérêt différent de celui du type de crédit	3	5	15
R12. dépassement des habilitations du montant	3	5	15
R5. dépassement du taux d'endettement pour les entreprises	3	4	12
R6. MEP de crédit pour un salarié d'une société non homologuée par un agent non habilité	4	3	12
R13. dépassement des habilitations de la durée	3	4	12
R15. octroi de crédit à un client qui dépasse la limite d'âge par un agent non habilité (pour les retraités)	3	4	12
R4. dépassement de la quotité cessible pour les salariés	4	3	12
R7. validation d'un crédit par un utilisateur non délégataire	2	5	10
R10. altération du montant autorisé	2	5	10
R9. altération du taux d'intérêt choisi pour valider le dossier	2	5	10
R11. altération de la durée de crédit autorisée	2	4	8
R8. octroi d'un crédit salarié avant la domiciliation du salaire	2	3	6
R14. validation d'un dossier rejeté	1	5	5
R1. existence de doublon de dossier	1	1	1

Source : Nous mêmes

CESAG - BIBLIOTHEQUE

La cartographie des risques c'est la formalisation de la cotation sous forme de matrice. Elle est présentée par la figure 10 ci-dessous.

Figure 10 : cartographie des risques du processus informatique de crédit



CESAG - BIBLIOTHEQUE

Source : Nous mêmes

- les risques de la zone rouge nécessitent des actions immédiates afin de diminuer la criticité du risque soit en agissant sur la probabilité ou sur l'impact pour le ramener dans la zone jaune à défaut d'atteindre un risque cible (zone verte) ;

- les risques de la zone jaune méritent une surveillance pour limiter leur manifestation ;
- la zone verte représente les risques cibles qui sont des risques acceptables car facilement corrigibles.

Tout l'intérêt des étapes précédentes était de pouvoir formuler des recommandations par rapport aux défaillances relevées afin d'apporter de la valeur ajoutée à l'évaluation des risques.

6.4. Recommandations pour la maîtrise des faiblesses constatées

Les recommandations seront formulées à partir des différentes remarques et manquements constatés au niveau de la fonction informatique et du processus informatique de gestion du crédit.

CESAG - BIBLIOTHEQUE

6.4.1. Recommandations relatives à la fonction informatique

Les recommandations pour la fonction informatique portent d'une part sur l'organisation de celle ci et d'autre part sur les contrôles généraux.

6.4.1.1. Organisation de fonction de la fonction informatique

Les recommandations suivantes concernent les faiblesses majeures de l'organisation de la fonction informatique.

1) Au regard de l'importance de la fonction informatique dans une banque, nous recommandons d'ériger la SDIO en une direction rattachée directement au DG pour lui permettre de participer au comité de direction afin de mieux remplir sa mission.
2) Renforcer le nombre du personnel de l'informatique pour pouvoir combler les postes vacants et ainsi éviter le risque de cumul de fonctions incompatibles.

6.4.1.2. Contrôles généraux informatiques

Les contrôles généraux comprennent tous les contrôles de l'infrastructure informatique nécessaires pour garantir l'efficacité du système informatique. Nos recommandations pour ces derniers sont de :

3) Prendre toutes dispositions nécessaires pour l'acquisition d'un site de secours.
4) Rendre effectif le stockage hors site des données informatiques conformément écrit au manuel des procédures .
5) Mettre à jour le manuel des procédures informatiques (exploitation et développements).

6.4.2. Recommandations relatives à la gestion informatique du crédit

La première recommandation est de voir avec la direction informatique les modalités d'informatisation de tout le processus de crédit (de demande du client jusqu'à la mise en place du crédit) pour garantir plus de compétitivité en réduisant le temps de l'étude des dossiers.

Les autres recommandations portent sur la maitrise des risques majeurs du processus de gestion du crédit : R2, R3 (annexe 4 FAR n°1 page 95) ; R12, R13 (annexe 4 FAR n°2 page 96) ; R16 (annexe 4 FAR n°3 page 97) ; R7 (annexe 4 FAR n°4 page 98) ; R4, R6 (annexe 4 FAR n°5 page 99).

CESAG BIBLIOTHEQUE

6.5. Plan de suivi des recommandations

Il ne sert à rien de formuler des recommandations s'il n'existence un système de suivi de leur mise en œuvre. C'est pourquoi nous proposons le tableau de suivi des recommandations ci-dessous :

Tableau 15 : Tableau de suivi des recommandations

Recommandations	Mesures correctives déjà prises ou actions prévues	Début	Fin	Observations sur les délais	Mise en œuvre des recommandations			Observations sur la mise en œuvre / nouvelles recommandations
					Total	Partiel	Pas du tout	

Source : Nous-mêmes à partir de YAZI (2011)

CESAG - BIBLIOTHEQUE

Conclusion

Ce chapitre a permis de déceler d'une part les principales forces et faiblesses de la fonction informatique et d'autre part d'évaluer les risques opérationnels majeurs de l'application informatique de gestion du crédit de la CNCAS. Il faut noter que l'identification des risques n'a pas concerné les crédits agricoles du fait de la révision en cours des procédures.

Il ressort de cette évaluation qu'il existe plusieurs lacunes dans la maîtrise des risques opérationnels liés à la gestion informatique du crédit de la CNCAS. A cet effet des recommandations ont été formulées pour la maitrise de ces risques.

CESAG - BIBLIOTHEQUE

CONCLUSION DE LA DEUXIEME PARTIE

La deuxième partie du mémoire a été pour nous le cadre pour mettre en œuvre les connaissances théoriques acquises au cours de notre formation en général, et celles de l'évaluation des risques applicatifs en particulier.

