CESAG Centre Africain d'études Supérieures en Gestion

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

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

Promotion 21 (2009-2010)

Mémoire de fin d'étude

THEME

Audit de l'assistance informatique : Cas de la Cellule d'Appui à l'Informatisation des Services Financiers et Fiscaux (CAISFF) du Mali

Présenté par :
Bourlaye KEITA

Dirigé par :
M. Alain SAWADOGO
Professeur associé CESAG

2010

DEDICACES

Je dédie ce mémoire à :

- ma très chère mère Dianténin CAMARA ;
- ma chère épouse Maïmouna SIDIBE ;
- à tous mes enfants et particulièrement les plus jeunes dont Rahmatou Bourlaye KEITA qui a la plus souffert de mon absence tout le temps qu'a duré cette formation.

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 :

- à son excellence Monsieur le Ministre de l'Economie et des Finances du Mali Sanoussi TOURE dont l'accord a suffi pour m'ouvrir les portes du financement de ladite formation ;
- au Secrétaire Général du Ministère de l'Economie et des Finances du Mali Mme SANGARE Niamoto BA ;
- au Directeur National du Contrôle Financier Alhassane Ag Hamed Moussa;
- au Directeur National Adjoint du Contrôle Financier N'Golo TRAORE.

Je remercie particulièrement le Coordonnateur de la CAISFF Mohamed Chérif KEITA et ses plus proches collaborateurs pour les documents qu'ils m'ont fournis, nécessaires à la rédaction du présent rapport. Ce travail est l'accomplissement d'une partie de mon rêve le plus lointain.

Au personnel de la DAF, de la DNCF, de la PGT, de la DGI, de la DGD, et de la DGB, et au personnel de leurs Cellules Informatiques, je les adresse tous mes remerciements 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 montré pour répondre à toutes mes attentes.

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 Comptabilité, Banque et Finance (ISCBF) qui m'a été d'un soutien considérable dans la réalisation du présent rapport de fin de cycle.

LISTE DES TABLEAUX ET FIGURES

LISTE DES SIGLES ET ABREVIATIONS

Sigles ou Abréviations	Dénomination du sigle ou de l'abréviation
AFAI	Association Française de l'Audit Informatique
ACCT	Agence Comptable Centrale du Trésor
AGETIC	Agence d'Exécution des Techniques de l'Information et de la Communication
AT	Admission Temporaire
BCS	Bureau Central de la Solde
BDM	Banque de Développement du Mali
BIVAC	Bureau Veritas (BIVAC Mali)
BVG	Bureau du Vérificateur Général
CAISFF	Cellule d'Appui à l'Informatisation des Services Financiers et Fiscaux
CAO	Conception Assistée par Ordinateur
CESAG	Centre Africain d'Etudes Supérieures en Gestion
CERTS	Computers Emergency and Response Team
CFAO	Conception et Fabrication Assistée par Ordinateur
CIT	Cellule Informatique du Trésor
CIS	Cellule de l'Informatique et de la Statistique
CLUSIF	Club de la Sécurité des Systèmes d'Information Français
COCO	Criteria On Control Committee
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CTI	Comité Technique Informatique
DBA	Database Administrator (Administrateur de Bases de Données)
DESS	Diplôme d'Etudes Supérieures Spécialisées
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DFM	Direction des Finances et du Matériel
DGB	Direction Générale du Budget
DGD	Direction Générale des Douanes
DGI	Direction Générale des Impôts
DGMP	Direction Générale des Marchés Publics
DME	Division des Moyennes Entreprises
DNCC	Direction Nationale du Commerce et de la Concurrence
DNCF	Direction Nationale du Contrôle Financier

DRH	Direction des Ressources Humaines
DRT	Direction Régionale des Transports
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
FO	Fibre Optique
FE	Fréquence de l'Evénement
GLPI	Gestion Libre du Parc Informatique
ICRISAT	International Crops Research Institute for the Semi-Arid Tropics
IFAC	International Federation of Accountants
ISA	International Standards of Auditing
IT	Immatriculation Temporaire
LAN	Local Area Network
MARION	Méthode d'Analyse des Risques Informatiques Optimisée par Niveau
MEHARI	Méthode Harmonisée d'Analyse de Risques
MEF	Ministère de l'Economie et des Finances
NIF	Numéro d'Identification Fiscale
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OSI	Open Systems Interconnection
PDI	Programme de Développement Informatique
PGT	Paierie Générale du Trésor
PME	Perte Moyenne par Evénement
POCA	Pratiques d'Organisations Communément Admises
PRED	Programme de Reforme Economique pour le Développement
PTF	Partenaires Techniques et Financiers
Q	Question
RGD	Recette Générale du District (de Bamako)
RSI	Directeur ou responsable informatique
RSSI	Responsable de la sécurité des systèmes d'information
SAF	Service Administratif et Financier
SATOM	Société Africaine des Travaux d'Outre-Mer
SDI	Schéma Directeur Informatique
SEI	Software Engineering Institute
SGBD	Systèmes de Gestion de Bases de Données
SIGTAS	Système d'Information de Gestion des Taxes et Assimilées

SQL	Structured Query Language
TAAO	Techniques d'Audit Assistées par Ordinateur
TIC	Techniques de l'Information et de la Communication
TRIE	Transport Routier Inter-Etat
UATT	Union Africaine de Transport et de Transit
V	Validation
VLAN	Virtual Local Area Network

TABLE DES MATIERES

INTRODUCTION GENERALE

Les directions des organisations prospères qui comprennent que l'informatique doit être gérée comme une entreprise (selon les principes de bonne gouvernance), agissent pour:

- aligner la stratégie informatique avec la stratégie de l'entreprise ;
- mesurer la performance de l'informatique ;
- démontrer la valeur des investissements technologiques ;
- identifier les coûts des projets et des services informatiques ;
- gérer les ressources humaines et financières ;
- maîtriser les risques opérationnels ;
- améliorer les capacités informatiques à budget constant.

Un système informatique est un ensemble organisé de ressources (matériel, logiciel, personnel, données, procédures...) permettant d'acquérir, de stocker, de communiquer des informations sous forme de données, textes, images, sons... dans des organisations.

Pour avoir une bonne maîtrise des risques dans le domaine de l'assistance informatique, cela requiert une bonne gouvernance informatique. Ce qui repose d'abord sur la maîtrise des projets et des opportunités d'investissement afin d'allouer efficacement les ressources humaines ou financières. Cela revient aussi à gérer les risques et les délais de production, à avoir une vision globale du portefeuille informatique.

La gestion des risques est le processus par lequel ceux-ci sont évalués en utilisant une approche systématique qui identifie et organise par priorité les risques, et qui ensuite met en place les stratégies pour les atténuer. Cette approche comprend à la fois la prévention des problèmes potentiels et la détection au plus tôt des problèmes actuels. C'est un processus itératif qui demande la participation du personnel à tous les niveaux de l'organisation.

C'est dans cet ordre d'idée que les responsables du Ministère de l'Economie et des Finances de la République du Mali créèrent en juillet 1994 la Cellule d'Appui à l'Informatisation des Services Financiers et Fiscaux (CAISFF). A cette époque leurs soucis avaient pour noms : la prévention des risques, la qualité de l'information comptable et financière, leur délai de production, l'optimisation des ressources (financières et humaines) et de la sauvegarde du patrimoine de l'Etat.

Antérieurement à la création de la CAISFF en juillet 1994, les différents services du Ministère de l'Economie et des Finances évoluaient en vase clos sur le plan informatique. De ce fait, chaque service dans le rôle qui est le leur de production, de diffusion ou de reporting de l'information comptable, financière ou statistique rencontrait des difficultés. Ces difficultés devenaient de plus en plus récurrentes l'évolution de la technologie imposant davantage l'informatique comme outil de travail indispensable. Ainsi, ces problèmes bien que propres à chaque service, de même nature ou différents, convergeaient vers le Cabinet du Ministre de l'Economie et des Finances. Une harmonisation de la politique d'informatisation au niveau du Département de l'Economie et des Finances était donc nécessaire. Cette harmonisation s'imposait de plus en plus aux dits services car ils devraient échanger des données. Et comme si rien n'était fait pour faciliter les choses, cet échange de données était difficile car lesdits services n'utilisaient pas les mêmes applications informatiques. Alors fallait- t-il passer par de longues procédures de conversion de données ? Ceci était possible si la ressource humaine qualifiée existait pour le faire. De là est née l'idée de créer une structure qui sera chargée d'orienter, de planifier et d'harmoniser la politique d'informatisation au niveau du Ministère de l'Economie et des Finances. Cette coordination est fortement corrélée à la gestion des risques qu'ils soient stratégiques ou opérationnels.

Dans le cadre de l'assistance informatique, la Cellule d'Appui à l'Informatisation des Services Financiers et Fiscaux (CAISFF) préconise des solutions pour améliorer la qualité de service apportée par les outils informatiques et assure aux utilisateurs :

- la pérennité et la cohérence des solutions proposées ;
- une indépendance vis-à-vis des fournisseurs, constructeurs et/ou éditeurs du marché ;
- une intégration simple, efficace et au meilleur coût à l'existant ;
- des investissements justifiés par un retour sur investissement quantifiable et rapide.

Il s'agit de savoir comment auditer une assistance informatique par l'approche par les risques.

En l'absence d'un audit de l'assistance informatique les conséquences sont les suivantes :

- temps de réponse assez long pour l'intervention d'une assistance informatique ;
- dysfonctionnement des systèmes informatiques sans possibilités d'un retour à une situation normale ;

- possibilités d'usurpation d'identité ;
- absence d'une bonne gouvernance informatique ;
- retard dans le traitement des opérations ;
- dysfonctionnement du réseau informatique ;
- dysfonctionnement des applications informatiques ;
- non mise à niveau de la connaissance des utilisateurs ;
- mécontentements des utilisateurs ;
- non fiabilité de l'information comptable, financière et statistique ;
- retard dans la prise de décisions stratégiques sur la base desdites informations comptables, financières et statistiques.

Malgré l'existence de la CAISFF depuis seize (16) ans, toutes les directions du MEF ne disposent toujours pas d'applications informatiques couvrant tous leurs besoins.

L'ACCT dont la PGT est un pan, présente toujours son TOFE sous Excel. La DNCF quant à elle, dispose d'un TOFE automatisé (produit à partir d'une application). Mais quand il s'agit de produire d'autres situations comme l'appui budgétaire, communication et énergie, elle concoctera des chiffres sous Excel.

La DGD continue à présenter ses chiffres du suivi des recettes douanières sous Excel.

La DGI, même si elle se targue de l'amélioration des recettes fiscales, continue à présenter les situations de suivi de ces recettes sous Excel.

La DGB continue de travailler dans son PRED (Programme de Reforme Economique pour le Développement) dont la première version date du début des années quatre vingt.

Alors que toutes ces directions bénéficient de l'assistance de la CAISFF. Dans ce contexte, est-il possible de disposer d'informations comptables et financières fiables ? Qu'en est-t-il des situations statistiques ?

Ces informations qu'elles soient comptables, financières, économiques ou statistiques doivent servir à la prise de décisions importantes. Et nul n'ignore l'intérêt que les partenaires au développement de nos Etats, au premier rang desquels le FMI et la BM, accordent beaucoup d'importance à leur fiabilité.

Devant l'impossibilité d'automatiser ces informations à travers des applications informatiques, que vaut vraiment l'assistance de la CAISFF ?

L'objectif général de l'étude est de recueillir les besoins des utilisateurs et informaticiens des directions du MEF assistées, de les mettre à la disposition de l'équipe dirigeante de la CAISFF pour qu'elle l'incorpore dans sa stratégie (façon de faire). Elle s'appuiera ainsi sur les processus identifiés comme ses faiblesses pour mener à bien son assistance informatique tout en veillant sur ceux reconnus comme forces pour maîtriser les risques s'y rapportant. Il sera proposé une cartographie des risques informatiques dont la CAISFF s'inspirera pour maîtriser les risques opérationnels. Des recommandations seront formulées desquelles découlera un plan d'action si le nombre de pages qui nous est impartie le permet.

L'objectif spécifique est de faire profiter le MEF en premier lieu de notre formation dont il en est le bailleur.

Compte tenu de l'intérêt des partenaires au développement pour des informations comptables, financières et statistiques fiables et de la situation des directions du MEF décrite plus haut, la question que l'on est en droit de se poser est : quel est l'apport de la CAISFF dans l'amélioration des services informatiques au sein du MEF ?

A cela on pourrait ajouter de questions spécifiques comme : l'organisation informatique du MEF est-elle pertinente ?

L'assistance menée par la CAISFF se fait-elle dans les règles de l'art ? (politiques de sécurité physique et logique, conduite des projets, analyse et conception, réalisation, intégration, déploiement, formation des utilisateurs, perfectionnement des informaticiens, etc.).

La CAISFF a-t-elle réellement comblé les attentes des services financiers et fiscaux qui ont suscité sa création ?

Bien que nos consultations aient porté sur l'audit de l'assistance informatique , il ne sera pas tenu en compte au cours de ce travail de l'assistance ou maintenance matérielle assurée par les acteurs externes aux services financiers et fiscaux. Nous tiendrons compte de toute assistance dont on peut contrôler les risques et performances.

Ce thème intéresse deux (2) usagers :

· **La CAISFF :**

cette étude permettra à la CAISFF de disposer d'informations en provenance des directions du MEF sur sa mission. Ce qui lui permettra de mener à bien sa mission d'assistance informatique. Elle connaîtra ses points forts et ses points faibles en matière d'assistance informatique. De ce fait elle fera des efforts au niveau des processus de celle-ci identifiés comme ses points faibles tout en ne négligeant pas ceux considérés comme points forts.

· **NOUS - MEMES :**

cette étude nous permettra de mettre en pratique nos acquis théoriques, de maîtriser la démarche d'élaboration d'une cartographie des risques pour le processus de l'assistance informatique. Elle nous réjouira également d'avoir conduit un tel projet dans une grande structure au Mali qu'est le MEF à travers la CAISFF.

Ce travail s'articulera autour de trois parties essentielles :

1. L'introduction générale : elle mettra en relief la problématique de l'assistance informatique.

2. La première partie : la revue de littérature dans laquelle, nous présenterons les processus de l'assistance informatique et ses différents acteurs, le contrôle interne de l'assistance informatique. Nous identifierons les risques informatiques et leurs conditions de maîtrise, la méthodologie de l'étude, les outils et techniques de collecte et d'analyse de données.

3. La deuxième partie : réservée au cadre pratique, nous présenterons les services financiers et fiscaux. Nous dégagerons les points forts et points faibles de la CAISFF par direction assistée après les constats et les tests, ferons des recommandations et proposerons une cartographie des risques informatiques.

La conclusion générale mettra fin à toutes ces parties.

PARTIE I – CADRE THEORIQUE

INTRODUCTION

La dépendance des organisations de façon générale et des entreprises de façon particulière envers leurs systèmes informatiques a augmenté face à l'évolution des technologies d'information et de communication qui a affecté leurs systèmes comptables et de contrôle interne. En effet, la dématérialisation des documents tend à devenir totale (zéro papier), augmente la vulnérabilité du système d'information et engendre pour l'entreprise de nouveaux risques qu'elle est appelée à maîtriser. Malheureusement cette dématérialisation des documents a encore du temps devant elle dans l'administration publique malienne. Ainsi l'entreprise ou l'organisation devra t-elle disposer d'une structure d'assistance informatique pour réduire les temps d'attente en cas de dysfonctionnement des applications, des logiciels, du matériel, du réseau informatique.

Selon l'ISA (International Standards of Auditing) 401 de l'IFAC (International Federation of Accountants), un environnement informatique existe lorsqu'un ordinateur, quels que soient son type et ses capacités, est utilisé pour le traitement d'informations financières d'importance significative pour l'audit, que cet ordinateur soit exploité par l'entité ou par un tiers. Dans ce contexte, les professionnels comptables dont essentiellement les auditeurs ne peuvent pas ignorer ce concept de technologies d'information et de communication pour la planification de leurs travaux.

Il implique, de la part de l'auditeur, un minimum de connaissance en matière d'informatique sans pour autant devenir un expert en ce domaine ; ce qui justifie la possibilité de recours à des experts en systèmes d'information. Par ailleurs, l'approche d'audit adoptée par les auditeurs doit prendre en compte ce nouveau contexte et les nouveaux risques qui peuvent prendre naissance. Cette mise à niveau de l'approche d'audit est une préoccupation majeure des organismes professionnels dans le monde et des cabinets internationaux. C'est cette particularité qui nous emmène à cette étude sur l'audit de l'assistance informatique.

La mission d'audit informatique couvre parfois l'ensemble du système d'information notamment pour la mise en place d'un contrat d'infogérance, d'un contrat d'assistance ou d'un contrat de maintenance informatique, mais le plus souvent, elle est ciblée sur un point précis. L'audit d'un environnement informatique peut concerner l'évaluation des risques informatiques de la sécurité physique, de la sécurité logique, de la gestion des changements, du plan de secours, etc.

CHAPITRE I - PRESENTATION DU PROCESSUS DE L'ASSISTANCE INFORMATIQUE

1ntroduction

L'informatisation en gestion apparaît comme une action qui consiste pour une organisation (Entreprise) à automatiser un ensemble d'opérations et des tâches de gestion dont le but est d'obtenir des gains d'efficacité voire de productivité.

Il existe deux types de systèmes d'informations sous forme de parties informelles et de parties formelles. Ces dernières sont visibles à travers les documents qu'elles produisent en application de règles et des procédures explicites reliées aux rôles, fonctions et tâches déjà prescrits par l'organisation et elles sont peu dépendantes des individus.

Le second système (système informel) est également vital pour l'entreprise ou l'organisation, laisse peut de traces visibles et s'appuie sur des règles floues, imprécises et de référentiels implicites. Il est très dépendant des individus et de l'état des relations qu'ils entretiennent.

Si la mise en œuvre de l'informatique dans une gestion soulève des difficultés, c'est qu'elle repose sur l'extension de la partie formelle du système d'information (S.I). Cette extension suppose une réflexion sur l'organisation et, en particulier une clarification et un partage des informations et règles de fonctionnement.

Informatiser c'est donc aussi conduire à une action de changement. C'est pour soutenir les utilisateurs dans le cadre de ce changement que l'assistance informatique trouve sa raison d'être.

1.1 Définition de l'assistance informatique

L'assistance désigne un appui extérieur destiné à lever un ou des obstacle(s). Cet appui peut être fourni par une structure ou une personne. Cet appui peut concerner plusieurs aspects de l'informatique à travers les domaines d'intervention ci-après :

- l'environnement PC et les périphériques associés ;
- les outils bureautiques inscrits au catalogue de l'entreprise ou de l'organisation;
- les produits d'intérêt général (messagerie, intranet, postes mobiles…) ;
- certaines applications déployées dans le réseau.

En France, l'article 4.1.16 de la circulaire ANSP/DGEFP/DGAS n° 1-2007 du 15/05/2007, stipule : « S'agissant d'une activité d'assistance aux personnes, l'offre de service comprend obligatoirement l'initiation ou la formation au fonctionnement du matériel informatique et aux logiciels non professionnels en vue de permettre leur utilisation courante, ainsi que, tout ou partie des prestations suivantes :

- livraison au domicile de matériels informatiques ;
- installation et mise en service au domicile de matériels et logiciels informatiques ;
- maintenance logicielle au domicile de matériels informatiques ;
- sont exclus le dépannage ou l'assistance informatique effectuée à distance (Internet, téléphone...), la réparation, la vente de matériels et de logiciels. Si un prestataire souhaite exercer l'une de ces activités, il ne peut le faire qu'au titre d'un organisme doté d'une personnalité juridique distincte de celui qui est agréé ;
- le matériel informatique se définit comme le micro-ordinateur personnel ainsi que les accessoires et périphériques faisant partie de son environnement immédiat. Sont donc exclus de ce périmètre, les matériels audio, photo et vidéo numériques. Ainsi, à titre d'illustration, une initiation pourra-t-elle concerner l'importation dans le micro-ordinateur ? Le traitement de données en provenance d'un appareil photo numérique ? Mais cette initiation ne pourra jamais concerner l'initiation au maniement de l'appareil photo numérique lui-même » (Mulot Déclic, 2010 : 1).

Un aspect non moins important est l'assistance matérielle à travers les contrats de maintenance que l'organisation ou l'entreprise peut établir avec le fournisseur pour bénéficier de ce service.

La mise en place d'un contrat de maintenance informatique permet de garantir le fonctionnement, la gestion, l'évolution et le suivi du système d'information des entreprises. Elle leur permet de bénéficier des services d'un prestataire disponible et expérimenté pour résoudre leurs problèmes quotidiens.

« Les services proposés peuvent être plus ou moins évolués selon les contraintes, taille et objectifs de l'entreprise. Ils peuvent aller d'une assistance ponctuelle ou régulière jusqu'à l'utilisation d'un directeur ou responsable informatique (RSI) en temps partagé. Ces services

peuvent concerner une solution d'infogérance informatique complète du système d'information et du parc informatique, et peut comprendre :

- la maintenance préventive (vérification du fonctionnement, mise à niveau du système et anticipation des problèmes éventuels) ;
- la supervision du système (analyse de la santé du système, gestion de la sécurité et des alertes, surveillance et suivi des ressources …) ;
- des prestations d'exploitation (création de compte ou de boites aux lettres, gestion des sauvegardes, ..) ;
- l'assistance aux utilisateurs (support et résolution des problèmes courants) ;
- la maintenance curative (correction des dysfonctionnements, dépannage, …) ;
- la gestion du parc informatique, des garanties matériels et licences logiciels ;
- la veille technologique afin d'envisager les futures évolutions et d'être au fait des meilleurs produits et services adaptés à l'entreprise » (easeo, 2008 – 2010 : 1).

I.2 Objectifs de l'assistance informatique

Dans une organisation ou une entreprise, se munir d'une structure d'assistance informatique a pour objectifs essentiels :

- sécuriser les actifs informationnels de l'entreprise ou de l'organisation;
- harmoniser et homogénéiser le parc informatique au niveau du fonctionnement ;
- améliorer le service rendu par les informaticiens ou les fournisseurs de services informatiques ;
- réduire les coûts liés à l'acquisition des actifs informationnels (matériels, logiciels, applications, systèmes d'exploitation, dispositifs de sécurité informatique etc) ;
- bénéficier des compétences d'un prestataire spécialisé sur les solutions mises en œuvre à l'organisation ou à l'entreprise ;
- mettre en place les outils les plus performants, les plus fiables et conviviaux, respectant les principes et préoccupations de développement durable ;
- d'assurer un service au meilleur coût.

I.3 Processus de l'assistance informatique

Un processus est défini par Lorino comme « un ensemble d'activités reliées entre elles par des échanges de produits ou d'information et contribuant à la fourniture d'une même prestation à un client interne ou externe de l'entreprise ». On pourrait étendre cette définition aux organisations.

Un processus est par essence permanent, regroupe un ensemble d'activités ayant en commun l'élaboration d'un produit ou d'un service et être descriptible par un diagramme temporel de flux.

En recourant au concept de valeur de Michael Porter, les processus peuvent être scindés en trois catégories :

- les processus stratégiques ;
- les processus « cœur de métier » ou primaires ;
- les processus supports ou secondaires.

Les processus stratégiques définissent la stratégie globale de l'organisation, son pilotage et sa communication. Ils sont menés par la direction générale ou l'instance dirigeante.

Les processus primaires s'intéressent à la production, à la logistique (transport, stockage), à l'approvisionnement, à la conception et à la vente. Ces processus pourraient concerner :

- les applications elles-mêmes ;
- les centres de traitement des applications ;
- le développement des applications ;
- le réseau qui permet les échanges des données traitées par les applications ;
- les risques propres aux Tiers (échanges et responsabilités externes) ;
- etc.

Les processus secondaires quant à eux définiront les ressources humaines (recrutement, gestion des carrières, formation), s'intéresseront au processus d'amélioration ainsi que la maîtrise des risques de l'organisation.

Nous présenterons les processus sans forcément faire cette distinction formelle, mais tous se retrouvent là-dedans.

1.3.1 Gestion du courrier et de la documentation informatique

Les activités qui composent ce processus sont le classement, la lecture et l'affectation du courrier, l'élaboration de correspondances.

1.3.2 Réunions et présentations

Ce processus est composé d'activités comme assister aux réunions du Comité informatique, faire des présentations s'il y a lieu. En outre, il peut s'agir de dépouillement d'appels d'offres ou de valider de candidatures d'étudiants à la demande de stages.

1.3.3 Conduite de projets

Les activités de ce processus sont structurées de la façon suivante : la planification et le lancement de projets, l'élaboration des cahiers de charges, le suivi de projet, le bilan critique, le contrôle qualité et le suivi de prestataires externes.

1.3.4 Analyse et conception

L'analyse de l'existant, la formulation des spécifications fonctionnelles, des spécifications techniques et le suivi des prestataires externes sont les différentes activités qui composent ce processus.

1.3.5 Réalisation

Les activités ont pour noms ici le développement, la revue de code, le paramétrage de progiciels et les tests unitaires.

1.3.6 Intégration

Ce processus concerne l'assemblage des modules et les tests d'intégration.

1.3.7 Déploiement

Il consiste à élaborer le dossier d'installation, à migrer les données, élaborer le dossier d'exploitation, à suivre les prestataires externes et à installer les applications.

1.3.8 Formation des utilisateurs

Il s'agit ici de l'élaboration de programmes et supports, de l'organisation et de la délivrance de formation, de l'élaboration de guide d'utilisateur.

1.3.9 Perfectionnement des informaticiens

L'informatique étant un domaine où la technologie évolue assez rapidement, il convient de garder le contact avec cette évolution par la mise à niveau permanente des acteurs de l'assistance informatique que sont les informaticiens. Une veille technologique doit être de vigueur pour mieux assurer cette assistance.

1.3.10 Maintenance applicative

Elle concerne la qualification des anomalies, la modification de programmes ou paramètres, la mise à jour de la documentation, l'adaptation par rajout de modules, les tests des modifications et de non régression, le suivi des contrats de maintenance, le suivi de traitement d'anomalie c'est-à-dire les indicateurs incidents/interventions.

1.3.11 Gestion du programme informatique

L'élaboration du plan stratégique, la conception de programme annuel d'activités, le suivi de l'exécution de programme et des prestataires externes constituent ses premières

activités. Ensuite viennent l'élaboration du programme annuel d'activités, des plans d'action, du budget informatique et l'évaluation du personnel informatique.

1.3.12 Administration des systèmes

Son champ est assez large. Elle concerne l'installation et la configuration des systèmes, de la base de données, leur analyse et l'optimisation de leurs performances. Elle englobe aussi la maintenance des systèmes, de la base de données et leur surveillance. La gestion du parc de systèmes, l'installation et la configuration de postes de travail, des périphériques utilisateurs et la gestion des licences rentrent également dans son champ d'application.

1.3.13 Sauvegarde /restauration

Ce processus concerne les programmes sources, les données d'utilisateurs, les applications, les logiciels, la base de données, les versions des applications, les versions des logiciels, les serveurs et la sécurité système. La documentation, le site web, la configuration réseau, le firewall (pare-feu), la gestion des supports magnétiques, la définition des normes et procédures en sont parties intégrantes.

1.3.14 Gestion de la sécurité

Elle consiste à définir des stratégies de sécurité et leurs critères de mise en place. Elle concerne l'installation et la mise à jour des antivirus, la gestion des virus, des habilitations (comptes agents et comptes stagiaires), des mots de passe, la gestion des accès aux locaux informatiques, des indicateurs d'incidents, des licences et la définition des normes et procédures.

1.3.15 Maintenance matérielle

Bien vrai que nous ayons exclu de notre champ d'étude sa partie externalisée, elle constitue un processus dont on ne saurait occulter. Elle comporte les activités suivantes : le diagnostic des pannes, la réparation des pannes, la maintenance préventive, le suivi des prestataires extérieurs, la gestion des indicateurs de pannes, la gestion des pièces détachées

et définition des normes et procédures.

1.3.16 Production

La planification de l'exploitation, l'exploitation des applications, l'allocation des ressources (séminaires, étudiants, agents), la définition de normes et procédures sont les principales activités qui la composent.

1.3.17 Mise en œuvre des progiciels

Elle concerne le paramétrage, le déploiement des logiciels, l'adaptation par rajout de modules, la formation des utilisateurs, l'assistance aux utilisateurs, la définition de normes et procédures et la gestion des licences.

1.3.18 Maintenance des progiciels

Les différentes activités de ce processus sont l'adaptation par rajout de modules, le test des modifications, la mise à jour de la version en production et de la documentation, la formation des utilisateurs, la définition des normes et procédures et la gestion des licences.

1.3.19 Administration des réseaux

C'est le processus dont le champ est le plus large. Elle couvre l'élaboration du schéma de réseau, l'analyse et l'optimisation de ses performances, sa supervision et sa maintenance. Ce processus englobe également la définition et la mise en place des règles sur le firewall, son administration, la gestion du parc d'éléments d'actifs (routeurs), l'installation et la configuration des équipements. Les autres activités ont pour noms l'installation et la configuration des accès à internet, des commutateurs, le contrôle de la disponibilité de la ligne internet, le brassage et la mise en réseau des équipements, la gestion des relations avec les fournisseurs, la gestion des indicateurs de réseau, la définition des normes et procédures.

1.3.20 Administration du site web

La conception du site web, son pilotage, sa mise à jour, la gestion des indicateurs et la définition des normes et procédures sont ses principales activités.

