Université d'Abomey-Calavi

N° d'ordre :

École Doctorale des Sciences de l'Ingénieur (ED-SDI)

Mémoire de Master Recherche

Présenté pour l'obtention du grade de

Master Recherche en Télécommunications et Réseaux Informatiques de l'Université d'Abomey-Calavi

EVALUATION DU SYSTEME D'INFORMATION DU RESEAU DES COMPTABLES DIRECTS : CAS DU TRESOR PUBLIC TOGOLAIS

Réalisé et présenté par

SALAMI Morou

Promotion : 2021-2022

Directeur de mémoire :
Tahirou DJARA
Maître de Conférences Université d'Abomey-Calavi
(Bénin)

Encadreur :
Dr Matine OUSMANE
Enseignant à l'Université d'Abomey-Calavi
(Bénin)

Sommaire

Dédicace

Grâce au Très Miséricordieux Allah, j'ai pu achever ce travail.

Je le dédie particulièrement à mes parents.

Remerciements

Je tiens d'abord et avant tout à remercier ALLAH, le Tout Puissant qui m'a facilité la rédaction de ce mémoire de Master Recherche. Le travail n'aurait pu connaître un aboutissement heureux sans son assistance et sa protection.

J'exprime ma totale déférence et ma reconnaissance au Professeur Tahirou DJARA, Maître de Conférences des Universités du CAMES, Coordonnateur de la filière des Télécommunications et Réseaux Informatiques de l'École Doctorale des Sciences de l'Ingénieur qui a assumé la lourde charge de Directeur de mémoire. Je le remercie du fond du cœur pour ses nombreuses marques de soutien ainsi que les encouragements dont j'ai bénéficié de sa part tout au long de ces travaux. Je lui témoigne ma profonde gratitude.

J'exprime également ma profonde reconnaissance au Dr Matine OUSMANE enseignant à l'Université d'Abomey-Calavi, qui a assuré mon encadrement, sous la direction du Professeur Tahirou DJARA. Je ne saurais jamais le remercier assez pour avoir dirigé et orienté mes travaux de mémoire. Puisse Dieu le lui rendre au centuple.

Je voudrais tout particulièrement remercier tout le corps enseignant de l'École Doctorale Science de l'Ingénieur de l'Université d'Abomey-Calavi pour l'enseignement reçu durant la formation. Qu'ils soient assurés de ma reconnaissance.

Mes remerciements vont également à l'endroit du personnel, pour les précieux conseils et orientations au sein de l'Ecole Doctorale des Sciences de l'Ingénieur.

Je tiens à remercier tous les membres de mon jury pour avoir consacré une partie de leur précieux temps afin de juger mon travail, surtout dans le contexte de la pandémie de COVID-19. A ma petite famille, je tiens à dire un grand merci pour leur affection qui m'a été d'une grande utilité.

Pour finir, j'adresse mes sincères remerciements à tous mes parents, amis, collègues, Responsables Administratifs et tous ceux qui ont contribué de quelque manière à la réalisation de cette œuvre.

Résumé

Dans ce travail, nous présentons l'évaluation du système d'information du réseau des comptables directs du trésor public togolais. Dans une première étape, nous avons fait le parcours réglementaire, matériel, applicatif et sécuritaire du système d'information comptable et financière de la Direction Générale du Trésor et de la Comptabilité Publique (DGTCP) depuis les structures déconcentrées jusqu'au niveau des services centraux de ladite direction générale.

Nous avons analysé l'ensemble du système d'information de la DGTCP pour ressortir les insuffisances à chaque niveau de la chaine de la dépense publique afin d'améliorer la qualité de l'information financière et comptable de l'Etat, de renforcer les contrôles, de garantir la sécurité des informations et la maitrise des fraudes internes et externes.

Dans une deuxième étape, afin d'apporter des solutions aux insuffisances relevées, nous avons déployé le système intégré de gestion des finances publiques dans une blockchain. Avec la solution blockchain proposée, toute modification ou altération d'un compte est impossible. La fiabilité et la sécurisation des documents comptables sont ajoutés au bloc et scellés interdisant ainsi toutes sortes de manipulations.

Mots clés : DGTCP, Finance Publique, Système d'Information financière et comptable, blockchain.

Abstract

In this work, we present the evaluation of the information system of the network of direct accountants of the Togolese public treasury. In a first step, we made the regulatory, material, application and security course of the accounting and financial information system of the General Directorate of the Treasury and Public Accounting (DGTCP) from the decentralized structures to the level of the central services. of the said general management.

We analyzed the entire information system of the DGTCP to highlight the shortcomings at each level of the public expenditure chain in order to improve the quality of the financial and accounting information of the State, to strengthen the controls , to guarantee the security of information and the control of internal and external fraud.

In a second step, in order to provide solutions to the shortcomings identified, we deployed the integrated public finance management system in a blockchain. With the proposed blockchain solution, any modification or alteration of an account is impossible. The reliability and security of the accounting documents are added to the block and sealed thus prohibiting all kinds of manipulations.

Keywords: DGTCP, Public Finance, Financial and Accounting Information System, blockchain.

LISTE DES SIGLES ET ABREVIATIONS

BTOC : **B**ordereau de **T**ransfert des **O**pérations **C**omptables

CPE : **C**omptables **P**rincipaux de l'**E**tat

DGTCP : **D**irection **G**énérale du **T**résor et de la **C**omptabilité **P**ublique

MEF : **M**inistère de l'**E**conomie et des **F**inances

MIB : **Management I**nformation **B**ase

MESR : **M**inistère de l'**E**nseignement **S**upérieur et de la **R**echerche

MTP : **M**inistère des **T**ravaux **P**ublics

MEPSA : **M**inistère de l'**E**nseignement **P**rimaire et **S**econdaire et de L'Alphabétisation

MEAHV : **M**inistère de l'**E**levage, **A**griculture, **H**ydraulique **V**illageoise

MS : **M**inistère de la **S**anté

MAEP : **M**inistère de l'**A**griculture, **E**levage et de la **P**èche

METFP : Ministère de l'Enseignement Technique et de la Formation Professionnelle

OID : **O**bject **I**dentifier

SD : **C**omptables des **S**tructures **D**éconcentrées

SIGFiP : **S**ystème **I**ntégré de **G**estion des **F**inances **P**ubliques

MP : **S**ystème **S**imple **N**etwork **M**anagement **P**rotocol

TR : **T**résorerie **R**égionale

TP : **T**résorerie **P**rincipale

T : **T**résorerie

P : **Payeur**

TPMDC : **T**résorerie **P**rincipale des **M**issions **D**iplomatiques et **C**onsulaires

LISTE DES FIGURES ET IMAGES

LISTE DES TABLEAUX

INTRODUCTION GENERALE

Le monde de l'information aujourd'hui en plein essor, amène les uns et les autres à la recherche de solutions adéquates au traitement rationnel des données. L'informatique occupe donc une place sans cesse grandissante dans l'automatisation des tâches quotidiennes. Bien que son utilisation soit une réalité de tous les jours, la gestion de certaines tâches nécessite une amélioration pour protéger le patrimoine informationnel de la gestion des finances publiques.

1. Contexte

Dans le but de faire face aux limites des systèmes de gestion intégré des finances publiques, la Direction Générale du Trésor et de la Comptabilité Publique (DGTCP) ayant, entre autres, à sa charge l'organisation des services comptables veut toujours rendre plus efficace son système de gestion des deniers publics.

La Comptabilité de l'Etat se révèle être un outil précieux dans la gestion des finances publiques. Toutes les opérations comptables (dépenses, recettes et trésorerie) effectuées par le Trésor public sont retracées mensuellement dans la balance générale des comptes du Trésor. La bonne tenue de ces opérations éclaire les autorités publiques dans leur prise de décision.

Les Comptables Principaux de l'Etat (CPE), les Trésoriers Régionaux (TR), les Trésoriers Principaux (TP), les Trésoriers (T) et les Payeurs (P) sont les acteurs du réseau des comptables directs du Trésor. **[1]**

Les comptables des services déconcentrés du Trésor sont les représentants de la Direction Générale du Trésor et de la Comptabilité Publique. Ils sont situés dans une hiérarchie unique placée sous la seule autorité du Directeur Général du Trésor et de la Comptabilité Publique[1].

[1] Il s'agit de l'organigramme de la DGTCP : voir annexe1 du document

Le Trésor public dont la vocation principale est la centralisation des opérations financières de l'Etat, s'efforce, à tout instant, d'accomplir régulièrement ses missions de recouvrement des recettes, de paiement des dépenses et de gestion de la trésorerie de l'Etat à l'aide de l'outil informatique. Le Trésor public dans l'exécution de ses missions, a connu une phase de traitement manuel sur la tenue de la comptabilité de l'Etat puis un processus d'informatisation en cours.

2. Problématique

Dans le but de faire ressortir l'incidence de cette automatisation, nous nous sommes assigné une hypothèse de travail. S'il est vrai que l'informatisation a contribué à améliorer l'information financière et comptable de l'Etat, il n'en demeure pas moins que des difficultés subsistent encore dans cette automatisation des tâches.

En effet, quelques fois après la "couverture - intégration" des opérations de transferts reçus d'un autre comptable, on constate un dysfonctionnement de l'application du Système Intégré de Gestion des Finances Publiques (SIGFiP)[2] qui fait que les comptes de contrepartie n'apparaissent pas. La non apparition de ces comptes de contrepartie entraine donc un déséquilibre de la balance du comptable assignataire de l'opération et, par conséquent, un déséquilibre de la balance générale agrégée des comptes du Trésor.[3]

Il existe aussi des difficultés relatives à la couverture des opérations de transferts reçus des Comptables des Structures Déconcentrées (C.S.D), lorsque les opérations ne sont pas saisies selon leurs natures. Autrement dit, les montants de différentes natures d'opérations sont saisis en un seul montant comme étant une même nature d'opération.

On note également le manque de contrôle d'accès à l'application par un même utilisateur sur plusieurs ordinateurs sans déconnexion préalable, le problème d'optimisation de la base de données vu la lenteur d'exécution des requêtes et la

[2] Le SIGFiP est l'application informatique de l'exécution du budget de l'Etat depuis la phase administrative jusqu'à la phase comptable
[3] Balance consolidée des trois CPE

lenteur du réseau informatique, le problème de la sécurité des données, du personnel et des locaux de travail.

Au regard de toutes ces difficultés, surgissent des interrogations :

- le réseau des comptables directs du Trésor dispose-t-il de ressources matérielles et humaines suffisantes pour les défis qui se profilent à l'horizon ?

- qu'est-ce qui est à l'origine d'un tel état de fait ?