En effet cette partie n'est rien d'autre que le déroulement du modèle d'analyse élaboré à partir de la revue de littérature qui nous a permis d'aboutir à l'étude du degré de maitrise des risques opérationnels liés à la gestion informatique du crédit de la CNCAS. Et à la suite de cela, on a pu formuler des recommandations afin de corriger les différentes anomalies et faiblesses décelées.

CESAG - BIBLIOTHEQUE

CONCLUSION GENERALE

CESAG - BIBLIOTHEQUE

Aujourd'hui le développement des technologies de l'information et de la communication a contribué très fortement au développement et à l'expansion des institutions financières de sorte que l'ensemble des processus des banques repose sur l'outil informatique.

Le crédit étant le produit bancaire qui fait le plus de profit aux banques ; c'est ce qui justifie le choix de notre thème de mémoire qui porte de façon générale sur « l'évaluation des risques informatiques » et particulièrement « l'évaluation des risques liés à l'application informatique de gestion du crédit : cas de la CNCAS ».

A cet effet, nous avons structuré notre mémoire autour deux parties :

- une partie théorique qui nous a permis de faire la revue de littérature avec deux chapitres : les contrôles applicatifs et l'évaluation et méthodes d'analyse des risques applicatifs ; et un troisième chapitre qui constitue la méthodologie de l'étude.
- une partie dite cadre pratique qui constitue le lieu de mettre en œuvre la démarche d'évaluation avec trois chapitres :
  - présentation de la CNCAS ;
  - description du processus de gestion du crédit de la CNCAS et de son traitement informatique;
  - évaluation des risques opérationnels liés à l'application informatique de gestion du crédit.

CESAG - BIBLIOTHEQUE

La réalisation de cette étude nous a édifiés sur le degré de criticité des risques liés à la gestion informatique du crédit de la CNCAS qui était notre question principale de recherche. Elle a aussi permis de faire l'évaluation des risques de la fonction informatique de la banque.

Au terme de cette évaluation, nous avons pu identifier plusieurs faiblesses du contrôle interne informatique tant du coté des contrôles généraux que celui des contrôles applicatifs. L'étude nous permet de confirmer aussi que la maîtrise des risques applicatifs repose sur le remplacement des contrôles manuels et des contrôles en aval quand cela est possible par respectivement des contrôles automatiques et des contrôles en amont autrement dit préventifs.
L'apport de ce mémoire est de :

- fournir à la CNCAS une connaissance sur le niveau de l'efficacité du système de maîtrise des risques opérationnels liés à l'application de gestion du crédit avec l'élaboration de la cartographie des risques ;
- et de formuler des recommandations pour la maîtrise de ces risques.

Cependant il appartiendra à la Direction Générale de la banque de prendre les dispositions nécessaires, avec les différents services concernés, pour définir les solutions techniques qui découlent de nos recommandations. Dans le cas où l'état actuel du progiciel bancaire ne permet pas d'intégrer avec efficacité les solutions envisagées, nous préconisons de faire des développements internes d'applications qui répondent au mode d'organisation de la banque.

CESAG - BIBLIOTHEQUE

ANNEXES

CESAG - BIBLIOTHEQUE

Annexe 1 : Questionnaire de Prise de connaissance

Entretien avec le Chef d'agence de Dakar :

1. En quoi consiste votre travail de chef d'agence c'est à dire quelles sont les principales tâches que vous accomplissez au quotidien ?

2. Quelles sont les différentes étapes du processus de gestion des crédits dans Delta et qui sont les différents acteurs qui interviennent au niveau de chaque étape et quels sont leurs niveaux de responsabilité ?

3. Pour chacune de ces étapes, quelles sont les procédures mises en œuvre ?
(contrôle, autorisation, validation, …)

4. Quels sont les différents documents utilisés pour l'exécution des différentes tâches ?
5. Quelles sont les difficultés récurrentes que vous rencontrez avec le logiciel DELTA BANK?

6. Quelles sont les incidents que vous rencontrez avec Delta-Bank ?

7. En cas de survenance de problèmes majeurs dans delta-bank, en informez-vous la DI ? Si OUI comment et à qui ?

8. Vos préoccupations sont-elles prises en compte à temps ? Ou bien une solution de secours ? Etes-vous satisfait des prestations de la SDIO en général ?

9. votre mot de passe est-il changé régulièrement ? Quel est la fréquence ?

10. Quelles sont vos attentes quant à la réalisation de cette mission d'évaluation de Delta-Bank ?

12. Demande observation physique mise en place dans delta.

Source: nous-mêmes

CESAG - BIBLIOTHEQUE

Entretien avec le responsable de l'informatique :

1. En quoi consiste votre travail de Directeur informatique ?

2. Qui sont vos collaborateurs et en quoi consistent leurs tâches?

3. Pouvez-vous me présenter l'organisation interne de votre direction (organigramme, nombre de collaborateurs, …) ?

4. Quelles sont vos attentes quant à la réalisation de cette mission ?

5. Demander l'accord pour rencontrez ses collaborateurs et prendre des RV avec ces derniers.

CESAG - BIBLIOTHEQUE

Annexe 2 : Questionnaire de contrôle interne

I. Organisation générale

1. Y a-t-il un audit périodique (interne ou externe) portant au minimum sur la conformité des contrôles programmés des applications stratégiques ?
2. Existe-t-il un organigramme à jour de la SDIO ?
3. Une définition des fonctions est-elle précisée pour chaque poste figurant dans l'organigramme ?
4. Le service informatique est-il rattaché à un niveau hiérarchique correspondant à sa mission au sein de l'entreprise ?
5. Les effectifs sont-ils suffisants pour faire face aux travaux prévus et imprévus ?
6. Le manuel des procédures informatiques est-il à jour ?
7. Existe-t-il des besoins informatiques importants de l'entreprise non pris en compte ou retardés de façons significatives ?
8. Chaque projet fait-il l'objet d'un avant projet et d'un cahier des charges consignés par le service informatique et le service utilisateur ?
9. Au cours des 3 dernières années, votre établissement a-t-il subi un préjudice, conséquences d'un dommage informatique :
   - accident matériel ?
   - accident applicatif ?
   - erreurs ?
   - malveillance ?