1.3.21 Assistance aux utilisateurs

Elle couvre le recueil des demandes d'assistance, le traitement des demandes d'assistance, le suivi des demandes d'assistance, la gestion des indicateurs et la définition des normes et procédures.

1.3.22 Gestion du parc informatique

Elle concerne la réception d'équipements informatiques, la gestion des prêts d'équipements informatiques, l'affectation et livraison d'équipements informatiques et la mise à rebut du matériel retiré d'inventaire. Le retrait d'équipements du parc informatique, le suivi du parc informatique (entrée / sortie), la définition des normes et procédures, gestion de la garantie et celle des indicateurs de mouvements viennent boucler la liste des activités de ce processus.

1.3.23 Architecture

La définition de l'architecture des systèmes, de l'architecture applicative, des normes et procédures, de l'architecture des réseaux et l'élaboration de spécifications techniques sont les activités de ce processus.

1.3.24 Support et conseil aux activités

Les activités ont ici pour noms support et conseil aux activités externes, support et conseil aux équipes de développement, et aux appels d'offres.

I.4 Acteurs de l'assistance informatique

Parmi les acteurs en assistance informatique nous pouvons dénombrer :

1.4.1 Le Technicien de maintenance

Le technicien de maintenance informatique (parfois appelé technicien support ou technicien d'exploitation) est chargé de s'assurer du bon fonctionnement des postes de travail, des logiciels et des périphériques (imprimantes, etc.) des utilisateurs et, en cas de panne, être en mesure de les dépanner.

Au-delà des compétences techniques (fonctionnement de l'ordinateur, assemblage de l'ordinateur, connaissances des systèmes d'exploitation des utilisateurs) nécessaires au bon déroulement de sa mission, le technicien de maintenance doit savoir être à l'écoute des utilisateurs et faire preuve de patience et d'ouverture d'esprit.

Par ailleurs, un esprit critique d'analyse est nécessaire afin de déterminer méthodiquement d'où la panne peut venir, éventuellement en posant les bonnes questions aux utilisateurs, avec une approche pédagogique non technique (Commentçamarche.net, 2008 : 1).

1.4.2 Le Hot Liner

Le technicien support (parfois appelé téléassistant, technicien de hot line ou tout simplement hot liner) est un technicien de maintenance informatique. Il est chargé de dépanner les utilisateurs à distance (généralement par téléphone ou par d'autres moyens de communication tel que l'IP phone) dans leurs utilisations d'outils informatiques, notamment en cas de panne. Lorsque le technicien support travaille dans un centre d'appel (help desk), il peut être amené à gérer des utilisateurs de différentes sociétés.

La plupart du temps, le technicien support ne gère que les problèmes techniques de niveau 1, c'est-à-dire qu'il prend connaissance de l'identité de l'appelant et du problème rencontré et les consigne dans une base de données. Aidé par une base de connaissances, recensant les principales questions/réponses, il diagnostique le problème et tente de trouver une solution dans un délai qui lui est fixé par son employeur. Au-delà de ce délai ou en cas de compétences insuffisantes, le problème est acheminé à un expert, chargé de résoudre les problèmes de niveau 2.

A l'instar du technicien de maintenance, le hot liner doit posséder de réelles compétences techniques (hardware et software) ainsi que des qualités d'écoute des utilisateurs et de médiation. Le hot-liner doit posséder un esprit d'analyse méthodique et faire preuve de

rigueur afin de déterminer les bonnes questions à poser à l'utilisateur, tout en arrivant à estimer son niveau en informatique afin de ne pas être trop/peu technique.

Par ailleurs, afin de pouvoir dépanner les utilisateurs à distance, le hot liner doit maîtriser les outils de télémaintenance permettant de prendre la main sur une machine à distance (Commentçamarche.net, 2008 : 1).

1.4.3 Le Technicien réseau

Le technicien réseau a pour mission d'intervenir sur les équipements ou le câblage du réseau afin d'assurer une qualité de service optimale aux utilisateurs. Dans les grandes entreprises, le technicien réseau pourra intervenir sous la responsabilité d'un administrateur réseau ou d'un ingénieur réseau connaissant parfaitement l'architecture du réseau d'entreprise.

Selon les organisations ou entreprises, le périmètre d'intervention du technicien peut varier parmi les champs suivants :

- monitoring de l'activité du réseau ;
- intervention au niveau du câblage, notamment dans les baies de brassage ;
- configuration des équipements du réseau (routeur, commutateur, etc.) ;
- analyse de la sécurité du réseau ;
- relations avec les services après-vente des distributeurs de matériel réseau.

En cas de dysfonctionnement grave, le technicien réseau doit être en mesure de juger de l'insuffisance de ses capacités et faire appel, au cas échéant à des spécialistes.
Le technicien réseau doit posséder de sérieuses connaissances sur les principaux types de câblages, les équipements et les protocoles réseau.

Par ailleurs, posséder aussi un esprit d'analyse méthodique est indispensable pour pouvoir diagnostiquer l'origine d'une panne, d'un encombrement du réseau ou de pertes de paquets (Commentçamarche.net, 2008 : 1).

1.4.4 L'Administrateur réseau

L'administrateur réseau (également appelé gestionnaire de réseau) est chargé du maintien et de l'évolution de l'infrastructure réseau de l'entreprise.

L'infrastructure réseau fait aujourd'hui partie intégrante de la plupart des entreprises, si bien qu'une indisponibilité du réseau peut parfois se traduire en pertes financières non négligeables pouvant dans certains rares cas conduire à la faillite.

L'administrateur réseau doit permettre de surveiller l'activité du réseau, de faire intervenir rapidement des techniciens en cas de congestion ou de problèmes d'accès. Il doit ainsi posséder une connaissance très précise de tous les équipements réseau, des différents protocoles de communication, du modèle OSI (Open Systems Interconnexion) et des différentes architectures réseau. Ce modèle décrit les concepts utilisés et la démarche suivie pour normaliser l'interconnexion de systèmes ouverts (un réseau est composé de systèmes ouverts lorsque la modification, l'adjonction ou la suppression d'un de ces systèmes ne modifie pas le comportement global du réseau).

Il est également en charge de la gestion des comptes des utilisateurs, de leur création à l'arrivée de nouveaux personnels et à leur destruction au moment de leur départ. Par ailleurs, compte tenu de l'évolution rapide des technologies et des supports de transmission, l'administrateur réseau doit assurer une veille permanente afin de faire évoluer l'infrastructure réseau de l'entreprise.

En relation avec le responsable sécurité, l'administrateur réseau est chargé de mettre en œuvre des dispositifs de protection adaptés, de surveiller les journaux d'activités et de mener une veille sur les alertes de sécurité. Afin d'anticiper tous les risques potentiels, il devra mettre au point un plan de reprise définissant les actions à entreprendre pour rétablir l'accès au plus vite, dans le respect de la politique de sécurité de l'entreprise (Commentçamarche.net, 2008 : 1).

1.4.5 L'Administrateur de bases de données

L'administrateur de bases de données (parfois appelé responsable de bases de données ou en anglais « database administrator », noté DBA est chargé du maintien et de l'évolution des bases de données constituant le système d'information de l'entreprise.

Etant donné le caractère stratégique des données dont il a la charge, l'administrateur de bases de données doit posséder de solides bagages en informatique. Il doit notamment avoir une bonne connaissance des principaux SGBD (systèmes de gestion de bases de données), du langage SQL. Ce qui lui permettra d'interroger les SGBD. Il doit également connaître quelques langages de programmation, afin d'être en mesure d'automatiser certaines tâches.

Ses responsabilités font de lui le garant de l'intégrité du système d'information de l'entreprise. Par ailleurs, des connaissances pointues du SGBD peuvent être nécessaires pour optimiser les requêtes, les paramètres du SGBD ou pour mettre au point des outils de supervision de l'accès aux bases.

L'administrateur de bases de données peut être amené à servir de support pour les utilisateurs d'applications clients ou les équipes de développement afin de les dépanner, de les conseiller ou de les aider à élaborer des requêtes complexes.

En relation avec le responsable sécurité, l'administrateur de bases de données devra mettre au point des stratégies et des procédures de sauvegarde et de restauration des données afin d'assurer la pérennité des données dont il a la charge.

Au-delà des compétences techniques, l'administrateur de bases de données doit avoir une bonne vision des applications de l'entreprise ou de l'organisation. Il doit être en mesure d'écouter les besoins des utilisateurs pour mettre au point ou modifier une base de données. Idéalement, il possède des bagages en matière de conception de systèmes d'information et de modélisation UML (Commentçamarche.net, 2008 : 1).

1.4.6 L'Ingénieur système

Un ingénieur système (parfois appelé responsable système) a pour mission la fiabilisation et l'évolution des installations matérielles et logicielles de l'entreprise ou de l'organisation.

En relation avec les équipes d'exploitation, l'ingénieur système doit veiller à établir un inventaire à jour du parc informatique de l'entreprise ou de l'organisation et définir une stratégie d'évolution. Par ailleurs, il doit s'assurer de l'utilisabilité des postes de travail et mettre en œuvre les outils permettant de simplifier le travail des personnels de l'entreprise ou de l'organisation. Il mène également une action de veille sur le hardware et le software.

Le métier d'ingénieur système demande une connaissance technique des systèmes, matériels et logiciels de l'entreprise ou de l'organisation, mais surtout des capacités relationnelles et organisationnelles de chef de projet afin de coordonner les équipes techniques. Il peut évoluer vers des tâches d'encadrement d'équipes de techniciens (Commentçamarche.net, 2008 : 1).

1.4.7 L'Ingénieur réseau

Un ingénieur réseau (parfois appelé ingénieur télécoms) est responsable du bon fonctionnement des réseaux de télécommunications de l'entreprise ou de l'organisation. En relation avec les équipes d'exploitation, il définit une stratégie d'évolution de l'infrastructure de télécommunication de l'entreprise ou de l'organisation.

Le métier d'ingénieur réseau demande des connaissances techniques de pointe dans le domaine des réseaux et télécommunications (infrastructures, câblage, protocoles, outils d'administration, sécurité, etc.), ainsi que des capacités relationnelles et organisationnelles de chef de projet afin de coordonner les équipes techniques. Il peut évoluer vers des tâches d'encadrement d'équipes de techniciens.

Un ingénieur en télécommunications doit maîtriser plusieurs spécialités parmi lesquelles électronique, informatique, techniques de transmission, ainsi que des notions sur la gestion des entreprises (Commentçamarche.net, 2008 : 1).

1.4.8 L'Analyste programmeur (développeur)

Le métier de développeur (également nommé analyste-programmeur) consiste à concevoir et à développer une application informatique, c'est-à-dire transcrire un besoin en une solution informatique écrite dans un langage informatique. Historiquement, le développement informatique était assuré par un chef de projet, chargé de l'expression des besoins, un analyste, chargé de la modélisation et d'un programmeur chargé du codage. La fonction d'analyste est au programmeur, ce que la conception est à la réalisation. Il s'agit en effet d'un métier de conception consistant à traduire fonctionnellement le besoin d'un client et à proposer une modélisation informatique. Les deux fonctions d'analyste et de programmeur sont de plus en plus confondues, d'où l'appellation analyste-programmeur, synonyme de développeur.

La mission du développeur consiste autant à faire évoluer des applications existantes que d'en modéliser de nouvelles.

Le métier d'analyste-programmeur demande des connaissances techniques spécifiques en développement informatique, en particulier en programmation objet et en génie logiciel. La connaissance de la modélisation UML est généralement nécessaire. La modélisation consiste à créer une représentation simplifiée d'un problème: le modèle. Grâce au modèle il est

possible de représenter simplement un problème, un concept et le simuler. La modélisation comporte deux composantes :

- l'analyse, c'est-à-dire l'étude du problème ;
- la conception, soit la mise au point d'une solution au problème.

Le modèle constitue ainsi une représentation possible du système pour un point de vue donné. Le développeur doit également maîtriser un langage de programmation, voire plusieurs, tels que Java (et l'environnement J2EE), C++ ou le Framework .NET.

Enfin, la maîtrise de l'anglais est indispensable dans la mesure où le développeur est amené à se documenter sur des sujets pointus et peut être en relation avec des correspondants étrangers (Commentçamarche.net, 2010 : 1).

1.4.9 L'Architecte de systèmes d'information

L'architecte de systèmes d'information conçoit l'architecture du système d'information, c'est-à-dire qu'il conçoit les différentes briques du système d'information (SI) et leur imbrication et est chargé de leur évolution. L'architecte de systèmes d'information est au système d'information de l'entreprise ce que l'architecte est à son bâtiment, si ce n'est que le système d'information est plus amené à évoluer.

Pour mener à bien sa mission, l'architecte de système d'information doit en premier lieu étudier les besoins du client (sa direction ou bien le client chez qui il est en mission). En plus, il doit établir une cartographie du système en analysant l'existant, puis proposer un modèle d'architecture. Enfin, il doit mettre en œuvre ladite cartographie en choisissant une infrastructure matérielle et logicielle.

L'architecte de systèmes d'information travaille généralement en équipe, en relation le cas échéant avec un ingénieur système et un ingénieur réseau, et en interface avec les différentes directions métier de l'entreprise ou de l'organisation.

Le métier d'architecte de système d'information est extrêmement stratégique car il conditionne le fonctionnement de toute l'entreprise ou de l'organisation.

Outre ses compétences techniques, l'architecte de SI doit maîtriser l'organisation de l'entreprise et son infrastructure technique. Il doit également posséder d'excellentes capacités relationnelles et stratégiques, ainsi qu'un goût certain pour la négociation, dans la mesure où il travaille en transversal avec sa direction, avec les utilisateurs et avec les fournisseurs de solutions techniques (Commentçamarche.net, 2009 : 1).

1.4.10 Le Webmaster (Administrateur de site web)

Le webmaster (également appelé administrateur de site web ou webmestre) est chargé du maintien et de l'évolution du site web de l'entreprise ou de l'organisation. A ce titre, il travaille à définir l'architecture et l'arborescence du site web, en concertation éventuellement avec un ergonome, pour la navigation, un directeur artistique pour la charte graphique et un responsable éditorial pour le contenu. En règle générale, le webmestre n'est pas chargé directement de la partie éditoriale. Il est chargé néanmoins de réaliser ou de coordonner les développements informatiques pour l'évolution ou la maintenance du site. Enfin, selon les cas, il peut également être chargé du référencement du site.

Le métier de webmaster allie des connaissances techniques à une vision stratégique, avec une touche de créativité. Ainsi, le webmaster doit posséder un profil technique et une bonne connaissance à minima des standards du web :

- HTML
- Javascript
- CSS
- XML.

Dans le cas d'un site dynamique (la majorité des cas), le webmestre devra en plus connaître les principaux langages de script correspondant à ceux choisis par l'entreprise ou l'organisation, et posséder des notions sur les bases de données. Parmi les principaux langages de script dynamiques à connaître, citons notamment les suivants :

- PHP
- ASP et .NET
- JSP.

Par ailleurs, le webmaster doit posséder de solides notions en termes de sécurité des applications web, de référencement dans les moteurs de recherche, ainsi que des bases juridiques pour respecter la règlementation en vigueur.

Enfin, le webmaster doit posséder des capacités d'écoute et des qualités relationnelles et organisationnelles afin d'être en mesure de coordonner les différents corps de métier concourant à la réalisation d'un site web (Commentçamarche.net, 2008 : 1).

1.4.11 Le Web designer

Le web designer conçoit l'identité visuelle des sites web et définit leur charte graphique (maquette, position des éléments graphiques, choix des images, couleurs, polices, etc.). L'objectif du web designer est de valoriser l'image de l'entreprise ou de l'organisation grâce aux éléments graphiques du site permettant de renforcer son identité visuelle et de procurer un sentiment de confiance à l'utilisateur. Il doit également travailler en concertation étroite avec l'équipe éditoriale afin de répondre aux attentes des utilisateurs et de leur permettre de trouver facilement l'information qu'ils cherchent.

Le métier de web designer est un métier essentiellement artistique, demandant des connaissances en matière d'infographie et une maîtrise des principaux logiciels graphiques.
Par ailleurs, le web designer doit connaître les standards du web, notamment le langage HTML, feuilles de style ou encore le Javascript.

Le web designer doit aussi posséder des notions basiques en termes de référencement, et d'ergonomie, notamment en ce qui concerne l'accessibilité des sites web (Commentçamarche.net, 2008 : 1).

1.4.12 L'Ergonome

Le métier d'ergonome consiste à améliorer l'environnement de travail de l'être humain. L'ergonomie se caractérise généralement selon deux composantes :

- l'efficacité, consistant à adopter des solutions appropriées d'utilisation d'un produit, au-delà du bon sens du concepteur ;
- l'utilisabilité, marquant l'adéquation aux capacités de l'utilisateur. Elle se décline en deux catégories :
    - confort d'utilisation, consistant à réduire au maximum la fatigue physique et nerveuse ;
    - sécurité, consistant à choisir des solutions adéquates pour protéger l'utilisateur.

L'ergonome doit donc travailler en transversal sur l'ensemble de la chaîne d'activité de l'entreprise ou de l'organisation, pour améliorer l'environnement de travail des personnels ou bien pour améliorer l'ergonomie des produits ou du site web de l'entreprise ou de l'organisation.

Il travaille à assurer un confort de navigation au sein d'interfaces web, en relation avec le webmestre, avec le « web designer » et les équipes éditoriales et participe à la conception de l'architecture du site, de la structuration des pages et de sa navigation.

L'ergonome doit posséder des connaissances propres à son secteur d'activité, ainsi qu'un bagage professionnel en psychologie, physiologie, sociologie, organisation du travail, voire en médecine.

Lorsqu'il travaille sur le site web de l'entreprise ou de l'organisation, l'ergonome doit posséder des notions en termes de conception de sites web et en connaître les contraintes techniques. Enfin, il doit posséder des capacités d'écoute et des qualités relationnelles et organisationnelles afin de connaître les différents corps de métier de l'entreprise ou de l'organisation et d'être en mesure de coordonner des actions de sensibilisation et de formation (Commentçamarche.net, 2011 : 1).

1.4.13 Le Chef de produit

Le rôle du chef de produit est de suivre le cycle de vie d'un produit, et de penser à son évolution de manière à améliorer les ventes. Il doit posséder des qualités relationnelles et organisationnelles dans la mesure où il joue un rôle d'interface avec l'ensemble des acteurs participant au cycle de vie du produit (production, développement, marketing, avant-vente et après-vente) (Commentçamarche.net, 2008 : 1).

Dans la présente étude, ce poste ne sera pas étudié s'agissant d'une organisation publique produisant des services et non des produits.

1.4.14 Le Consultant informatique

La plupart du temps employé par une société de services et en mission chez un client, le consultant informatique joue un rôle d'analyse, d'évaluation des besoins, de conseil et de proposition de solutions.

On distingue généralement :

- le consultant junior, ayant peu d'années d'expériences en tant que consultant,
- le consultant senior, bénéficiant d'une expérience réussie d'au moins 2 à 4 années en cabinet de conseil.

Le métier de consultant nécessite un goût du contact et un intérêt pour la réalisation de missions de conseil en complète autonomie, ce qui implique notamment d'être à l'écoute du client et de faire preuve de diplomatie. Outre des compétences techniques avérées sur son domaine d'intervention, le consultant doit faire preuve de capacités d'analyse et de synthèse.

Enfin, le consultant mène une activité de veille permanente pour être à la pointe de l'information technologique et être en mesure de conseiller au mieux ses clients (Commentçamarche.net, 2008 : 1).

1.4.15 Le Chef de projet informatique

La mission du chef de projet informatique consiste à piloter un projet informatique, de son idée de départ au déploiement généralisé. Les tâches du chef de projet sont nombreuses :

- définition du projet, recensement des besoins ;
- élaboration du cahier des charges ;
- chiffrage du coût du projet ;
- encadrement de l'équipe de réalisation ;
- suivi et « reporting » de l'avancement du projet, en termes de qualité, de coût et de délai.

Le chef de projet doit avant tout avoir des compétences en matière de gestion de projet, c'est-à-dire notamment une organisation méthodique et rigoureuse et le sens du relationnel, ainsi que des connaissances techniques dans son domaine d'intervention (Commentçamarche.net, 2008 : 1).

1.4.16 Le RSSI (responsable de la sécurité des systèmes d'information)

Le RSSI (responsable de la sécurité des systèmes d'information) est chargé de la définition et de la mise en œuvre de la politique de sécurité de l'entreprise ou de l'organisation. Il possède en outre un rôle stratégique d'information, de conseil et d'alerte de la direction générale sur les risques en matière de sécurité informatique.

Le RSSI a un triple rôle : « à la fois technique (informatique et sécurité), organisationnel (coordination des actions entreprises) et surtout garant de l'adéquation de la mise en œuvre de la politique de sécurité avec les objectifs assignés par la direction générale » (Hillion, février 2002 : 23).

La fonction de RSSI est essentiellement managériale et consiste à encadrer une équipe d'ingénieurs et de techniciens d'exploitation, dont il organise et contrôle le travail. Il doit avoir des connaissances pointues sur les réseaux, les systèmes et la sécurité des systèmes d'information. Par ailleurs, étant donné ses fonctions d'encadrement, il doit posséder des qualités relationnelles et avoir une expérience de conduite de projets (Commentçamarche.net, 2008 : 1).

1.4.17 Le Directeur des Systèmes d'Information (DSI)

Le Directeur des Systèmes d'Information (également appelé DSI) possède une double compétence de manager et de technicien. Il est chargé de l'adéquation des systèmes d'information à la stratégie de l'entreprise ou de l'organisation, de définir et de gérer les budgets et de coordonner les équipes techniques.

Le directeur des systèmes d'information est considéré comme faisant partie de la Direction de l'entreprise ou de l'organisation. A ce titre, il participe au Comité de Direction et doit prendre en compte les demandes des autres directions et rendre compte de son activité.

Le métier de Directeur des Systèmes d'Information demande de solides bagages techniques en informatique et une vision stratégique de l'innovation et du changement, couplés à des aptitudes de management.

Par ailleurs, le DSI doit posséder une approche méthodique et rigoureuse de son métier, des qualités relationnelles vis-à-vis de ses équipes et des capacités de négociation. Enfin, il doit maîtriser l'anglais dans une approche de relation avec les partenaires internationaux de l'entreprise ou de l'organisation (Commentçamarche.net, 2008 : 1).

L'assistance informatique repose sur les processus informatiques. Elle implique de ce fait beaucoup d'acteurs. Ces acteurs doivent avoir de solides formations en informatique pour mener à bien leur mission. « Si le métier d'auditeur est bien un métier de technicien (connaître la comptabilité, la fiscalité, les normes professionnelles…) et d'évaluateur (apprécier un taux d'amortissement, une provision pour risque client…), ces connaissances sont totalement inutiles si elles ne peuvent être utilisées grâce à un excellent contact humain entre l'auditeur et son client » (Dayan & al. 2004 : 937).

On pourrait étendre le même raisonnement à l'assistance informatique dont les acteurs, en plus des compétences techniques, doivent avoir des qualités relationnelles confirmées.

CHAPITRE II - EVALUATION DU CONTROLE INTERNE DE L'ASSISTANCE INFORMATIQUE

Pour étudier un système, il est important de savoir comment il fonctionne. Ce fonctionnement est généralement l'action coordonnée des différents éléments du système d'une organisation. « Un système ou une organisation ne fonctionne efficacement que lorsqu'il est pourvu de mécanismes de régulation, de contrôle et de correction. L'ensemble de ces mécanismes, destinés à assurer le fonctionnement harmonieux et efficace du système ou de l'organisation, constitue le contrôle interne » (Pigé, 2007 : 9).

Le contrôle interne de l'assistance informatique s'appuie sur le contrôle interne de la fonction informatique. Dans ce domaine, on retrouve :

- « l'organigramme du service ;
- la description de la configuration matérielle ;
- une description succincte des logiciels ;
- la liste des progiciels ;
- les principales notes relatives à l'activité informatique dans l'entreprise et à l'organisation de service ;
- le plan informatique ;
- le budget du service informatique ;
- les comptes rendus des dernières réunions du comité informatique » (Derrien, 1992 : 208).

Nous aborderons les différents thèmes de ce chapitre sous forme de questions qu'un auditeur est susceptible de se poser. Les réponses aux questions constituent les dispositifs du contrôle interne du thème abordé.

2.1 L'organisation générale du service informatique

Existe-t-il un organigramme écrit du département informatique ?

L'existence d'un organigramme écrit s'impose dès lors que l'effectif du département dépasse une dizaine de personnes. Cet organigramme doit être à jour et doit couvrir l'ensemble des fonctions nécessaires à la bonne marche du service. De ce fait, il est souhaitable que des fiches de définition de fonctions existent pour les postes fonctionnels. Parmi ces postes, on peut citer entre autres le responsable des méthodes, l'administrateur de bases de données, le

responsable de la sécurité, etc. L'analyse de ces fiches permettra de découvrir les fonctions non couvertes.

2.2 La planification de l'activité informatique

Existe-t-il un comité informatique responsable des principaux choix stratégiques ?
Il est important que sa composition soit hétérogène. Il doit être composé des représentants de la Direction générale, des responsables de chaque direction de l'entreprise ou de l'organisation ainsi que des principaux responsables de la direction informatique.
La présence en son sein des représentants des utilisateurs est vivement conseillée par certains spécialistes (Schick & al. 2001 : 49).
Existe-t-il un plan informatique ou SDI ?

« Le schéma directeur aura pour objectif de définir les axes d'évolution du système d'information nécessaires à la cohérence avec la stratégie. Il mettra en perspective les évolutions à réaliser sur une durée de un à trois ans. Il permettra de définir les priorités et de lister les projets à réaliser pour atteindre les objectifs. Il permettra de mettre en place une planification des réalisations pour qu'elles soient synchronisées avec la satisfaction des besoins de la stratégie » (Gillet & al. 2008 : 146).

L'élaboration d'un plan informatique est souvent jugé périlleuse compte tenu de la rapidité de l'évolution des techniques.

Si un plan informatique trop détaillé peut être voué à une obsolescence rapide, par contre un plan trop imprécis ne sera d'aucune utilité (Derrien, 1992 : 49).

Malgré ce contraste, la planification doit demeurer au cœur du système même si elle doit faire l'objet d'une remise en cause permanente.

2.3 Les relations avec les services utilisateurs

Existe-t-il un suivi de la qualité du service fourni ?
Des instruments de mesure doivent fournir une estimation de cette qualité de service à savoir :

- disponibilité des serveurs ;
- temps de réponse moyen des transactions ;
- fréquence des incidents par application.

Est-il prévu dans les services utilisateurs une fonction de correspondant informatique ?

Dans chaque service, le correspondant informatique est l'interface entre les informaticiens et les utilisateurs. Outre une bonne maîtrise de l'activité de son service, il doit posséder une bonne culture générale informatique lui permettant de conseiller de manière efficace les utilisateurs et de formaliser les demandes de maintenance émanant de son service.

En l'absence de cette fonction, il est évident que tôt ou tard, des demandes contradictoires parviendront au service informatique.

2.4 La séparation des fonctions

Existe-t-il dans l'organisation du service informatique une séparation entre les fonctions d'études et celles d'exploitation ?

Les principes d'un bon système de contrôle interne conduisent à ce que soient séparées les fonctions :

- des utilisateurs ;
- du personnel d'études ;
- du personnel d'exploitation.

Les utilisateurs ont accès aux transactions pour lesquelles ils sont habilités.

Le personnel d'études développe et teste les nouveaux logiciels dans un environnement d'essai dédié à cet effet. Si les essais sont concluants, il en demande la mise en exploitation. Par contre, le personnel d'études n'a pas accès aux fichiers en exploitation par quelque moyen que ce soit. De ce fait :

- il ne connaît pas le mot de passe des utilisateurs de l'application qu'il a développée ;
- il n'a pas accès aux fichiers et aux bibliothèques de programmes d'exploitation ;
- il ne met pas lui-même en exploitation les logiciels qu'il a développés.

Le personnel d'exploitation est responsable de la mise en exploitation et de la production des logiciels développés par le personnel d'études. En revanche, il ne doit en aucun cas développer ou mettre à jour lui-même des logiciels.

2.5 Les relations avec les fournisseurs

Tout choix de prestataire matériel ou logiciel donne-t-il lieu à un appel d'offres ?

La réponse au QCI relatif au choix des matériels ou logiciels est développé en annexe n° 1, page 110. Elle nous édifie davantage sur l'existence ou pas d'un système de contrôle interne adéquat.

2.6 Les procédures de développement et de maintenance des logiciels

Est-il toujours réalisé une étude d'opportunité préalablement au lancement de la conception d'une nouvelle application ?

L'étude d'opportunité doit inclure notamment :

- la présentation succincte des fonctions à développer ;
- les principales contraintes de mise en œuvre ;
- si nécessaire, une présentation des différentes solutions techniques entre lesquelles il conviendra d'arbitrer ;
- une estimation des volumes à traiter ;
- une estimation des coûts prévisionnels et, le cas échéant, des gains financiers attendus ;
- un échéancier prévisionnel de mise en œuvre (Derrien, 1992 : 64).

Est-t-il rédigé un cahier de charges préalablement au lancement de la réalisation de nouveaux logiciels ?

Sans que la liste ne soit exhaustive, on peut, au titre des principaux documents contenus dans le cahier de charges citer :

- la description des fonctions à développer ;
- la description des grilles de saisie et de consultation ;
- les traitements à réaliser ;
- la liste et le contenu des principaux états à éditer ;
- la liste et le contenu des fichiers constitutifs de l'application (à l'exception des fichiers de travail) ;
- l'estimation des volumes à traiter ;
- l'échéancier de mise en œuvre et de démarrage de l'application.