- comment l'améliorer et l'optimiser ?

Pour trouver la réponse à ces inquiétudes, nous avons choisi de réfléchir sur le thème : « **L'évaluation du système d'information du réseau des comptables directs : Cas du Trésor Public Togolais ».**

Le choix d'un tel thème s'explique par la nécessité d'améliorer la qualité de l'information comptable et financière produite au niveau des services centraux et des structures déconcentrées de la DGTCP.

3. Objectifs

A partir de la problématique décrite dans la section précédente, nous nous fixons comme objectif de proposer une solution efficace pour améliorer la gestion des finances publiques.

Notre travail n'a pas pour objet d'étudier la tenue de la comptabilité de l'Etat, mais plutôt de faire une analyse du système d'information actuel afin de lui apporter une optimisation dans la gestion automatisée des tâches comptables. L'approche méthodologique de notre travail consiste à faire d'abord l'étude de l'existant à travers le questionnaire et l'interview (échantillon de 82 personnes : les responsables du service informatique, comptable et les utilisateurs du progiciel) que sont les techniques de collecte d'informations[4], ensuite le constat des résultats obtenus[5] et enfin l'approche de solution.

[4] Voir document fiche de collecte des données en annexe
[5] Voir document résultat du questionnaire en annexe

4. Organisation

Le présent mémoire faisant le point de nos travaux est divisé en deux parties. La première partie comporte deux chapitres. Dans le premier chapitre, nous avons défini notre cadre de recherche qui nous a permis d'exposer le cahier de charge de notre travail. Dans le second chapitre de notre étude, nous avons présenté et évalué le système d'information étudié.

La seconde partie comprend également deux chapitres. Dans le troisième chapitre, nous avons proposé une solution d'amélioration du système avec la technologie blockchain. Dans le quatrième chapitre de notre étude, nous avons présenté les résultats obtenus et procédé à une discussion de ces derniers.

PREMIERE PARTIE : ETAT DE L'ART, CAHIER DE CHARGE ET ETUDE DE L'EXISTANT DU PROJET

CHAPITRE I : ETAT DE L'ART, CAHIER DE CHARGE DU PROJET

La réforme de la comptabilité de l'État a pour ambition de moderniser les comptes de l'État. L'informatisation de la comptabilité de l'État a connu plusieurs étapes avec pour but d'améliorer la gestion des finances publiques. Dans l'exécution des dépenses de l'État, il existe la phase administrative et celle dite comptable. Au Togo, c'est la Direction Générale du Trésor et de la Comptabilité Publique (DGTCP) qui s'occupe de la partie comptable. Dans ce premier chapitre, nous présenterons le cadre institutionnel (1.1) et juridique (1.2) de la DGTCP.

1.1. Le cadre institutionnel de la DGTCP

Dans ce titre, nous présenterons la Direction Générale du Trésor et de la Comptabilité Publique à travers son historique, sa situation géographique, sa structure organisationnelle.

1.1.1. La présentation du cadre

Le cadre de notre étude est la DGTCP qui assure la comptabilité de l'État.

1.1.1.1. Historique de la DGTCP

Le Trésor public est l'administration qui désigne, au sein du Ministère chargé des finances, le réseau des comptables publics et qui exerce une tutelle sur un certain nombre de secteurs de la vie économique.

Jusqu'en 1923, Lomé n'était qu'une paierie ayant à sa tête un Payeur dépendant du Trésorier Payeur du Dahomey (actuel Bénin).

L'importance des opérations effectuées par la paierie de Lomé et la réforme monétaire intervenue le 21 février 1923 sous l'impulsion du commissaire de la République, le Ministre Français des colonies, Monsieur Albert SARRAUT, et celui des finances, Monsieur Charles LASTEYRIE, ont proposé la création d'une Trésorerie indépendante au Togo. Le décret fut signé le 13 septembre 1923 par le président français Alexandre MILLERAND et Promulgué par le Gouverneur BONNECARRERE par arrêté n° 220 du 30 octobre 1923. Le service de la trésorerie sous mandat fut dirigé par un Trésorier

Payeur Général (TPG) sous l'autorité des ministres français des finances et des colonies jusqu'à l'indépendance.

A son accession à l'indépendance en 1960, le Togo créa son propre service du Trésor par ordonnance n° 61/03 du 20 mars 1961. Compte tenu des insuffisances de cette ordonnance, le décret n° 89/13 portant organisation et attribution de la DGTCP fut pris le 06 février 1989.

En 2001, le Trésor public sera marqué par une autre mutation pour prendre en compte le contexte de l'intégration économique au sein des États membres de l'Union Économique et Monétaire Ouest Africaine (UEMOA) par l'adoption du décret n° 2001/155/PR du 20 août 2001 portant organisation et attribution de la DGTCP. **[2]**

Pour adapter les réalités togolaises aux normes communautaires, un comité de réforme fut mis en place par arrêté n°142/MFBP/DGTCP du 19 novembre 2007.

Cette réforme conduira à distinguer en dehors du cabinet du Directeur général, les structures administratives d'une part et les postes comptables d'autres parts.

1.1.1.2. Situation géographique et mission

1.1.1.2.a. Situation géographique

La Direction Générale du Trésor et de la Comptabilité Publique (DGTCP) est situé dans l'enceinte du Centre Administratif des Services Économiques et Financiers (C.A.S.E.F.). Son immeuble, en forme ovoïdale, compte trois (03) étages. Elle est limitée au Nord par le parking du Ministère de l'Économie, des Finances et de la Planification du Développement (M.E.F.P.D), au sud par la cantine du MEFPD, à l'est par le MEFPD, à l'Ouest par le Stade Omnisport de Lomé et l'hôtel 2 Février.

1.1.1.2.b. Mission de la DGTCP

La DGTCP assure entre autres missions :

- l'élaboration des règles de la comptabilité publique, des plans comptables de l'État et les autres organismes publics;
- l'élaboration des instructions relatives aux opérations de recettes, de dépenses et de trésorerie;
- l'exécution des actions de contrôle et surveillance nécessaires à la sauvegarde des intérêts du trésor public;

- le concourt à l'élaboration de la politique budgétaire, monétaire, économique et financière de l'État;
- la surveillance du respect par les comptables publics des textes législatifs et réglementaires;
- le contrôle des opérations des comptables publics;

la gestion, la coordination financière et des études relatives à l'équilibre de la trésorerie de l'État. **[3]**

1.1.2. Les structures organisationnelles

La structure organisationnelle de la DGTCP est de type hiérarchique. (**Annexe 1**).

Le décret n° 2001/115/PR du 20 août 2001 portant organisation et attributions de la Direction Générale du Trésor et de la Comptabilité Publique est la base juridique du fonctionnement de la dite Direction.

Aux termes de ce décret, la DGTCP comprend les organes suivants :

- la Direction Générale ;
- le Cabinet de la DGTCP ;
- les Directions;
- les Structures comptables centrales et déconcentrées.

1.1.2.1. Les structures administratives

Les Directions participent à l'élaboration et à la conduite de la politique monétaire et financière de l'État et contribuent à la détermination des grandes orientations de l'État en matière de politique de gestion des entreprises publiques. Elles ont pour mission la réglementation et l'organisation de la gestion des deniers publics et la gestion des moyens humains et matériels mis à la disposition de la DGTCP.

Elles comportent les directions suivantes :

- la Direction du Trésor (DT);
- la Direction de la Comptabilité Publique (DCP);
- la Direction du Personnel et du Matériel (DPM);
- l'Agence Judiciaire du Trésor (AJT);
- la Direction de la Dette Publique (DDP). **[3]**

1.1.2.2. Les postes comptables

1.1.2.2.a. Les postes comptables centraux

Ils assurent la gestion des deniers publics, l'exécution des opérations de trésorerie ainsi que la centralisation informatique de la comptabilité générale de l'État et l'édition des états y afférents. Ils ont pour mission essentielle des dépenses du budget de l'État, des comptes d'affectation spéciale et de la tutelle des régies d'avances. Ils assurent également le recouvrement et la centralisation des ressources du budget de l'État et veille à l'administration et à la supervision de toutes autres structures de recettes publiques.

Elles comprennent :

- l'Agence Comptable Centrale du Trésor (ACCT),
- la Paierie Générale du Trésor (PGT),
- la Recette Générale du Trésor (RGT). **[3]**

1.1.2.2.b. Les structures comptables déconcentrées

Les structures comptables déconcentrées de la D.G.T.C.P sont les Trésoreries Régionales (T.R), Les Trésorerie principales (T.P), la Trésorerie Principale des Missions Diplomatiques et Consulaires (T.P.M.D.C), Les Trésoreries (T). **[4]**

1.2. Le cadre juridique de la DGTCP

Le cadre juridique est régie par le décret n° 2008-092/PR portant régime juridique applicable aux comptables publics du 29 juillet 2008. Le présent décret fixe le régime juridique applicable aux comptables publics et assimilés.

Dans ce chapitre nous présenterons les attributions des comptables publics, les obligations, les responsabilités et en fonction du statut juridique leur classification.

1.2.1. Attributions et obligations des comptables publics

Sont comptables publics, les fonctionnaires et agents régulièrement habilités à effectuer les opérations de prise en charge et de recouvrement des rôles et des ordres de recettes, pour le compte de l'État, des collectivités territoriales, des établissements publics, des services et organismes assujettis aux règles de la comptabilité publique.

1.2.1. 1. Attributions des comptables publics

Les comptables publics sont en charge des opérations suivantes :

- la prise en charge et le recouvrement des rôles et des ordres de recettes qui leur sont remis par les ordonnateurs, des créances constatées par un contrat, des recettes de toute nature que les organismes publics sont habilités à recevoir;
- la prise en charge et le règlement des dépenses;
- la garde et la conservation des fonds, valeurs et titres appartenant ou confiés à l'État ou aux autres organismes publics;
- l'exécution des opérations de trésorerie;

la tenue de la comptabilité du poste comptable qu'ils dirigent. **[5,22,24,26]**

1.2.1. 2. Obligations des comptables publics

Tout comptable public est personnellement et pécuniairement responsable de :

- la conservation des fonds et valeurs dont il a la garde, de la position des comptes de disponibilités qu'il surveille ou dont il ordonne les mouvements;
- la justification de ses opérations, ainsi que de l'exacte concordance entre leur résultat et la position de ses comptes de disponibilité;

la régularité des dépenses qu'il décrit ainsi que de l'exécution de celles qu'il est tenu de faire. **[6,27]**

1.2.2. Responsabilités et classification

Les comptables publics sont responsables de la prise en charge et de l'encaissement régulier des recettes dont le recouvrement leur est confié.