II. Sécurité

10. Y a-t-il un dispositif de protection du matériel de télécommunications (unités, contrôleurs, modems, têtes de ligne…) ?
11. Les virements et opérations financières télématiques, les transferts d'informations stratégiques ou confidentielles sont-ils uniquement supportés par des réseaux professionnels spécifiques (type SWIFT) ?
12. Y a-t-il un système automatique de contrôle d'accès aux salles des ordinateurs ?
13. Y a-t-il une redondance réelle locale des serveurs et des organes stratégiques (contrôleurs) ?
14. Est-elle testée périodiquement (au moins 1 fois par an) ?
15. Si oui, quand c'était le dernier test ?
16. La solution de secours est-elle testée au moins chaque trimestre ?
17. Y-a-t'il un système de secours de la climatisation des salles machines (redondance) ?
18. Y-a-t'il un système d'extincteur automatique dans la salle des machines (unités centrales, serveurs, …) ?
19. Y a-t-il un système de régulation (onduleur) de l'alimentation électrique ?
20. Y-a-t'il un système de secours de l'alimentation électrique des salles machines ?
21. Existe-il une stratégie de la sécurité portant sur la protection :
    - Des accès physiques ?
    - Des procédures de sauvegarde, restauration et reprise ?

CESAG - BIBLIOTHEQUE

22. Existe-t-il des procédures limitant l'accès physique aux actifs informatiques ?
23. L'entreprise a-t-elle mis en place un système de détection de fumée ?
24. Existe-t-il un système d'extincteur automatique ?
25. L'entreprise a-t-elle mis en place un système de :
    - Détection de fumée ?
    - Détection d'incendie ?
26. Existe-t-il un dispositif suffisant permettant de prévenir ou de limiter les dégâts des eaux ?
27. Les procédures permettent-elles un contrôle suffisant dans les domaines suivants :
    - Protection contre les accès non autorisés ?
    - Journalisation des modifications ?

III. Exploitation

28. L'exploitation repose-t-elle sur des procédures cataloguées dont l'accès est limité et contrôlé ?
29. Y a-t-il une documentation d'exploitation complète et mise à jour pour l'ensemble des applications ?
30. Existe-t-il des dispositions pour protéger les enregistrements contre la destruction accidentelle et assurer une exploitation continue ?
31. Existe-t-il des méthodes permettant de reconstituer les fichiers à la suite d'erreurs mineures de traitement ou de destruction mineure d'enregistrement ?
32. Quels sont les contrôles qui permettent périodiquement de s'assurer que les tables ne contiennent pas des données fictives ? par exemple modification non autorisée dans le fichier client.
33. Existe-t-il des procédures de contrôle des entrées, des rejets et des traitements ?
34. Existe-t-il un système de contrôle qui permet de s'assurer que tous les comptes ont fait l'objet de prélèvement d'agios ?
35. Existe-t-il un système de détection des comptes dormants ?
36. Les instructions d'exploitation pour les applications comprennent-elles, notamment :
    - Un descriptif du flux des applications ?
    - Les procédures de paramétrages ?
    - La liste des fichiers nécessaires ?
    - Les procédures de sauvegarde, de restauration et de reprise ?
37. Le manuel de procédures d'exploitation prévoit-il :
    - Une séparation entre les activités développement et exploitation ?
    - Une séparation des taches d'exploitation et de contrôle au sein de l'activité exploitation ?
    - Une interdiction absolue aux équipes d'exploitation de corriger les erreurs et de modifier les programmes ou le contenu des fichiers ?
    - Des consignes en cas d'incidents ?
    - Des consignes en cas de sinistres ?

CESAG - BIBLIOTHEQUE

IV. Administration système

38. Y a-t-il un seul responsable titulaire de la fonction de gestion et de mise en place des droits d'accès ?
39. Le progiciel de contrôle d'accès prend-il en compte tous les accès locaux et à distance sans exception ?
40. Existe-t-il un système d'identification et d'authentification par mot de passe (ou carte) pour chaque utilisateur ?
41. Le responsable des mots de passe procède t-il régulièrement à la maintenance avec les utilisateurs des profils d'accès selon l'évolution de la banque ?
42. Existe-t-il une traçabilité des données ?
43. Le système génère t-il les numéros de compte automatiquement lors de la création d'un nouveau client ?
44. Existe-t-il des procédés de journalisation des accès permettant d'analyser les éléments suivants :
    - Autorisation des sollicitations (fichier, programme, transaction) ?
    - Localisation et fréquence des forçages ?
    - Changement des profils d'accès ?

V. Procédures de sauvegarde et de reprise

45. Y-a-t'il un stock de matériel de sauvegarde des données ?
46. Y a-t-il des procédures écrites concernant l'archivage / désarchivage spécifique à chaque type de support ?
47. Y a-t-il des procédures de reprise automatique des applications en cas d'interruption accidentel de l'exploitation (points de reprise, journal image avant, etc.) ?
48. Possède-t-on une sauvegarde de la documentation des études et de la documentation d'exploitation dans des locaux protégés ?
49. Existe-t-il des procédures formalisées de sauvegarde et de restauration ?
50. La périodicité des sauvegardes est-elle adaptée aux besoins de l'entreprise ?
51. Pour les applications considérées comme vitale, est-il procédé à une duplication des sauvegardes ?
52. Existe-t-il des procédures de stockage des sauvegardes hors site ?
53. Le stockage des sauvegardes sur site et hors site est-il réalisé dans des armoires ignifuges ?