Existe-t-il des normes en matière de développement d'applications ?

Les points suivants à titre d'exemple seront imposés :

- l'étude préalable ;
- le cahier des charges ;
- l'analyse technique ;
- les normes de programmation.

Existe-t-il des normes en matière de programmation ?

Pour être respectées, ces normes doivent être consignées dans un document écrit, et diffusées à l'ensemble du personnel d'études.

Pour les normes qui concernent le contenu détaillé des programmes, on peut citer :

- les noms des fichiers , les noms des zones dans les fichiers , les noms des étiquettes dans les programmes , etc.

Les principales phases de mise en œuvre d'un projet sont-elles prévues dans le processus de développement de nouvelles applications ?

Les principales d'entre elles sont :

- la formation des utilisateurs ;
- la documentation de l'application ;
- l'implantation physique des matériels ;
- la validation des logiciels ;
- la sécurité.

2.6.1 La formation des utilisateurs

Elle a pour but d'éviter une utilisation anarchique du système, un désintérêt voire un rejet de la nouvelle application par les utilisateurs.

2.6.2 La documentation

On distingue trois types de documentation :

- la documentation d'études destinée aux équipes de développement et de maintenance ;
- la documentation d'exploitation destinée au personnel de production ;
- la documentation destinée aux utilisateurs.

La documentation d'études doit contenir la description du contenu des fichiers, des chaînes de traitement, celle détaillée des programmes et l'historique des opérations de maintenance.

Quant à la documentation d'exploitation, elle doit contenir l'ensemble des informations et consignes nécessaires au personnel de production que sont :

- la description et les organigrammes des chaînes de traitement ;
- les consignes de préparation ;
- la description des contrôles de l'exploitation à réaliser lors de chaque traitement ;
- les consignes de pupritage.

Enfin la documentation destinée aux utilisateurs doit contenir la description générale des applications, la description des transactions, des états à éditer et l'explication des messages d'anomalies.

2.6.3 L'impact du nouveau système sur l'organisation et les procédures administratives

Pour mettre en place un nouveau système informatique, il est impérieux de mener une réflexion sur l'organisation du travail ainsi que la mise en place de nouvelles procédures. Ce qui a pour intérêt d'éviter que les procédures administratives soient mal adaptées au système d'information.

2.6.4 L'implantation physique des matériels

Un des aspects le plus important dans ce domaine est la compatibilité des matériels. Ladite implantation concerne aussi le nombre et la localisation géographique des terminaux, écrans et imprimantes.

2.6.5 La validation des logiciels

Deux méthodes complémentaires conduisent à la validation des logiciels : les jeux d'essai et l'exploitation en double.

Les jeux d'essai permettent de simuler les cas réels. Dans un premier temps, ils sont conçus et réalisés par des informaticiens pour s'assurer que les logiciels sont conformes au cahier de charges. Dans un second temps, les utilisateurs en effectueront pour valider l'adéquation aux besoins. Les utilisateurs sont en définitive l'ultime contrôle avant le démarrage de celle-ci.

L'exploitation en double quant à elle, malgré la charge de travail qu'elle impose (double saisies, double contrôles de un à trois mois), est un moyen très efficace lorsque la nouvelle application remplace les logiciels aux fonctions similaires.

2.7 La gestion des sauvegardes

Les objectifs fondamentaux d'une bonne politique de sauvegarde sont :

- permettre le démarrage de chacune des chaînes de traitement en cas d'incident (exemple : redémarrage d'une chaîne interrompue par une panne d'alimentation électrique, ou par un incident logiciel) ;
- permettre de pallier un incident sur un support physique (exemple : un incident sur un disque rend celui-ci illisible et impose son remplacement physique, puis le rechargement de son contenu à partir d'une sauvegarde) ;
- permettre le redémarrage sur un site extérieur en cas de destruction totale du site de production.

Les réponses aux questions suivantes nous édifierons davantage sur l'intérêt de ses sauvegardes en matière de contrôle interne de l'assistance informatique.

L'ensemble des logiciels et fichiers nécessaires au développement et à l'exploitation est-il régulièrement sauvegardé ?

Rentrent impérativement dans ce cadre les logiciels de base, les fichiers et logiciels d'application de l'environnement d'exploitation, ceux de l'environnement d'études.

Procède-t-on à des sauvegardes sur site extérieur (back-up) ?

Si elle existe, cette procédure doit être préalablement testée pour déceler les imperfections de la procédure théorique (mémoire centrale insuffisante, fichiers non sauvegardés, utilisateurs non connectés, etc.).

La reprise sur site extérieur doit impliquer la mise en œuvre de procédures dégradées. Si tel est le cas, celles-ci doivent être définies. Ainsi doit-on définir les applications et les utilisateurs prioritaires le site de secours permettant rarement de « traiter » les applications dans les mêmes conditions que le site initial.

Enfin une solution de plus en plus adoptée par les entreprises et les organisations est l'existence en leur sein de deux sites éloignés l'un de l'autre, dont chacun est capable d'assumer le back-up de l'autre.

2.8 La sécurité physique

Il s'agit ici de caractéristiques essentielles du contrôle de la sécurité physique des salles réservées aux ordinateurs et serveurs s'il en existe. Si tel n'est pas le cas, il s'agit de l'accès aux matériels informatiques.

Les principales questions susceptibles d'être posées dans ce domaine sont ci-dessous récapitulées.

L'accès physique à l'environnement informatique est-il protégé ?

La règle d'or est de réglementer strictement l'accès à la salle machine : salle contenant les ordinateurs, serveurs et tout autre matériel sensible.

« Une sécurité physique adéquate est basée sur les principes suivants : situation …contrôle d'accès…sécurité contre l'incendie…fourniture d'énergie…environnement de travail…réseau » (Angot & al. 2004 : 276).

La localisation de la salle machine et son agencement (étage, fenêtres, murs…) doit tenir compte des risques d'émeutes, de conflit social ou de toute intrusion malveillante par effraction. L'implantation du site secours doit être tenue confidentielle.

Les locaux sont-ils protégés contre l'incendie ?

Dans ce domaine, il est à distinguer :

- les dispositifs de détection généralement basés la détection de la fumée ;
- les dispositifs d'extinction au titre desquels on peut citer le gaz halon, le gaz carbonique, l'eau (utilisation de sprinkers).

Les locaux sont-ils protégés contre les dégâts des eaux ?

On évitera d'installer une salle machine au sous-sol dans une zone marécageuse. Si elle est située au rez-de-chaussée, des dispositions doivent être prise pour surélever les matériels informatiques par rapport au niveau du sol et éviter ainsi toute inondation.

Un système de détection des intrusions et virus est-il prévu ?

Les faisceaux lumineux, les détecteurs de bruit et la télésurveillance permettent de déceler d'éventuelles intrusions après le départ des derniers informaticiens ou utilisateurs. L'achat d'antivirus avec licence d'exploitation protège le parc informatique contre les virus.

Le centre informatique est-il protégé contre les défauts d'alimentation électrique ?

La dotation des salles informatiques en prises ondulées protègent contre les coupures d'alimentation électrique de courte durée.

Pour les délestages de longue durée ou pour les cas de grève du service fournisseur d'électricité, seuls les groupes électrogènes peuvent y pallier.

Dans tous les cas, il doit être tenu compte du rapport coût/bénéfice que l'entreprise ou l'organisation tire de la prise de décisions d'une telle envergure.

2.9 Les bases de données

La généralisation de l'utilisation des SGBD dans le développement des applications a conduit à la création de fonctions et de tâches nouvelles dont celles d'administrateur de données ou d'administrateur de bases de données.

Existe-t-il un administrateur de données ?

L'administrateur de données a pour rôle la gestion des données de l'entreprise ou de l'organisation, ou pour les applications importantes, la gestion des données de l'application.
Il est garant de la cohérence et de la non-redondance des données gérées par le SGBD.
Il est bon de distinguer la notion d'administrateur des données de celle d'administrateur de base de données. Tandis que le premier est responsable des données de l'entreprise ou de l'organisation, le second est responsable de l'implantation physique des bases, de leur optimisation et de leur cohérence technique.

Un « dictionnaire des données » est-il utilisé ?

Le « dictionnaire des données » est un progiciel qui facilite la gestion des données par l'administrateur et leur utilisation par les équipes de développement.

Procède-t-on à des travaux de recherche d'optimisation de la base de données ?

L'absence d'optimisation conduit dans certains cas à des temps de réponse des applications interactives ou à des temps d'exécution des travaux différés tout à fait inacceptables.

2.10 La gestion des réseaux

La mise en œuvre d'un réseau nécessite le choix de logiciels cohérents les uns avec les autres, puis leur implantation et leur paramétrage.

Existe-t-il une cellule technique de gestion des réseaux ?

Le choix des réseaux nécessite des études techniques et économiques. Cette fonction est généralement dévolue à une cellule technique. Les choix techniques et économiques doivent être justifiés, les nouvelles configurations testées.

Existe-t-il une cellule d'assistance réseau ?

Contrairement à la cellule technique précédemment citée, celle-ci a un rôle essentiellement d'assistance aux utilisateurs. Ces fonctions concernent :

- l'installation des nouveaux postes ;
- première assistance téléphonique en cas de problème ;
- maintenance si celle-ci n'est pas confiée à des sociétés spécialisées ;

- gestion de certaines tables.

Les accès au réseau sont-ils contrôlés ?

Il existe l'identification logique par mot de passe et l'identification par tout moyen physique.

- L'identification logique par mot de passe

Les règles de base en la matière sont ci-dessous énoncées.

Les mots de passe sont affectés individuellement à chaque utilisateur. Ils doivent être modifiés régulièrement. Pour une réelle confidentialité, le mot de passe doit être modifié par son propriétaire. Le trimestre parait une périodicité raisonnable pour cette modification.

Les mots de passe doivent être suffisamment sophistiqués. Pour ce faire, il est préférable d'éviter les initiales de l'utilisateur, sa date de naissance, la date de création du mot de passe lui-même. Si c'est les cas, quelques tentatives suffisent pour les démasquer.

La table des mots de passe doit être elle-même protégée. Tout utilisateur doit être déconnecté après plusieurs tentatives d'accès infructueuses. Une désactivation d'un code utilisateur après trois tentatives d'accès avec des mots de passe erronés est généralement admise. Les utilisateurs doivent être sensibilisés aux risques qui peuvent découler du « prêt » de leur mot de passe (Derrien, 1992 : 114 – 115).

Dans cette partie, il ne faut pas omettre la suppression des mots de passe pour les cas de mutation, de départ à la retraite et de licenciement (Schick & al. 2004 :45).

- L'identification par tout moyen physique

Il existe des systèmes d'autorisation d'accès par carte à mémoire. D'autres systèmes d'identification peuvent être cités comme la reconnaissance vocale, l'identification des empreintes digitales, du fond de l'œil etc. Certains de ces systèmes sont développés au chapitre trois.

On se rend compte que l'évaluation du contrôle interne de l'assistance informatique ne s'arrête pas uniquement à la fonction d'assistance aux utilisateurs. Elle va de l'organisation générale du service informatique à la gestion des réseaux en passant par l'élaboration du cahier de charges préalablement à la réalisation des applications, l'appel d'offres de leur réalisation, les procédures de développement et de maintenance des applications ou logiciels. Elle inclue aussi les choix des matériels informatiques, leur implantation physique, la validation des logiciels, la gestion des sauvegardes, la sécurité physique.

L'informatique étant une science où la technicité est assez poussée, les choix matériels et logiciels méritent l'avis de spécialistes pour la réussite des projets et applications issues desdits projets.

CHAPITRE III - MAITRISE DES RISQUES OPERATIONNELS LIES AUX PROCESSUS DE L'ASSISTANCE INFORMATIQUE

La survenance d'un événement qu'il soit d'origine interne ou externe peut avoir des répercussions sur l'atteinte des objectifs. Les événements peuvent, de ce fait, avoir un impact soit négatif, soit positif ou les deux simultanément. Les événements ayant un impact négatif constituent des risques.

« Dans ce contexte, un risque se définit comme suit :

un risque représente la possibilité qu'un événement survienne et nuise à l'atteinte des objectifs » (IFACI & al. 2009 : 23).

Les événements ayant un impact négatif, tels que des pannes, des incendies ou des pertes de crédit, empêcheront la création de valeur ou la destruction de la valeur existante.

Les auteurs du COSO II poursuivent en ajoutant que : « ...les événements ayant un impact positif peuvent compenser les impacts négatifs ou constituer des opportunités. Une opportunité se définit comme suit :

une opportunité est la possibilité qu'un événement survienne et contribue à l'atteinte des objectifs.

Par opportunité, on entend la possibilité qu'un événement survienne et ait une incidence positive sur la réalisation des activités permettant d'atteindre les objectifs. Les opportunités constituent des leviers pour la création ou la préservation de valeur ».

3.1 Définition de risques informatiques

Le risque informatique est défini comme tout « événement pouvant affecter le système d'information et engendrer des dommages ou des pertes éventuelles » (Naaima, février 2002 : 36). L'auteur poursuit en distinguant deux catégories de risques : ceux associés à des processus de gestion et ceux associés à un patrimoine.

« Les risques associés aux processus de gestion sont ceux générés par les méthodes, les techniques et les procédures de gestion et du contrôle interne ». Tandis que « les risques associés à l'existence d'un patrimoine sont ceux générés par toutes sortes de menaces pouvant impliquer l'altération, la disparition matérielle ou informationnelle du système d'information ».

Il ajoute tout de même que « …l'absence d'une stratégie, l'utilisation des méthodes ou techniques inadaptées, le manque de compétences et la faiblesse des processus de gestion, peuvent constituer des facteurs de risque ».

Dans Risk IT (ISACA) la définition suivante est donnée :

« le risque informatique peut être désigné comme 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).

Ainsi défini, le risque informatique est-il spécifique ? L'ISACA donne des exemples et liens de risques métiers. Parmi eux, figurent :

- « interruption des activités d'une entreprise en raison d'une indisponibilité du SI :
  - panne d'un composant du réseau (par exemple un routeur) ;
  - incendie de la salle machine ;
  - intrusion d'un pirate et destruction des bases de données ;
  - plan de secours n'ayant pas suivi les évolutions récentes des.systèmes.
- Fraude sur les systèmes de paiement :
  - accès inapproprié aux données : possibilité d'intervention directe sur les fichiers d'interface, sans supervision
  - absence de contrôles au sein des processus achats : « 3-way match principle »
  - anomalies de séparation des tâches au sein de la communauté d'utilisateurs : le demandeur n'est pas l'acheteur
  - pas d'outil de détection d'anomalies en place sur les données : modification des données fournisseurs
  - capacité des équipes informatiques à intervenir sur le code source des applications et à mettre en production sans point de contrôle » (AFAI, 2010 : 12 – 13).

3.2 Conditions de maîtrise du risque informatique

Toute organisation qui aurait trouvé la réponse aux cinq questions suivantes, aurait rempli les conditions de maîtrise du risque informatique. Ces questions sont formulées sous forme d'objectifs du contrôle interne. Ces questions sont les suivantes :

- être sûr de la pérennité de fonctionnement des systèmes informatiques et de la protection du matériel ;
- être sûr de la protection des accès logiques aux systèmes informatiques ;

- être sûr de la maîtrise des relations avec les sociétés extérieures (fournisseurs, sous-traitants) ;
- être sûr de l'efficacité de l'organisation de la fonction informatique en interne et en relation avec les utilisateurs ;
- être sûr de la fiabilité du système d'information.

3.3 Types de risques

On distinguera ici les risques intrinsèquement informatiques différents des risques fonctionnels portant sur les traitements confiés aux applications. On pourrait alors parler de risque spécifique appartenant à quatre domaines :

- « le risque sur le système d'information ;
- le risque sur les études informatiques;
- le risque sur les traitements informatiques ;
- le risque lié aux télécommunications » (Maders & al. 2009 : 41 – 42).

3.3.1 Le risque sur le système d'information

« Il est aussi appelé « risque d'architecture ». Il correspond au risque lié à l'architecture générale du système d'information (applications, bases de données, systèmes), des matériels utilisés (ordinateurs, terminaux, micro-ordinateurs..) et de l'organisation des traitements (batch, temps réel) de l'entreprise » (Maders & al. 2009 : 41).

Le risque évoqué au premier plan est la non adéquation du système d'information d'une organisation à l'état de celle-ci. Ensuite viennent les risques qui se rapportent à la confidentialité, à l'intégrité et à la disponibilité des données. Ces trois risques sont considérés comme classiques du système d'information. Certains auteurs parlent de pérennité à la place de disponibilité.

« La pérennité est la capacité du système d'offrir d'une manière continue les informations nécessaires au fonctionnement de l'entreprise.

L'intégrité de l'information se définit à travers son authenticité, son identification, son exactitude et son exhaustivité.

La confidentialité, c'est la capacité du système d'information de se prémunir contre l'indiscrétion, le détournement et la fraude » (Naaima, février 2002 : 36).

Le risque étant défini comme son contraire, l'incapacité d'un système d'information à assurer les principes ci-dessus décrits constitue un facteur de risque.

Les risques correspondant à la disponibilité (ou pérennité) des données sont les pannes du système, les interruptions de traitement ou l'inefficacité des règles de conservation des données.

Les risques liés au manque d'intégrité des données sont nombreux. Ils vont « du rapport financier inexact à la décision de gestion erronée par ce que reposant sur des données inexactes ou incomplètes » (IFACI, 1993 : 7).

3.3.2 Le risque sur les études informatiques

Il correspond au risque lié à la phase de conception des programmes informatiques (erreur de compréhension, mauvaise couverture des besoins (risques produits)……). Il est aussi appelé « risque de conception », « risque applicatif », « risque développeur », « risque de maintenance » ou « risque de sécurité logique ».

Pour éviter ces risques, des questions qui ne sont nullement exhaustives reviennent généralement.

- Comment sont achetées ou développées les solutions informatiques ?
- Comment sont installés et validés les nouveaux systèmes informatiques ?
- Comment est assurée la maintenance du système d'information ?
- Quelle est la qualité du support fourni aux utilisateurs ?
- Comment sont gérés les problèmes d'exploitation quotidiens ?
- Comment sont gérées les fonctions externalisées ?
- Comment sont gérées les sauvegardes et existe-t-il un plan de secours ?
- Comment est définie la mise en œuvre de la sécurité logique ?
- La sécurité physique est-elle satisfaisante ?

Lorsque le projet informatique représente un investissement de grande importance, ou lorsqu'il peut avoir une incidence sur le système comptable, il est pertinent d'apprécier l'existence et l'efficience des procédures de gestion de projet. Cela, au regard des risques financiers généralement encourus ou des conditions d'établissement des comptes.

La gestion des projets informatiques présente les risques majeurs suivants : le risque de non-atteinte des performances, le risque de surcoût et le risque de retard. Les techniques d'analyse de risques utilisées sont l'œuvre de l'initiateur du projet. Elles reposent sur une analyse des compétences du constructeur et de ses sous-traitants.

Le risque de non-atteinte des performances : il porte sur les performances techniques et/ou opérationnelles (produit livré non-conforme aux spécifications, refus des utilisateurs). Le consultant doit s'assurer que les techniques utilisées sont connues et maîtrisées par l'ingénierie (le constructeur). Le consultant (indépendant ou société), doit être un expert du domaine concerné. Un véritable benchmarking s'impose à ce niveau : examiner le degré d'expérience sur chacune des technologies et leur degré de compatibilité, collecte d'informations de la disponibilité constatée sur les installations équivalentes.

Le risque de surcoût : il consiste à réexaminer par le consultant, le montant des investissements prévus par l'initiateur du projet.

Le risque de retard : il consiste pour le consultant, à faire une revue du planning de réalisation tout en faisant un examen critique des délais prévus pour chacune des tâches (Desroches & al. 2005 : 135).

3.3.3 Le risque sur les traitements informatiques

« Appelé « risque de système », « risque de sécurité logique », « risque de pénétration », « risque d'altération des données », il correspond aux risques liés au fonctionnement des applications en production et des logiciels systèmes qu'utilise l'organisation » (Maders & al. 2009 : 42). Ces risques couvrent l'accès aux ressources, les traitements proprement dits, les produits résiduels (listings, fichiers magnétiques, bandes.....) et leur conservation.

Le risque correspondant à la confidentialité est l'accès illégitime aux données (IFACI, 1993 : 6). Il peut provenir de deux causes : un accès non justifié à certains traitements comme l'accès aux mouvements de modification des paiements par le personnel du service achat ou une protection inadaptée des fichiers de l'application. Dans ce dernier cas, il peut s'agir de la possibilité pour les ingénieurs système de modifier n'importe quelle donnée enregistrée dans le système.

3.3.3.1 Erreurs d'exploitation

Ces erreurs prennent des formes variées : effacement accidentel de fichiers, supports ou copies de sauvegarde, chargement d'une version incorrecte de logiciel ou de copie de sauvegarde, lancement d'un programme inapproprié.

Le recours à des systèmes automatisés de gestion des applications permet de réduire le rôle joué par les opérateurs humains et de faire baisser le nombre de ces erreurs.
Outre ces cas, l'audit interne et le contrôle interne peuvent aider à la maîtrise des risques de façon générale, et aux risques informatiques de façon particulière. Le contrôle interne par la mise en place d'une organisation sécurisée et l'audit interne par l'identification des risques tout en faisant des recommandations pour leur traitement.

3.3.4 Le risque lié aux communications

« Il correspond au risque lié à la perte d'information par altération du support des données transmises par l'organisation (téléphone, télex, messagerie, réseaux informatiques, Internet…) » (Maders & al. 2009 :42), d'où le nom de « risque réseau » qui lui est souvent conféré.

3.4 Maîtrise des risques informatiques

L'informatique peut venir à son propre secours dans la maîtrise des risques. C'est le cas des inexactitudes de saisie, de transmission et d'utilisation de l'information et des erreurs d'exploitation.

3.4.1 Maîtrise des risques liés au système d'information

Pour maîtriser les risques liés à la disponibilité des données, il faut l'existence de :

- systèmes à tolérance de pannes ;
- redondances au niveau matériel et logiciel ;
- journal ou fichier de mouvements créés pour l'interactif ;
- d'images avant et après du fichier maître ou des enregistrements de mouvements pour faciliter la restauration ;
- logiciel de reprise permettant la restauration des fichiers dans l'état correspondant au dernier mouvement correctement traité ;
- traitement en fichier miroir créant des enregistrements en double et les stockant sur un disque différent (ou dans certains cas, à un autre emplacement), et cela à des fins de restauration.

Ces mesures permettent de diminuer le risque d'interruption de service ou d'arrêt du traitement.

Quant aux atteintes à la confidentialité, elles peuvent être maîtrisées par la mise en place de fonctions d'identification et d'authentification des utilisateurs. Ces fonctions peuvent être intégrées dans l'application proprement dite ou réalisées à travers un logiciel de contrôle d'accès. Les contrôles d'accès ont pour but de respecter la séparation des tâches. C'est le cas d'un utilisateur qui sera autorisé à consulter les données mais non à les modifier et vice versa. Les contrôles d'accès se font à travers l'utilisation de mots de passe. « Le logiciel interagit avec les demandes d'accès aux fonctions automatisées et autorise l'accès après saisie du numéro d'identification d'utilisateur et du mot de passe approprié » (IFACI, 1993 : 6).

Outre ces mesures, on peut prévoir la protection des menus et/ou des fonctions des systèmes applicatifs. La limitation de l'accès physique peut garantir que seuls les utilisateurs autorisés ont accès au système informatique. En voici quelques unes des techniques de contrôle des accès physiques :

- « les terminaux sont situés dans des endroits sûrs et surveillés ;
- des identifiants physiques tels que cartes ou clés sont nécessaires pour utiliser les terminaux. Ces cartes ou clés ne sont délivrées qu'aux personnes autorisées » (IFACI, 1993 : 7).

Pour maîtriser les atteintes liées à l'intégrité, il doit exister un schéma décrivant l'architecture des systèmes d'information (achats, ventes, stocks, comptabilité, trésorerie, immobilisations, paie/personnel….). « Il doit aussi exister des interfaces appropriées entre les systèmes et applications :

- absence de double saisie ;
- contrôle automatique des saisies ;
- contrôle des échanges de données (états d'exception, comptes rendus d'interfaces) » (Schick & al. 2004 : 51).

3.4.2 Maîtrise des études informatiques

Pour maîtriser les études informatiques, il faut :

- un engagement clair et une collaboration active de la direction ;
- l'intervention de gestionnaires de projets expérimentés ;

- une méthodologie adaptée, complétée par des procédures et des standards de développement appropriés ;
- un environnement de contrôle de qualité ;
- des budgets détaillés ;
- un planning détaillé des tâches ;
- une définition claire des responsabilités ;
- un suivi systématique écrit destiné à toutes les parties et notamment à la direction.

« La fiabilité des études préalables conditionne dans une large mesure le bon fonctionnement du système informatique » (Barry, 2004 : 242).

3.4.3 Maîtrise des risques sur les traitements informatiques

Différentes méthodes de protection de l'information sont utilisées pour maîtriser les risques sur les traitements informatiques. Ainsi, ne dit-on pas que : « qui sait garder son secret, connaît le chemin du succès ». Les techniques utilisées pour protéger les données vont de la cryptographie à la biométrie en passant par l'identification et l'authentification.

« L'identification est le processus par lequel l'utilisateur ou le service, fournit un identifiant unique pour justifier son identité.

L'authentification est le processus par lequel l'utilisateur ou le service, fournit une preuve de son identité (secret partagé, caractéristique physique, etc.) » (Calé & al. 2007 : 119).

A travers ces mécanismes, le système mis en place s'assure de l'identité de l'utilisateur en l'autorisant à accéder aux ressources, selon les droits qui lui ont été concédés.

L'utilisation de mot de passe caractérise les processus d'identification et d'authentification. Le mot de passe peut être statique ou dynamique (utilisable une seule fois). L'utilisation du mot de passe statique répond elle-même à des critères de sécurité comme :

- sa durée de validité ;
- le nombre de tentatives autorisées avant de « bloquer le compte » ;
- le nombre minimum de caractères devant composer le mot de passe ;
- la nature des caractères devant le composer (purement alphabétique, alphanumérique ou les deux avec insertion de caractères spéciaux) ;
- l'interdiction d'utiliser les noms propres, prénoms, noms de lieux et dates de naissance.

La biométrie quant à elle, « désigne l'ensemble des moyens qui permettent de s'assurer de l'identité d'une personne en fonction de caractéristiques morphologiques ou de traits comportementaux (écritures, etc.) qui lui sont propres» (Calé & al. 2007 : 122).

L'empreinte digitale, la forme et la taille de la main, le visage (écart entre les yeux, largeur de la bouche, etc.), le réseau sanguin de la rétine, la structure de l'iris sont certains des nombreux caractères physiologiques utilisés par la biométrie. Elle fait également usage de caractères comportementaux comme l'écriture (vitesse de déplacement, angle d'inclinaison du stylo, variation de la pression sur la feuille…), et la voix.

Malheureusement son coût de mise en œuvre est généralement élevé et le taux de reconnaissance n'est pas intégral (100%): cas d'une personne enrhumée devant utiliser un système de reconnaissance vocale. C'est aussi le cas d'un doigt qui n'est pas très propre ou qui comporte de légères coupures devant être reconnu par ses empreintes digitales. Telles sont des raisons parmi tant d'autres qui ont limité l'expansion de la biométrie.

Mais l'informatique, qui peut être à l'origine d'un certain nombre d'erreurs humaines, peut venir « à son propre secours », notamment si l'on a le bon sens de prévoir :

- des contrôles de robustesse (limite d'un champ de saisie évitant un débordement dans les champs suivants) ;
- des filets de sécurité (« une date d'expiration » qui suspend automatiquement un utilisateur dont le contrat se termine à une date précise).

3.4.4 Maîtrise des risques liés aux communications

Pour maîtriser les risques liés à la communication, les mesures suivantes s'imposent. Pour les fichiers sensibles, éviter les procédures de transferts de supports magnétiques « par porteurs ». Le fichier pourrait ne jamais arriver à son destinataire.

Pour éviter le risque de diffusion d'informations confidentielles, on prévoira par exemple que certains états sensibles soient édités en présence du responsable utilisateur de l'application.

Inclure dans les fichiers « sensibles » des pièges permettant de vérifier qu'ils n'ont pas été diffusés à l'extérieur. Lorsque des fichiers du genre sont susceptibles d'intéresser des entreprises ou organisations concurrentes, (fichiers clients ou fournisseurs), l'utilisation de pièges permet de mettre immédiatement en évidence toute utilisation non autorisée. Le piège

peut consister à inclure dans ledit fichier le nom et l'adresse d'un des dirigeants mal orthographiés.

Prévoir si nécessaire des procédures de validation de données contenues dans les fichiers sensibles. Le cas le plus connu est celui des fichiers de virement de paie transmis par les entreprises et organisations à leurs banques. Ils doivent contenir un enregistrement en-tête de totalisation, permettant de valider leur contenu. Cette méthode permet de confondre tout fraudeur (qui se trouve généralement dans la population informatique) qui modifierait le montant de son salaire sur le fichier virement sans penser à modifier l'enregistrement de totalisation.

Détruire systématiquement après utilisation des états contenant des informations sensibles au lieu de les mettre à la poubelle.

3.5 Modes de collecte de l'information

Les techniques de collecte d'informations généralement utilisées sont les suivantes :

- les techniques qualitatives ;
- les techniques quantitatives.