1.2.2.1. Responsabilités

Les comptables publics sont tenus notamment de :

- s'assurer de l'autorisation de percevoir les recettes dont le recouvrement leur est confié;
- délivrer une quittance régulière au débiteur et d'inscrire les recettes perçues dans leur comptabilité;
- contrôler la régularité des réductions et des annulations de titres de perception.**[7]**

1.2.2.2. Classification

Selon leur statut juridique, les comptables publics sont:

- principaux ou secondaires;
- centralisateurs ou non centralisateurs.

Sont comptables principaux, les comptables publics qui, sous l'autorité du ministre chargé des Finances, exécutent leurs opérations et en rendent compte au juge des comptes. Ce sont notamment l'agent comptable central du trésor, le receveur général du trésor et le payeur général pour l'État.

1.3. Le cahier de charge du projet

La réforme de la comptabilité de l'État a pour ambition de moderniser les comptes de l'État. L'informatisation de la comptabilité de l'État a pour but d'améliorer la gestion des finances publiques. Les réformes engagées au Togo depuis 2006 ont permis de mettre en place le Système Intégré de Gestion des Finances Publiques (SIGFiP) qui prend en compte l'automatisation des opérations comptables.

1. 3.1. Rapport de stage

Le stage s'est déroulé à la Direction Générale du Trésor et de la Comptabilité Publique (DGTCP) du Ministère de l'Économie et des Finances (MEF) sous la supervision de l'agent comptable central du trésor (ACCT).

Le passage à la DGTCP nous a permis d'analyser le système de traitement du circuit de la dépense publique en général et celui du réseau des comptables directs du Trésor. Ce passage nous a permis d'étudier l'architecture du système applicatif et réseau, d'apprécier la configuration des serveurs, d'auditer la base de données implémentée, de faire l'inventaire du matériel informatique et des logiciels en utilisation.

Après avoir fait l'étude de l'existant, nous avons accordés des interviews aux cadres et agents fonctionnels et techniques de la chaine de la dépense. Ces derniers ont relevé les insuffisances et les difficultés rencontrées dans l'utilisation des applications métiers.

1.3.2. Présentation du projet

La présence des équipements passifs comme les hubs qui augmente le risque d'intrus obtenant l'accès au réseau et menant une attaque d'écoute nécessite une amélioration. Le schéma de conception de câblage pour l'interconnexion des différents équipements n'est pas bien géré : les extrémités des câblages interconnectés aux commutateurs ne sont pas bien organisées. L'absence d'un suivi d'entretien de câblage peut être un point faible pour la sécurité du câblage.

Chaque service possède une imprimante configurée et partagée sur un poste utilisateur. Ceci peut entrainer une vulnérabilité vue que toute panne du PC où est configuré l'imprimante engendre une panne générale pour tous les connectés.

Il y a également un défaut de climatisation de la salle serveur du système informatique et réseau, alors que les équipements informatiques sont conçus pour travailler dans un environnement spécifique pour respecter les conditions normales de fonctionnement.

Le ministère ne dispose pas un détecteur contre l'humidité et les dégâts d'eau, Il y a risque de propagation de l'eau dans la salle connectique ce qui peut causer des incidents.

Le manque de groupe électrogène doté d'une grande capacité et fonctionnant en mode relai automatique fait que les utilisateurs se retrouvent dans une obscurité totale pendant la coupure d'électricité.

La plupart des postes utilisateurs ne possèdent pas de session. Ceci offre à l'intrus la possibilité de collecter un ensemble d'information sur la cible (nom utilisateur, partage).

Aucun mécanisme n'est pris en considération pour lutter contre les attaques sur 12 mots de passe. Un intrus peut mener une attaque pour collecter les mots de passe afin d'accéder aux ressources matériels mises en question.

Quelques fois après la "couverture - intégration" des opérations de transferts reçus d'un autre comptable, on constate un dysfonctionnement de l'application du Système

Intégré de Gestion des Finances Publiques (SIGFiP)[6] qui fait que les comptes de contrepartie n'apparaissent pas. La non apparition de ces comptes de contrepartie entraine donc un déséquilibre de la balance du comptable assignataire de l'opération et, par conséquent, un déséquilibre de la balance générale agrégée des comptes du Trésor.[7]

Il existe aussi des difficultés relatives à la couverture des opérations de transferts reçus des Comptables des Structures Déconcentrées (C.S.D), lorsque les opérations ne sont pas saisies selon leurs natures. Autrement dit, les montants de différentes natures d'opérations sont saisis en un seul montant comme étant une même nature d'opération.

On note également le manque de contrôle d'accès à l'application par un même utilisateur sur plusieurs ordinateurs sans déconnexion préalable, le manque d'identification des machines connectées dans le réseau local, le problème d'optimisation de la base de données vu la lenteur d'exécution des requêtes et la lenteur du réseau informatique.

Il y a aussi l'absence d'un calendrier périodique pour la maintenance préventive des ordinateurs et l'irrégularité de la mise à jour des antivirus.

L'accès des locaux de travail n'est pas conditionné par les badges de sécurité.

Au regard de toutes ces difficultés, surgissent des interrogations :

- le réseau des comptables directs du Trésor dispose-t-il de ressources matérielles et humaines suffisantes pour les défis qui se profilent à l'horizon ?

- qu'est-ce qui est à l'origine d'un tel état de fait ?

Pour trouver la réponse à ces inquiétudes, nous avons choisi de réfléchir sur le thème : **« L'évaluation du système d'information du réseau des comptables directs : cas du Trésor public Togolais ».**

[6] Le SIGFiP est l'application informatique de l'exécution du budget de l'Etat depuis la phase administrative jusqu'à la phase comptable
[7] Balance consolidée des trois comptables principaux de l'Etat (CPE)

Le choix d'un tel thème s'explique par la nécessité d'améliorer la qualité de l'information comptable et financière de l'État.

1.3.3. Contexte et objectifs du projet

Les attentes du Ministère de l'Économie et des Finances (MEF) sur ce projet d'audit et sécurité informatique consistent à acquérir un ensemble d'approches de solutions visant à améliorer la qualité de l'information financière et comptable de l'État. Elles visent également à renforcer les contrôles, l'optimisation de la base de données, la sécurité des informations et la maitrise des fraudes internes et externes. Les fonctions de la solution cible doivent couvrir les besoins suivants :

- ✓ l'optimisation de la base de données;
- ✓ le renforcement des mesures sécuritaires du système applicatif et réseau;
- ✓ l'amélioration des outils de développement;
- ✓ l'assouplissement du Système Intégré de Gestion des Finances Publiques (SIGFiP) dans son utilisation.

1.3.4. Périmètre fonctionnel et technique du projet

Les spécifications fonctionnelles et techniques de l'audit du SIGFiP doivent couvrir les besoins suivants :

- ✓ la prise en compte de l'ensemble des dispositions applicatives et sécuritaires;
- ✓ l'optimisation de la base de données;
- ✓ l'examen des méthodes d'organisation, de contrôle, et de planification des services informatiques;
- ✓ l'appréciation de la formation, de la qualification et de l'aptitude du personnel;
- ✓ l'appréciation de la qualité, de l'accès, de la disponibilité et de la facilité de compréhension de la documentation;
- ✓ le descriptif des matériels, logiciels et documentations;
- ✓ l'appréciation d'adéquation entre les besoins et le système d'information;

- ✓ l'amélioration des outils de développement;
- ✓ la mise en place d'une solution côté hardware pour la gestion d'autorisation d'accès au réseau;
- ✓ la mise en place d'une solution software pour la gestion de domaine permettant de définir les ressources auxquelles l'ordinateur connecté peut avoir accès;
- ✓ La mise en place d'une solution de détection d'intrusion dans le réseau.

1.3.5. Planification du projet

Tableau I.1 : Planification des tâches du projet

La planification du projet consiste à déterminer et à ordonnancer les taches du projet, à estimer leurs charges et à déterminer les profils nécessaires à leur réalisation. Le tableau ci-dessous résume les différentes taches réalisées :

A partir du tableau de définition des tâches à réaliser, nous avons illustrer notre travail à travers la méthode PERT et le diagramme de Gantt.

1.3.5.1. La méthode PERT

Tâches	Durée (jours)	Condition d'antériorité
A. Phase d'avant-projet	05	-
B. Phase d'audit et d'analyse détaillée	45	A
C. Phase de proposition des solutions	15	B
D. Phase de test et d'observations	15	C
E. Phase de mise en production	30	D
F. Phase de recette du projet	05	E

La méthode PERT (Program Evaluation and Review Technology) est une méthode conventionnelle utilisable en gestion de projet, développée aux Etats-Unis dans les années 1950. Elle fournir une méthodologie pour décrire, représenter, analyser et suivre de manière logique les tâches à réaliser.

Avec la méthode PERT, on utilise un graphe de dépendances. Pour chaque tâche, on indique une date de début et de fin au plus tôt et au plus tard. Le diagramme permet de déterminer le chemin critique qui conditionne la durée minimale du projet.

Le but est de trouver la meilleure organisation possible pour qu'un projet soit terminé dans de meilleurs délais, et d'identifier les tâches critiques, c'est-à-dire les tâches qui ne doivent souffrir d'aucun retard sous peine de retarder l'ensemble du projet.

Dans la méthode PERT, on calcule deux valeurs pour chaque étape :

- ✓ la date au plus tôt : il s'agit de la date à laquelle la tâche pourra être terminée au plus tôt, en tenant compte du temps nécessaire à l'exécution des tâches précédentes;
- ✓ la date au plus tard: il s'agit de la date à laquelle une tâche doit être terminé à tout prix si l'on ne veut pas retarder l'ensemble du projet.