VI. Maintenance

54. L'entreprise a-t-elle souscrit un contrat de maintenance des applications ?
55. Si oui, ce contrat est-il :
    - Préventif ?
    - Curatif ?
56. Quel est le délai d'intervention à partir de la demande :
    - Moins de 24 heures ?
    - Moins de 48 heures ?
    - Moins de 5 jours ?
    - Non défini dans le contrat ?

CESAG - BIBLIOTHEQUE

57. Y a-t-il un plan de renouvellement des équipements informatiques ?
58. Y a-t-il des procédures écrites de révision appliquées systématiquement avant la mise en exploitation pour toute création ou maintenance d'une application ?

CESAG - BIBLIOTHEQUE

Annexe 3 : Grille d'analyse des tâches de la fonction informatique

Tâches	Nature	Personnes intervenant dans les tâches			
		SG	SDIO	CSSP	CSDSU
1. Administrer la fonction informatique	A	x	x		
2. Administrer les serveurs	A			x	
3. Administrer la base de données	A			x	
4. Administrer le réseau	A			x	
5. Gérer la sécurité (physique, logique)	Ex			x	
6. Effectuer les sauvegardes	Ex			x	
7. Stocker les sauvegardes	Ex			x	
8. Développer les applications	D				x
9. Mettre à jour les applications	D				x
10. Développer des requêtes	D				x
11. Documenter les applications	D				x
12. Rédiger les guides utilisateurs	D				x
13. Former les utilisateurs	D				x
14. Exploiter les applications	Ex			x	
15. Transférer les données	Ex			x	
16. Gérer les mots de passe	Ex				x
17. Enquêter sur les forçages	C				x
18. Contrôler la salle des machines	C			x	
19. Entretenir les équipements	C			x	
20. Administrer les maintenances	A			x	
21. Suivre les contrats de maintenance	A			x	
22. Assister les utilisateurs	Ex				x

SG : secrétaire général
SDIO : Sous directeur informatique et organisation
CSSP : chef service systèmes et production
CSDSU : chef service développement et support utilisateurs

Nature des tâches :

A : administration (autorisation)
Ex : exécution
C : contrôle (supervision)
D : développement (conception)

CESAG - BIBLIOTHEQUE

Annexe 4 : Feuille de révélation des risques (FAR)

CNCAS	Feuille d'analyse des risques (FAR)	**ETUDE : Evaluation des risques liés au processus informatique de gestion du crédit**	
Période de base de l'étude : Octobre à Décembre 2011		**Réf : Annexe 04 FAR n°1**	**Folio : 1 / 1**

Risques identifiés :

R3 : choix d'un taux d'intérêt différent de celui du type de crédit

R2 : choix d'un crédit pour un client qui n'a pas le profil requis

Faits constatés :

- il existe des dossiers qui ont le même type de crédit mais les taux d'intérêt ne correspondent pas avec le taux pour ce type de crédit.
- le résultat des tests indique que pour certains crédits le profil du client ne correspond pas avec le type de crédit qui lui a été accordé (cf. rapports sur les réalisations du Contrôle Général).

Causes explicatives :

- le paramétrage des taux d'intérêt selon le type de crédit n'est pas effectif (R3).
- le paramétrage des lignes de crédit selon le profil du client n'est pas effectif (R2).

Conséquences réelles ou potentielles :

- des pertes financières ;
- la fraude ;
- l'anarchie ;
- des plaintes de la part du client ;
- des pertes d'image et de compétitivité.

Recommandations :	**Directions responsables :**
Prendre toutes les dispositions nécessaires pour rendre effectif : - le paramétrage des taux d'intérêt selon le type de crédit ; - le paramétrage des lignes de crédit selon le profil du client.	SDIO, DCR et DCG

Chef de mission :	**Auditeur :** Papa Makha BEYE	**Responsable du domaine audité**

CESAG BIBLIOTHEQUE

CNCAS	Feuille d'analyse des risques (FAR)	**ETUDE : Evaluation des risques liés au processus informatique de gestion du crédit**	
Période de base de l'étude : Octobre à Décembre 2011		**Réf : Annexe 04 FAR n°2**	**Folio : 1 / 1**

Risques identifiés :

Dépassement des habilitations par rapport au montant et à la durée des crédits (R12 et R13).

Faits constatés :

Le résultat des tests indique que certains délégataires dépassent leurs habilitations en termes de montant et de durée qui leur sont accordés (cf rapports sur les réalisations du Contrôle Général).

Causes explicatives :

négligence de la SDIO : oubli de remettre à niveau les habilitations après une autorisation de dépassement à un délégataire.

Conséquences réelles ou potentielles :

- des pertes de chiffre d'affaires prévisionnel ;
- l'anarchie.

Recommandations :	**Directions responsables :**
- Prendre toutes les dispositions nécessaires pour rendre effectif le paramétrage des taux d'intérêt selon le type de crédit ;	DG, DCR, SDIO
- S'il y a autorisation de dépassement pour un délégataire, faire de sorte qu'elle soit pour un nombre d'opérations précise.	SDIO

Chef de mission :	**Auditeur :** Papa Makha BEYE	**Responsable du domaine audité**

CESAG - BIBLIOTHEQUE

CNCAS	**Feuille d'analyse des risques (FAR)**	**ETUDE : Evaluation des risques liés au processus informatique de gestion du crédit**	
Période de base de l'étude : Octobre à Décembre 2011		**Réf : Annexe 04 FAR n°3**	**Folio : 1 / 1**

Risques identifiés :

R16 : Non saisie de la garantie (si nécessaire) avant la validation du crédit.