3.5.1 Les techniques qualitatives

Parmi les évaluations réalisées selon les techniques qualitatives, certaines sont exprimées en termes subjectifs tandis que d'autres le sont en termes objectifs. Toutefois, dans un cas comme dans l'autre, la qualité des évaluations dépend fortement des connaissances et du discernement des personnes qui ont en charge ces évaluations, de leur compréhension des événements potentiels et du contexte. Dans les techniques qualitatives, on distingue deux échelles d'évaluation : la classification et l'ordonnancement encore appelé hiérarchisation.
La classification consiste à regrouper les risques par catégories de type économique, technologique ou environnemental. Les nombres ne sont affectés aux événements qu'à des fins d'identification tout comme les numéros figurant sur les maillots des joueurs d'une équipe sportive, et les éléments (joueurs) ne peuvent être ni classés par ordre d'importance (complémentarité oblige), ni hiérarchisés, ni additionnés.
L'ordonnancement ou hiérarchisation consiste à classer les événements par ordre d'importance. Les éléments sont alors qualifiés « d'élevés », de « moyens », de « faibles » ou

de tout autre qualificatif approprié. Ainsi, le management peut établir que l'élément 1 est supérieur à l'élément 2. C'est le cas par exemple que le management évalue la probabilité qu'un nouveau virus informatique vienne perturber ses systèmes soit supérieur à la probabilité que des collaborateurs non autorisés transmettent des informations confidentielles.

Nous proposons ci-dessous un exemple de hiérarchisation de risques dans une échelle de probabilités relative à des événements affectant les activités informatiques. Cet exemple est tiré du COSO II REPORT.

Tableau n° 1 : « Exemple de hiérarchisation des risques »

Niveau	Qualificatif	Probabilité de survenue	Risque
1	Rare	Très faible	Panne prolongée du système du fait d'actes terroristes ou délibérés
2	Improbable	Faible	Catastrophe naturelle ou événement provoqué par un tiers (société de service public) obligeant à avoir recours au plan de continuité
3	Possible	Modérée	Sécurité informatique attaquée par des pirates
4	Probable	Elevée	Le personnel utilise les ressources de l'organisation pour accéder à des informations non appropriées sur Internet
5	Presque sûr	Très élevée	Le personnel utilise les ressources de l'organisation à des activités de messagerie privée.

Source : COSO II REPORT (2009 : 208)

3.5.2 Les techniques quantitatives

Elles sont utilisées lorsqu'il existe suffisamment d'informations permettant d'estimer la probabilité d'occurrence ou l'impact d'un risque sur la base d'évaluations par intervalle ou par ratio. Les méthodes quantitatives intègrent des techniques statistiques, les techniques non statistiques et de benchmarking. L'aspect le plus important des techniques quantitatives est de tenir compte de la disponibilité de données fiables quelques soient leurs sources (interne ou externe).

Les techniques statistiques : elles évaluent la probabilité d'occurrence et l'impact d'une série de résultats sur la base d'hypothèses de comportements des événements.

Les techniques non statistiques sont utilisées afin de quantifier l'impact d'un événement potentiel sur la base d'hypothèses mais sans affecter la probabilité de survenance de l'événement. Elles comportent l'analyse par sensibilité et l'analyse par scénario.

L'analyse de la sensibilité est utilisée pour évaluer l'impact des variations normales, des paramètres influençant les événements potentiels. Il peut s'agir par exemple des évaluations de risques opérationnels comme l'effet sur le volume des ventes, du temps de réponse du centre d'appel ou du nombre de défauts de fabrication.

Le benchmarking est défini comme « un processus de recherche, d'échange et d'utilisation des bonnes pratiques » (Bilodeau, décembre 2002 : 42). Yves Bilodeau poursuit en disant que « la recherche c'est l'étude des organisations, des processus, de méthodes. L'échange c'est la réciprocité des informations, l'interaction. L'utilisation c'est l'aboutissement, la mise en œuvre des résultats. Les bonnes pratiques sont le fruit du savoir-faire, de l'expérience ; elles sont du domaine du concret et non du concept ».

3.6 Les critères de cotation des risques informatiques

Elle consiste à classer les risques selon leur gravité. On distingue généralement quatre classes de risques : le risque catastrophique, le risque critique ou grave, le risque significatif ou majeur et le risque mineur ou négligeable.

Le risque catastrophique : il correspond au risque qui a des conséquences telles que de dommages importants sur l'homme comme la mort, l'invalidité et des blessures graves ; mais aussi la destruction totale du système et/ou de son environnement.

Le risque critique ou grave : on lui associe les conséquences telles que :

- blessures graves non permanentes ;
- destruction partielle ou indisponibilité importante du système ;
- arrêt d'un projet ou d'une activité.

Le risque significatif ou majeur est celui qui a des conséquences comme :

- blessures légères ;
- arrêt de la mission sans destruction ou indisponibilité importante.

Le risque mineur ou négligeable comme son nom l'indique correspond au risque dont les conséquences sont de moindres importances voire négligeables. On cite à titre d'illustration :

- la perte de redondance ;

- la perte de confort.

A la gravité, est associée la survenance. La survenance est elle aussi de quatre ordres avec au bas de l'échelle la survenance improbable, suivie de la survenance rare, elle-même suivie de la survenance occasionnelle et au sommet la survenance fréquente.

La cote du risque est obtenue en multipliant la probabilité de survenance par sa gravité. La cote à attribuer aux risques se fait de 1 (un) à 5 (cinq). Cinq représente la cote la plus élevée et un la cote la plus faible. Les cotes se lisent dans un tableau appelé matrice d'appréciation que d'autres appellent aussi « Diagramme gravité-survenance des risques » dont nous reproduisons ci-dessous un exemple.

Figure n°1: « Diagramme Gravité-Survenance et Risques »

SURVENANCE				
Fréquent	X	X	X	X
Occasionnel	X	X	X	X
Rare	X	X	X	X
Improbable	X	X	X	X
	Négligeable	Marginal	Critique	Catastrophique **GRAVITE**

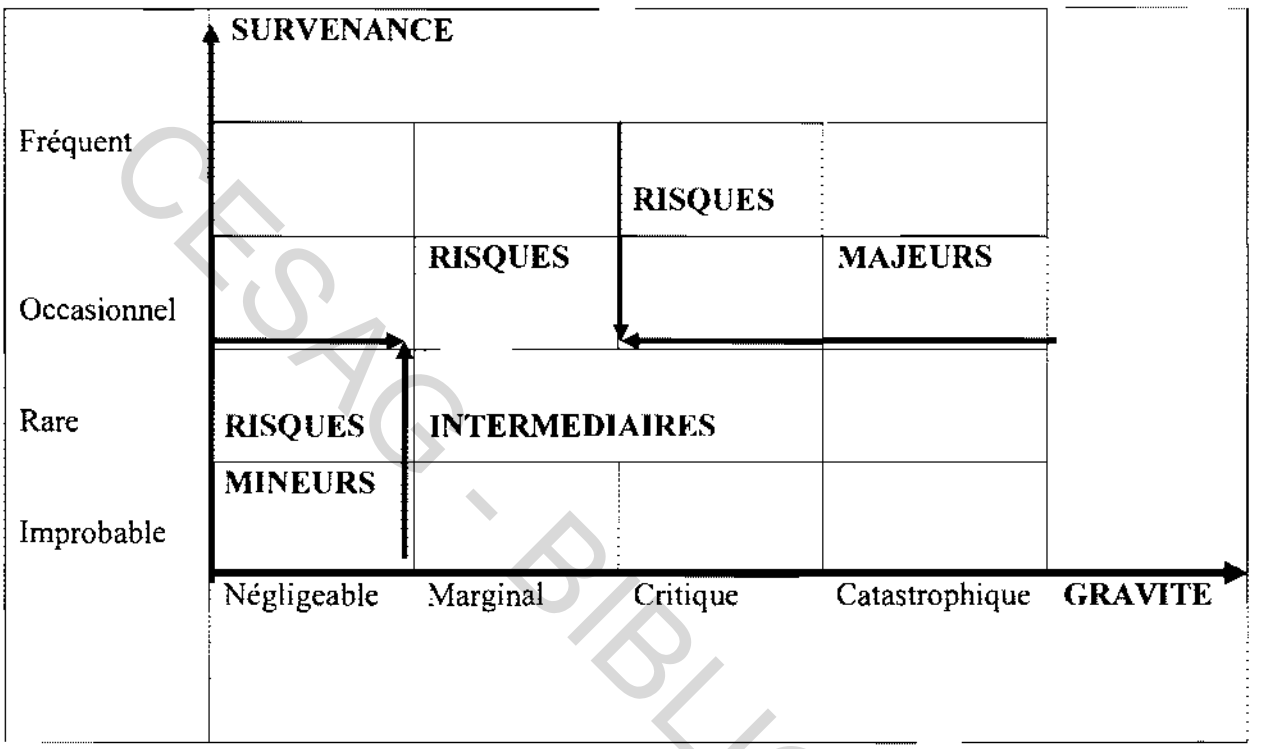
Source : NGUEMA Octave Jokung (2008 : 135)

Une analyse des risques classés suivant leur gravité et leur survenance conduit à les classer en trois catégories :

- risques majeurs ;
- risques intermédiaires ;
- risques mineurs.

Cette classification est faite suivant le jugement de la Direction Générale et des spécialistes de la gestion des risques de l'organisation. Ce qui nous conduit au « Diagramme Gravité-Survenance et Classes ».

Figure n°2 : « Diagramme Gravité-Survenance et Classes »

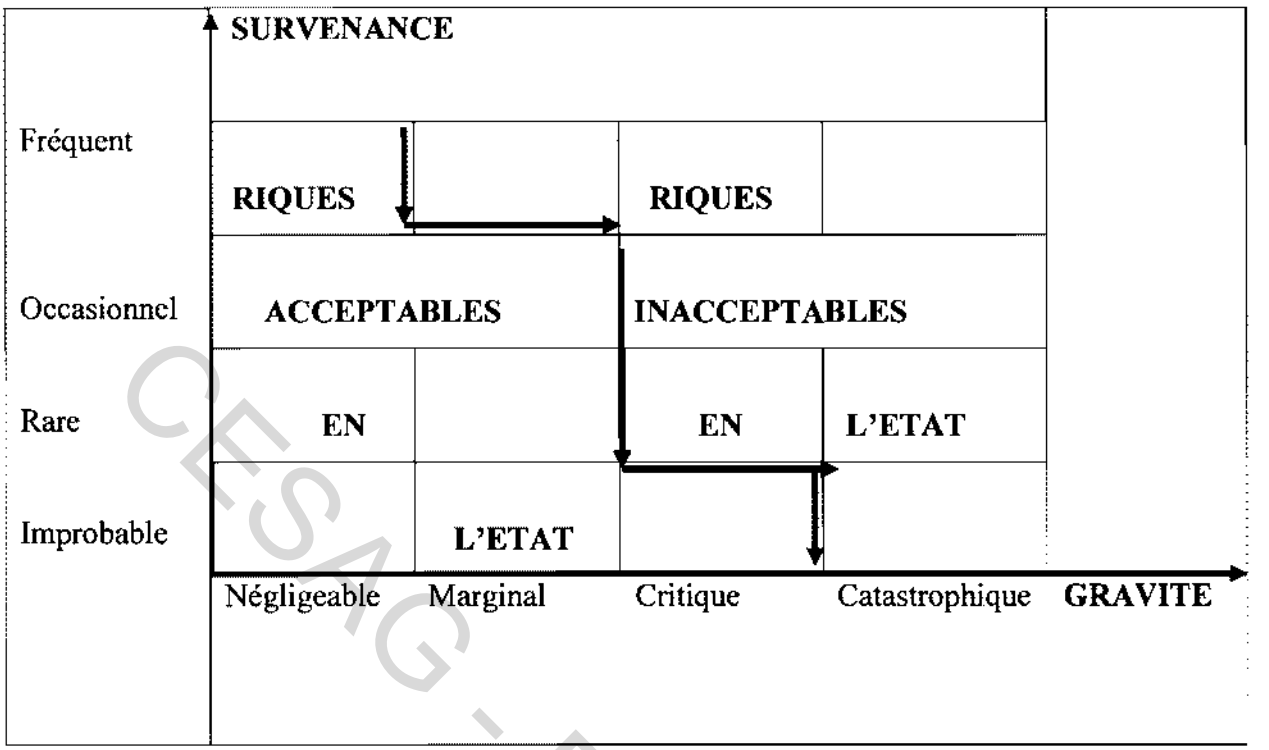


Source : NGUEMA Octave Jokung (2008 : 136)

Cette classification conduit à la notion d'appétence pour le risque. L'appétence pour le risque est le niveau de risque qu'une organisation est prête à accepter dans le cadre de sa mission (ou de sa vision).

Ainsi, suivant les objectifs de l'organisation, la Direction Générale et les spécialistes de la gestion des risques (risk managers s'il en existe) indiqueront les limites acceptables pour tel ou tel risque. Ce qui conduit à une classification en risques acceptables en l'état et en risques non acceptables. Ces derniers devront être réduits par des traitements appropriés d'où le « Diagramme Gravité-Survenance et Acceptabilité ».

Figure n°3 : « Diagramme Gravité-Survenance et Acceptabilité»



Source : NGUEMA Octave Jokung, (2008 : 137)

Le COSO II REPORT (le mangement des risques de l'entreprise) devenu une référence internationale en matière de gestion des risques, remplace dans notre schéma l'abscisse « survenance » par « impact » et l'ordonnée « gravité » par « probabilité ». La probabilité est alors soit improbable, soit possible, soit probable, soit presque certain. Quant à l'impact, il est soit mineur, soit modéré, soit majeur.

En plus des mesures ci-dessus citées pour maîtriser les risques informatiques, il existe des méthodes de gestion et d'analyse desdits risques. Parmi elles, on peut citer EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) et MEHARI (Méthode Harmonisée d'Analyse de Risques) (Desroches & al. 2007 : 207).

EBIOS est une méthode développée et maintenue en France par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information). Créée en 1995, elle se compose de cinq guides (Introduction, Démarche, Techniques, Outillages pour l'appréciation des risques, Outillages pour le traitement des risques) et d'un logiciel support. La méthode a pour objectif principal de permettre à tout organisme, notamment ceux de l'Etat de déterminer les actions

de sécurité qu'il convient d'entreprendre. EBIOS convient pour un système déjà existant ou à concevoir.

OCTAVE est publié par le Software Engineering Institute (SEI) de la Carnegie Mellon University, reconnue dans le domaine de la sécurité des SI (fédération des Computers Emergency and Reponse Team – CERTS). Cette méthode repose sur la possibilité de réaliser une analyse des risques de l'intérieur de l'organisation, exclusivement avec des ressources internes.

MEHARI (Méthode Harmonisée d'Analyse de Risques) est dérivée de MARION (Méthode d'Analyse des Risques Informatiques Optimisée par Niveau). Cette migration a été faite en 1997 par le CLUSIF (Club de la Sécurité des Systèmes d'Information Français), concepteur des deux méthodes.

En conclusion, les caractéristiques de l'environnement informatique d'une entité peuvent entraîner un risque inhérent élevé et avoir une conséquence à terme sur la continuité de l'exploitation. Une organisation fortement dépendante de son informatique peut voir remise en cause son activité en cas de défaillance majeure survenant dans son système d'information.

C'est ainsi que dans certains domaines, certaines organisations ont vu leur activité connaître un dysfonctionnement.

Dans le domaine des médias, le matin du 22 octobre 2002, pas de « Libération », pas d'« Humanité », ni d'« Echos », ni de « France Soir », ni de quotidiens régionaux dans les kiosques parisiens. Une panne informatique aux nouvelles messageries de la presse parisienne retarde la distribution et empêche les chroniqueurs de faire leur travail.

Dans le domaine des transports, le 28 septembre 1998, la ville de Dublin (Suède) connaît un embouteillage monstrueux parce que la mise à jour de feux tricolores a abouti à la déconnexion de 140 (cent quarante) carrefours.

Le 4 juin 1996, pour parler du domaine spatial, et peut être de l'incident le plus spectaculaire, lors du premier lancement d'Ariane 5, une erreur informatique modifie la trajectoire du lanceur et impose de le détruire en vol (Desroches & al. 2005 : 192).

Le contrôle interne de l'assistance informatique ne diffère pas fondamentalement du contrôle interne des autres activités. Elle conserve tout de même ses spécificités par rapport à d'autres activités. On pourrait fondamentalement noter comme différence l'automatisation de certaines tâches que l'on appelle couramment les tâches programmées. Il peut s'agir de

l'interface entre deux ou plusieurs applications qui s'exécutent à partir d'une période donnée de la journée, ou des sauvegardes qui s'exécutent à la fin d'une journée de travail. Ces sauvegardes peuvent s'effectuer sur un même site géographique ou sur des sites différents d'un serveur à un autre.

Quant à la séparation des fonctions, elle est elle-même exigée par la fonction informatique. Ainsi, la gestion des bases de données, la gestion de réseaux et la gestion de la sécurité sont généralement des tâches distinctes. On pourrait aussi parler au niveau de l'organisation générale du service, de séparation de fonctions « études-exploitation-utilisateurs ».

A l'intérieur même d'une de ses fonctions comme la gestion des bases de données, la séparation existe par les contrôles hiérarchiques. Dans ce cas, l'enregistrement d'une opération et sa validation sont assurées par des personnes distinctes.

Qu'en est-il alors des risques ? Ils sont pour la plupart des risques inhérents c'est-à-dire liés à l'activité informatique. On pourrait citer entre autres les risques d'accès non autorisés au réseau, l'indisponibilité d'un support de transmission de données, risque de sanctions pénales en cas d'utilisation de logiciels sans licence, risque de détérioration du parc existant en cas de présence de virus, etc.

L'assistance informatique doit permettre de prendre des mesures préventives afin de juguler les différents risques capables de nos jours, de mettre en péril l'intégrité des données de l'organisation. Elle doit aussi permettre la production d'informations fiables tout en restant à l'écoute des utilisateurs.

CHAPITRE IV - APPROCHE METHODOLOGIQUE DE MAITRISE DES RISQUES INFORMATIQUES

Ce chapitre a pour objet de présenter la méthodologie de recherche. Celle-ci s'est effectuée à travers le modèle d'analyse, les techniques de collecte des données et les outils d'analyse de ces données. Le modèle d'analyse que nous avons utilisé est inspiré du système RADAR. Parmi les techniques de collecte de données, nous avons fait usage de l'analyse documentaire, de l'échantillonnage statistique, des interviews, de l'observation physique et de la narration. Pour analyser ces données, des questionnaires de contrôle interne dont des modèles sont joints en annexe ont été utilisés. Le tableau d'identification des risques développé au chapitre 7, paragraphe 7.9.6.1 a servi de base à la construction de la cartographie des risques informatiques.

4.1 Modèle d'analyse

Il est inspiré du système RADAR (Resources of Audit Department Allocated by Risk) (Rénard, 2010 : 406). Ce modèle repose sur l'appréciation du contrôle interne. Un contrôle interne formalisé, et appliqué de façon permanente est considéré comme minimisant sensiblement tout risque. Ainsi, avons-nous utilisé une échelle de valeur à trois niveaux :

- contrôle interne adapté coté à un (1) point ;
- contrôle interne insuffisant coté à trois (3) points ;
- contrôle interne inexistant coté à cinq (5) points.

L'autre composante du système RADAR que nous avons utilisé est l'appréciation de la fréquence du risque. C'est une appréciation qualitative et repose sur la vulnérabilité de l'unité auditée. Elle est jugée subjective car c'est l'auditeur même qui la détermine à partir des informations recueillies. Nous avons retenu trois niveaux de vulnérabilité :

- vulnérabilité faible coté à un (1) point ;
- vulnérabilité moyenne coté à trois (3) points ;
- vulnérabilité forte coté à cinq (5) points.

Le coefficient du risque est obtenu en multipliant le niveau de contrôle interne par la vulnérabilité. Trois niveaux de coefficient du risque ont été retenus :

- risque minimal avec coefficient du risque allant de un (1) à cinq (5) points ;
- risque moyen avec coefficient du risque allant de neuf (9) à quinze (15) points ;

- risque maximal avec coefficient du risque allant de seize (16) à vingt cinq (25) points.

4.2 Techniques de collecte des données

Pour mener à bien notre mission, les techniques suivantes de collecte de données ont été utilisées : l'analyse documentaire, l'échantillonnage statistique, l'interview, l'observation physique et la narration.

4.2.1 L'analyse documentaire

Elle a consisté à l'analyse de certaines procédures écrites. Force est de reconnaître que la CAISFF en manque énormément. Mais certains processus comme nous l'avons décrit au chapitre un, bénéficient de procédures clairement définies. Parmi eux, on peut citer la sauvegarde /restauration, la sécurité et l'architecture.

Quant à d'autres processus comme la gestion du parc informatique, elle est faite en tenant compte de la réglementation relative au code des marchés publics et de la comptabilité- matières. Des activités de ce processus, celles relevant du domaine du code des marchés publics sont : la livraison et la réception d'équipements informatiques, la gestion de la garantie. S'agissant de l'affectation de ces matériels, la mise au rebut du matériel retiré d'inventaire, le retrait d'équipements du parc informatique, le suivi du parc informatique (entrées / sorties), relèvent de la comptabilité-matières. En République du Mali, cette discipline qu'est la comptabilité-matières dispose d'un manuel de procédures.

Précisons aussi que le processus réunions/présentations bénéficie en partie des dispositions du code des marchés publics en ce qui concerne son activité dépouillement des offres.

.Les autres processus ne disposent pas de procédures écrites.

4.2.2 Le sondage statistique

« Le sondage statistique (ou sondage aléatoire, ou échantillonnage) est une technique qui permet, à partir d'un échantillon prélevé aléatoirement dans une population de référence, d'extrapoler à la population les observations effectuées sur l'échantillon, avec une certitude spécifiée et une précision désirée » (Lemant & al. 1995 : 215).

« Par population il faut entendre l'ensemble de référence, c'est-à-dire l'ensemble des unités observées. Elle est composée d'individus ou d'unités statistiques.

Un individu ou une unité statistique est tout élément de la population.

L'effectif total est le nombre d'unités statistiques ou d'individus observés.

Le caractère est l'aspect particulier de l'individu auquel on s'intéresse. Il peut être quantitatif ou qualitatif. S'il est quantitatif, il peut être discret ou continu. Un caractère est qualitatif s'il est lié à une observation ne faisant pas l'objet d'une mesure » (Chauvat & al. 1996 : 3 – 4).

Exemple : la population malienne peut être caractérisée par :

- le sexe (masculin ou féminin) ;
- l'état matrimonial (célibataire, marié, veuf, divorcé).

Un caractère est quantitatif s'il est mesurable. Il est :

- discret si les valeurs observées sont isolées ;
- continu s'il peut prendre toute valeur d'un intervalle réel.

On traite comme caractère continu tout caractère discret dont on a regroupé les valeurs dans des classes.

Notre population était composée d'informaticiens de la CAISFF, de ceux des Cellules informatiques du MEF et des utilisateurs. Une partie de cette population prise par structure du MEF a constitué notre échantillon.

4.2.3 Les interviews (entretiens)

« Une interview est un entretien avec une personne en vue de l'interroger sur ses actes, ses idées, etc… et de divulguer la teneur de l'entretien…..C'est une technique de recueil d'informations qui permet l'explication et le commentaire, et donc apporte une plus-value importante à la collecte des informations factuelles et des éléments d'analyse et de jugement :

- informations factuelles : communication de données chiffrées sur un marché, une affaire, présentation d'un document probant… ;
- éléments d'analyse : expression par l'audité de ses préoccupations par rapport à des faits constatés… ;
- éléments de jugement : appréciation d'un fait dans un environnement (connaissiez-vous telle décision lorsque vous avez négocié telle affaire ?), commentaire d'un résultat, mise en évidence d'une situation exceptionnelle… » (Lemant & al. 1995 : 181).

Nous avons demandé des interviews dans le but d'obtenir des informations se rapportant à l'assistance informatique de la CAISFF. Ces interviews ont concerné les informaticiens des Cellules informatiques auprès des directions du MEF, ceux de la CAISFF et les utilisateurs des applications développées par la CAISFF ou dont la maintenance est

effectuée par elle. Un extrait de la liste des personnes qui nous ont accordé des interviews figure à l'annexe n° 4, page 114.

4.2.4 L'observation physique

« L'observation physique est une technique de contrôle qui consiste à examiner la façon dont une procédure est exécutée au sein de l'entité….il s'agit d'observer (ni de compter, ni de questionner, ni d'analyser des documents» (Obert & al. 2008 : 187).

Notre observation ne s'est pas faite de façon clandestine. Elle s'est réalisée conformément à notre calendrier de rotation. Par exemple un temps creux entre deux interviews a été mis à profit pour observer les insuffisances ou les dysfonctionnements du système informatique. Nous avons par là pratiqué de l'observation directe constatant par nous-mêmes lesdits insuffisances ou dysfonctionnements sans intermédiaire et la réactivité de la CAISFF à assister les directions du MEF dans la résolution des problèmes posés.

4.2.5 La narration

Elle a pour but de faire décrire par l'audité un cadre général alors que l'interview a lieu dans un but bien précis. Contrairement à l'interview qui est préparée, la narration ne le nécessite pas car il s'agit de donner la parole à l'audité. L'auditeur se contentera de l'écouter et de noter s'il le faut de façon intégrale, la narration de son interlocuteur.

L'audit nécessitant toujours un climat de confiance, « laisser parler les gens est encore le meilleur moyen d'obtenir leur adhésion » (Rénard, 2010 : 355). Nous avons de ce fait demandé à nos interlocuteurs de nous décrire de façon générale l'assistance que les apporte la CAISFF sur le plan informatique.

La narration rapporte toujours plus d'informations que l'on ne s'y attend. Ces informations supplémentaires, pourront ultérieurement servir l'auditeur dans ses investigations.

4.3 Les outils d'analyse des données

Les outils d'analyse que nous avons utilisés ont été les questionnaires de contrôle interne et le tableau d'identification des risques.

4.3.1 Les questionnaires de contrôle interne

« Le Questionnaire de Contrôle Interne est une grille d'analyse dont la finalité est de permettre à l'auditeur d'apprécier le niveau et de porter un diagnostic sur le dispositif de contrôle interne de l'entité ou de la fonction auditée. Il est composé d'une liste de questions n'admettant en principe que les réponses « oui » ou « non », qui servent à recenser les moyens en place pour atteindre les objectifs du contrôle interne » (Lemant & al. 1995 : 195).

Ces questionnaires ont été administrés à des responsables informatiques, à des chefs de divisions ou à des utilisateurs. Deux méthodes ont été utilisées pour l'administration des questionnaires : distribuer le questionnaire sur support papier à un échantillon choisi pour qu'il le remplisse, ou l'intégrer aux guides d'entretien pour les interviews. Un extrait de la liste des personnes qui nous ont accordé des interviews figure à l'annexe n°4, page 114. Quant au guide d'entretien, un modèle est représenté à l'annexe n°5, page 116.

4.3.2 Le tableau d'identification des risques

Il est développé au chapitre 7, paragraphe 7.9.6.1. C'est le même tableau qui nous a servi à établir la cartographie des risques informatiques. Par rapport aux processus identifiés, les risques se rapportent : à la déontologie ; au système d'information ; au patrimoine ; à l'informatique ; à l'image ; à l'administration ; à la pédagogie.

Les outils ci-dessus décrits sont d'une importance capitale. Ils auront servi à la mise en œuvre de la deuxième partie de ce mémoire. D'autres outils dont nous n'avons pas parlé compte tenu de leur inexistence à la CAISFF méritent d'être mentionnés. Il s'agit de l'organigramme hiérarchique à partir duquel nous aurions pu construire l'organigramme fonctionnel. Ce dernier révèle la totalité des fonctions existantes et permet d'aller voir, si on trouve leur traduction dans les analyses de postes.

La grille d'analyse des tâches quant à elle, permet de relier l'organigramme fonctionnel à l'organigramme hiérarchique et justifier les analyses de postes (Rénard, 2010 : 335 – 336).

Conclusion Première Partie

Que ce soit les processus de l'assistance informatique (chapitre 1), le contrôle interne de l'assistance informatique (chapitre 2), la maîtrise des risques informatiques (chapitre 3), la sécurité, même si elle n'est pas abordée de la même manière, est au cœur de tout le système informatique. Ainsi, l'achat d'un logiciel avec licence d'exploitation a-t-il pour but d'éviter non seulement des poursuites judiciaires, mais aussi d'éviter la propagation de virus dans le système informatique. La naissance des virus même a augmenté l'ingéniosité de l'homme en se prémunissant de parades contre eux pour mieux se sentir en sécurité (les antivirus). « Ces attaques de virus, vers, chevaux de Troie, etc., qui peuvent détruire, détériorer les fichiers, mais qui jouent aussi un rôle d'espion et permettent à un hacker de s'introduire dans une entreprise pour obtenir des informations spécifiques » (Bertin, 2007 : 256).

Un des objectifs du contrôle interne est la sauvegarde des actifs. Beaucoup de points évoqués au chapitre 2 rentrent dans ce cadre.

La maîtrise des risques quant à elle, a pour but d'anticiper sur tout événement pouvant empêcher l'atteinte des objectifs.

De ce fait, nous pensons que « les sept (7) principes d'action de sécurité se doivent d'être connus et appliqués :

principe n°1 : la sécurité des personnes doit primer sur toute autre considération,

principe n° 2 : il vaut mieux prévenir que guérir,

principe n° 3 : la voix de la sécurité est indépendante,

principe n° 4 : la sécurité d'ensemble est la résultante organisée des efforts de chacun,

principe n° 5 : errare humanum est perseverare diabolicum,

principe n° 6 : l'effort de sécurité doit être adapté aux objectifs,

principe n° 7 : les résultats de l'effort de sécurité se mesurent » (Desroches & al. 2005 : 19).