16

La figure ci-dessous illustre le schéma PERT :

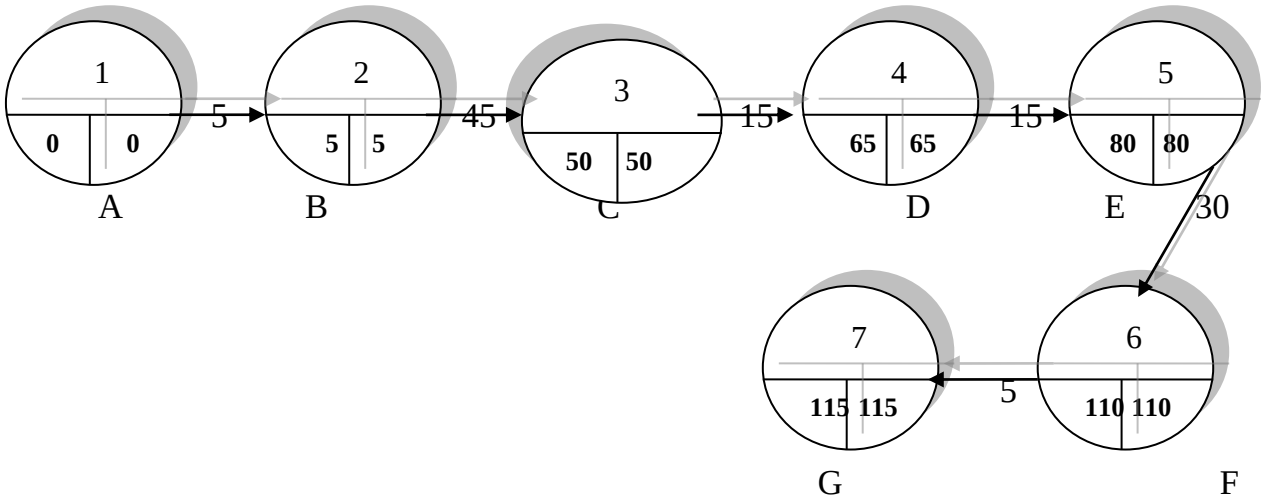


Figure I.1 : Schéma PERT

1.3.5.2. Diagramme de GANTT

Le diagramme de Gantt est un outil utilisé (souvent en complément d'un réseau PERT) en ordonnancement et en gestion de projet et permettant de visualiser dans le temps des diverses tâches composant un projet. Il s'agit d'une représentation d'un graphe connexe et orienté, qui permet de représenter graphiquement l'avancement du projet. Cet outil répond à deux objectifs : planifier de façon optimale ainsi que communiquer sur le planning établi et les choix qu'il impose. Le diagramme permet :

- ✓ de déterminer les dates de réalisation d'un projet;
- ✓ d'identifier les marges existantes sur certaines tâches;
- ✓ de visualiser le retard ou l'avancement des travaux;

Dans un diagramme de Gantt on représente :

- ✓ en abscisse les unités de temps (exprimées en mois, en semaine ou en jours);
- ✓ en ordonnée les différents postes de travail (ou les différentes tâches).

Le diagramme de Gantt complète l'information produite dans le digramme [17] Celui-ci permet d'analyser toutes les relations qui existent entre les activités, de dégager les séquences d'activités, d'identifier le chemin critique et les dates de début et de fin (au plus tôt et au plus tard) de chaque activité. Le diagramme de Gantt permet de choisir les dates qui seront effectivement retenues pour réaliser les activités et, éventuellement, de montrer les relations entre les activités et donc les incidences en termes de retard.

En d'autres termes, le PERT est un outil d'analyse alors que le Gantt est un outil de planification. Une autre différence entre les deux outils est aussi le lien qui existe entre la durée des tâches et l'espace utilisé pour les représenter dans les diagrammes. Dans un diagramme de Gantt, l'espace est directement proportionnel à la durée alors que dans un diagramme de PERT, la durée n'est pas gérée graphiquement, toutes les activités ayant la même taille dans le diagramme, quelle que soit leur durée. Ces

différences font que le diagramme PERT est plus complexe à utiliser, car il est moins proche de la réalité.

La figure I.2 se trouvant à la page 18, permet de définir les modes des tâches, la désignation, la durée d'exécution de la tâche, la date début et date fin, la dépendance entre les tâches et les ressources disponibles pour exécuter la tâche. Ainsi, une chronologie de la réalisation des tâches est représentée de façon automatique et précise. La figure I.2 à la page 18 illustre le diagramme de Gantt.

Tâche					
-Phase avant projet	**5 jours**	Jeu 02/11/17	Mer 08/11/17		
collecte et préparation des éléments nécéssaires au bon déroulement du projet	1 jour	Jeu 02/11/17	Jeu 02/11/17		Informaticien
mobilisation des équipes	1 jour	Ven 03/11/17	Ven 03/11/17		direction
réunion de lancement du projet	1 jour	Lun 06/11/17	Lun 06/11/17	2	Informaticien
détermination du périmetre technique et fonctionnel	1 jour	Mar 07/11/17	Mar 07/11/17	4DD	Informaticien
mise en place de l'environnement du projet	1 jour	Mer 08/11/17	Mer 08/11/17	5DD	Informaticien
-Phase d'audit et d'analyse détaillée	**45 jours**	Mer 08/11/17	Mar 09/01/18		
les différents parties faisant office d'audit	1 jour	Mer 08/11/17	Mer 08/11/17	4	Informaticien
module applicatif	10 jours	Mer 08/11/17	Mar 21/11/17	8DD	Informaticien
module base de données	10 jours	Mer 08/11/17	Mar 21/11/17	9DD	Informaticien
module système et réseau	10 jours	Mer 22/11/17	Mar 05/12/17	10	Informaticien
module sécurité	14 jours	Mer 06/12/17	Lun 25/12/17	11	Informaticien
-Phase de proposition des solutions	**15 jours**	Mar 26/12/17	Lun 15/01/18	12	
solution applicative	3 jours	Mar 16/01/18	Jeu 18/01/18	13	Informaticien
solution base de données	4 jours	Ven 19/01/18	Mer 24/01/18	14	Informaticien
solution système et réseau	4 jours	Jeu 25/01/18	Mar 30/01/18	15	Informaticien
solution sécurité	4 jours	Mer 31/01/18	Lun 05/02/18	16	Informaticien
-Phase de test et d'observations	**15 jours**	Mar 06/02/18	Lun 26/02/18	17	direction;Informat

18

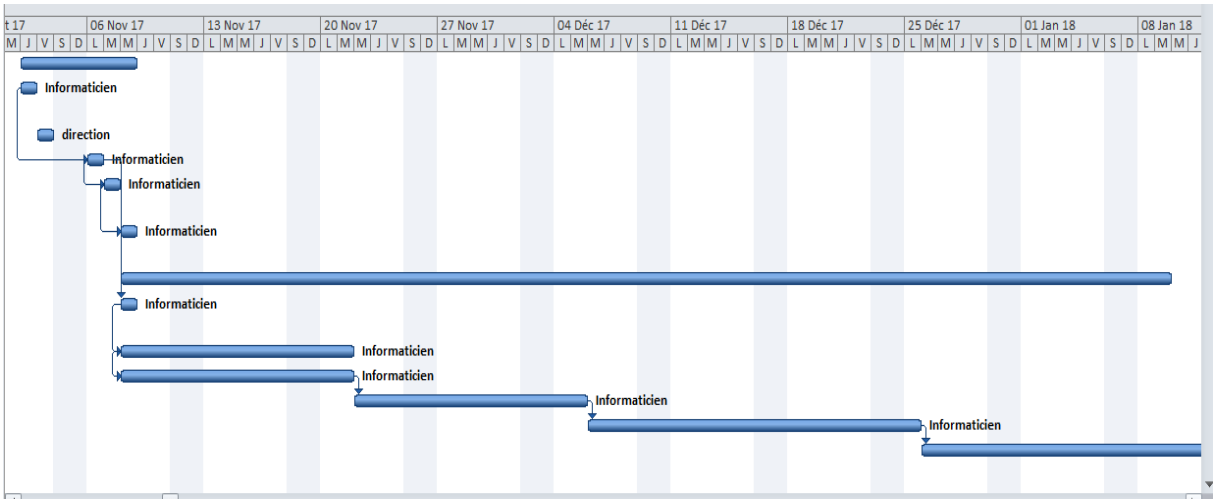


Figure I.2 : Diagramme de Gantt

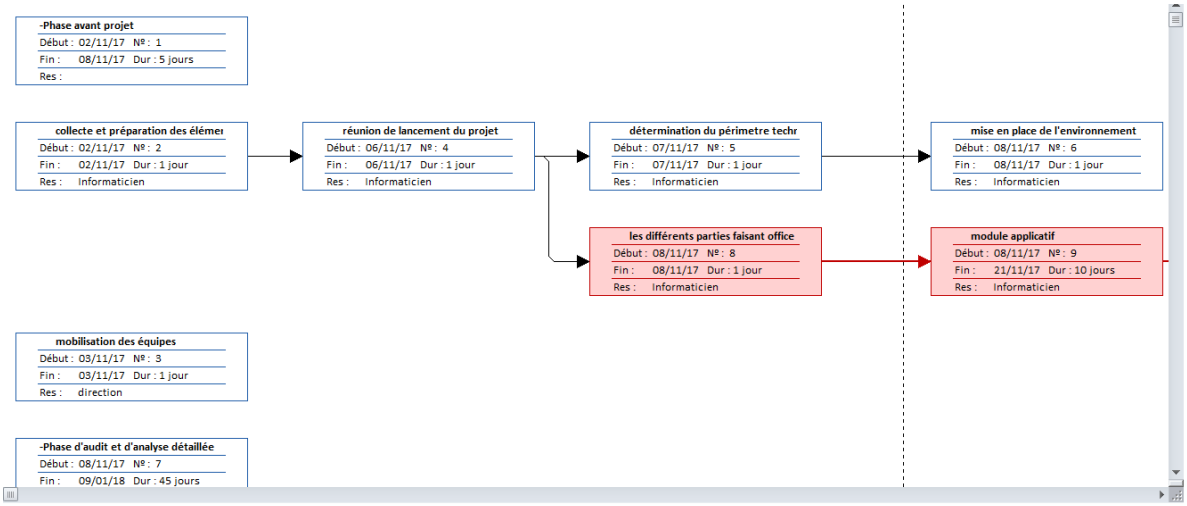


Figure I.3 : Schéma réseau et chronologie des tâches du projet

Le périmètre du projet définit par le cahier de charge va nous permettre de faire l'étude de l'existant et de proposer une solution d'amélioration du système comptable et financier.

CHAPITRE II : PRESENTATION ET ANALYSE DE L'EXISTANT

Dans ce chapitre, nous allons commencer par la présentation du système existant et terminer par son analyse.

2.1. Le Système Intégré de Gestion des Finances Publiques (SIGFiP)

L'évolution de la technologie a rendu obsolète le progiciel FOX - PROW. Pour y remédier les autorités ont pris la décision d'introduire un nouveau logiciel qui va intégrer l'ensemble du processus depuis les services ordonnateurs jusqu'aux comptables publics.

Le SIGFiP est régi par l'arrêté n° 249/MEF/SP-PRPF du 22 octobre 2009 portant création, attributions et organisation d'une cellule d'administration du Système Intégré de Gestion des Finances Publiques au sein du Ministère de l'Economie et des Finances en attendant la création d'une direction du SIGFiP. **[8]**

C'est un logiciel informatique qui relie les différents acteurs des finances publiques et qui leur permet d'exécuter en temps réel des dépenses et des recettes du budget de l'Etat, des comptes spéciaux du Trésor et des budgets annexes.