Faits constatés :

Il existe des crédits pour lesquels la prise de garantie n'est pas effective avant leur mise en place (cf rapport de novembre du Contrôle Général sur les réalisations).

Causes explicatives :

Le délégataire de pouvoir est libre de valider le crédit avant l'effectivité de la garantie.

Conséquences réelles ou potentielles :

- des pertes financières ;
- la fraude ;
- l'anarchie.

Recommandations :	**Directions responsables :**
Prendre toutes les dispositions nécessaires pour que la cellule juridique ait un droit de regard avant la validation des crédits pour attester de la prise de garantie effective.	DG, DCR, DOER, CAJRC, SDIO

Chef de mission :	**Auditeur :** Papa Makha BEYE	**Responsable du domaine audité**

CESAG - BIBLIOTHEQUE

CNCAS	Feuille d'analyse des risques (FAR)	**ETUDE : Evaluation des risques liés au processus informatique de gestion du crédit**	
Période de base de l'étude : Octobre à Décembre 2011		**Réf : Annexe 04 FAR n°4**	**Folio : 1 / 1**

Risques identifiés :

R7 : validation d'un crédit par un utilisateur non délégataire de pouvoir.

Faits constatés :

Il existe deux utilisateurs non délégataires qui valident des dossiers de crédit (cf rapports de novembre et décembre sur les réalisations).

Causes explicatives :

Oubli de changer le profil de l'utilisateur à la fin de l'intérim d'un délégataire.

Conséquences réelles ou potentielles :

- fraude ;
- anarchie.

Recommandations :	**Directions responsables :**
Prendre les dispositions nécessaires pour la mise à jour des profils utilisateur à la fin d'un intérim.	DCR, SDIO

Chef de mission :	**Auditeur :** Papa Makha BEYE	**Responsable du domaine audité**

CESAG - BIBLIOTHEQUE

CNCAS	**Feuille d'analyse des risques (FAR)**	**ETUDE : Evaluation des risques liés au processus informatique de gestion du crédit**	
Période de base de l'étude : Octobre à Décembre 2011		**Réf : Annexe 04 FAR n°5**	**Folio : 1 / 1**

Risques identifiés :

R4 : dépassement de la quotité cessible pour les salariés.

R6 : octroi de crédit pour un salarié d'une société non homologuée par un agent non habilité.

Faits constatés :

- existence de plusieurs mises en place de crédits dont le montant des échéances dépasse largement la quotité cessible du salarié ;
- existence de crédits pour des salariés de sociétés non homologuées mis en place par des agents non habilités pour ce type de crédit (cf. rapports du Contrôle général sur les réalisations de la période de l'étude).

Causes explicatives :

- le tableau d'amortissement du crédit n'est pas synchronisé avec la quotité cessible du salarié, le contrôle est manuel (R4) ;
- la liste des sociétés n'est pas implémentée dans le système d'information, c'est un contrôle manuel (R6).

Conséquences réelles ou potentielles :

- des plaintes du client pour le rallongement de la durée du crédit ou des litiges avec l'inspection du travail (R4) ;
- le rallongement du crédit, des défauts de paiement, des pertes de chiffre d'affaires prévisionnel (R6).

Recommandations :	**Directions responsables :**
- faire en sorte qu'il y ait une synchronisation entre le montant des échéances et la quotité cessible ; - implémenter dans le système la liste des sociétés homologuées par la banque.	SDIO

Chef de mission :	**Auditeur :** Papa Makha BEYE	**Responsable du domaine audité**

CESAG - BIBLIOTHEQUE

Annexe 5 : Tableau des forces et faiblesses de la fonction informatique

Activité/Tâche		Objectif	Risques	Pratiques d'Organisation Communément Admises (POCA) / Indicateurs	Constat	Observations
1	organisation générale de l'informatique	définir l'organisation et le fonctionnement de l'informatique	responsabilités mal définies	existence d'un organigramme à jour	non	il existe un organigramme mais il y a des postes vacants
			non atteinte des objectifs	rattachement hiérarchique à niveau lui permettant de mener à bien sa mission	non	l'informatique est une Sous Direction et ne participe pas au comité de direction ; le niveau le plus approprié est directement à la DG
			cumul de fonctions	séparation des fonctions	oui	Cette séparation pourrait être théorique car il y a des postes vacants
			exécution disparate des tâches	manuel des procédures	oui	manuel non exhaustif car ne traite pas des activités de développement
			non prise en compte de tous les besoins	priorisation des demandes	oui	
				effectif suffisant	non	
2	sécurité physique	protéger les locaux et matériels informatiques	accès non autorisé aux locaux	système de contrôle d'accès aux locaux et du matériel	oui	
			incident électrique	système de régulation de l'alimentation électrique	oui	
				système de secours de l'alimentation électriques des salles machines	oui	
			incendie	système de détection de fumée	oui	
				dispositif d'extincteur automatique	oui	