Les décideurs, les concepteurs et les exploitants doivent les avoir à l'esprit avant toute considération de performance, de coût et de délai.

PARTIE II – CADRE PRATIQUE

INTRODUCTION

Dans cette deuxième partie, nous présenterons la CAISFF et les services financiers et fiscaux. L'objectif ici est de cerner les missions de la CAISFF et de celles des services financiers et fiscaux qu'elle encadre sur le plan informatique. Ceci nous conduira aux constats et recommandations par direction du MEF.

Dans cette partie, les applications conçues ou maintenues de façon évolutive par la CAISFF seront décrites. Cette description a pour but de mettre en exergue l'apport de la CAISFF dans l'assistance des services financiers et fiscaux.

Nous décrirons par la suite l'existant pour mettre en relief les forces et les faiblesses du contrôle interne au niveau de la structure auditée : la CAISFF. Une cartographie des risques par rapport à la fréquence des événements et au dispositif de maîtrise des risques sera proposée.

CHAPITRE V - PRESENTATION DE LA CAISFF ET DES SERVICES FINANCIERS ET FISCAUX

L'information comptable et financière est tant pour les organisations de taille réduite que pour les Etats, un instrument de gestion et de bonne gouvernance. D'une part, il doit permettre la prise de décisions stratégiques. De ce fait, leur caractère fiable, intègre et exhaustif ne doit faire l'objet d'aucun doute.

D'autre part, les partenaires au développement desdits Etats (FMI et BM) accordent tellement d'importance à sa fiabilité, que leur aide en est souvent dépendante. D'où toute l'importance que nos Etats accordent à sa production, au respect de sa périodicité de production et tout ce qui peut faire que cette information soit irréprochable. C'est à cette tâche que les services financiers et fiscaux et la CAISFF du Mali doivent s'atteler.

5.1 Présentation de la CAISFF

Avant la mise en place de la CAISFF, les différentes directions composant le Ministère des Finances ont évolué de manière autonome et sans aucune coordination dans leurs projets d'informatisation. Devant les priorités comme :

- disposer d'informations comptables et financières rapides et fiables ;
- améliorer le niveau des recettes fiscales ;
- assurer une meilleure gestion des dépenses publiques ;
- renforcer la maîtrise de la masse salariale et des dépenses publiques en général ;
- apurer le fichier du personnel de la Fonction Publique et celui du Bureau Central des Soldes (BCS) afin de mettre en place un fichier unique du personnel ;
- moderniser la préparation, l'exécution et le suivi du budget ;
- moderniser la gestion des contribuables et des impôts au sein de la Direction Générale des Impôts (DGI) ;
- moderniser l'administration fiscale de l'Etat ; la création d'une structure s'imposait.

C'est pour pallier cette insuffisance que la Cellule d'Appui à l'Informatisation des Services Financiers et Fiscaux a été créée par Décision N°00111/MFC-CAB du 20 juillet 1994. Elle est chargée d'animer et de coordonner l'ensemble des activités se

rapportant à l'informatisation des services du Ministère des Finances et plus particulièrement les administrations fiscales et financières.

5.2 Mission et objectifs

Elle a pour fonction de:

- définir les politiques et orientations en matière d'informatisation,
- assurer la coordination des différents projets d'informatisation financés par les partenaires au développement dans les différentes structures du département des Finances,
- définir et suivre l'application de la politique de normalisation au niveau des équipements, de la sous-traitance, des progiciels, des outils de développement, des méthodes, de la qualité, des systèmes d'information, de la maintenance des matériels et des progiciels, de la formation, des réseaux informatiques, de la sécurité et des projets,
- examiner tous les rapports ayant trait aux activités d'information ;
- conseiller le ministre sur tous les problèmes se rapportant à l'informatique et aux Nouvelles Technologies de l'Information et de la Communication (NTIC) ;
- établir un réseau informatique interconnecté, performant, sécurisé et évolutif entre les différents services financiers et fiscaux ;
- relever le niveau de fonctionnement des centres informatiques existants dans les différentes directions (Direction Générale des Douanes DGD, Direction Nationale du Trésor et de la Comptabilité Publique DNTCP, Direction Générale du Budget DGB, Direction Générale des Impôts DGI, Direction Nationale du Contrôle Financier DNCF, Direction Administrative et Financière DAF, etc. ;
- établir un réseau de communication avec les usagers ;
- aménager un centre informatique central facilitant l'intégration fonctionnelle des systèmes d'information du Ministère des Finances ;
- établir un schéma directeur informatique pour le département des finances.

5.3 Activités

Les activités de la CAISFF consistent à apporter un appui aux différentes directions du MEF pour leur permettre d'atteindre les objectifs qui sont les leurs. Cet appui se fait sous deux formes : l'appui technique et l'appui matériel.
L'appui technique comporte trois variantes : la variante détachement, la variante de correspondance et la variante d'appui ponctuel.

Quant à l'appui matériel, il se fait dans la limite du budget alloué à la CAISFF, tant les besoins sont élevés et les ressources malheureusement limitées. L'appui peut concerner les matériels informatiques (ordinateurs, imprimantes, etc.) et les matériels de communication communément appelés matériels de réseau (routeurs, radios etc.). Les appuis en matériels informatiques nous ont été signalés au niveau de la DAF. L'appui très précieux en matériels de communication a eu lieu en début d'hivernage 2010 lorsque la pilonne du Centre VI des impôts a été victime des intempéries. Des radios et des routeurs et divers matériels de communication ont été fournis par la CAISFF, un Centre des impôts ne pouvant rester sans encaisser de recettes.

5.4 Structure organisationnelle

Nous n'avons pu nous procurer ni d'organigramme, ni de manuel de procédures de la CAISFF. Ce qui constitue une faiblesse du contrôle interne au niveau de la CAISFF qu'il conviendrait de combler sans délai.

5.5 Présentation des Services Financiers et Fiscaux

Les services visités sont : la DAF, la DNCF, la PGT, la DGI , la DGD et la DGB.

5.5.1 Direction Administrative et Financière (DAF)

La Direction Administrative et Financière (DAF) a été créée par la Loi N°88-47/AN-RM du 05 avril 1988. Si la structure fonctionne toujours au moment de notre passage (suivant notre calendrier de stage du 14 au 16 septembre 2010) sous cette appellation, des changements ont déjà été entrepris en vue de la scinder en Direction des Ressources Humaines d'une part et en Direction des Finances et du Matériel d'autre part.

La Direction des Ressources Humaines est créée par l'Ordonnance N°09-009/ P-RM du 04 mars 2009 auprès d'un département ou d'un groupe de départements ministériels. Elle est chargée de :

- concevoir et mettre en œuvre les plans et programmes de développement des ressources humaines ;
- appliquer la législation régissant les ressources humaines ;
- assurer la gestion des cadres organiques des services du département ou du groupe de départements ministériels ;
- assurer le suivi du système d'information et de communication sur les ressources humaines ;
- apporter un appui-conseil aux chefs de service du département ou du groupe de départements ministériels dans le domaine de la gestion des ressources humaines ;
- assurer le suivi et le développement du dialogue social.

Le Décret N°09 136/ P-RM du 27 mars 2009 fixe les modalités d'organisation et de fonctionnement de la Direction des Ressources Humaines.

Ainsi, au titre de l'Organisation et de la Direction, la Direction des Ressources Humaines est dirigée par un Directeur nommé par décret pris en Conseil des Ministres, sur proposition du Ministre compétent.

Le Directeur des Ressources Humaines est chargé sous l'autorité du Ministre, de diriger, programmer, coordonner et contrôler les activités de service. Il est assisté d'un adjoint qui le remplace de plein droit en cas de vacance, d'absence ou d'empêchement.

Le Directeur adjoint est nommé par arrêté du Ministre. Le même arrêté fixe également ses attributions spécifiques.

Le Décret N°09 137/ P-RM du 27 mars 2009 fixe les modalités d'organisation et de fonctionnement de la Direction des Finances et du Matériel.

Au titre de l'Organisation et de la Direction, la Direction des Finances et du Matériel est dirigée par un Directeur nommé par décret pris en Conseil des Ministres, sur proposition du Ministre compétent.

Le Directeur des Finances et du Matériel est chargé sous l'autorité du Ministre, de diriger, programmer, coordonner et contrôler les activités de service. Il est assisté d'un adjoint qui le remplace de plein droit en cas de vacance, d'absence ou d'empêchement.

Le Directeur adjoint est nommé par arrêté du Ministre. Le même arrêté fixe également ses attributions spécifiques.

5.5.2 Direction Nationale du Contrôle Financier (DNCF)

L'Ordonnance N° 85-30-PRM du 19 Décembre 1985 crée un service central dénommé Direction Nationale du Contrôle Financier en République du Mali.

Aux termes de l'article 2 de l'Ordonnance ci-dessus citée, la Direction Nationale du Contrôle Financier a pour missions de:

- assurer le contrôle permanent des finances de la République du Mali (Budget d'Etat, Budgets Annexes, Budget des Collectivités et tous autres Budgets et Comptes Publics ainsi que les opérations de trésorerie correspondantes) ;
- exercer un contrôle financier au sein des entreprises nationalisées, des sociétés d'Etat, des Offices, des Régies, des sociétés d'économie mixte et des Etablissements Publics ;
- informer et de conseiller le Ministre chargé des Finances, pour tout projet de réglementation, d'instruction ou de décision ayant des répercussions sur les finances de la République du Mali.

Les modalités de fonctionnement et les règles d'organisation de la Direction Nationale du Contrôle Financier sont fixées par le Décret N° 04-546 P – RM du 23 Novembre 2004.

Ainsi, la DNCF comprend :

- au niveau central :
  - en staff, la Cellule de Documentation et de l'Informatique chargée de :
  - rechercher, reproduire et archiver toute documentation nécessaire à l'accomplissement des missions de la Direction Nationale du Contrôle Financier ;
  - suivre l'informatisation du service et la maintenance du matériel informatique ;
  - en live :
  - la Division Contrôle de Dépenses ;
  - la Division Organismes Personnalisés ;
  - la Division Situations Périodiques et Analyses.

5.5.3 Paierie Générale du Trésor (PGT)

La PGT est créée par l'Ordonnance du 04 mars 2002. Comme service rattaché, la PGT a pour mission :

- l'exécution des dépenses ordonnancées et sans ordonnancement préalable de l'ordonnateur principal, des ordonnateurs secondaires ministériels du Budget national ;

- l'exécution des recettes et des dépenses des comptes spéciaux ;
- la centralisation et l'intégration des opérations des postes comptables des représentations diplomatiques et consulaires.

La PGT est dirigée par un Payeur Général nommé par décret pris en Conseil des Ministres, sur proposition du ministre chargé des Finances.

5.5.4 Direction Générale des Impôts (DGI)

La DGI est créée par l'Ordonnance N°02- 058/ P-RM du 05 juin 2002. La DGI a pour mission d'élaborer et de veiller à la mise en œuvre des éléments de la politique nationale en matière de fiscalité intérieure. A cet effet, elle est chargée de :

- préparer la réglementation fiscale relative aux impôts, droits et taxes intérieures et d'en assurer l'application ;
- asseoir, liquider, contrôler et recouvrer les impôts, droits et taxes intérieures perçus au profit de l'Etat ou, le cas échéant, des collectivités territoriales et des organismes publics ou parapublics ;
- gérer le contentieux fiscal.

Le Décret N°02-332/ P-RM du 06 juin 2002 fixe les modalités d'organisation et de fonctionnement de la DGI. Il est modifié par le Décret N°05-253/ P-RM du 06 juin 2005 en ses articles 17, 18, 19 et 20.

La DGI est dirigée par un Directeur Général nommé par décret pris en Conseil des Ministres, sur proposition du ministre chargé des Finances. Il est chargé de diriger, coordonner, animer et contrôler les activités de la DGI. Il est assisté et secondé d'un Directeur Général Adjoint qui le remplace de plein droit en cas de vacance, d'absence ou d'empêchement.

Le Directeur Général Adjoint est nommé par arrêté du Ministre sur proposition du Directeur Général des Impôts. Le même arrêté fixe également ses attributions spécifiques.

La DGI comprend :

- trois Cellules en staff :
  - la Cellule des Affaires Générales ;
  - la Cellule Planification et Suivi ;
  - la Cellule Communication ;
- cinq sous-directions en live :
  - la Sous-Direction Organisation et Contrôle des Services ;

- la Sous-Direction Législation Fiscale et Contentieux ;
- la Sous-Direction Informatique ;
- la Sous-Direction des Grandes Entreprises ;
- la Sous-Direction Recherches et Appui à la Vérification.

La sous-direction informatique, interlocutrice de la CAISFF, sera la seule à être présentée en détail.

La sous-direction informatique : elle est chargée de procéder à l'informatisation progressive des activités de la DGI. Elle planifie et met en œuvre l'informatisation du service dans les conditions requises de sécurité, d'intégrité et de confidentialité des données. Elle évalue les besoins en formation dans son domaine de compétence.

La sous-direction informatique comprend deux divisions :

- la Division Réseaux et Gestion des Systèmes de Production ;
- la Division Développement et Maintenance du système d'information.

5.5.5 Direction Générale des Douanes (DGD)

Elle est crée par l'Ordonnance 90-58/ P-RM du 10 octobre 1990.

La Direction Générale des Douanes est chargée de:

- élaborer les éléments de la politique douanière,
- élaborer et d'appliquer la législation et la règlementation douanière relatives aux échanges extérieurs,
- prêter son concours à l'application d'autres règlementations notamment celles relatives aux changes, à la santé, à la sécurité, aux Eaux et Forêts, et à la protection du patrimoine culturel,
- liquider les droits et taxes exigibles à l'occasion de l'importation ou de l'exportation des marchandises,
- rechercher, de constater et de réprimer la fraude, de poursuivre les infractions à la règlementation des changes,
- gérer les relations douanières internationales.

Le Décret N° 90-391/P-RM fixe les modalités d'organisation et de fonctionnement de la DGD. La DGD est dirigée par un Directeur nommé par Décret pris en conseil des Ministres sur proposition du Ministre chargé des finances.

Le Directeur Général est chargé de définir la politique de son service, d'élaborer les grandes orientations de ses activités, de programmer, diriger, coordonner et contrôler leur exécution.

La DGD comporte des sous-directions qui se subdivisent en divisions et sections.

Les sous-directions des Douanes sont :

- la sous-direction de l'Inspections des Services ;
- la sous-direction des Affaires Générales ;
- la sous-direction de la Règlementation, de la Fiscalité et des Relations Internationales ;
- la sous-direction des Recettes, de la Statistique et de l'Informatique ;
- la sous-direction des Enquêtes Douanières et de la Surveillance Territoriale.

Le Directeur Général des Douanes est assisté et secondé d'un Directeur Général Adjoint qui le remplace en cas d'absence ou d'empêchement. Il est nommé par arrêté du Ministre chargé des Finances. Le même arrêté précise ses attributions spécifiques.

5.5.6 Direction Générale du Budget (DGB)

La direction Générale du Budget est créée par la Loi N°06-003/ du 06 janvier 2006. Elle a pour mission d'élaborer les éléments de la politique nationale en matière budgétaire et d'assurer la coordination et le contrôle de sa mise en œuvre.

A ce titre, elle :

- coordonne la préparation du projet de loi de finances ;
- suit l'exécution du budget de l'Etat ;
- assure l'analyse et formule des avis et des propositions sur les mesures comportant ou susceptibles d'avoir une incidence financière sur les finances publiques ;
- veille à la mise en œuvre des actions de modernisation de la gestion budgétaire.

La Direction Générale du Budget est dirigée par un Directeur Général nommé par décret pris en Conseil des Ministres, sur proposition du Ministre chargé du budget.

Le Directeur Général du Budget est chargé sous l'autorité du Ministre chargé du budget, de diriger, animer, coordonner et contrôler les activités de Direction.

Il est ordonnateur délégué du budget de l'Etat et est assisté et secondé d'un Directeur Général Adjoint qui le remplace de plein droit en cas de vacance, d'absence ou d'empêchement.

Le Directeur Général Adjoint est nommé par arrêté du Ministre chargé du Budget, sur proposition du Directeur Général. Le même arrêté fixe également ses attributions spécifiques.

La Direction Générale du budget comprend :

- en staff :
  - la Cellule Informatique ;
  - une Régie d'Avance.
- En live :

Cinq (5) sous –Directions :

- la Sous - Direction Cadrage Budgétaire ;
- la Sous- Direction Préparation et suivi du Budget ;
- la Sous- Direction Aides Extérieures ;
- la Sous- Direction Engagements et Ordonnancements ;
- la Sous- Direction Affaires Générales.

La cellule informatique est chargée de la coordination et du suivi de l'ensemble des activités liées à l'informatisation de la chaîne de la dépense au niveau de la direction, des directions administratives et financières des départements ministériels, des directions régionales du budget et des autres services financiers des institutions.

Sont rattachés à la Direction Générale du Budget :

- le Transit Administratif ;
- le Bureau Central de la solde.

Comme on s'en rend compte à la lecture de cette présentation, les missions des services financiers et fiscaux sont diverses et variées. Tous travaillant sous la tutelle du MEF vers lequel les données produites convergent, une harmonisation de leur politique d'informatisation s'avérait nécessaire. Ce qui permettra au MEF de faire face à ces obligations à double titre :

- disponibilité de situations statistiques sur le plan national ;
- disponibilité des informations comptables et financières fiables vis-à-vis des PTF permettant la prise de décisions importantes.

CHAPITRE VI - ORGANISATION DE L'ASSISTANCE INFORMATIQUE

Selon Henry Mintzberg « une organisation est un ensemble relativement stable d'acteurs tournés vers des objectifs généraux communs et qui, en vue de leur réalisation, recourent à une division du travail (une spécialisation des tâches) et à des modalités de coordination et de contrôle » (Dayan & al. 2004 : 53).

Ce qui nous intéresse dans cette définition, ce sont les aspects division du travail et les modalités de coordination. La CAISFF pour mener à bien sa mission d'assistance informatique, a besoin de spécialistes couvrant tous les processus énoncés au premier chapitre : administration des réseaux, des systèmes, du site web, sauvegarde/restauration, gestion de la sécurité, etc. En plus, une coordination entre la CAISFF comme organisation et les différentes directions du MEF s'avère nécessaire.

6.1 Les procédures existantes

Pour valider nos conclusions en matière de contrôle interne de la fonction informatique, nous avons procéder aux tests ci-dessous.

Question : existe-t-il un organigramme de service ?

Validation : nous n'avons pu obtenir de copie d'organigramme qu'il soit administratif ou fonctionnel.

Question : existe-t-il un plan informatique ou SDI ?

Validation : nous n'avons pu obtenir de copie du plan informatique ou du SDI.

Q : existe-t-il un suivi de l'activité du personnel informatique ?

V : nous n'avons pu nous procurer de fiches d'activité qu'elles soient récentes ou pas des travailleurs de la CAISFF.

Q : tout choix de prestation matérielle ou logicielle donne-t-il lieu à un appel d'offres ?

V : nous avons pu obtenir l'appel d'offres du SDI. Mais compte tenu de la confidentialité des appels d'offres, nous n'avons pu obtenir l'analyse des réponses des offres car le dépouillement était en cours au moment de notre passage.

En compensation, nous avons eu accès à l'analyse des réponses à une des dernières acquisitions importantes de matériels informatiques. Il s'agit de l'équipement en matériels informatiques (ordinateurs, imprimantes, onduleurs) de la DNCF. Ce marché, bien que

financé par la Coopération Française, a fait l'objet d'appel d'offres piloté par la CAISFF. Ce qui nous permet de nous assurer de la permanence des appels d'offres pour les choix importants de prestations matérielles ou logicielles.

Q : existe-t-il un comité technique informatique ?

V : il existe un comité technique informatique où sont représentées toutes les directions du MEF.

Q : quelle est la périodicité des réunions du comité technique informatique ?

V : les réunions du CTI sont bihebdomadaires en période de projet (développement d'une application au profit d'une ou de plusieurs directions du MEF, extension du réseau informatique). Ainsi avions-nous pu obtenir des anciens comptes rendu de l'interconnexion de certaines DAF au réseau de l'AGETIC avec un nœud à la CAISFF. En dehors de ces périodes de projet, le CTI peut durer sans se réunir comme c'était le cas au moment de notre passage (il ne s'est pas réuni depuis près de six mois).

Outre ces tests qui concernent l'organisation générale du service informatique, des tests ont été faits dans d'autres domaines que nous considérons comme des points forts où il existe une description des processus. Ce sont :

- la sauvegarde /restauration ;
- la gestion de la sécurité ;
- la gestion du parc informatique ;
- l'architecture.

Les tests sont faits dans l'ordre chronologique ci-dessus énoncé.

Q : les sauvegardes permettent-elles de traiter dans un délai satisfaisant tous les types d'incident ?

V : grâce à la procédure existante, le crash du serveur de base de données intervenu un beau matin de l'année 2007, n'a pas perturbé la production. La sauvegarde de la fin de journée de la veille a été vite restaurée et mise à la disposition de la production. Malgré l'impact élevé que pourrait avoir un tel incident, il a été minimisé grâce au dispositif de contrôle interne existant.

Les procédures concernant la sécurité sont décrites au paragraphe 6.3 du présent chapitre.

Q : l'acquisition, l'utilisation et la sortie des matériels informatiques sont-elles coordonnées ?

V : les achats de matériels informatiques sont faits conformément au code des marchés publics en vigueur : appels d'offres quand la valeur des matériels atteint dix huit millions de francs CFA (décret n° 08-485/PRM du 11 août 2008 portant procédures de passation,

d'exécution et de règlements des marchés publics et des délégations de services publics), mise en concurrence pour les achats en-deçà dudit seuil. La sortie desdits matériels appelée reforme, se fait conformément aux règles de la comptabilité-matières qui dispose au Mali d'un manuel de procédures.

Q : l'homogénéité de la configuration et la compatibilité des matériels entre eux sont-elles prises en compte au niveau de l'architecture ? (Delsol & al. 1999 : 263).

V : toutes les nouvelles installations de matériels informatiques ont leur plage de codification uniformisée pour permettre leur compatibilité dans le réseau.

Ces domaines ci-dessus décrits peuvent être considérés comme les points forts de la CAISFF. Après avoir pris connaissance de leur existence théorique par suite d'interviews et d'analyse documentaire, ces domaines existent dans la réalité. Leur fonctionnement permet de limiter l'impact des risques associés.

6.2 Suivi de l'activité d'assistance informatique et services rendus

Q : comment s'effectue le suivi de l'activité d'assistance informatique et des services rendus ?

V : au niveau de la CAISFF, le suivi de l'activité se fait à travers les réunions hebdomadaires. Chaque vendredi, les agents de la CAISFF se réunissent sous l'autorité du coordonnateur pour faire le point des activités en cours. A cet effet, il est fait usage des tableaux de suivi pour savoir le niveau d'évolution de l'activité et la personne responsable de l'activité.

En plus, les agents de la CAISFF travaillent en collaboration avec les Cellules informatiques auprès des directions du MEF.

6.3 Sécurité requise pour l'assistance informatique

Q : l'accès physique à l'environnement informatique est-il protégé ?

V : l'accès du local abritant les matériels de la CAISFF (ordinateurs, serveurs, onduleurs, etc.) est sécurisé. Pour les travailleurs de la CAISFF, l'accès est conditionné à la carte magnétique dont tous disposent. Pour les visiteurs, un service de gardiennage de jour et de nuit s'occupe de le faire pour eux après enregistrement des coordonnées du visiteur dans un registre. La téléphonie IP sert de liaison entre le service de gardiennage et les travailleurs de la CAISFF.

Q : l'accès physique aux salles où sont situés les matériels informatiques (ordinateurs, serveurs, supports magnétiques, armoires ignifuges, etc.) est-il contrôlé ?

V : à la CAISFF, l'accès à la salle serveur est strictement réservé. L'intérêt de telle mesure est d'éviter les risques de vols de matériels et d'informations, de fraudes et d'actes de malveillance.

Q : les matériels sont-ils suffisamment protégés contre des agressions dues aux dégâts des eaux, à l'air ambiant, à l'incendie, à l'hygrométrie, aux poussières, à la température, etc. ?

V : la salle des serveurs est surélevée par rapport aux autres bureaux se trouvant au rez-de - chaussée en prévision des dégâts des eaux.

Le bâtiment est pourvu d'un système d'alerte incendie et d'un groupe électrogène dont le système d'allumage se déclenche automatiquement en cas de coupure d'électricité. Les salles sont munies de dispositifs d'extinction et d'air conditionné.

Q : la CAISFF n'encourt-elle pas de sanction pénale pour l'implantation de progiciels sans licence d'utilisation ?

V : toutes les implantations de progiciels sont effectuées avec licence d'utilisation. Ce qui a pour intérêt d'éviter les risques de sanctions pénales et les risques de détérioration du parc informatique en cas de présence de virus dans les logiciels utilisés sans licence.

Ces tests nous permettent de confirmer que les matériels et logiciels sont protégés contre les sinistres (incendie, inondation) ou contre des actes de malveillance (vol, sabotage) et contre les risques juridiques. Il existe une stratégie de sauvegarde à la CAISFF. Outre la stratégie que nous présenterons dans les annexes, nous avons relaté au point 7.10.1.2 l'existant en terme de sécurité.

Il n'existe tout de même pas de sauvegarde sur un site géographique extérieur à la CAISFF. Ce qui n'augure pas d'une garantie suffisante en cas de sinistre.

6.4 Moyens (Humains, Matériel, Logiciels) utilisés pour l'assistance informatique

Q : la CAISFF utilise-t-elle un personnel suffisamment qualifié ?

V : l'équipe technique qui pilote la C.A.I.S.F.F est composée actuellement (en plus du coordinateur de la cellule), de 13 informaticiens dont 6 Ingénieurs, 7 Techniciens supérieurs qui ont le profil suivants :

- un (1) ingénieur de développement responsable de la qualité, de la méthode et des normes ;
- deux (2) ingénieurs de développement, administrateurs de la base de données ORACLE ;
- un (1) ingénieur de développement responsable de la veille technologique ;

- deux (2) ingénieurs réseau et systèmes, responsables du matériel, des réseaux et systèmes d'exploitation ;
- et sept (7) analystes programmeurs.

Les ingénieurs de développement sont également des chefs de projet. Ils assurent en collaboration avec les autres membres de l'équipe, la conception, la réalisation et la mise en œuvre des projets qui sont à leur charge.

Q : quels sont les moyens matériels dont dispose la CAISFF pour assurer son assistance ?

V : les moyens matériels sont constitués des matériels informatiques des différentes directions du MEF et de ceux de la CAISFF. En plus des matériels informatiques, le réseau interconnecté du MEF est utilisé pour mener à bien cette assistance. Pour la communication, il faut noter que le système de téléphonie IP existe entre la CAISFF et toutes les directions avec à la base un document récapitulant les numéros par service.

Toutes les applications métiers du MEF évoluent en environnement Oracle. Les moyens logiciels utilisés sont les applications métiers des différentes directions du MEF.

La CAISFF doit faire de gros efforts dans la formalisation de certaines de ses procédures. Sur plusieurs processus identifiés, un nombre limité bénéficie de procédures écrites. Certains processus tirent leur formalisation des dispositions générales de l'administration publique malienne comme le code des marchés publics et la comptabilité-matières. Ce qui réduit considérablement les procédures proprement formalisées par la CAISFF.

CHAPITRE VII CONSTATS – RECOMMANDATIONS

Notre mission s'est déroulée conformément au calendrier de rotation établi par le Coordonnateur de la CAISFF, à l'intention des directeurs des administrations ci-dessous indiquées :

- Cellule d'Appui à l'Informatisation des Services Financiers et Fiscaux ;
- Direction Administrative et Financière ;
- Direction Nationale du Contrôle Financier ;
- Paierie Générale du Trésor ;
- Direction Générale des Impôts ;
- Direction Générale des Douanes ;
- Direction Générale du Budget.

Le calendrier de rotation est joint après les annexes avec les dates indicatives pour les différentes directions.

7.1 Applications bureautiques

Elles sont acquises avec les nouveaux matériels informatiques. Elles sont constituées essentiellement des applications bureautiques de traitement de texte et des tableurs. Les applications bureautiques rencontrées dans les différentes structures du Ministère de l'Economie et des Finances sont : Microsoft Word, Microsoft Excel, Microsoft Powerpoint……

7.2 Direction Administrative et Financière (DAF)

7.2.1 Application métier

Seules les applications métiers qui ont été développés par la CAISFF, ou dont la maintenance évolutive est assurée par elle, seront décrites. La DAF n'en possède pas.

7.2.2 Constats

Au niveau de cette structure, une bonne appréciation est faite de l'assistance de la CAISFF.

Cette assistance concerne les domaines comme la maintenance du matériel informatique, la rechange du matériel informatique dans certains cas, l'analyse des offres techniques des appels d'offres de matériels informatiques. Tel est l'avis de 75% de notre échantillon.

Dans le cadre de l'entretien du matériel informatique, les agents de la CAISFF sont appréciés pour la promptitude de leurs interventions. Dès que la date d'entretien arrive, le matériel est nettoyé même en l'absence de l'utilisateur.

Pour ce qui est de l'analyse des offres techniques, on note la présence effective des agents de la CAISFF à tous les appels d'offres du genre. Cet avis est confirmé en totalité par les éléments de notre échantillon (100%).