2.1.1. Le schéma fonctionnel du SIGFiP

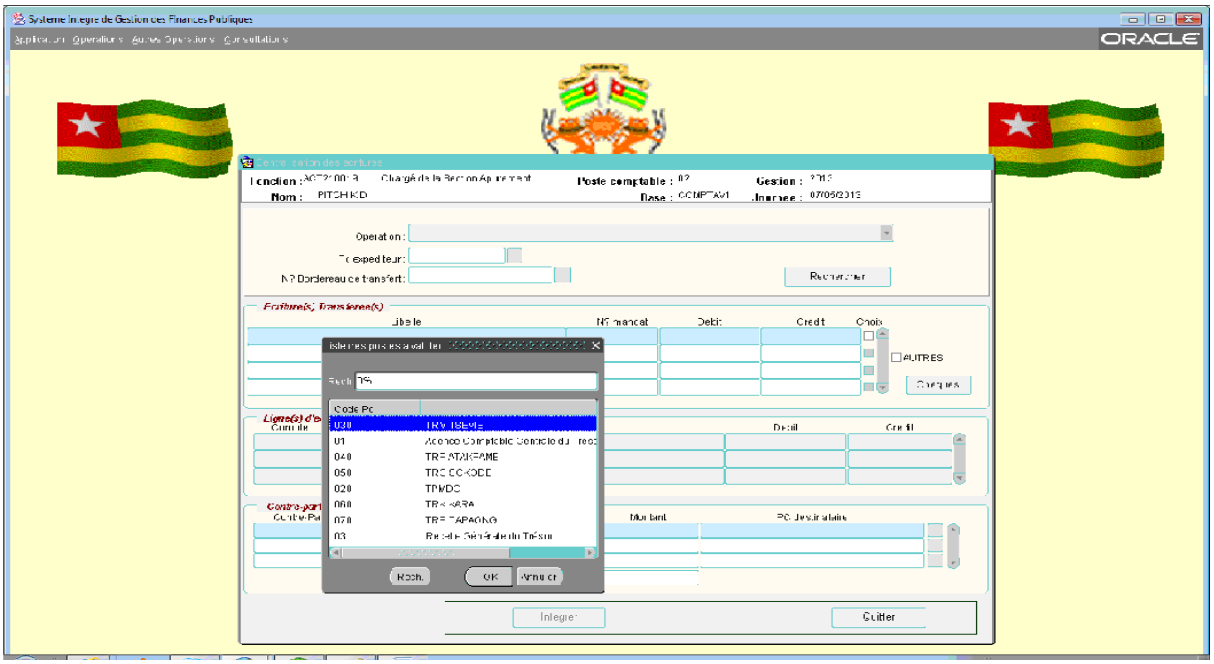
Le schéma fonctionnel englobe l'ensemble des fonctionnalités du progiciel (annexe 2). La DGTCP utilise le module SIGTA (SIGFiP Comptabilité). Ce module est opérationnel au Trésor public depuis janvier 2010 et les balances générales mensuelles du Trésor y sont produites.

2.1.2. L'exploitation de l'application SIGFiP

Le SIGFiP est aujourd'hui, dans l'optique d'améliorer la gestion de la trésorerie, une forme moderne de gestion du budget de l'État. Actuellement, toutes les écritures comptables sont interactives.

La mise en application du module SIGFiP Comptabilité a permis aux utilisateurs d'abandonner les fiches d'écritures telles que les fiches de débit, de crédit et de centralisation. Les écritures comptables sont passées directement dans l'application.

Ainsi, toute opération traitée à un poste comptable non assignataire est transférée au comptable assignataire par un Bordereau de Transfert des Opérations Comptables (BTOC) pour couverture et intégration à l'aide du formulaire ci-dessous :



<u>Figure II.1</u> : Formulaire de couverture et d'intégration des opérations comptables

Le module SIGTA a pour objectifs principaux :

- ✓ de suivre les actes de dépenses en provenance des ordonnateurs délégués ;
- ✓ de comptabiliser les opérations de chaque poste comptable ;
- ✓ de rejeter les titres de confirmation ou les demandes de paiement en cas d'insuffisances de crédit ;
- ✓ de mettre en application des données budgétaires ;
- ✓ d'optimiser l'exécution des dépenses, des recettes et de la trésorerie par une réduction des délais de traitement et un renforcement des contrôles afin d'éviter toutes formes de dérapages (double paiement, paiements indûs) ;

- ✓ d'améliorer la cohérence et la qualité des données comptables et statistiques avec l'édition automatique de la situation d'exécution budgétaire et comptable ;
- ✓ de réduire les délais dans le circuit des dépenses sans sacrifier les contrôles jugés nécessaires ;
- ✓ d'assurer la fluidité de l'information tout le long de la chaîne et la production régulière des tableaux de bord correspondants (grand livre, balance) ;
- ✓ d'assurer la disponibilité des informations économiques et financières sous toutes les formes de synthèse désirées ;
- ✓ d'étendre le SIGFiP à tous les acteurs du réseau des comptables directs du Trésor (chaque utilisateur disposerait sur son bureau d'un ordinateur relié à la machine centrale dite serveur) ;
- ✓ de réduire les tensions sur la trésorerie ;
- ✓ de réguler la consommation des crédits budgétaires alloués aux différents services ;
- ✓ de mettre en adéquation le niveau des dépenses à effectuer et les prévisions de ressources à recouvrer;
- ✓ d'assurer la production de la qualité de l'information financière et comptable;
- ✓ de sécuriser les données du patrimoine de l'État.

Le SIGFiP à lui seul ne suffit pas. Il faut aussi l'intervention des acteurs.

2.1.3. Les différents intervenants dans le progiciel

Pour réaliser ces missions, plusieurs acteurs interviennent dans l'application. Ces acteurs sont : les administrateurs du système informatique, les comptables principaux de l'Etat, les comptables, les guichetiers, les caissiers principaux, les teneurs de comptes, les agents de transfert, les agents de consignation, les agents de règlements, les agents de paiement, les agents de vérification, les agents d'ordres de recette, les agents de traitements (compte de dépôt, régie d'avance, exonération, etc…)

L'administrateur peut créer d'autres utilisateurs dans le système pouvant également avoir accès au réseau « SIGTA ». Les autres acteurs ne sont que des utilisateurs du système. Chaque utilisateur a son nom utilisateur et son mot de passe.

L'écran de la figure III.2 à la page 23 permet à l'utilisateur de se connecter à l'application :

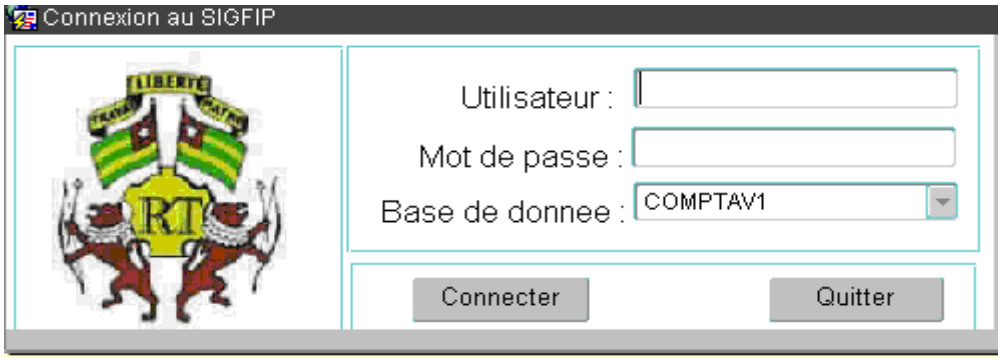


Figure II.2 : Formulaire de connexion au SIGFiP

Lorsque le nom d'utilisateur et le mot de passe sont corrects, l'utilisateur accède à l'écran d'accueil suivant :

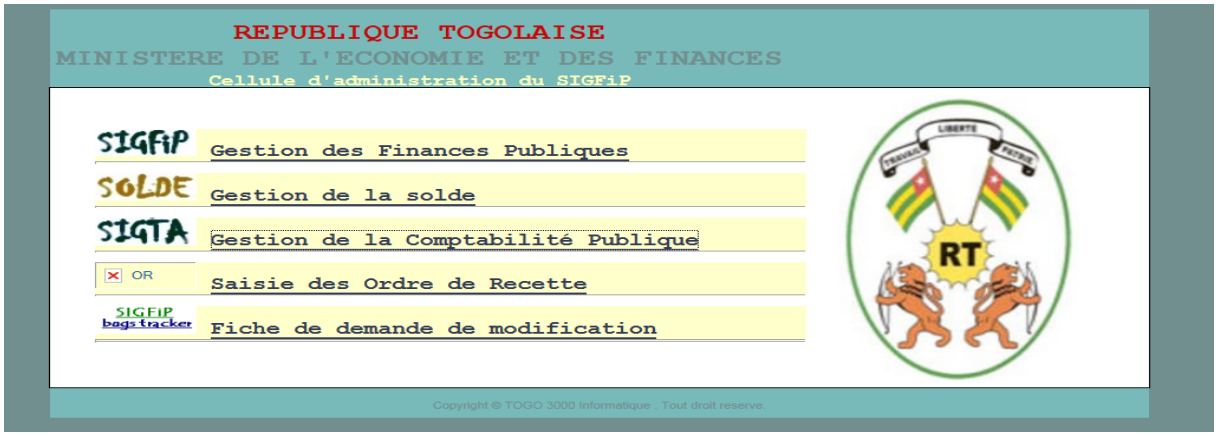


Figure II.3 : Ecran d'accueil aux différents modules du SIGFiP

Le clic sur le module « SIGTA » donne lieu à l'affichage ci-dessous :

24

Figure II.4 : Ecran du menu général des utilisateurs

Le sous menu comporte plusieurs rubriques en fonction du traitement à effectuer. A partir dudit menu, chaque utilisateur effectue le traitement qui le concerne dans le système.

Que ce soit à l'Agence Comptable Centrale, à la Paierie Générale ou à la Recette Générale du Trésor, les divisions "comptabilités" respectives sont chargées de :

- ✓ centraliser et valider les opérations comptables;
- ✓ tenir et suivre les comptes financiers;
- ✓ apurer et intégrer les opérations effectuées par les autres structures comptables ;
- ✓ produire les états et situations comptables et extracomptables ;
- ✓ produire le compte de gestion.

Pour réaliser ces fonctions, chaque division Comptabilité a un chef chargé de valider les opérations comptables.

Les menus utilisés à chaque poste comptable diffèrent selon les opérations à valider. Dans le menu « opérations comptables », on choisit « validation prise en charge des actes » et on clique sur « recherche ». On vérifie et sélectionne les actes (mandat, chèque Trésor) à prendre en charge puis on clique sur « valider ».