CESAG - BIBLIOTHEQUE

			dégâts des eaux	dispositif permettant de limiter les dégâts des eaux	non	
3	sécurité logique et administration système	protéger les données de l'entreprise, des applications et du système d'information	accès non autorisé aux données	logiciel de contrôle d'accès au système	oui	
			dépassement des habilitations	mise à jour des profils d'accès	oui	
			non existence de piste d'audit	traçabilité des données, des opérations et des connexions	oui	
			intrusion ou attaque logique	système de protection du réseau	oui	
			indisponibilité du système	redondance réelle serveurs	oui	
4	exploitation des applications et du système	s'assurer du bon déroulement de l'exploitation et des traitements	erreur d'exploitation et de paramétrage	instructions d'exploitation des applications comprenant un descriptif du flux des applications ; les procédures de paramétrages et les fichiers nécessaires	non	inexistence d'instructions écrites
			non exhaustivité des traitements	existence d'un état de contrôle des mouvements rejetés non encore corrigés	oui	
			non continuité de l'exploitation	existence d'un site de secours	non	en cours de mise en œuvre
			indisponibilité du système	redondance réelle serveurs	oui	
			destruction accidentelle des données	existence de méthodes permettant de reconstituer les fichiers à la suite d'erreurs mineures	oui	

CESAG - BIBLIOTHEQUE

5	Sauvegardes	assurer la continuité de l'exploitation	inexistence de sauvegardes	système de sauvegarde automatique	oui	sauvegarde en ligne
			indisponibilité des sauvegardes	stockage sur site		
				stockage hors site	non	site de secours en cours de mise en œuvre
6	développement d'application		non conformité avec les besoins exprimés	existence d'un cahier des charges	non	le manuel des procédures ne couvre pas le développement
				validation des tests avec les utilisateurs	non	
7	Maintenance		manque de prestataires	existence d'un contrat de maintenance préventive et curative	oui	
			vétusté du matériel	existence d'un plan de renouvellement des équipements	oui	selon l'amortissement des équipements
			modification non autorisée	existence de procédures écrites de révision appliquées systématiquement avant toute maintenance d'une application	oui	

Source : Adaptée de RENARD (2010 : 239)

CESAG - BIBLIOTHEQUE

Annexe 6 : Tableau d'évaluation de la conception et de l'efficacité des contrôles

Risques opérationnels	Activités et contrôles limitant le risque	test pour éléments probants sur le succès des mesures	Résultat du test	Evaluation du contrôle
R1. existence de doublon de dossier	attribution automatique des numéros de dossier	vérifier la séquence des numéros de dossier sur l'échantillon	Il n'existe pas de doublons dans l'échantillon ; la continuité de la séquence numérique est permanente.	Très élevé
R2. choix d'un crédit pour un client qui n'a pas le profil requis	les lignes de crédit sont paramétrées selon le type de client	comparer le profil client avec le type de crédit mis en place de l'échantillon	Le résultat des tests indique que 71% des profils client de l'échantillon ne sont pas éligible au type de crédit accordé. Le contrôle présente des faiblesses d'application	Insuffisant
R3. choix d'un taux d'intérêt différent de celui du type de crédit	le taux est paramétré dans le système selon le type de crédit choisi	comparer les taux d'intérêt de la banque par type de crédit avec ceux de l'échantillon de crédits accordés	53% de l'échantillon ont le même type de crédit mais les taux d'intérêt ne correspondent pas avec le taux pour ce type de crédit : faiblesse d'application	Moyen
R4. dépassement de la quotité cessible pour les salariés	l'utilisateur édite le tableau d'amortissement et fait le rapprochement entre échéances et quotité cessible	rapprochement entre échéances et quotité sur l'échantillon de crédits aux salariés	le montant des échéances dépasse largement la quotité cessible du salarié pour 77% des cas. Le contrôle est insuffisant.	Insuffisant

CESAG - BIBLIOTHEQUE

R5.	dépassement du taux d'endettement pour les entreprises	contrôles utilisateur : analyse financière	vérifier si le aux d'endettement n'est pas dépassé	Nous n'avons pas pu disposer des dossiers d'entreprises pour vérifier leurs informations financières	Moyen
R6.	MEP de crédit pour un salarié d'une société non homologuée par un agent non habilité	contrôle utilisateur : vérifier la société du salarié sur la liste des sociétés homologuées	rapprochement, pour les crédits destinés aux salariés, le nom de la société du client avec la liste des sociétés homologuées	Les tests révèlent 63% de non conformité.	Insuffisant
R7.	validation d'un crédit par un utilisateur non délégataire	profil et habilitations des utilisateurs	comparer les noms des délégataires avec ceux d'un échantillon des réalisations	78% des crédits de l'échantillon sont validés par des délégataires	Elevé
R8.	octroi d'un crédit salarié avant la domiciliation du salaire	en plus du certificat de domiciliation, l'utilisateur doit vérifier le virement du salaire dans le compte du client	prendre un échantillon de crédits aux salariés, vérifier si le salaire est domicilié avant l'octroi du crédit	21% des dossiers sont des crédits mis en place avant la domiciliation du salaire	Elevé
R9.	altération du taux d'intérêt choisi pour valider le dossier	le champ du taux est grisé	test de permanence sur un échantillon et essai de la modification du taux avec quelques profils utilisateur	Lors de l'observation pratique de la mise en place d'un crédit on a constaté que le champ du taux d'intérêt était modifiable.	Elevé