Cependant, toutes les attentes des travailleurs de la DAF ne sont pas comblées vis-à-vis de la CAISFF. C'est ainsi qu'à l'unanimité, les éléments de notre échantillon reconnaissent un besoin énorme de formation des utilisateurs la DAF ne disposant pas d'informaticien.

A la DAF, on éprouve le besoin d'une application de gestion du personnel. Au moment de notre passage, les agents de la Division chargée du personnel n'ont plus de maîtrise sur le personnel des régions, alors qu'auparavant, ils pouvaient consulter la situation administrative d'un agent de la région de Kidal comme de n'importe quelle autre région.

Aussi, faut-il noter des problèmes récurrents de déconnexion au réseau informatique obligeant les utilisateurs à travailler à des heures indues (soit tard le soir ou tôt le matin des dépenses comme les salaires de la CAISFF, de la CARFIP ne pouvant attendre longtemps).

Des problèmes de connexion au réseau nous ont contraint à reporter l'entretien de Mamadou Coulibaly chargé de l'ordonnancement et des liquidations des dépenses au 29 septembre 2010 alors qu'il aurait dû se tenir entre le 13 et le 15 septembre 2010.

Les responsables de la DAF (Directeurs et Chefs de Divisions) reconnaissent tout de même que l'utilisation de l'ordinateur et du réseau local a contribué à :

- réduire le temps de travail ;
- faciliter les prises de décision ;
- améliorer la qualité du service rendu ;
- réduire les coûts de transport (téléphonie IP).

Ces constats nous permettent de dégager les points forts et les points faibles de la CAISFF à travers les processus informatiques identifiés plus haut. Comme points forts on note la maintenance matérielle, la gestion du parc informatique à travers l'activité participation aux dépouillements d'appels d'offres. Par contre ses points faibles sont les processus formation

des utilisateurs, maintenance réseau, maintenance applicative, support et conseil aux activités, analyse et conception. Ces aspects nous conduisent aux recommandations.

7.2.3 Recommandations

Les recommandations de la DAF sont les suivantes :

- développer une application informatique de gestion du personnel au profit de la DAF pour que la future Direction des Ressources Humaines puisse pleinement jouer son rôle ;
- former les agents chargés de la gestion du personnel de la DAF ou de la future DRH à la maîtrise de cette application ;
- améliorer la fluidité du réseau informatique compte tenu de l'interconnexion du réseau de l'AGETIC au réseau du MEF ;
- former les utilisateurs de la DAF (futures DRH et DFM) à la maîtrise de l'outil informatique notamment les logiciels bureautiques (Microsoft Word, Microsoft Excel, Microsoft Powerpoint, etc.) ;
- affecter un informaticien comme correspondant permanent à la DAF pour respecter au moins la norme un informaticien pour quinze (15) utilisateurs ;
- sensibiliser davantage les utilisateurs sur la sécurité informatique par ces temps de TIC pour limiter les risques d'attaques virales et ceux de panne d'ordinateurs ;
- mettre à la disposition des utilisateurs de l'application métier (PRED) un manuel pour limiter leur dépendance de la Cellule informatique du budget.

7.3 Direction Nationale du Contrôle Financier (DNCF)

7.3.1 Applications métiers

Il existe aujourd'hui deux applications métiers à la DNCF : l'application du même nom « application DNCF » et l'«application PRED ».

7.3.1.1 L'« application DNCF »

Elle sert au suivi de la comptabilité des engagements et des liquidations des dépenses budgétaires. De ce fait, elle permet la production de situations périodiques d'exécution du

budget d'Etat comme le TOFE (Tableau des Opérations Financières de l'Etat), les situations récapitulatives de l'exécution du budget, les situations détaillées, les situations sélectives, etc.

7.3.1.2 L'«application PRED »

L'«'application PRED » est décrite dans la partie DGB. Son module « suivi et exécution des dépenses » est exploité par la DNCF. Il existe une interface entre L'«application DNCF » et l'«'application PRED » en vue de l'abandon du premier.

Les tests que nous avons opérés ici concernent le processus de développement des nouvelles applications et les différents types de documentation.

Q : est-il toujours réalisé un cahier de charges préalablement au lancement de la réalisation de nouveaux logiciels ?

V : nous avons pu nous procurer à travers la CAISFF le cahier de charges de la réalisation de l'application « DNCF » datant de l'année 2004.

Q : les principales phases de mise en œuvre d'un projet sont-elles prévues dans le processus de développement des nouvelles applications ?

V : pour valider cette question, nous avons abordé les points suivants :

- la formation des utilisateurs ;
- la documentation de l'application ;
- la validation des logiciels.

En ce qui concerne la formation des utilisateurs, il a été reconnu lors de nos entretiens et d'administration de questionnaires qu'ils sont formés à l'utilisation d'une nouvelle application avant sa mise en exploitation. Nous avons pu disposer de listes de présence de deux formations des utilisateurs de «l'application PRED ». Les formations ont eu lieu à l'AGETIC durant les semaines du 03 au 07 novembre et du 10 au 14 novembre de l'année 2008. Nous avons pu obtenir le programme de formation des utilisateurs de « l'application DNCF » signé du Directeur et s'étendant sur la période du 04 au 25 avril 2005.

Quant à la documentation, nous en avons distingué trois types dans la partie théorique (chapitre trois) : la documentation d'études, celle d'exploitation et celle destinée aux utilisateurs.

Si la documentation destinée aux utilisateurs existe pour l'application « PRED », elle n'existe pas pour l'application « DNCF ». Les autres types de documentation n'existent pas pour ces deux applications.

La validation des nouvelles applications est faite par les utilisateurs à travers les jeux d'essai. L'objectif ici est de valider l'adéquation de l'application aux besoins exprimés dans le cahier de charges. En plus des jeux d'essai, l'exploitation en double nous a été signalée à la DNCF lors du passage de l'application « suivi de l'exécution des dépenses » développée sous DBASE à l'application « DNCF » qui évolue dans un environnement ORACLE.

7.3.2 Constats

Un agent de la CAISFF est désigné comme représentant permanent auprès de ladite structure. Ses efforts sont reconnus de façon positive mais jugés insuffisants compte tenu de l'étendue des problèmes rencontrés. Ce second aspect serait dû à la non maîtrise intégrale et parfaite des applications développées sous ORACLE par les informaticiens de la Cellule informatique DNCF qui reconnaissent être relégués au rang d'utilisateurs. Ce qui est d'ailleurs confirmé par notre échantillon d'utilisateurs en répondant aux questions ci-dessous : Pensez-vous que les ressources humaines actuelles de la Cellule Informatique de votre structure sont suffisantes pour couvrir tous vos besoins en assistance informatique ?
Pensez-vous que la Cellule Informatique de votre structure est suffisamment outillée pour couvrir vos besoins.

A la première question, 83% de notre échantillon répondent non contre 13% de oui. A la seconde question, 71% répondent non contre 29% de oui. Notre échantillon a couvert 81% des utilisateurs de la portion centrale (21 utilisateurs sur 26). Le reste de l'échantillon a été complété par les utilisateurs des structures décentralisées.

La correspondante CAISFF gère les problèmes d'interface entre les deux applications en exploitation au Contrôle Financier (PRED et DNCF).

La totalité des personnes interrogées répondent que malgré les difficultés et l'ampleur de la tâche, l'assistance de la CAISFF les aide à atteindre les objectifs. Avec l'assistance de la CAISFF, la DNCF arrive à remplir une de ses fonctions essentielles : la production des situations d'exécution du budget d'Etat. L'exhaustivité à ce niveau est assurée. Les situations d'exécution du budget d'Etat produites concernent non seulement ceux des différents ministères, mais aussi des régions et ceux des organismes personnalisés communément appelés EPA (Etablissement Public à caractère Administratif).

Malgré l'atteinte des objectifs grâce à l'assistance de la CAISFF, d'autres priorités demeurent. Ainsi, 65% de notre échantillon feront des observations pour combler leurs attentes.

7.3.3 Recommandations

Ces recommandations sont formulées par ordre de priorité. Ce sont :

- former les informaticiens de la Cellule Informatique du Contrôle Financier à maîtriser Oracle (SQL, Oracle forms et Reports) ;
- former les informaticiens de la Cellule Informatique du Contrôle Financier sur les systèmes AIX et autres systèmes utilisés par les différents serveurs de données et serveurs d'application ;
- former les informaticiens de la Cellule Informatique du Contrôle Financier à la maîtrise des applications « PRED » et « DNCF ». Ceci rendrait le Contrôle Financier plus indépendant vis-à-vis de la CAISFF et de la Cellule PRED de la Direction Générale du Budget ;
- faire procurer au Contrôle Financier les logiciels de statistique (SPSS et autres). Ceci éviterait la production de situations parallèles sous les applications bureautiques (Excel) comme le suivi de l'appui budgétaire ou créer des états correspondants dans les applications en exploitation ;
- développer pour le Contrôle Financier un logiciel de gestion du courrier ;
- former les utilisateurs du Contrôle Financier à la maîtrise des SIGD comme PRED version 5 et autres ;
- développer ou concevoir pour le Contrôle Financier une seule application permettant de prendre en compte toutes les données des dépenses publiques afin de faciliter la production des situations d'exécution du budget d'Etat ou ;
- rendre Internet disponible sur tous les ordinateurs des utilisateurs.

La Cellule Informatique du Contrôle Financier a le mérite de pratiquer de façon permanente le Hepdesk (formation des utilisateurs à l'interne). Soixante trois pour cent (63%) de notre échantillon ont des connaissances dans les applications bureautiques (Microsoft Word, Microsoft Excel etc.) et Internet.

Ces constats et recommandations permettent de dégager comme points forts de la CAISFF la conduite de projets, l'analyse et la conception, la réalisation, l'intégration, le déploiement et la maintenance applicative. Rappelons que la CAISFF a contribué à toutes les phases de développement de « l'application DNCF ». Les processus perfectionnement des informaticiens, formations des utilisateurs aux SIBD apparaissent comme points faibles.

7.4 Paierie Générale du Trésor (PGT)

7.4.1 Application métier

L'application métier s'appelle « DEPENSES ». Elle a vu le jour vers les années 2000. Elle sert à la saisie, au traitement des mandats de paiement et à leur règlement dans les comptes financiers. Ainsi, avons-nous effectué le test ci-dessous.

Q : l'application « DEPENSES » couvre-t-elle tous les besoins de la PGT ?

V : une des faiblesses de l'application « DEPENSES » est qu'il n'est pas prévu la dedans de module pour le suivi des marchés. Ce suivi est fait parallèlement dans Microsoft Excel, d'où une charge de travail supplémentaire pour les agents surtout quand il s'agit de marchés pluriannuels.

Il existe une deuxième application « TABOR » sur laquelle la CAISFF n'intervient pas. L'«application TABOR » est réservée à la comptabilité.

7.4.2 Constats

A la PGT, l'assistance de la CAISFF porte essentiellement sur le réseau, les difficultés rencontrées dans le fonctionnement de l'« application DEPENSES » et les serveurs.

Le rôle de la Cellule informatique auprès de la DNTCP (Direction Nationale du Trésor et de la Comptabilité Publique) est éclipsé compte tenu de l'éloignement de celle-ci et de la proximité de la CAISFF.

A la PGT, les attentes ne sont pas entièrement comblées vis-à-vis de la CAISFF.

En ce qui concerne la rapidité d'intervention de la CAISFF, cinquante pour cent (50%) de nos interlocuteurs la juge lente, vingt cinq pour cent (25%) la trouve rapide, les vingt cinq pour cent (25%) restant ont un avis mitigé (ni lente ni rapide).

Concernant les deux premiers points de l'assistance apportée (réseau et « application DEPENSES ») à la PGT, la CAISFF doit préciser aux utilisateurs de la PGT les domaines d'intervention de ses agents, car on ne sait pas à la CAISFF qui fait quoi. Ce qui veut dire que lorsqu'il y a un problème sur le réseau ou sur l'« application DEPENSES », on ne sait pas à qui s'adresser. Ce qui constituait une réponse à nos deux questions tests que nous énumérons ci-dessous :

- existe-t-il une cellule technique de gestion des réseaux ?
- existe-t-il une cellule d'assistance réseau ?

La réponse est naturellement non sinon la confusion ci-dessus évoqué n'aurait pas sa raison d'être.

La rupture fréquente du réseau est signalée par soixante quinze pour cent (75%) de nos interlocuteurs. L'observation ayant été une des techniques d'audit utilisée, nous avons constaté par nous-mêmes les 24 et 29 septembre 2010 des ruptures de réseau.

S'agissant de la formation des utilisateurs, la responsabilité est imputée à la Cellule Informatique de la DNTCP. Ainsi, soixante pour cent (60%) de l'échantillon qui ont répondu à nos questionnaires n'ont pas de connaissances sur les logiciels bureautiques (Microsoft Word, Microsoft Excel, etc.). Ce qui est confirmé par cinquante pour cent (50%) de nos interlocuteurs qui disent que la majorité des utilisateurs de la PGT apprennent l'informatique sur le tas (10 à 20 % du personnel formés en informatique selon eux).

Autres problèmes évoqués, c'est la pléthore d'utilisateurs par ordinateur et par bureau : deux à trois personnes par ordinateur et quatre à cinq personnes par bureau.

Par ailleurs, à la PGT, l'organisation informatique du MEF n'est pas jugée très pertinente (au sommet la CAISFF, les Cellules informatiques auprès des directions au niveau intermédiaire et à la base les utilisateurs). Ce schéma est assez lourd et très administratif selon nos interlocuteurs qui pensent qu'il peut engendrer un conflit d'intérêt entre la CAISFF et lesdites Cellules. Il est souhaité de disposer d'un département informatique auprès de chaque poste comptable comme c'est le cas en France.

7.4.3 Recommandations

Ces constats nous conduisent aux recommandations suivantes:

- améliorer la qualité du réseau informatique qui connaît des difficultés d'accès et de fluidité deux (2) jours sur cinq (5) ;
- préciser aux utilisateurs de la PGT leur interlocuteur en cas de problème réseau ou en cas de problème sur l'«application DEPENSES » ;
- faire assurer le Helpdesk (formation des utilisateurs par les informaticiens à l'interne) par la Cellule Informatique de la Direction Nationale du Trésor et de la Comptabilité Publique (80 à 90% des utilisateurs de la PGT apprennent l'informatique sur le tas) ;
- doter la PGT en équipements informatiques adéquats permettant à chaque utilisateur de disposer d'un ordinateur (aujourd'hui, à la PGT, il existe un ordinateur pour au moins trois utilisateurs) ;

- mettre à la disposition de la PGT un environnement de travail plus spacieux ;
- instaurer des réunions périodiques entre les utilisateurs de la PGT et la CAISFF ;
- prévoir à la PGT une Cellule information à l'intention des usagers à laquelle sera affecté un ou des ordinateurs. Les opérateurs économiques pourront s'y adresser pour savoir le niveau de traitement de leurs titres de paiement (mandats de paiement et avis de crédit). Ceci éviterait d'interrompre les agents de la PGT dans l'exécution de leurs tâches quotidiennes ;
- créer auprès de chaque poste comptable un département informatique (comme en France) car la Cellule informatique auprès de la DNTCP est jugée trop administrative et il n'est pas évident qu'elle puisse couvrir les besoins de Bamako et des régions ;
- prévoir dans l'«application DEPENSES » ou dans les futures applications à acquérir un module de suivi des marchés (y compris les marchés pluriannuels).

Compte tenu de ce qui précède, on ne saurait attribuer de point fort à la CAISFF concernant l'assistance apportée à la PGT. La maintenance applicative, l'administration du réseau, la formation des utilisateurs, l'analyse et la conception et l'assistance aux utilisateurs sont les points faibles.

7.5 Direction Générale des Impôts (DGI)

7.5.1 Application métier

L'application métier à laquelle la CAISFF a contribué au développement et au déploiement est SIGTAS. Dans SIGTAS, c'est toute la chaîne opérationnelle des impôts qui se retrouve: organisation d'une structure, spécifications des tâches des uns et des autres (rôle d'un Chef de Centre d'Impôts, rôle d'un caissier), vérification de comptabilité des entreprises, etc. SIGTAS est doté de sept (7) principales fonctions qui sont : gestion des contribuables, émission de rôles, dossier, vérification – réclamation, recouvrement, recoupement et administration.

Malgré la date lointaine de la réalisation de SIGTAS, nous avons néanmoins réalisé les tests qui suivent.

Q : existe-t-il des normes en matière de développement d'applications ?

V : nous avons pu avoir les normes de développement de SIGTAS conservés sous format électronique. Mais cette appréciation n'est que formelle car nous n'avons pouvoir de contrôler ni leur qualité, ni leur exhaustivité.

Q : les projets font-ils l'objet d'une coordination suffisante ?

V : nous avons pu obtenir les comptes rendus du groupe de travail composé d'informaticiens et d'utilisateurs à l'occasion du développement de SIGTAS.

Q : est-il procédé régulièrement à des contrôles de qualité de l'application SIGTAS ?

V : des états tirés sous SIGTAS nous ont été présentés. Ils répondent jusque là aux besoins pour lesquels ils ont été conçus. Ils peuvent être modifiés avec la naissance de nouveaux besoins.

7.5.2 Constats

L'assistance de la CAISFF a débuté à la DGI à partir des années 1999. Cet appui a d'abord consisté à jouer un rôle de coordination et d'appui conseil dans les différents projets de la DGI parallèlement à l'appui du partenaire canadien.

La CAISFF apporte aussi un appui matériel à la DGI. La dernière en date et non des moindre, est l'octroi de matériels réseau à la DGI en ce début d'hivernage 2010 après la chute de la pilonne du Centre VI des Impôts.

La CAISFF apporte un appui partiel à la DGI pour les problèmes de DBA, en mettant à la disposition de la DGI des ressources humaines extérieures.

La CAISFF est associée à l'extension du réseau de la DGI pour parler du Comité réseau. La CAISFF constitue d'ailleurs à juste titre la porte d'entrée des autres réseaux vers le réseau du MEF (cas de l'interconnexion avec l'AGETIC).

La CAISFF est associée à certains projets de grande envergure de la DGI comme la gestion informatisée des vignettes qui va nécessiter l'extension du réseau DGI aux structures partenaires telles que les Directions Régionales des Transports (DRT).

Toutes les formations qui concernent les informaticiens du MEF sont assurées par la CAISFF. Les dernières en date sont celles qui ont porté sur les thèmes « sécurité réseau » et « Windows server et UNIX ». Elles ont respectivement eu lieu à « General Computec » il ya un peu plus d'un an et à CFAO Technologies aux environs de 2005.

La CAISFF et le partenaire canadien ont assuré un appui précieux à la DGI dans le cadre de la migration de ses applications vers le système d'exploitation 10 G.

La DGI dispose d'une certaine autonomie vis-à-vis de la CAISFF car son service informatique assure la gestion et la maintenance de ses serveurs. On dénombre environ trente deux serveurs (32) et quatre cents (400) postes de travail. Il existe en plus un serveur d'antivirus qui dispache les mises à jour sur les autres postes de façon automatique.
Quant à la sécurité, des procédures alternatives sont prévues en vue d'assurer la continuité de l'exploitation.

Le local qui abrite la DME (Division des Moyennes Entreprises) est doté d'un réseau qui a été installé par la CAISFF.

A la DGI, la CAISFF n'a pas de points faibles. Il n'a que des points forts. Ils ont pour noms conduite de projets, analyse et conception (cas de SIGTAS), réalisation, intégration, déploiement, support et conseil aux activités, administration du réseau et perfectionnement des informaticiens.

7.5.3 Recommandations

A la DGI, on pense d'une part que la CAISFF les aide à atteindre leurs objectifs, mais d'autre part, la recommandation principale formulée est d'allouer un budget plus conséquent à la CAISFF. Car pendant que certaines Directions du MEF demandent une application à la CAISFF, la DGI demandera la fibre optique. Ce qui leur permet de dire qu'à l'état actuel des choses, les objectifs de la DGI sont au-delà des moyens de la CAISFF.

7.6 Direction Générale des Douanes (DGD)

7.6.1 Applications métiers

Les applications métiers en service à la DGD sont : l'«application exonération », l'«application TRIE » et l'application « SYDONIA++ ».

7.6.1.1 L'«application exonération »

Aux termes de nos interviews, nous concluons que l'assistance de la CAISFF a permis la conception, le développement et la mise en production d'une application pour l'administration des douanes. Cette application si elle ne couvre certes pas tout le champ de travail de l'administration des douanes, mais, a quand même beaucoup amoindri les

problèmes liés à la gestion des exonérations. L'«application exonération » a instauré une certaine transparence dans la gestion des exonérations. Elle a établi de la célérité dans le traitement des dossiers d'exonération, a mis fin aux dépassements, a réduit la charge de travail, a permis la maîtrise du traitement des dossiers. Avec l'«application exonération » les statistiques sont devenues plus fiables pour les types d'exonération pris en compte. Elle a aussi résolu les problèmes liés à l'archivage des documents. L'«application exonération » a enfin résolu les cas des titres qui restaient cinq années durant sans être exécutés. Cependant, des problèmes demeurent. Leur prise en compte permettra non seulement de parfaire l'application, mais de prendre en compte les préoccupations des utilisateurs.

Malgré cet enthousiasme observé chez les utilisateurs de cette application, nous avons procédé aux tests ci-dessous.

Q : s'il a été fait le choix de développer certaines applications en interne (comme c'est le cas ici), ce choix a-t-il été dûment justifié ?

V : ce choix se justifiait par l'urgence des besoins d'alors, la présence de compétences au niveau de la CAISFF, et l'incertitude de trouver sur le marché une application qui puisse répondre aux réalités nationales nous a-t-on dit.

Q : procède-t-on à des sauvegardes sur site extérieur ?

V : les données du PDI ne sont sauvegardées qu'au CIS, donc pas de sauvegarde sur un site extérieur.

Q : le centre informatique est-il protégé contre les défauts d'alimentation électrique ?

V : à l'opposé des autres directions du MEF pourvus en prises ondulées et en groupe électrogène, le PDI ne possède ni l'un ni l'autre.

7.6.1.2 L'«application TRIE »

Elle comprend les modules transfert de données, administration, gestion d'escorte et statistique. Cette application fut conçue en son temps pour les Bureaux de douanes de Kouri et de Zégoua grands pourvoyeurs en recettes du budget d'Etat malien avant le début de la crise ivoirienne en septembre 2002. A cette époque, il était fréquent que des citernes transportant marchandises liquides, ou des camions transportant des marchandises solides se perdent d'un Bureau de douanes de départ à un Bureau de douanes de destination sous des prétextes aussi divers que variés comme coulage, braquage, etc.

Aujourd'hui, tout cela n'est qu'un triste souvenir. L'«application TRIE » fonctionne en merveille dans les deux postes ci-dessus cités et étendue aux autres postes douaniers.

L'application « SYDONIA++ » relève de la compétence de la CIS (Cellule de l'Informatique et de la Statistique ».

7.6.2 Constats

. Après le développement de ces deux applications, la CAISFF s'occupe de leur maintenance, de la formation des utilisateurs. Leur développement a connu les processus généralement admis à savoir la conduite du projet, l'analyse et la conception, la réalisation, les tests de validation, l'intégration, le déploiement, la formation des utilisateurs et l'assistance aux utilisateurs. Nous les considérons comme les points forts de la CAISFF.

La CAISFF est aidée dans l'accomplissement des autres processus comme l'administration du système, la sauvegarde/restauration, l'administration du réseau et l'archivage des données par la CIS.

Compte tenu des difficultés signalées au niveau de la fluidité du réseau et du besoin de son extension, l'administration du réseau constitue un point faible. A elle, s'ajoute le perfectionnement des informaticiens car l'informaticien détaché de la CAISFF n'a jamais bénéficié de formation depuis son détachement auprès de la DGD.

L'application exonération étant la seule en exploitation à la DGD (l'application TRIE est en exploitation dans les zones frontalières), l'essentiel des recommandations ont porté sur l'élargissement de son champ de couverture.

7.6.3 Recommandations

Ces recommandations sont ainsi formulées :

- étendre l'«application exonération » à toutes les catégories de régime dérogatoire afin d'uniformiser les procédures de traitement des exonérations au niveau de la DGD;
- étendre l'«application exonération » aux régions dans un délai raisonnable compte tenu de tous les avantages que la portion centrale en tire ;
- recycler et former de façon permanente les douaniers à la maîtrise de la réglementation douanière, la maîtrise de l'«application exonération » en étant souvent tributaire ;
- organiser périodiquement des séances de formation ou de recyclage à l'intention des utilisateurs de l'«application exonération » en leur faisant découvrir ou en leur

rappelant toutes ses possibilités (prorogation de titres d'exonération, gestion des sous-traitances, etc.) ;

- améliorer si nécessaire les fonctionnalités de l'«application exonération » de façon progressive en tenant compte et des besoins des utilisateurs et de la réglementation fiscale ;
- interconnecter la DGMP et la DGD pour une meilleure prise en charge des marchés publics exonérés ;
- interconnecter la DNCC et la DGD pour une prise en charge éventuelle des intentions d'importation exonérées ;
- améliorer la fluidité du réseau informatique de la DGD tout en tenant compte du rapport coût / bénéfice en ciblant la fibre optique ;
- assurer la mise à niveau des informaticiens du PDI pour leur permettre de maintenir le cap ;
- assurer la protection des ordinateurs par l'achat de licences d'antivirus performants avec des mises à jour régulières ;
- mettre deux (2) ordinateurs supplémentaires à la disposition des usagers et assurer leur entretien ;
- pourvoir le PDI de prises ondulées pour pallier les coupures d'électricité de courte durée.

7.7 Direction Générale du Budget (DGB)

7.7.1 Application métier

C'est l'application commune à tous les services de la chaîne de la dépense (DAF, DNCF, PGT).

« L'application PRED » comprend les modules suivants : préparation du budget en ligne, préparation de la loi de finances, notification de crédits, virement de crédits, suivi et exécution des dépenses, suivi et visa des dépenses, traitement des mandats de paiement.

Cette application n'a pas été conçue par la CAISFF. Mais la CAISFF est dernièrement intervenue la dessus pour établir des interfaces entre elle et les applications « DNCF » et « DEPENSES » (maintenance évolutive).

Q : les procédures de maintenance des logiciels sont-elles formalisées ?

V : la maintenance de PRED par les informaticiens de la CAISFF serait une décision administrative prise à la suite d'une concertation des services de la chaîne de la dépense au cabinet du Ministre. Elle n'a pas fait l'objet d'une demande écrite.

7.7.2 Constats

Pour ce service, la CAISFF joue un rôle de conseiller dans le cadre de la mise en œuvre du Schéma Directeur Informatique (SDI) du MEF. La DGB fait également recours à la CAISFF pour les ressources humaines qu'elle n'a pas à son niveau. Cela est fréquent notamment pour les problèmes de réseau et d'analyse en base de données. C'est pourquoi, dans le cadre de l'extension d'un de ses nœuds réseau, la DGB a récemment adressé une requête à la CAISFF faute de disposer de ressources humaines qualifiées dans ce domaine.

En termes d'appui logistique, excepté l'achat d'imprimantes pour le compte du Bureau Central de la Solde (BCS), la DGB ne fait pas de requête à la CAISFF dans ce sens.
Dans le cadre des achats de serveurs, la CAISFF participe aux appels d'offres pour apprécier les spécifications techniques.

Pour autant, les attentes de la DGB ne sont pas toutes comblées. Pour preuve, il y a plus d'un an, une demande avait été adressée à la CAISFF pour connecter au réseau DGB un de ses bureaux situé au rez de chaussée de l'immeuble «Hôtel des Finances ». De nos jours, cette demande n'est toujours pas satisfaite.

Autre point important, qu'il s'agisse d'un problème de réseau ou de base de données, une certaine confusion règne quant à l'identification de l'interlocuteur direct au niveau de la CAISFF.

La DGB travaille avec des structures qui ont besoin de résultat. De ce fait, les résultats comptent beaucoup dans toutes les actions entreprises par la DGB envers ses partenaires y compris la CAISFF. Ainsi, la CAISFF doit observer une certaine réactivité et plus de diligence dans la prise en compte des préoccupations des différentes Directions du MEF.

De nos jours, la CAISFF ne dispose pas de ressource humaine qualifiée pour intervenir sur les serveurs. Ce qui crée une certaine dépendance vis-à-vis des prestataires extérieurs.

Ces aspects nous conduisent aux recommandations.

7.7.3 Recommandations

Ce sont :

- recruter des ressources humaines compétentes capables de résoudre les problèmes des Directions du MEF et de limiter la dépendance de la CAISFF vis-à-vis de l'extérieur (cas des serveurs notamment) ;
- rendre plus disponibles et plus réactives les ressources humaines de la CAISFF dans la résolution des problèmes des Directions du MEF ;
- former les informaticiens des Directions du MEF et ceux de la CAISFF à la maîtrise des technologies en exploitation (trois tiers, 10G, etc.) ;
- informer les Directions du MEF des achats de licences effectués et les déployer dans les dites Directions ;
- rester à l'écoute des Directions du MEF en vue d'une meilleure prise en charge de leurs besoins ;
- organiser des rencontres périodiques avec les Cellules Informatiques des différentes Directions du MEF pour une meilleure prise en compte de leurs préoccupations ;
- renforcer les capacités en ressources humaines de la Cellule Informatique de la DGB en tenant compte du rapport nombre d'utilisateurs par informaticien (soit quinze (15) utilisateurs pour un (1) informaticien). Ladite Cellule couvre non seulement la DGB, les DAF, les SAF des institutions mais aussi les régions.