Le menu ci-après illustre entre autres, une opération de validation des actes comptables.

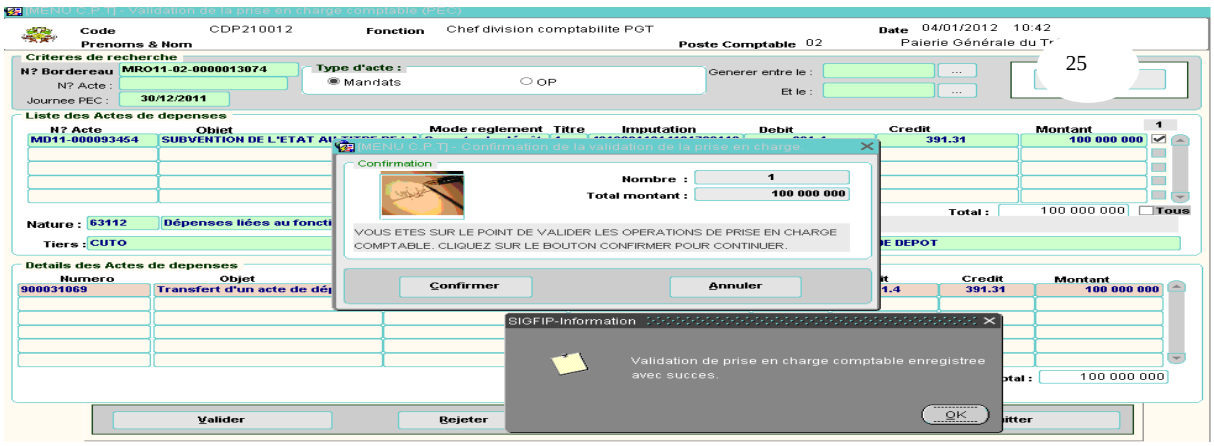


Figure II.5 : Ecran de validation des actes comptables

Notons qu'il existe des cas où le contrôle de paiement de la dépense n'est pas concluant. Dans ce cas on assiste au rejet pur et simple du titre de paiement. Le rejet informatique se fait comme suit : sélectionner le mandat à rejeter, cliquer sur l'onglet rejeter pour sélectionner ou saisir le motif de rejet et éditer le bordereau de rejet en double (original et copie). L'écran ci-après est utilisé :

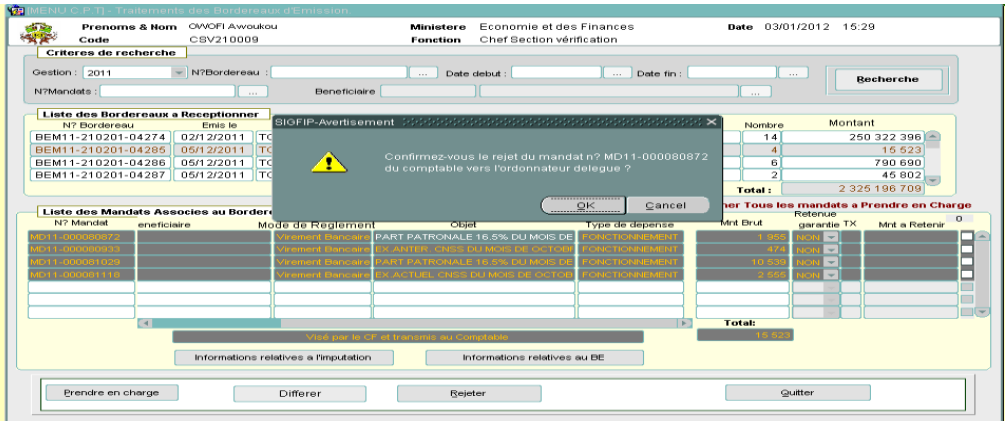
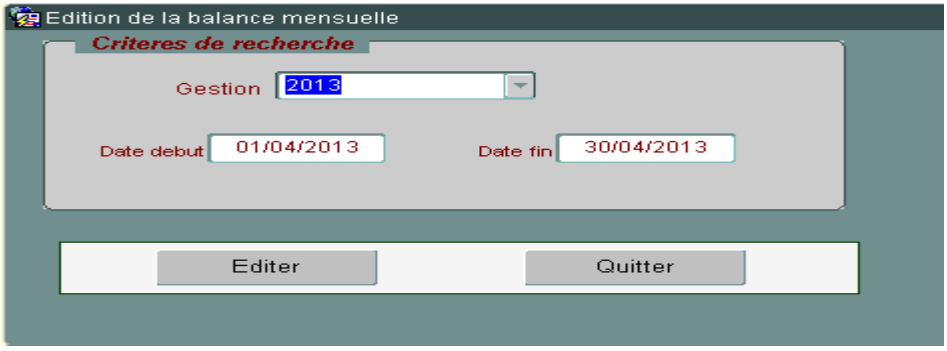


Figure II.6 : Ecran de contrôle de paiement de la dépense publique

Pour réaliser la production et l'analyse de la balance générale périodique des comptes, on utilise le menu « éditions comptables ».

Dans ce menu, on choisit d'abord « Balance », ensuite on précise la gestion et la période voulue et enfin on clique sur « Editer ». La fenêtre ci-dessous illustre l'idée :



26

Figure II.7 : Ecran d'édition de la balance mensuelle des opérations comptables

On obtient le résultat suivant selon le type d'opération (grand livre ou balance).

MINISTERE DE L'ECONOMIE ET DES FINANCES — REPUBLIQUE TOGOLAISE — Direction Generale du Tresor et de la Comptabilité Publique

Travail-Liberté-Patrie

GRAND LIVRE — DATE D'EDITION 07/05/2013

Poste comptable : Paierie Générale du Trésor

Période du : 01/03/2013 30/03/2013 GESTION 2013

N° du compte	Intitulé du compte	Balance Débit	Balance Crédit
391.30	Transfert des dépenses	893 023 862	1 296 988 590

Journée	Montant Debit	Montant Crédit
04/03/2013	20 559 406	0
05/03/2013	8 430 000	0
06/03/2013	4 548 800	162 606

Figure II.8 : Ecran d'affichage d'état comptable "Grand Livre"

Les montants au débit correspondent aux opérations pour lesquelles le comptable n'est pas assignataire. Ce dernier transfère ces opérations au comptable assignataire. Par contre les montants au crédit correspondent aux opérations de transfert reçues d'autres comptables mais pour lesquelles le comptable qui les reçoit est assignataire.

L'écran ci-dessous à la page suivante correspond à l'édition de la balance. Celle-ci retrace toutes les opérations effectuées dans le mois avec regroupement par nature desdites opérations.

Il n'y a pas que l'étude du schéma fonctionnel, il faut aussi faire une analyse technique du progiciel SIGFiP.

2.2. La couverture technique du SIGFiP

L'élément technique du Système Intégré de Gestion des Finances Publiques concerne la couverture du progiciel sur l'étendue du territoire. Techniquement, le progiciel est doté des serveurs installés à la centrale avec un schéma réseau dédié à cet effet. En plus, on constate que les postes appliquent une architecture à trois niveaux (appelé architecture 3-tiers). Cela signifie qu'il y a un niveau intermédiaire, c'est-à-dire il existe une architecture partagée entre trois ressources :

- ✓ Premièrement, un client "ordinateur demandeur de ressources" équipé d'une interface utilisateur chargée de la présentation. Elle correspond à la partie visible et interactive de l'application pour les utilisateurs. On parle d'interface homme-machine.

- ✓ Deuxièmement, un serveur d'application est chargé de fournir la ressource mais faisant appel à un autre serveur. Il correspond à la partie fonctionnelle de l'application, celle qui implémente la logique métier, et qui décrit les opérations que l'application opère sur les données en fonction des requêtes des utilisateurs, effectuées au travers de la couche de présentation

- ✓ Troisièmement, un serveur de base de données, fournissant au serveur d'application les données dont il a besoin. Il correspond à la partie gérant l'accès aux données de l'application. Ces données peuvent être propres à l'application, ou gérées par une autre application.

- Appréciation

  L'implémentation de cette architecture est plus efficace du faite qu'elle se base sur la technologie web.

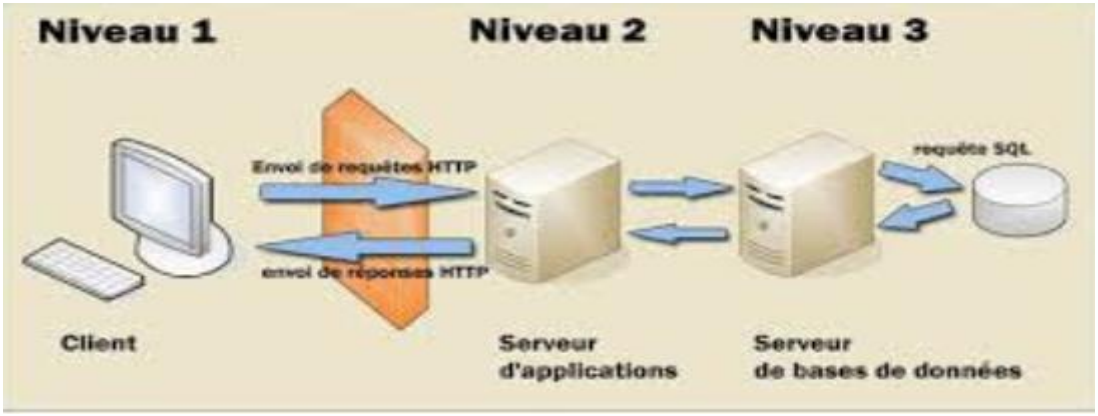


Figure II.9 : Schéma système architecture 3 tiers

2.2.1. Les caractéristiques techniques des équipements

Les équipements sont composés d'ordinateurs appelés serveurs, d'ordinateurs pour les utilisateurs (PC) et les autres éléments informatiques indispensables pour la mise en

place du système informatique. Il faut noter que les caractéristiques ne sont pas les mêmes selon les équipements.

2.2.1.a. Les serveurs

Les serveurs sont des systèmes électroniques dotés de caractéristiques particulières pour pouvoir répondre à une configuration technique adéquate. Le tableau ci-après illustre le contenu desdits serveurs.