CESAG BIBLIOTHEQUE

R10.	altération du montant autorisé	Séparation des fonctions entre l'agent instructeur et le décisionnaire : le dernier nommé saisit directement la décision de banque dans le système et mentionne le montant autorisé sur la fiche synoptique du dossier qui est transmis à l'agent instructeur	demander les fiches synoptiques de mises en places, sonder et vérifier la conformité des montants autorisés et ceux mis en place.	Les tests relèvent une conformité entre montants autorisés et ceux mis en place à 78%	Elevé
R11.	altération de la durée de crédit autorisée	Séparation des fonctions entre l'agent instructeur et le décisionnaire : le dernier nommé saisit directement la décision de banque dans le système et mentionne la durée autorisée sur la fiche synoptique du dossier qui est transmis à l'agent instructeur	demander les fiches synoptiques de mises en places, sonder et vérifier la conformité des durées autorisées et celles mises en place.	Les tests relèvent une conformité entre durées autorisées et celles mises en place 74%	Elevé
R12.	dépassement des habilitations par rapport au montant	profil et habilitations des utilisateurs	choisir quelques mises en place par des délégataires et comparer les montants accordés à ceux des pouvoirs qui leur sont délégués (cf. note de service délégation de pouvoirs)	43% crédits sont accordés par des délégataires dont le montant dépasse leurs habilitations.	Moyen

CESAG - BIBLIOTHEQUE

R13. dépassement des habilitations par rapport à la durée	Idem	choisir quelques mises en place par des délégataires et comparer la durée des crédits avec celle des pouvoirs qui leur sont délégués (cf. note de service délégation de pouvoirs)	Il existe plusieurs crédits accordés par des délégataires dont la durée dépasse leurs habilitations pour 59%.	Moyen
R14. validation d'un dossier rejeté	En cas de rejet, le décisionnaire le saisit dans le système et l'inscrit dans le dossier puis le transmet à l'agent instructeur	sélectionner quelques dossiers de rejet et vérifier est ce qu'ils ont été mis en place ou non	Les tests ne révèlent pas de MEP de dossiers défavorables dans notre échantillon.	Très Elevé
R15. octroi de crédit à un client qui dépasse la limite d'âge par un agent non habilité (pour les retraités)	Contrôle utilisateur (manuel) : l'utilisateur vérifie l'âge du client de profil « retraité » à l'aide de sa CNI	vérifier l'âge de quelques bénéficiaires de profil « retraité » pour le comparer avec l'âge limite fixé par la banque. Vérifier aussi le décisionnaire.	43% des crédits sont mis en place par des agents non habilités pour retraités dépassant l'âge limite.	Moyen
R16. non saisie de la garantie (si nécessaire) avant validation	L'instructeur du dossier saisit la garantie et le délégataire vérifie la conformité avant de valider le crédit dans le système	sélectionner quelques dossiers et envoyer les références à la Cellule juridique qui doit préciser si oui ou non les garanties requises ont précédé la mise en place du crédit.	Il existe des crédits pour lesquels la prise de garantie n'est pas effective avant leur mise en place pour 41% de l'échantillon	Moyen

Source : Nous mêmes

CESAG BIBLIOTHEQUE

BIBLIOGRAPHIE

CESAG - BIBLIOTHEQUE

BIBLIOGRAPHIE

A. Ouvrages

1. ANGOT Huges, FISCHER Christian & THEUNISSEN Baudouin (2004), *Audit comptable audit informatique*, Editeur De Boeck-wesmael, Bruxelles, 299 pages.
2. AUBERT Benoit A. & BERNARD Jean-Grégoire (2004), *Mesure intégrée du risque dans les organisations*, Ed les presses de l'université de Montréal, Montréal, 523 pages.
3. BARTHELEMY Bernard & COURRÈGES Philippe (2004), *Gestion des risques : méthodes d'optimisation globale 2e éd*, Editions d'Organisation, Paris, 471 pages.
4. BLANCHIN & al (2009), *Maturité des outils de gouvernance IT*, Université de Lyon 1, Lyon, 62 pages.
5. CARPENTIER Jean-François (2009), *La sécurité informatique dans la petite entreprise : Etat de l'art et bonnes pratiques*, Editions ENI, Nantes, 276 pages.
6. CNCC (2003), *Prise en compte de l'environnement informatique et incidence sur la démarche d'audit*, CNCC Edition, Paris, 260 pages.
7. COOPERS & LYBRAND (2002), *La nouvelle pratique du CI*, Les éditions d'organisation, Paris, 384 pages.
8. DERRIEN Yann(1992), *Les techniques de l'audit informatique*, Dunod, Paris, 240 pages.
9. DESMOULINS Nicolas (2009), *Maîtriser le levier informatique: Accroître la valeur ajoutée des systèmes d'information*, Pearson Education France, Paris, 259 pages
10. DESROCHES Alain, LEROY Alain & VALLÉE Frédérique (2003), *La gestion des risques : principes et pratiques*, Lavoisier, Paris, 286 pages.
11. GARSOUX Monique (Mars 2005), COBIT, une expérience pratique, *Revue de l'AFAI n°78* : 4 – 8, Paris.
12. GUILLON Bernard (2007), *Risque, formalisations et applications pour les organisations*, Editions l'Harmattan, Paris, 316 pages.
13. HENRY Alain & MONKAM-DAVERAT Ignace (2001), *Rédiger les procédures de l'entreprise : Guide pratique*, 3ème édition, Edition d'Organisation, Paris, 184 pages.
14. IFACI (1993), *Audit et contrôle des systèmes d'information : module 5, Audit des systèmes applicatifs*, Editeur IFACI, Paris, 136 pages.
15. KHADIR Sofiane-Maxime (2004), Sécurité des Systèmes d'Information : du Principe d'Exclusion à la Gestion d'Identité, *Revue de l'AFAI n°* 75 : 12-14, Paris.
16. LY Henri (2005), *L'audit technique informatique*, Lavoisier, Paris, 230 pages.
17. MADERS Henri-Pierre & MASSELIN Jean Luc (2006), *Contrôle interne des risques*,

CESAG - BIBLIOTHEQUE

2ème Edition, Editions d'Organisation, Paris, 261 pages.