A la lumière de ces constats et recommandations, la mise à jour des progiciels et la maintenance applicative apparaissent comme les points forts de la CAISFF. Par contre, les processus perfectionnement des informaticiens, la gestion des programmes informatiques, l'administration du réseau, l'assistance aux utilisateurs et les réunions et présentations demeurent ses points faibles au niveau de la DGB.

7.8 CAISFF

A la CAISFF, on regrette qu'une structure aussi importante reste toujours à l'étape de projet. Cette position a fait perdre à la CAISFF ses premiers cadres pour des banques et organismes internationaux . Ceux qui sont restés ne le sont pas faute de mieux mais par conviction que la structure peut jouer un rôle capital dans la fiabilisation des données du MEF.

A l'étape de projet, l'emploi n'est pas garanti, le projet étant limité dans le temps. C'est cette insécurité de l'emploi qui pousse les informaticiens de la CAISFF à partir. Ainsi,

les responsables du MEF, en l'occurrence le Ministre de l'Economie et des Finances, doit prendre des mesures pour pérenniser la structure et stabiliser son personnel.

.

Les agents de la CAISFF sont confrontés à d'autres facteurs externes les limitant dans l'accomplissement de leurs tâches. Ces facteurs se rencontrent au niveau des Cellules Informatiques auprès des directions du MEF qui ne les suivent pas toujours dans les solutions proposées sur le plan informatique. C'était le cas quand la CAISFF avait conseillé aux informaticiens de la DGB d'évoluer vers l'architecture trois tiers. C'est trois ans après qu'ils l'ont accepté. Ce retard aurait pu être évité.

A la CAISFF, les informaticiens se plaignent de la multiplicité des applications au niveau de la chaîne de la dépense (DAF, DNCF, PGT). Ils pensent qu'une base de données unique serait mieux pour la chaîne de la dépense où chaque direction aurait son module. Cet aspect qui a été à maintes fois expliqué par eux, semble ne pas être entendu comme si chaque direction du MEF avait un intérêt derrière son application ou dans les attributions de marché les concernant.

Tous ces aspects ci-dessus évoqués, convainquent les informaticiens de la CAISFF à une redéfinition des rôles et missions et de la CAISFF et des Cellules Informatiques des différentes directions du MEF.

Les rôles et missions ainsi redéfinis, seront appliqués sans ambiguïté.

Avant que cela ne se fasse, tous les espoirs reposent désormais sur le Schéma Directeur Informatique dont le dépouillement de l'appel d'offre est en cours, pour prendre en compte certainement ces préoccupations.

7.9 Analyse de l'existant

7.9.1 Description de l'infrastructure existante et des services associés

La description a pour but ici de mettre en évidence les procédures formalisées ou pas au niveau de la CAISFF à défaut de les reproduire toutes en annexes.

7.9.1.1 Réseau informatique

Le MEF au niveau central s'est doté d'un réseau de production performant entièrement commuté et homogène utilisant le matériel CISCO et mettant en œuvre une architecture basée sur la typologie bus-étoile.

Architecture physique :

ce réseau de production du MEF relie le Cabinet, le Secrétariat Général, la CAISFF et plusieurs services du MEF situés à Bamako à savoir : la DGB, le BCS, la DAF, la DNCF, la DNTCP, la PGT, la RGD, l'ACCT et la Cellule Informatique du Trésor (CIT).

Le réseau de production du MEF est constitué de deux sites principaux : le site de l'Hôtel des Finances (quartier du fleuve) et celui de la CAISFF.

Chaque site possède son propre LAN subdivisé en plusieurs VLANs avec un CISCO 4006 (pour le nœud principal) et plusieurs switchs CISCO 2950 (pour la subdivision en vlan). Les deux sites sont reliés à travers les CISCO 4006 par fibre optique avec une vitesse de 100 Mb/s en canal montant et 100 Mb/s en canal descendant ce qui fait un débit total en Full duplex de 200 Mb/s. Le nœud principal de la CAISFF est connecté à un router CISCO 2600 qui est ensuite connecté à un Proxy Serveur qui permet la connexion à Internet par VSAT (boucle radio). Pour des raisons de sécurité un deuxième routeur CISCO 2600 a été placé au niveau de la DGB pour assurer le back up du routeur principal. L'interconnexion physique des différents services est faite de la manière suivante :

le site de l'Hôtel des Finances regroupe les services suivants : le Cabinet, le Secrétariat Général, la DGB, la DNCF, la DAF ainsi que le centre de formation du MEF.

Le site de la CAISFF regroupe : la CAISFF, le BCS, la DNTCP, l'ACCT, la PGT, la RGD et la CIT.

Architecture logique : deux sites composent le réseau logique du MEF :

l'Hôtel des Finances

Ce site forme un réseau local dont l'architecture est basée sur la topologie bus-étoile mettant en œuvre la technologie de réseau virtuel appelé VLAN (Virtual Local Area Network) regroupant les services suivants du MEF : le Cabinet, le Secrétariat Général, la DGB, le BCS, DNCF, la DAF ainsi que le centre de formation du MEF.

Chacun des VLANs est constitué d'un ou plusieurs service(s), défini sur un ou plusieurs Switch(s) 2950 et/ 3550 selon le type d'information (Voice ou Data), à 24 ou 48

ports selon l'importance du nombre de postes au sein du service. Ces Switchs 2950 et/ 3550 sont ensuite connectés au Switch CISCO 4006 (situé dans la salle informatique de la DNB) soit par Fibre Optique (FO) soit par lien RJ45 sur port Gigabit pour atteindre un débit proche de 1 Gigabit par seconde entre les services.

La CAISFF

Le LAN (Local Area Network) du site de la CAISFF est configuré de la même manière que le site de l'Hôtel des Finances à savoir une architecture basée sur une topologie en bus-étoile mettant en œuvre les VLANs. Ce site regroupe les services suivants : la CAISFF, la DNTCP, l'Agence Centrale Comptable du Trésor (ACCT), la PGT, la Recette Générale du District (RGD), la Cellule Informatique du Trésor (CIT).

Les switchs de chaque service sont connectés au Switch CISCO 4006 (situé dans la salle serveur de la CAISFF) par Fibre Optique qui est ensuite connecté au routeur CISCO 2600.

Sur ce routeur des sous-interfaces sont définies sur l'interface ETH0. Ces sous-interfaces sont au nombre de neuf (9) numérotées de 2 à 10 (le VLAN 1 étant réservé au domaine d'administration) correspondant au nombre de vlans implémentés sur le réseau.

Chaque sous-interface sert d'une part de passerelle et d'autre part de serveur DHCP aux stations qui sont présentes dans son vlan.

7.9.1.2 Sécurité

Matériel et logiciel de sauvegarde

L'existant au niveau de la CAISFF se résume comme suit :

- lecteur : DRTape 20/40 DAT (3 internes), DDS HP Storage Works DAT 40 (2 internes et 1 externe), HP SurStore DAT 8 (1 externe) ;
- médias : DAT 4/6 Go, 12/24 Go, 20/40 Go ;
- logiciel: Backup Exec de Veritas et ntbackup.

Plage d'horaire d'intervention du système :

- arrêt de la base : 23h ;
- lancement de la sauvegarde : 23h 15 ;
- redémarrage de la base : 05h du matin.

7.9.1.3 Postes clients

Les postes clients sont installés à la CAISFF et dans les différentes structures du MEF. Ils sont visibles à la CAISFF à travers le logiciel GLPI.

7.9.1.4 Serveurs

Il existe des serveurs de base de données, des serveurs de test, des serveurs d'application, des serveurs de sauvegarde tous hébergés à la CAISFF.

7.9.1.5 Imprimantes et scanners

Chaque direction du MEF dispose de ses imprimantes. Comme les postes clients, elles sont consultables à travers le logiciel GLPI.

7.9.2 Maintenir en condition opérationnelle l'infrastructure informatique

Cette opérationnalité concerne le réseau informatique, la sécurité, les serveurs, les services de support aux utilisateurs etc.

7.9.2.1 Prestations concernant le réseau informatique

L'ensemble du réseau du MEF est interconnecté. La CAISFF est consultée pour avis technique pour toute extension de réseau (nouvelle installation). Elle est toutefois sollicitée pour les modifications concernant le réseau existant.

7.9.2.2 Prestations concernant les serveurs

Seuls les serveurs logés à la CAISFF sont entretenus par ses informaticiens. La DGI et la DGD disposent d'une certaine autonomie en la matière. Actuellement, les sauvegardes de ces deux directions sont externalisées à la CAISFF.

7.9.3 Fourniture du service de support aux utilisateurs

Une équipe de maintenance de cinq personnes ont été recrutées pour assumer cette tâche. Une ligne directe de téléphone est mise à la disposition des utilisateurs leur permettant d'appeler pour tout besoin du genre. Pour les dépannages qui concernent le réseau, il existe une équipe de première assistance. Cette équipe fait remonter les problèmes de réseau au responsable réseau de la CAISFF ou à son suppléant.

7.9.4 Prestations concernant la sécurité

Toutes les bases hébergées au sein de la CAISFF sont importantes. La stratégie de sauvegarde mise en place dépend des bases qui sont :

1- base de données salaires : contient toutes les informations permettant le calcul des salaires des fonctionnaires et contractuels de l'Etat ;

2- base de données HIST : contient l'historique des fiches signalétiques des agents de l'Etat ;

3- base de données TABOR centralisation : contient les données comptables au niveau central ;

4- base de données dépenses : contient les informations relatives aux opérations de décaissement de l'Etat ainsi que la comptabilité auxiliaire au niveau des postes centraux ;

5- base de données DRMali : abrite les informations par rapport aux dépenses et recettes centralisées ;

6- base de données dépense/RGD : contient les informations relatives aux opérations de décaissement au niveau de la Recette Générale du District.

A ces données, il faut ajouter celles de la DNCF, de la DGB. La CAISFF abrite les sauvegardes externalisées de la DGI.

7.9.5 Le suivi des services d'assistance

Le suivi des services d'assistance est assuré par le logiciel GLPI. Ce logiciel permet de savoir quelles sont les activités terminées, non terminées et celles en cours. Il permet aussi de faire l'inventaire des matériels informatiques (ordinateurs, imprimantes).

7.9.6 Proposition d'une cartographie des risques informatiques

Avant de proposer une quelconque cartographie des risques, nous allons suivre la démarche communément admise. Elle consiste à identifier les risques, les évaluer et les hiérarchiser. « Il s'agit pour l'audit d'identifier les risques (et leur nature), de les évaluer, d'estimer leur probabilité de se manifester » (Rouff, juin 2000 : 50).

Notre identification va se faire sur la base des check-lists (liste déjà préconçue qui énumère l'ensemble des risques possibles afin de voir si chaque liste concerne l'entité ou pas). Cette méthode sera combinée à l'identification des risques sur la base des risques opérationnels déjà survenus au sein de l'entité : identification par analyse historique. Des entretiens avec deux personnes désignées sur trois, nous avons permis de mettre en œuvre cette deuxième méthode.

7.9.6.1 Identification des risques informatiques

Bien que conçu sur la base d'une check-list, seules les activités menées par la CAISFF ont été retenues.

Tableau n°2 : Identification des risques informatiques

Numéro d'ordre	Processus	Activités	Déontologie	SI	Patrimoine	Informatique	Juridique	Image	Administratif	Pédagogique
01	Gestion du courrier et de la documentation informatique	Classement			X				X	
		Lecture et affectation du courrier							X	
		Elaboration de correspondances					X	X	X	
02	Réunions et présentations	Réunion							X	
		Présentation								X
		Assister aux réunions du Comité							X	
		Jury de validation candidature Etudiant					X			
		Dépouillement des offres	X				X		X	
			X							
03	Conduite de projets	Planification de projet	X						X	
		Lancement de projet							X	
		Elaboration des cahiers de charges	X	X					X	
		Suivi de projet		X					X	
		Bilan critique de projet		X					X	
		Contrôle qualité							X	
		Suivi de prestataires externes					X		X	
04	Analyse et Conception	Analyse de l'existant		X						
		Spécifications Fonctionnelles		X		X			X	
		Spécifications Techniques		X		X				
		Suivi des prestataires externes							X	

Numéro d'ordre	Processus	Activités	Déontologie	SI	Patrimoine	Informatique	Juridique	Image	Administratif	Pédagogique
05	**Réalisation**	Développement		X		X			X	
		Revue de code				X				
		Paramétrage de progiciel				X				
		Tests unitaires				X				
06	**Intégration**	Assemblage des modules		X		X				
		Test d'intégration		X		X				
07	**Déploiement**	Elaboration du dossier d'installation		X					X	
		Migration des données				X				
		Elaboration du dossier d'exploitation				X			X	
		Suivi des prestataires externes					X			
		Installations applications (séminaires, Etudiants, Laboratoires)				X				
08	**Formation des utilisateurs**	Elaboration de programmes et supports		X					X	X
		Organisation de formation							X	X
		Délivrance de formation								X
		Elaboration de guide utilisateur		X					X	
09	**Perfectionnement informaticiens**	Formation	X					X	X	X
		Veille technologique		X		X				
10	**Maintenance applicative**	Qualification des anomalies		X					X	
		Modification de programmes ou paramètres				X			X	
		Mise à jour de documentation		X		X			X	
		Adaptation par rajout de modules				X				
		Tests des modifications				X				
		Tests de non régression				X				
		Suivi des contrats de maintenance		X			X			
		Suivi de traitement d'anomalie		X					X	
		indicateurs (incidents/interventions)		X					X	
11	**Gestion du programme informatique**	Elaboration du Plan stratégique							X	
		Conception de programme annuel d'activités							X	
		Suivi de l'exécution de programme							X	
		Suivi des prestataires externes							X	
		Bilan du programme annuel d'activités					X		X	
		Elaboration des plans d'action							X	
		Elaboration du budget informatique							X	
		Evaluation du personnel informatique		X					X	
12	**Administration des systèmes**	Installation et configuration des systèmes		X		X				
		Installation et configuration de base de données		X		X				
		Analyse et optimisation des performances des systèmes		X		X				
		Analyse et optimisation des performances de base de données		X		X				
		Maintenance des systèmes		X		X				
		Maintenance de base de données		X		X				
		Surveillance des systèmes		X		X			X	
		Surveillance de bases de données		X		X			X	
		Gestion du parc de systèmes		X		X			X	
		Installation et configuration de poste de travail		X	X					
		Installation et configuration des périphériques utilisateurs		X	X					
		Gestion des licences		X	X	X	X	X	X	

Numéro d'ordre	Processus	Activités	Déontologie SI	Patrimoine	Informatique	Juridique	Image	Administratif	Pédagogique
13	Sauvegarde / Restauration	Programmes sources		X		X			X	
		Données Utilisateurs		X		X			X	
		Applications		X		X			X	
		Logiciels		X		X			X	
		Base de données		X		X		X	X	
		Versions applications		X		X			X	
		Versions logiciels		X		X			X	
		Serveurs		X		X			X	
		Sécurité système		X		X			X	
		Documentation		X		X			X	
		Site Web		X		X		X	X	
		Configuration Réseau		X		X			X	
		Firewall		X		X			X	
		Gestion des supports magnétiques			X				X	
		Définition des normes et procédures		X					X	
14	Gestion de la Sécurité	Définition des stratégies de sécurité		X		X				
		Mise en place des stratégies de sécurité		X		X				
		Installation et mise à jour des antivirus		X		X				
		Gestion des virus		X		X				
		Gestion des habilitations (comptes Agents)		X		X				
		Gestion des habilitations (comptes stagiaires)		X		X				
		Gestion des mots de passe		X		X				
		Gestion des accès aux locaux informatiques		X	X	X			X	
		Gestion des indicateurs d'incidents		X	X	X			X	
		Gestion des licences		X	X	X	X	X	X	
		Définition des normes et procédures		X	X	X	X	X	X	
15	Maintenance matérielle	Diagnostic des pannes			X					
		Réparation des pannes			X					
		Maintenance préventive			X		X			
		Suivi des prestataires extérieurs			X		X	X	X	
		Gestion des indicateurs de pannes		X					X	
		Gestion des pièces détachées		X	X				X	
		Définition des normes et procédures		X	X		X		X	
		Gestion des garanties			X		X		X	
16	Production	Planification de l'exploitation		X		X				
		Exploitation des applications		X		X				
		Certification des factures travaux informatiques		X	X	X				
		Facturation des impressions								
		Allocation de ressources (séminaires, étudiants,		X					X	
		Agents)		X	X	X			X	
		Gestion des indicateurs de production								
		Définition des normes et procédures		X		X			X	
				X		X			X	
17	Mise en œuvre des progiciels	Paramétrage		X		X				
		Déploiement des logiciels				X			X	
		Adaptation par rajout de modules				X				
		Formation des utilisateurs	X	X					X	
		Assistance aux utilisateurs		X					X	
		Définition des normes et procédures		X		X			X	
		Gestion des licences		X			X		X	
	Maintenance des progiciels	Adaptation par rajout de modules		X		X				
		Test des modifications		X		X				

Numéro d'ordre	Processus	Activités	Déontologie	SI	Patrimoine	Informatique	Juridique	Image	Administratif	Pédagogique
		Mise à jour de la version en production		X		X				
18		Mise à jour de la documentation		X		X			X	
		Formation des utilisateurs		X					X	
		Définition des normes et procédures		X		X			X	
		Gestion des licences		X		X	X		X	
		Elaboration du schéma de réseau		X	X	X				
		Analyse et optimisation des performances		X		X				
		Supervision du réseau		X		X				
		Maintenance du réseau		X	X	X				
		Définition et mise en place des règles sur le firewall		X		X				
		Administration du firewall		X	X	X				
	Administration des réseaux	Gestion du parc d'éléments actifs(routeurs)		X					X	
19		Installation et configuration des équipements			X	X			X	
		Installation et configuration des accès Internet		X		X				
		contrôle disponibilité de la ligne Internet		X		X				
		Installation et configuration des commutateurs				X				
		Brassage et mise en réseau des équipements				X				
		Gestion de la relation avec les fournisseurs								
		Gestion des indicateurs réseaux					X	X	X	
		Définition des normes et procédures		X	X	X			X	
		Conception du site Web		6		X		X	X	
20	Administration du site Web	Pilotage du Site Web		X		X		X	X	
		Mise a jour du Site Web		X		X		X	X	
		Gestion des indicateurs		X					X	
		Définition des normes et procédures		X		X			X	
		Recueil des demandes d'assistance		X	X	X			X	
		Traitement des demandes d'assistance		X	X	X			X	
21	Assistance aux utilisateurs	Suivi des demandes d'assistance		X	X	X			X	
		Gestion des indicateurs d'assistance		X	X	X			X	
		Définition des normes et procédures		X					X	
		Réception d'équipements informatiques			X				X	
		Gestion des prêts d'équipements informatiques			X				X	
		Affectation et livraison d'équipements informatiques			X				X	
	Gestion du parc	Mise au rebut du matériel retiré d'inventaire			X				X	
22	informatique	Retrait d'équipement du parc informatique			X				X	
		Suivi du parc informatique (entrées / sorties)			X				X	
		Définition des normes et procédures			X				X	
		Gestion de la garantie			X		X		X	
		Gestion des indicateurs de mouvements		X					X	
		Définition de l'architecture des systèmes		X		X				
		Définition d'architecture applicative		X		X				
23	Architecture	Définition des normes et procédures		X		X			X	
		Définition de l'architecture des réseaux		X		X				
		Élaboration de spécifications techniques		X		X				
		Support et conseil aux activités externes						X	X	
24	Support et conseils aux activités	Support aux équipes de développement		X		X			X	
		Support et conseil aux appels d'offres	X		X		X		X	

Source : Nous-même

7.9.6.2 Appréciation du contrôle interne

Elle va se faire par rapport à l'existence de procédures de contrôle interne, leur application effective ou non. Pour cela, nous allons utiliser les échelles de cotation indiquées dans le tableau ci-dessous. Ainsi, un risque se verra attribuer une de ses notes indiquant le dispositif de maîtrise des risques du contrôle interne.

Tableau n°3 : appréciation du dispositif de maîtrise des risques par le contrôle interne

Note	Qualité du contrôle interne	Description du niveau de contrôle interne
1	Adaptée	Il existe une procédure. Elle ne présente pas de lacunes. Elle est systématiquement appliquée.
3	Insuffisante	Il existe une procédure. Elle présente de lacunes. Elle n'est pas toujours appliquée.
5	Inexistante	Il n'existe pas de procédure.

Source : Inspiré de RENARD Jacques (2010 : 405) et Maders & al. (2009 : 67 – 68)

A ce critère de niveau de contrôle interne existant ou pas, il convient d'ajouter les deux autres de la cartographie : l'appréciation de la gravité et l'appréciation de la fréquence (Rénard, 2010 : 406 – 408).

7.9.6.3 Appréciation de la gravité du risque

Elle est censée mesurer l'importance des enjeux. C'est la raison pour laquelle elle est aussi appelée appréciation quantitative. Mais c'est là que réside toute la difficulté de cette méthode. Dans certains cas comme l'audit du service entretien, la valeur quantitative à retenir est le « budget annuel », ou le chiffre d'affaires pour un audit des ventes. Dans d'autres cas comme l'audit des installations de fabrication d'une usine, c'est la valeur desdites installations qui est à retenir. Ce qui correspond à notre cas. Mais comment évaluer les installations d'un réseau informatique où il n'existe aucune procédure formalisée ?

Par ailleurs, certains spécialistes (Pouliot & al. juin 2002 : 37) pensent que cette évaluation quantitative est du domaine des gestionnaires et non des auditeurs. De ce fait, ils font une

fragmentation des pertes opérationnelles en deux composantes : la fréquence annuelle de l'événement (FE du domaine de l'auditeur) et la perte moyenne par événement (PME du ressort du gestionnaire). « La perte moyenne par événement illustre quant à elle l'importance ou la sévérité moyenne de la perte. Par exemple, si cinq fraudes ont totalisé une perte de 30 000 euros, la PME est de 6 000 euros (30 000 euros ÷5 cas).

La PME est le point d'intérêt des gestionnaires car elle est étroitement reliée à une mesure de l'effet de leurs décisions tactiques sur la sévérité des pertes. En effet, c'est par l'entremise de leurs choix d'affaires que les gestionnaires peuvent contribuer à diminuer la perte moyenne par événement relié au risque opérationnel » (Pouliot & al. juin 2002 : 37).

Compte tenu de ce point de vue et de la difficulté d'évaluer quantitativement les pertes relatives aux actifs matériels et immatériels, nous ne tiendrons pas compte de cet aspect dans notre cartographie.

7.9.6.4 Appréciation de la fréquence du risque

Elle est qualitative. La fréquence annuelle de l'événement (FE) est un outil des auditeurs pour mesurer les contrôles mis en place. « La fréquence de l'événement représente l'occurrence de l'événement sur une base annuelle….La FE est le point de mire des auditeurs car elle est reliée de près à la mesure des contrôles en place » (Pouliot & al. juin 2002 : 37).
L'appréciation de la fréquence du risque est jugée subjective. Quatre cas de figure peuvent se présenter (Pouliot & al. septembre 2002 : 36 – 37).

- Cas où la fréquence (FE) et la sévérité moyenne (PME) sont élevées : ce sont des situations invraisemblables pouvant entraîner l'arrêt de l'activité de l'entité.
- Cas où la fréquence (FE) et la sévérité moyenne (PME) sont faibles : ce sont des situations dont doivent rêver toute organisation car les pertes sont sous contrôle et les risques sont bien gérés.
- Cas où la fréquence (FE) est élevée alors que la sévérité moyenne (PME) est faible : l'auditeur doit introduire de nouveaux contrôles (ou modifier ceux déjà en place) en vue de diminuer la fréquence.
- Cas où la fréquence (FE) est faible alors que la sévérité moyenne (PME) est élevée : le gestionnaire doit réduire la sévérité par ses décisions tactiques. Il doit pouvoir envisager plusieurs scénarios dont le recours à l'assurance. Dans tous les cas, il doit tenir compte du rapport coût/bénéfice des différents scénarios.

Après des entretiens avec deux personnes désignées sur trois par le Coordonnateur de la CAISFF, nous avons retenu trois niveaux de vulnérabilité des risques récapitulés dans le tableau ci-dessous.

Tableau n°4 : Coefficient de vulnérabilité des risques

Numéro d'ordre	Niveau de vulnérabilité	Coefficient de vulnérabilité	Niveau de la fréquence et de la sévérité du risque
1	Vulnérabilité faible	1	Cas où la fréquence (FE) et la sévérité moyenne (PME) sont faibles.
2	Vulnérabilité moyenne	3	Cas où la fréquence (FE) est élevée alors que la sévérité moyenne (PME) est faible.
3	Vulnérabilité forte	5	Cas où la fréquence (FE) et la sévérité moyenne (PME) sont élevées. Cas où la fréquence (FE) est faible alors que la sévérité moyenne (PME) est élevée.

Source : Nous-même

Le coefficient du risque est alors obtenu en multipliant la note relative au dispositif de maîtrise du risque (qualité du contrôle interne) par le coefficient de vulnérabilité.

Le risque minimal aura pour borne inférieure : 1 x 1 = 1 (contrôle interne adapté multiplié par vulnérabilité faible).

Sa borne supérieure sera de : 1 x 5 = 5 (contrôle interne adapté multiplié par vulnérabilité forte).

Le risque moyen aura comme borne inférieure 3 x 3 = 9 (contrôle interne insuffisant multiplié par vulnérabilité moyenne).

Sa borne supérieure sera de : 3 x 5 = 15 (niveau de contrôle interne insuffisant multiplié par vulnérabilité moyenne).

Le risque maximal aura pour borne inférieure : 5 x 3 + 1 = 16 (contrôle interne insuffisant multiplié par vulnérabilité moyenne majoré d'un point).

Sa borne supérieure sera de : 5 x 5 = 25 (contrôle interne inexistant multiplié par vulnérabilité forte).

De ce calcul du coefficient global d'appréciation du risque, peut découler des situations d'ex aequo. Parmi elles, on peut par exemple citer :

- contrôle interne adapté multiplié par vulnérabilité faible = 1 x 5 = 5
- contrôle interne inexistant multiplié par vulnérabilité faible = 5 x 1 = 5.

Ces égalités apparentes seront réduites en considérant comme critère majeur l'appréciation du contrôle interne et comme critère mineur l'appréciation de la vulnérabilité parce que jugée très subjective. Ainsi, en présence des deux cas ci-dessus cités, bien vrai qu'ayant le même coefficient de risque (5), le premier sera considéré comme moins risqué que le second.

Tableau n°5 : Coefficients des risques relatifs aux processus de la CAISFF

Numéro d'ordre	Processus	Qualité du contrôle interne	Niveau de vulnérabilité	Coefficient du risque
01	Gestion du courrier et de la documentation informatique	5	5	25
02	Réunions et présentations	3	1	03
03	Conduite de projets	3	5	15
04	Analyse et Conception	3	5	15
05	Réalisation	3	5	15
06	Intégration	3	5	15
07	Déploiement	3	5	15
08	Formation des utilisateurs	5	3	15
09	Perfectionnement informaticiens	5	3	15
10	Maintenance applicative	5	3	15
11	Gestion du programme informatique	5	5	25
12	Administration des systèmes	3	5	15
13	Sauvegarde / Restauration	1	5	05
14	Gestion de la Sécurité	1	5	05
15	Maintenance matérielle	3	3	09
16	Production	5	5	25
17	Mise en œuvre des progiciels	3	3	09
18	Maintenance des progiciels	5	3	15
19	Administration des réseaux	3	5	15
20	Administration du site Web	5	3	15
21	Assistance aux utilisateurs	5	3	15

22	Gestion du parc informatique	1	5	05
23	Architecture	1	5	05
24	Support et conseils aux activités	5	3	15

Source : Nous – même

Les risques relatifs à certains processus comme la conduite des projets, l'analyse et la conception, la réalisation, l'intégration et le déploiement par le fait de l'usage de POCA (Pratiques d'Organisations Communément Admises) ont un coefficient de risque moyen. Ces POCA, selon les résultats de nos interviews, concernent la mise en place d'une équipe projet avec désignation d'un chef de projet, validation et essai par et avec les utilisateurs d'une nouvelle application avant son déploiement.

Par contre, d'autres processus comme la sauvegarde/restauration, la sécurité et l'architecture bénéficient de procédures clairement définies. Ce qui leur confère une qualité de contrôle interne adaptée et réduit par conséquent leur coefficient du risque.

Les procédures concernant la gestion du parc informatique sont décrites au paragraphe 6.1 du chapitre 6.

S'agissant de la gestion des programmes informatiques, elle est caractérisée par l'absence notoire de SDI, d'où son coefficient de risque élevé.

Quant à la gestion du personnel, une des activités du processus production, elle demeure toujours problématique. La CAISFF selon nos interlocuteurs, ne donne pas de garanties ou de motivations suffisantes pour maintenir son personnel. Le statut de projet de la CAISFF aidant à cela, les premiers cadres de la structure ont été débauchés par des banques et organismes internationaux (dont un à la BCEAO, un à la Banque de Développement du Mali BDM et un à ICRISAT Niger). Parmi les cas récents, on note un départ pour le Bureau du Vérificateur Général.

7.9.6.5 Hiérarchisation des risques

Après ces explications pour mieux comprendre les coefficients des risques, nous allons établir une table de classement suivant le numéro d'ordre des risques. Ce classement est appelé hiérarchisation suivant le coefficient du risque.