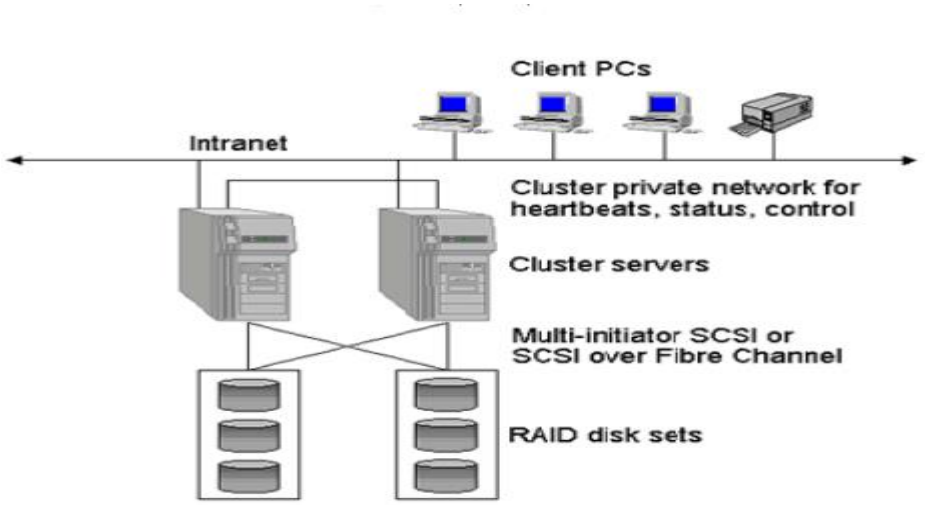
Tableau II.1 : Caractéristiques techniques des serveurs du SIGFIP

Constructeur	Bull
Description du serveur	Novascale 3045
Système d'exploitation	Linux
Facteur de forme	RACK 5U
Processeur	Itanuim II (IA-64) 1.6GHZ
Nombre de Processeur	Quatre
RAM (mémoire vive à accès en lecture et en écriture.**)**	128Go
Contrôleur de stockage	LSI Logic/Symbios Logic 53c1030
Baies de stockage pour serveur	FDA NEC iStorage 1000
Disque dur (support magnétique de stockage de données numériques).	2x146Go
Moniteur (l'écran où s'affichent les informations saisies ou demandées par l'utilisateur)	Ecran KVA
Réseaux Réseaux	1 Carte Intel Pro100Mps (Intel 82557/8/9, interface de management) 4 Cartes réseaux Ethernet Gigabit (2Intel Corporation 82571EB et 2Intel Corporation 80003ES2LAN) Backbone : Cisco catalyst 4507R-E Switch d'accès : Cisco catalyst 2960 Switch de distribution : Cisco catalyst 3750 Routeurs : Cisco 2821, 2921, 819, 1900 Firewalls : juniper SSG 350M, SSG 140, SSG20 Radio BLR : Redmax AN-100UX, Redmax SUO 3436F, Ubiquiti PowerBeam 5ac-400 VSAT: modem i-Direct X3, ub i-direct 15100-IF
Carte graphique (composant informatique qui gère l'affichage graphique)	ATI ES1000

Alimentation redondante	Oui
Lecteur de bande	Tandberg T5400
Ports E/S externes	Parallèle : Série ; Périphérique de pointage (souris) : 1 ; carte graphique : 1 ; clavier (no brand KVM A1)

Outre les caractéristiques physiques, les serveurs sont dotés d'une base de données structurée et d'une application conçue à partir des outils de développements du système de gestion de base de données Oracle.

Ces serveurs sont configurés en cluster (technologie haute disponibilité) avec une base de données Oracle 10g (Système de Gestion de Base de Données Relationnelles). Cette configuration est représentée par la figure II.10, à la page vingt neuf.



<u>Figure II.10</u> : Schéma configuration des serveurs en cluster.

Oracle Real Application Clusters (RAC) est une option de la base de données Oracle Entreprise Edition maintes fois primée. Oracle RAC est une base de données en grappe (ou "cluster") dotée d'une architecture de cache partagé qui s'affranchit des limitations des approches traditionnelles de non-partage ou de simple partage des disques, pour offrir une solution de base de données extrêmement évolutive et disponible pour toutes vos applications professionnelles. L'option Oracle Real Application Clusters (RAC) assure le déploiement d'une même base de données sur une grappe (ou cluster) de

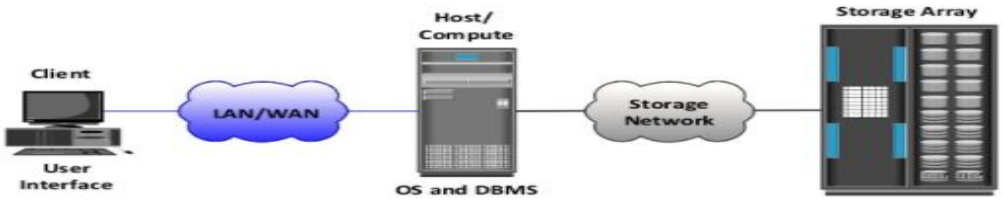
serveurs de façon transparente, garantissant ainsi une protection contre les pannes matérielles ou facilitant la mise en place des arrêts planifiés de maintenance. Oracle RAC apporte au meilleur de la technologie Oracle : disponibilité et évolutive.

- Recommandation

Face à l'augmentation des volumes et à la complexité des données sur lesquelles se base l'activité d'une organisation, nous recommandons l'hébergement de celles-ci dans un data center nécessitant d'être à la fois flexibles et évolutives.

Nous recommandons également l'externalisation du stockage des données afin de garantir la sécurité et la fiabilité de ces dernières. La solution de stockage extérieur des données en data center présente de nombreux avantages pour les entreprises. En faisant appel à ce processus, ces entreprises s'assurent de garder le contrôle de leur infrastructure. Elles profitent également d'une grande expertise dans le domaine du stockage : technologie de pointe (serveurs performants), évolutivité, mises à jour et sécurité maximale des installations ainsi que disponibilité totale des données stockées.

La figure II.11, ci – dessous, illustre l'implémentation du Data Center pour abriter toutes les informations financières et comptables de la DGTCP.



<u>Figure II.11</u> : Schéma Data Center : une solution complète pour les sociétés

Ces serveurs sont des ordinateurs principaux sur lesquels les utilisateurs se connectent pour effectuer le travail. Si un serveur tombe en panne, le second prend le relai. La baie de disque constitue le lieu de stockages de toutes les données financières et comptables.

2.2.1.b. Les postes de travail

Pour permettre aux utilisateurs du progiciel d'avoir accès aux serveurs, ces derniers sont dotés d'ordinateurs (PC). Les ordinateurs sont de trois types selon les constructeurs que sont le HP Compaq Home Edition, le NEC et le HP Pro 3010MT. Les caractéristiques de chaque type d'ordinateur sont résumées dans le tableau II.2 à la page trente deux.

N° Ordre			**Nbre PC Par type**
1	Constructeur	HP Compaq Home Edition	175
	Description du PC	DD : 150Go, RAM : 3Go, Processeur Core Duo	
	Système d'exploitation	Windows XP	
2	Constructeur	NEC	25
	Description du PC	DD : 150Go, RAM : 2Go, Processeur Core Duo	
	Système d'exploitation	Windows XP	
3	Constructeur	HP Pro 3010MT	150
	Description du PC	DD : 360Go, RAM : 4Go, Processeur :Core Duo	
	Système d'exploitation	Windows 7	

Tableau II.2 : Caractéristiques techniques de quelques ordinateurs connectés aux serveurs

Légende :

DD : disque dur ;

RAM : mémoire vive à accès en lecture et écriture (Read Only Memory);

Go : capacité d'un composant informatique à stocker l'information ;

Processeur : circuit électronique qui effectue les opérations arithmétiques et logiques.

- ✓ Appréciation

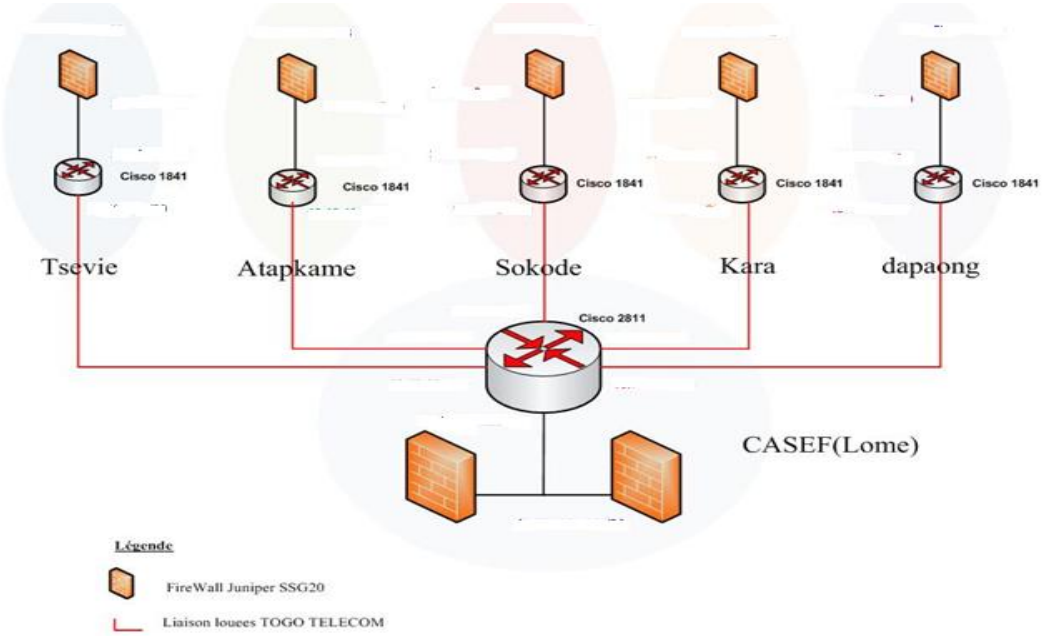
On constate que la configuration matérielle répond aux exigences minimales pour la configuration des applications et pour une exploitation facile et assurer une rapidité des traitements.

Pour une meilleure interconnexion des ordinateurs, l'équipement réseau informatique a été mis en place.

2.2.1.c. Schéma synoptique du réseau informatique

La mise en place du système réseau informatique a facilité l'interconnexion des utilisateurs et l'extension du SIGFiP en déconcentré. La figure ci-dessous illustre la configuration du réseau informatique.