18. MENTHONNEX Jean (1995), *Sécurité et qualité informatiques : nouvelles orientations*, Presses polytechniques et universitaires romandes, Lausanne (Suisse), 422 pages.
19. MOREAU Franck (2002), *Comprendre et gérer les risques*, Editions d'Organisation, Paris, 222 pages.
20. OBERT Robert (2004), *Audit et Commissariats aux comptes aspects internationaux*, 4ème édition, Edition DUNOD, Paris, 495pages.
21. RENARD Jacques (2010), *Théorie et pratique de l'audit interne*, Eyrolles Editions d'organisation, 7ème édition, Paris, 472 pages.
22. ROUFF Jean Loup (2001), Des concepts et des mots, *Revue Audit* n°153 : 12-27, Paris.
23. SCHICK Pierre, VERA Jacques, BOURROUILH-PAREGE Olivier (2010), *Audit interne et référentiels de risques*, Edition DUNOD, Paris, 339 pages.
24. THORIN Marc (2000), *L'audit informatique*, Éditeur Hermès Science Publications, Paris, 184 pages.
25. THUILLIER Pierre (1981), *Darwin and Co*, Éditions Complexes, Bruxelles, 210 pages.

B. Sources internet

26. AFAI (2007), *Prise en compte des risques informatiques dans la démarche de Risk management*, http://www.afai.fr/public/doc/365.pdf
27. AFAI (2008), *Contrôle interne et système d'information*, 2e édition, http://www.afai.fr/public/doc/4.pdf
28. AFAI (2008), *Guide d'audit des applications informatiques*, http://www.b3b.ch/wp-content/uploads/guide_audit_applications.pdf
29. AFAI (2010), *Cartographie des risques informatiques : exemples, méthodes et outils*, http://www.afai.fr/public/doc/545.pdf
30. AFAI (2011), *Gestion des ISSI*, http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-2011-Gestion-des-Incidents.pdf
31. BALLOY Didier (2002), *Le risque informatique, comment y remédier*, http://www.dballoy.unblog.fr/files/2008/05/cnamprobatoire1.pdf
32. BLAIN Fleur-Anne (2006), *Présentation générale des ERP et leur architecture modulaire*, ftp://ftp-developpez.com/fablain/pdf/presenterp.pdf
33. CGL (2005), *Grille de cotation des risques*, http://www.cgl-consulting.com/eva/grille-de-cotation-des-risques.pdf

CESAG - BIBLIOTHEQUE

34. CLUSIF (2006), *Méthode MARION*, http://i-a.ch/docs/CLUSIF_Marion.pdf, publié le 12 septembre 2006 ;
35. CLUSIF (2007), Guide de l'analyse des risques MEHARI, http://www.clusif.fr/fr/production/ouvrages/pdf/MEHARI-2007-Anarisk.pdf
36. CLUSIF (2010), Présentation générale MEHARI 2010, http-//www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Introduction.pdf
37. CLUSIF (2011), *Guide de la démarche d'analyse et de traitement des risques, version 2*, http-//www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Guide-demarche.pdf
38. Cour des comptes du Canton de Vaud (2009), *manuel de vérification de l'évaluation de la gestion des risques*, http://www.vd.ch/fileadmin/user_upload/organisation/dfin/sg-dfin/fichiers_pdf/Methodologie_-_Risques.pdf
39. CRAMRA (2004), *Evaluation des risques professionnels dans les BTP*, http://www.carsat-ra.fr/entreprise/risquesprof/pdf/sp1122.pdf
40. DELTAINFORMATIQUE (2005), *Ensemble des services*, http://www.delta-informatique.com/solution_overview_fr.htm, mis en ligne le 28/07/2005
41. DETAINFORMATIQUE (2005), Couverture fonctionnelle, http://www.delta-informatique.com/solution_functional_cov_fr.htm, mis en ligne le 28/07/2005
42. DELTAINFORMATIQUE (2009), http://images.ihb.de/p-510000-504133-D1/D1.pdf
43. FERMA (2003), *Cadre de référence de la gestion des risques*, http://www.theirm.org/publications/documents/French_Risk_Management_Standard_021203.pdf
44. GENEVA (2011), *Audit de la partie informatique du système de contrôle interne*, http://www.aud-it.ch/controle%20interne.html, visité le 25 Mai 2011
45. GUIDEINFORMATIQUE (2012), *Risques informatiques*, http://www.guideinformatique.com/definition-1220.htm
46. IIA (2005), *GTAG 1 : le contrôle des systèmes d'information*, https://na.theiia.org/standards-guidance/Member%20Documents/GTAG_1_FR_Final__1-30-09_.pdf
47. IIA (2009), *GTAG 8 : Audit des contrôles applicatifs*, https://na.theiia.org/standards-guidance/Member%20Documents/GTAG_8_FR_Final__Jan-22-2009_.pdf
48. IFAC (2007), *Guide ISA*
49. KPMG (2004), *Contrôle interne*, http://ddata.over-blog.com/xxxyyy/0/32/13/25/teil-6-cg-franz.pdf

CESAG-BIBLIOTHEQUE

50. Le comité de Bâle sur le contrôle bancaire (1998), *Cadre d'évaluation des systèmes de contrôle interne,* http://www.bis.org/publ/bcbs33_fr.pdf
51. PR4M4 (2010), *Techniques d'évaluation des risques norme ISO 31010,* http://www.pr4gm4.com/PR4GM4_31010_v03.pdf
52. PROTIVITI (2011), *Baromètre du Risk Management 2011*, http://www.protiviti.fr/fr-FR/Insights/Documents/Barometre-2011-site.pdf

CESAG - BIBLIOTHEQUE