Tableau n°6 : Hiérarchisation des risques suivant le coefficient du risque

Numéro d'ordre	Appréciation sur le contrôle interne	Risque encouru (impact)	Vulnérabilité (fréquence)	Coefficient du risque	Niveau de risque
11	Inexistant	5	Elevée	25	Elevé
16	Inexistant	5	Elevée	25	Elevé
01	Inexistant	5	Elevée	25	Elevé
24	Inexistant	5	Moyenne	15	Moyen
20	Inexistant	5	Moyenne	15	Moyen
18	Inexistant	5	Moyenne	15	Moyen
10	Inexistant	5	Moyenne	15	Moyen
09	Inexistant	5	Moyenne	15	Moyen
08	Inexistant	5	Moyenne	15	Moyen
19	Insuffisant	3	Elevée	15	Moyen
12	Insuffisant	3	Elevée	15	Moyen
07	Insuffisant	3	Elevée	15	Moyen
06	Insuffisant	3	Elevée	15	Moyen
05	Insuffisant	3	Elevée	15	Moyen
04	Insuffisant	3	Elevée	15	Moyen
03	Insuffisant	3	Elevée	15	Moyen
17	Insuffisant	3	Moyenne	09	Faible
15	Insuffisant	3	Moyenne	09	Faible
23	Adapté	1	Elevée	05	Faible
22	Adapté	1	Elevée	05	Faible
14	Adapté	1	Elevée	05	Faible
13	Adapté	1	Elevée	05	Faible
02	Insuffisant	3	Faible	03	Faible

Source : Inspiré de RENARD Jacques (2010 : 410)

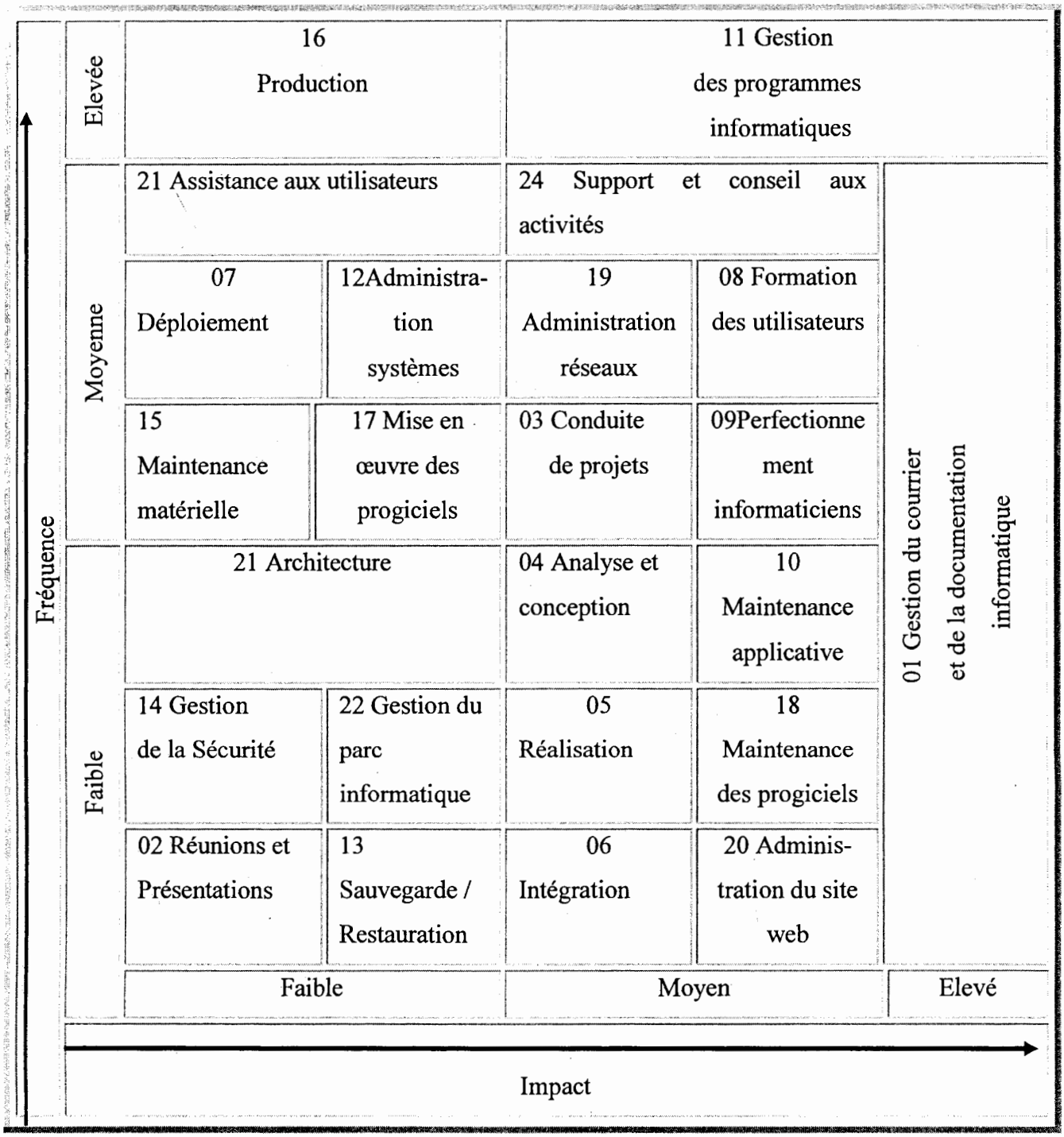
7.9.6.6 Présentation de la cartographie des risques

La cartographie des risques se présente comme une matrice à deux variables : la vulnérabilité représentée dans notre cas par la fréquence et l'impact qui correspond au risque encouru. La première variable repose sur le dispositif de maîtrise du risque c'est-à-dire la

qualité du contrôle interne. Ce qui peut influer sur la seconde variable en le limitant au cas où le risque se matérialiserait.

La figure suivante est une illustration de la cartographie des risques liés aux processus d'assistance informatique de la CAISFF. Elle est inspirée du système RADAR avec une composante de moins.

Figure n°4 : Cartographie des risques liés aux processus d'assistance informatique de la CAISFF



Source : Inspiré de RENARD Jacques (2010 : 408-409) et COSO II REPORT (2009 : 237)

De la cartographie des risques, peut découler un plan d'audit. Pour les processus dont le risque est faible, il y aura un audit tous les 4 ou 5 ans. Pour les processus dont le risque est jugé moyen, un audit tous les 3 ans. Les processus dont le risque est élevé, un audit est nécessaire tous les ans ou deux ans.

CONCLUSION GENERALE

Excepté à la PGT, l'organisation informatique au niveau du MEF est jugée pertinente. Au sommet il y a la CAISFF pour conseiller le Ministre chargé des finances, au niveau intermédiaire les Cellules informatiques auprès des directions et à la base les utilisateurs.

A la PGT, une Cellule Informatique auprès de la DNTCP est jugée trop administrative et assez lourde. De ce fait, elle ne peut résoudre les problèmes de la PGT et des trésoreries régionales. Pour preuve, compte tenu de leur éloignement de la PGT, leur rôle s'est confondu à celui de la CAISFF qui essaie tant bien que mal, de le jouer cumulativement avec le leur. Comme en France, on pense qu'il faut créer un département informatique auprès de chaque poste comptable.

Outre ce problème organisationnel, l'assistance de la CAISFF est différemment appréciée d'une Direction du MEF à une autre. La CAISFF en tant que porte étendard de l'informatique au sein du MEF, doit d'abord s'entourer des ressources humaines nécessaires à la réalisation de ces objectifs. Ce qui n'est aujourd'hui pas le cas. Cet état de fait entraîne une certaine dépendance de la CAISFF des prestataires extérieurs, ou une tentative des directions du MEF a trouvé une solution à leurs problèmes sans la CAISFF. Ce qui signifie qu'elle n'a pas comblé les attentes qui ont suscité sa création.

Il est aussi reproché à la CAISFF de ne pas être à l'écoute des Directions du MEF en vue de connaître leurs besoins et de trouver des solutions idoines. Ce qui explique la très grande dépendance de certaines Directions du MEF où des besoins énormes de formation des informaticiens et des utilisateurs existent (DAF, DNCF et PGT).

Des applications ont été développées pour la DGI, la DNCF, la DGD sans pour autant couvrir tous leurs besoins.

D'autres directions du MEF, mieux nanties que les autres, se sont entourées des compétences indispensables à la réalisation de leurs objectifs. Sont de cela la DGI et la DGB même si la première reconnaît bénéficier d'appui en matériels réseau.

Trois recommandations majeures s'avèrent nécessaires :

- prendre des dispositions réglementaires pour pérenniser la CAISFF en stabilisant en même temps son personnel ;
- définir les missions et attributions de la CAISFF et des Cellules Informatiques auprès des directions du MEF pour éviter tout conflit de compétence ;
- établir une politique de communication entre la CAISFF, les Cellules Informatiques et les utilisateurs ;

- formaliser les principes d'assistance de la CAISFF en prévoyant des procédures alternatives compte tenu du caractère urgent de certaines interventions et de l'évolution rapide de l'informatique.

Les deux premières recommandations s'adressent au Ministre de l'Economie et des Finances et les deux dernières au Coordonnateur de la CAISFF.

Si des principes de sécurité existent (sécurité physique et logique), la CAISFF doit davantage faire des efforts dans la formalisation de toutes ses procédures. A titre d'illustration, il n'existe aucune documentation pour les applications conçues par la CAISFF. Un site géographique extérieur de sauvegarde des données s'avère nécessaire pour pallier certains risques de sinistre.

ANNEXES

Annexe 1 : questionnaire de contrôle interne relatif au choix des matériels

- L'appel d'offres matériel
  - Est-il réalisé un appel d'offres pour le choix de matériel représentant des montants significatifs (dans la mesure où le matériel n'est pas imposé par une estimation préexistante) ?
  - Le cahier des charges matériel servant de support à l'appel d'offres inclut-il :
    - la description des applications à traiter ?
    - Une estimation des volumes, présents et à venir ?
    - La liste des contraintes d'exploitation : temps de réponse, durée des traitements, procédures de reprise, confidentialité… ?
    - Les dates de livraison de matériels à respecter ?
    - Le choix des prestations est-il formalisé et basé sur des critères concrets ?
- La négociation du contrat
  - Le contrat négocié avec le fournisseur choisi prévoit-il :
    - des pénalités en cas de retard dans les livraisons ?
    - Un engagement sur la capacité du matériel fourni à traiter les applications définies dans le cahier des charges, avec les volumes qui y sont estimées et en respectant les contraintes imposées ?
    - Un engagement sur les temps de réponse de système ?
    - Un engagement sur le coût des accroissements futurs de la configuration ?
    - Les conditions de la maintenance : coûts, modalités, délais d'intervention… ?
- Les conditions de maintenance
  - Existe-t-il un suivi qualitatif des matériels et de leur maintenance ?
    - Moyenne des temps de bon fonctionnement (MTBF) ?
    - Suivi des incidents et des pannes ?
    - Rapidité et qualité des interventions de maintenance ?
  - Le coût de la maintenance des matériels est-il estimé ?
    - Le délai d'intervention contractuel correspond-il aux besoins ?
    - Des solutions de type « maintenance tierce » ont-elles été étudiées ?
    - Les conditions sont-elles négociées régulièrement ?

Source : Derrien Yann (1992 : 60)

Annexe 2 : questionnaire de contrôle interne relatif au choix des progiciels

- Est-il rédigé un cahier des charges préalablement au choix des progiciels (sauf si celui-ci est imposé par une situation préexistante, ce qui est le cas de certains logiciels de base du constructeur) ?
- Le cahier des charges du progiciel inclut-il :
    - la description des fonctions à traiter ?
    - Les volumes à traiter ?
    - Les délais de démarrage ?
    - Les contraintes en matière de sécurité ?
    - Les données de base qui devront être gérées dans les fichiers ?
    - Une description des fonctions dont la livraison pourrait être demandée dans une deuxième étape ?
- Plusieurs progiciels sont-ils étudiés et comparés avant le choix définitif ?
- Le choix définitif s'appuie-t-il sur :
    - la qualité des propositions fournies ?
    - Des visites à des entreprises ou organisations disposant du progiciel ?
    - Des considérations générales sur le fournisseur : envergure, notoriété, qualité des interlocuteurs.... ?
    - Des considérations concernant le progiciel : nombre de référence, pérennité prévisible... ?
    - La qualité de la documentation du progiciel ?
- Le contrat passé avec le fournisseur prévoit-il :
    - un engagement à traiter les applications prévues au cahier des charges ?
    - Un engagement à traiter les volumes prévus au cahier des charges ?
    - Des pénalités en cas de retard du prestataire ?
    - La définition précise de l'assistance fournie : formation, documentation, assistance au démarrage, maintenance initiale... ?
    - Les conditions de la maintenance du progiciel ?
    - Les conditions de paiement du coût de la prestation ?
- Est-il prévu que l'entreprise ou l'organisation dispose des programmes sources ?

Même si le prestataire conserve la propriété du programme source, il est souhaitable que l'entreprise ou l'organisation dispose d'une copie. Ceci présente l' intérêt pour l'entité de pouvoir modifier elle-même les logiciels en cas de défaillance du fournisseur et permet pas de garantir la pérennité du progiciel.

- Est-il prévu une phase de validation du progiciel sur la base d'un jeu d'essai au moment du démarrage ?
- Dans l'utilisation ultérieure du progiciel :
    - est-il prévu un suivi qualitatif du progiciel : historique des bogues (anomalies de programme), rapidité de la maintenance.

Source : Derrien Yann (1992 : 60 – 61).

Annexe 3 : fiche d'enquête de satisfaction
et de recueil des besoins
Nom de la Structure : .....

Questionnaire	Réponse OUI/ NON
Connaissez-vous parfaitement le Système d'Information de votre structure ?	
Avez-vous des connaissances en informatique ?	
Avez-vous des connaissances sur les logiciels bureautiques ?	
Si oui, lesquels ?	
Avez-vous été sensibilisé sur la sécurité informatique ?	
Avez-vous des notions de sécurité informatique ?	
Avez-vous connaissance de l'existence d'une politique de sécurité au sein de votre structure ?	
Avez-vous lu cette politique de sécurité au cas où elle existerait ?	
Pensez vous que le système d'information de votre structure est assez sécurisé et assez contrôlé ?	
Connaissez-vous les dispositions ou règles minimales à prendre pour sécuriser votre ordinateur ?	
Pensez vous qu'un audit du système informatique est opportun à l'heure actuelle ?	
La Cellule Informatique de votre structure couvre-t - elle tous vos besoins ?	
Pensez vous que les ressources humaines actuelles de la Cellule Informatique de votre structure sont suffisantes pour couvrir tous vos besoins en assistance informatique ?	
Pensez vous que la Cellule Informatique de votre structure est suffisamment outillée pour couvrir vos besoins ?	
Depuis combien de temps les informaticiens de votre Cellule Informatique n'ont pas été formés ?	

Quel est le nombre d'informaticiens composant actuellement votre Cellule Informatique ?	
Quel est actuellement le nombre de personnes de votre structure utilisant des ordinateurs ?	
Quels sont les services que la CAISFF vous fournit ?	
Ces services répondent-ils à vos besoins ?	
Si non, quelles sont vos attentes vis à vis de la CAISFF ?	
Avez-vous connaissance d'une charte pour l'usage des services informatiques et internet au sein de votre structure ?	

Définir en quelques mots vos attentes de la Cellule informatique de votre structure :

Quels sont vos besoins en matière de formation et précisez les domaines ?

Quels sont vos besoins en matière d'acquisition ou de développement de logiciels ?

Source : Nous-même

Annexe 4 : extrait de la liste des personnes qui nous ont accordé des entretiens

Numéro d'ordre	Noms	Prénoms	Services	Fonctions ou Corps	Dates	Heures début Interview
1	MAGASSOUBA	Broulaye	DAF	Technicien supérieur culture	16/09/2010	08H 15
2	COULIBALY	Yacouba	DAF	Contrôleur des Finances	16/09/2010	13H 04
3	COULIBALY	Mamadou	DAF	Contrôleur des Finances	29/09/2010	13H 02
4	KONATE	Ibrahima	DNCF	Chef Cellule Informatique DNCF ibkonat@yahoo.fr	30/09/2010	14H 35
5	TAWATY	Mountaga	DNCF	Technicien supérieur Informatique mtawatym@yahoo.fr	30/09/2010	14H 35
6	TESSOUGUE	Rosalie TRAORE	DNCF	Technicien supérieur Informatique	30/09/2010	14H 35
7	KAMATE	Lassine	PGT	Inspecteur du Trésor	29/09/2010	10H 25
8	KONE	Mahamadou	PGT	Inspecteur du Trésor	29/09/2010	15H 07
9	DIONI	Gaoussou	PGT	Inspecteur du Trésor	04/10/2010	10H 10
10	NOMOKO	Djibril	DGI	Chef Division Réseau et Gestion du Système de Production	06/10/2010	10H 55
11	TRAORE	Aliou	DGI	Informaticien Division Réseau et	06/10/2010	15H 39

				Gestion du Système de Production		
12	MAIGA	Boubacar	DGD/PDI	Informaticien détaché CAISFF PDI	11/10/2010	09H 53
13	KEITA	Modibo Kane	DGD	Sous-directeur RFRI	14/10/2010	13H 50
14	SIDIBE	Soriba	DGD	Chef Bureau BEMEX	15/10/2010	09H 26
15	COULIBALY	Zoumana Mory	DGD	Chef Bureau du pétrole	15/10/2010	10H 42
16	AG ASSADEK	Alhassane	DGD/PDI	Coordonnateur PDI	15/10/2010	16H 02
17	SISSOKO	Moussa	DGB	Coordonnateur Cellule PRED DGB	20/10/2010	09H 45
18	BARRY	Amadou	DGB	Informaticien Cellule PRED DGB	20/10/2010	09H 45
//	SISSOKO	Moussa	DGB	Coordonnateur Cellule PRED DGB	21/10/2010	14H 42
20	KONE	Ousmane	DGB	Informaticien Cellule PRED DGB	21/10/2010	14H 42
19	HAIDARA	Ibrahima	CAISFF	Informaticien CAISFF	28/10/2010	08H 31
20	TALL	Mariam TOURE	CAISFF	Informaticien CAISFF mtall@finances.gov.ml	29/10/2010	08H 45
//	HAIDARA	Ibrahima	CAISFF	Informaticien CAISFF ihaidara@finances.gov.ml	29/10/2010	08H 20

Source : Nous-même

Annexe 5 : exemple de guide d'entretien concernant quelques domaines ciblés

Environnement social

Le taux de rotation du personnel informatique est-il cohérent ?
La politique de recrutement est-elle satisfaisante ?
La politique de rémunération est-elle conforme aux normes du marché ?
La qualification du personnel est-elle cohérente avec les fonctions exercées ?
Le recours à des prestataires extérieurs est-il maîtrisé ?
Y a-t-il eu dans le passé des événements marquants en matière de gestion du personnel ?
L'intérêt technique de l'activité informatique permet-il une motivation suffisante du personnel ?
La formation du personnel est-elle suffisante ?
Le contexte général de l'organisation est-il motivant ?

Source : Derrien Yann (1992 : 55 – 57)

La méthodologie de développement des applications

Est-il toujours réalisé une étude d'opportunité préalablement au lancement de la conception d'une nouvelle application ?
Avant tout développement de logiciels ou toute acquisition de progiciels, les avantages et les inconvénients respectifs de l'acquisition d'un progiciel et de la réalisation d'un système spécifique sont-ils analysés ?
Est-il réalisé un cahier de charge préalablement au lancement de la conception de nouveaux logiciels ?
Existe-t-il des normes en matière de développement d'applications ?
Existe-t-il des normes en matière de programmation ?
Les principales phases de mise en œuvre d'un projet sont-elles prévues dans le processus de développement de nouvelles applications ?
Les projets font-ils l'objet d'une coordination suffisante ?

Source : Derrien Yann (1992 : 63 – 71)

Annexe 6 : exemple du programme de validation des conclusions en matière de contrôle interne de la fonction informatique

L'organisation générale du service informatique

Question : existe-t-il un plan informatique ?
Validation : obtenir une copie du plan informatique.
Q : existe-t-il un suivi de l'activité du personnel informatique ?
V : contrôler les fiches d'activité les plus récentes pour quelques collaborateurs du service informatique.
Q : tout choix de prestation matérielle ou logicielle donne-t-il lieu à un appel d'offres ?
V : demander l'appel d'offres et l'analyse des réponses pour les dernières acquisitions les plus significatives ?

Les procédures de développement et de maintenance des applications

Q : est-il toujours réalisé un cahier des charges préalablement au lancement de la réalisation de nouveaux logiciels ?
V : demander les cahiers des charges des dernières applications mises en exploitation.
Q : existe-t-il des normes en matière de développement d'applications ?
V : demander le dossier des normes de développement et contrôler sa qualité et son exhaustivité.
Q : les projets font-ils l'objet d'une coordination suffisante ?
V : demander les comptes rendus de réunion des groupes de travail chargés de la coordination.

L'environnement de production

Q : est-il prévu une procédure permettant un redémarrage sur un site extérieur dans un délai satisfaisant ?
V : vérifier que la procédure a été testée depuis moins de six mois. Demander le compte rendu du test.

Source : Derrien Yann (1992 : 211)

BIBLIOGRAPHIE

1. **ANGOT Hugues, FISCHER Christian, THEUNISSEN Baudouin** (2004), *Audit Comptable Audit informatique*, 3ème édition, Editions De Boeck Université, Paris, 299 P.
2. **BARRY Mamadou** (2004), *Audit contrôle interne*, la Sénégalaise de l'Imprimerie, 267 P.
3. **BERTIN Elisabeth** (2007), *Audit interne Enjeux et pratiques à l'international*, Editions d'Organisations, Paris, 319 P.
4. **Bilodeau Yves** (Décembre 2002), Le fabuleux développement de l'informatique impose un regain de confidentialité, *Revue Audit,* (162) : 40.
5. **CALE Stéphane, TOUITOU Philippe** (2007), *La sécurité informatique : réponses techniques, organisationnelles et juridiques*, Lavoisier, Paris, 282 P.
6. **CHAUVAT Gérard, REAU Jean-Philippe** (1996), Statisques descriptives, Armand Colin, Paris, 205 P.
7. **Coopers & Lybrand** (2000), *La nouvelle pratique du contrôle interne*, 5ème tirage, Editions d'Organisation, Paris, 379 P.
8. **DAYAN Armand & al.** (2004), *Manuel de gestion*, vol. 1, 2ème édition, Editions ELLIPSES /AUF, Paris, P 1088.
9. **DELSOL Xavier & al.** (1999), *Guide d'audit des associations : le diagnostic juridique, social, fiscal, comptable financier et informatique*, 3ème édition, EDITIONS juris, 319 P.
10. **DERRIEN Yann** (1992), *Les techniques de l'audit informatique*, Paris : DUNOD, 240 P.
11. **DESROCHES Alain, LEROY Alain, VALLEE Frédérique** (2005), *La gestion des risques principes et pratiques*, LAVOISIER, Paris, 286 P.
12. **GILLET Michelle, GILLET Patrick** (2008), *Management des systèmes d'information*, DUNOD, Paris, 443 P.
13. **Hillion Jean-Claude** (Février 2002), Internet, ou la nécessité renforcée d'une réelle maîtrise du risque « systèmes d'information » dans les établissements de crédit, *Revue Audit*, (158) : 23.
14. **IFACI**, *Audit et Contrôle des Systèmes d'Information, Module 5, Audit des systèmes applicatifs*, 1993, 136 P.

15. **INSTITUT DE L'AUDIT INTERNE, PRICEWATERHOUSECOOPERS, LANDWELL & ASSOCIES** (2009), *LE MANAGEMENT DES RISQUES DE L'ENTREPRISE*, Cadre de référence • Techniques d'application COSO II REPORT, Editions d'Organisation, Paris, 338 P.
16. **LEMANT Olivier/ Groupe de recherche de l'Institut de l'Audit Interne (IFACI)** (1995), *La conduite d'une mission d'audit interne*, 2ème édition, DUNOD, Paris, 277 P.
17. **MADERS Henri Pierre et Jean Luc Masselin** (2009), *Contrôle interne des risques Cibler Evaluer Organiser Piloter Maîtriser,* 2ème Edition, Editions d'Organisation, Paris, 261 P.
18. **NAAIMA Mohamed** (Février 2002), Les technologies de l'information et de la communication sont entrées dans le champ d'action de l'audit interne (1ère partie), *Revue Audit,* (158) : 36.
19. **NGUEMA Octave Jokung** (2008), *Management des risques*, Editions Ellipses, Paris, 188 P.
20. **NICOLET Marie-Agnès, MAIGNAN Michel** (Avril 2005), Contrôle interne et gestion des risques opérationnels, *Revue Banque*, (668) : 52.
21. **NICOLET Marie-Agnès, MAIGNAN Michel** (Avril 2005), Contrôle interne et gestion des risques opérationnels, *Revue Banque*, (668) : 51 - 52.
22. **OBERT Robert, MAIRESSE Marie-Pierre** (2008), *DSCG 4 Comptabilité et audit, Manuel et Applications*, DUNOD, Paris, 569 P.
23. **OBERT Robert, MAIRESSE Marie-Pierre** (2008), *DSCG 4 Comptabilité et audit, Corrigés du Manuel*, DUNOD, Paris, 212 P.
24. **PIGE Bénoit** (2007), *Audit et Contrôle interne,* 2ème édition, Editions EMS, Paris, 216 P.
25. **POULIOT Daniel, BILODEAU Yves** (Juin 2002), Mesurer les risques en vue de les contrôler et de les gérer Première partie : L'approche par la fréquence annuelle et par la perte moyenne, *Revue Audit*, (160) : 37.
26. **POULIOT Daniel, BILODEAU Yves** (Septembre 2002), Mesurer les risques en vue de les contrôler et de les gérer Deuxième partie : L'approche matricielle des pertes, *Revue Audit*, (161) : 36 - 37.
27. **RENARD Jacques** (2010), *Théorie et pratique de l'audit interne*, 7ème édition, Editions d'Organisation, Paris, 469 P.

28. **ROUFF Jean-Loup** (juin 2000), Audit interne et risk management : deux activités spécifiques et complémentaires, *Revue Audit*, (150) : 50.

29. **SCHICK Pierre, LEMANT Olivier**, (2001), Guide de self-audit 184 items d'évaluation pour identifier et maîtriser les risques dans son organisation…ou créer un audit interne, Editions d'Organisation, Paris, 217 P.

Webographie

30. Commentçamarche.net (14/10/2008), Technicien de maintenance informatique, www.commentcamarche.net/contents/metiers-informatique/tecnicien-maintenance.php3

31. Commentçamarche.net (14/10/2008), Hot liner, www.commentcamarche.net/contents/metiers-informatique/hot-liner.php3

32. Commentçamarche.net (14/10/2008), Technicien réseau, www.commentcamarche.net/contents/metiers-informatique/technicien-reseau.php3

33. Commentçamarche.net (14/10/2008), Administrateur réseau, www.commentcamarche.net/contents/metiers-informatique/administrateur-reseau.php3

34. Commentçamarche.net (14/10/2008), Administrateur de bases de données, www.commentcamarche.net/contents/metiers-informatique/administrateur-bases-données.php3

35. Commentçamarche.net (14/10/2008), Ingénieur système, www.commentcamarche.net/contents/metiers-informatique/ingenieur-système.php3

36. Commentçamarche.net (14/10/2008), Ingénieur réseau, www.commentcamarche.net/contents/metiers-informatique/ingenieur-reseau.php3

37. Commentçamarche.net (28/03/2010), Analyste programmeur (développeur), www.commentcamarche.net/contents/metiers-informatique/analyste-programmeur-developpeur.php3

38. Commentçamarche.net (16/03/2009), Architecte de système d'information, www.commentcamarche.net/contents/metiers-informatique/architecte-si.php3

39. Commentçamarche.net (14/10/2008), Webmaster (Administrateur de site web), www.commentcamarche.net/contents/metiers-informatique/webmaster.php3

40. Commentçamarche.net (14/10/2008), Web designer, www.commentcamarche.net/contents/metiers-informatique/web-designer.php3

41. Commentçamarche.net (05/01/2011), Webmasting – Ergonomie d'un site web, www.commentcamarche.net/contents/web/ergonomie.php3

42. Commentçamarche.net (14/10/2008), Chef de produit, www.commentcamarche.net/contents/metiers-informatique/chef-produit..php3

43. Commentçamarche.net (14/10/2008), Consultant, www.commentcamarche.net/contents/metiers-informatique/consultant..php3

44. Comment Ça Marche Informatique (14/10/2008), Chef de projet informatique, www.commentcamarche.net/contents/metiers-informatique/Chef-projet-informatique.php3

45. Commentçamarche.net (14/10/2008), Directeur des Systèmes d'Information (DSI), www.commentcamarche.net/contents/metiers-informatique/dsi.php3

46. Commentçamarche.net (14/10/2008), RSSI (responsable de la sécurité des systèmes d'information), www.commentcamarche.net/contents/metiers-informatique/rssi-responsable-securite.php3

47. easeo (2008-2010), Audit informatique, www.easeo.fr/Prestations-de-service/audit-informatique.html

48. AFAI (08/04/2010), Cartographie des risques informatiques : exemples, méthodes et outils, www.afai.fr/public/doc/545/.pdf

49. Mulot Déclic (30/09/2010), Assistance informatique et Internet à domicile, www.mulot-declic/particuliers/definition-assistance-informatique-à-la-personne.php

50. easeo (2008 – 2010), Contrat de Maintenance informatique adapté aux TPE/PME, www.easeo/Prestations-de-service/maitenance-informatique.html