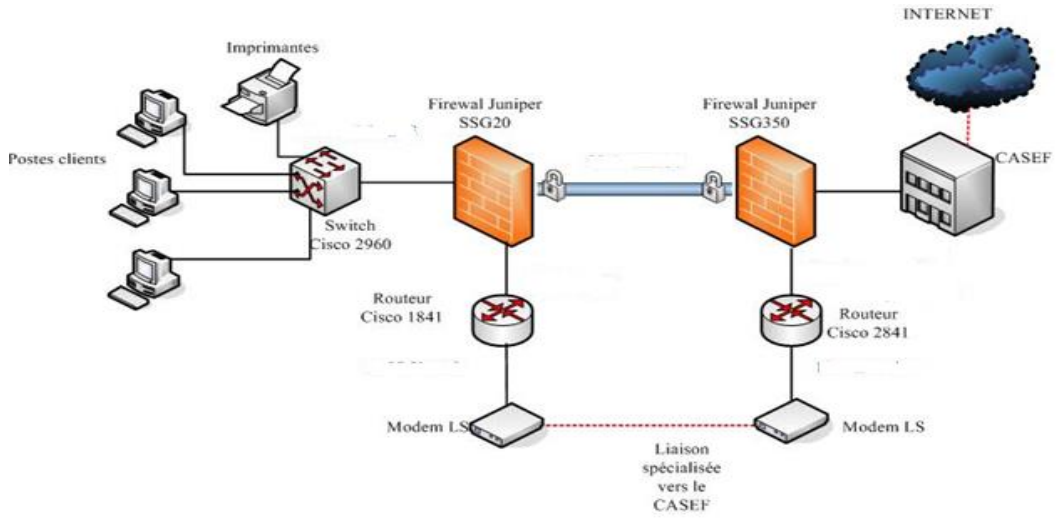
<u>Figure II.12</u> : Schéma synoptique d'extension SIGFiP dans les Trésoreries Régionales.



D'après le schéma, chaque site (Région) dispose d'un routeur[8] connecté au routeur principal situé au Centre Administratif des Services Economiques et Financiers (CASEF). L'adresse IP (Internet Protocol)[9] de chaque routeur identifie de façon unique le réseau. Pour des raisons de sécurité les adresses en question ne peuvent pas être affichées.

Le routeur principal est protégé par deux pare-feu que sont les Firewall[10] pour la sécurité des données. L'interconnexion entre les services centraux et les structures en déconcentré est faite par liaison TOGO TELECOM. De plus, chaque routeur des régions est aussi protégé par un pare-feu.

Ainsi, lorsqu'une information est destinée à une région donnée, elle passe par le routeur principal pour arriver au routeur spécifique selon l'adresse du destinataire et vice versa.



Pour une meilleure transmission d'information, la figure ci-dessus a été également configurée :

Figure II.13 : Schéma de transmission des données aux différents utilisateurs du progiciel.

[8] Equipement réseau qui interconnecte les sous réseaux
[9] Nom unique qu'on attribue à une machine dans un réseau
[10] Equipement qui protège le réseau contre les accès non autorisés

Ainsi, par liaison spécialisée (réseau de l'opérateur par ligne téléphonique), l'information arrive aux différents routeurs à travers le modem (modulateur et démodulateur)[11]. Ces derniers à leur tour véhiculent le message jusqu'au switch[12] (pont de transmission de l'information). Tous les ordinateurs connectés au switch accèdent à l'information selon l'adresse IP qu'ils portent. Précisons que cette technologie offre la possibilité d'installer une imprimante réseau. Chaque utilisateur peut facilement imprimer à distance.

La mise en place des équipements informatiques a énormément facilité l'extension du système dans les structures en déconcentré.

2.2.2. Les Switch et les Hubs

Les différents postes de travail sont interconnectés via les Switch et les hubs en cascade.

- ✓ Appréciation

Les Switch envoient directement le trafic seulement à la destination, contrairement aux hubs qui envoient le trafic à tous les ports et non seulement à la destination.
L'utilisation des hubs augmente le risque d'intrus obtenant l'accès au réseau et menant une attaque d'écoute.

- Recommandation

Il est conseillé de remplacer tous les équipements passifs par des équipements actifs.

2.2.3. Le câblage informatique

Le câblage informatique installé dans les bâtiments est conçu pour fonctionner de façon optimale pour permettre des évolutions futures. Tous les équipements sont interconnectés via le câblage de type paire torsadé catégorie 5. Les boitiers des prises muraux sont repérés par des étiquettes portant un numéro unique sur le réseau et qui est repéré facilement dans le panneau de brassage pour l'interconnexion avec les commutateurs "prise Rj45".

- ✓ Appréciation

[11] Equipement réseau qui sert à convertir les données numériques en signal analogique transmissible par le réseau
[12] Equipement réseau qui relie les postes utilisateurs

Le système de câblage installé fonctionne selon les besoins en terme de bande passante et de débit disponible.

Le schéma de conception de câblage pour l'interconnexion des différents équipements n'est pas bien géré : les extrémités des câblages interconnectés aux commutateurs ne sont pas bien organisées.

L'absence d'un suivi d'entretien de câblage peut être un point faible pour la sécurité du câblage.

2.2.4. Les imprimantes

Chaque service possède une imprimante configurée et partagée sur un poste utilisateur.

- ✓ Appréciation

La présence de ce type d'imprimante est un avantage pour le ministère du point de vue coût d'une part, mais aussi c'est une vulnérabilité vu que toute panne du PC où est configuré l'imprimante engendre une panne générale pour tous les connectés.

- ✓ Recommandation

Prévoir l'utilisation des imprimantes réseaux, où la configuration est gérée par l' administrateur réseau, et où l'attribution d'accès est selon le paramètre IP de l'imprimante et non d'un PC.

SUITE VOIR LA NUMEROTATION

2.3. La couverture du SIGFiP

Le SIGFiP couvre certains ministères des services centraux et en déconcentré. L'extension du progiciel a été effective dans les cinq régions avec des résultats encourageants. Ces régions sont : la région des Savanes (Dapaong), la région de la Kara (Kara), la région Centrale (Sokodé), la région des Plateaux (Atakpamé), la région Maritime (Tsévié).

2.3.1. La couverture de l'application dans les ministères

Elle est effective via la boucle locale radio (BLR) qui permet d'interconnecter les ministères bénéficiaires. Entre autres ministères on a :

- ✓ MESR : ministère de l'enseignement supérieur et de la recherche;
- ✓ MTP : ministère des travaux publics;

- ✓ MEPSA : ministère de l'enseignement primaire et secondaire et de l'alphabétisation;
- ✓ MEAHV : ministère de l'élevage, agriculture, hydraulique villageoise;
- ✓ MS : ministère de la santé;
- ✓ MAEP : ministère de l'agriculture, élevage et de la pèche;
- ✓ METFP : ministère de l'enseignement technique et de la formation professionnelle.

A ces ministères, s'ajoutent la trésorerie principale Lomé commune (TPLC), les trésoreries régionales, les services des forces armées togolaises (DSFAT) et les différentes structures centrales du MEF selon les niveaux. La figure II.14, ci - dessous, illustre l'extension du SIGFiP dans les ministères.

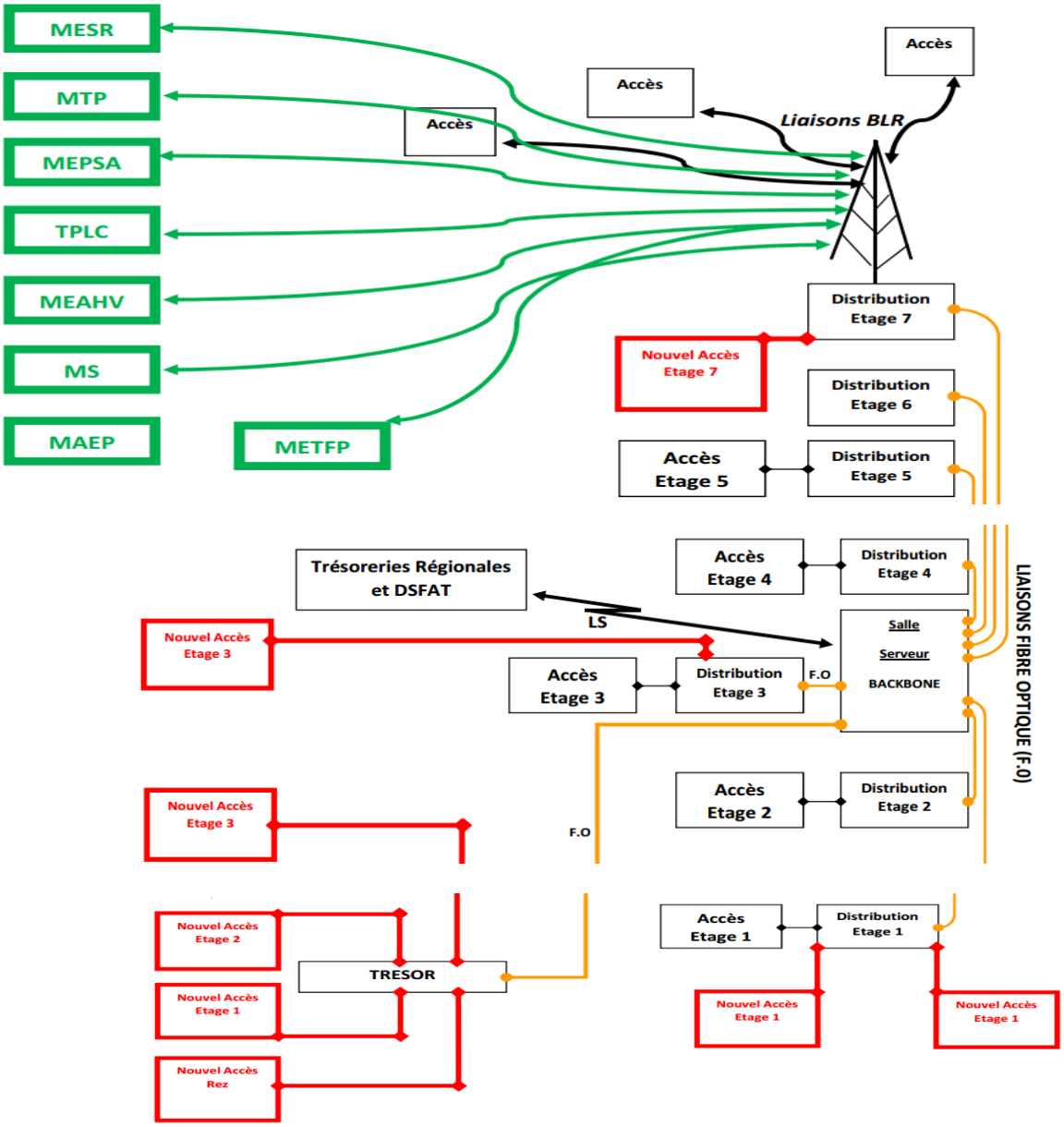


Figure II.14 : Schéma d'interconnexion et de distribution d'accès au réseau SIGFiP des différents services.

2.3.2. La couverture de l'application dans les services en déconcentré

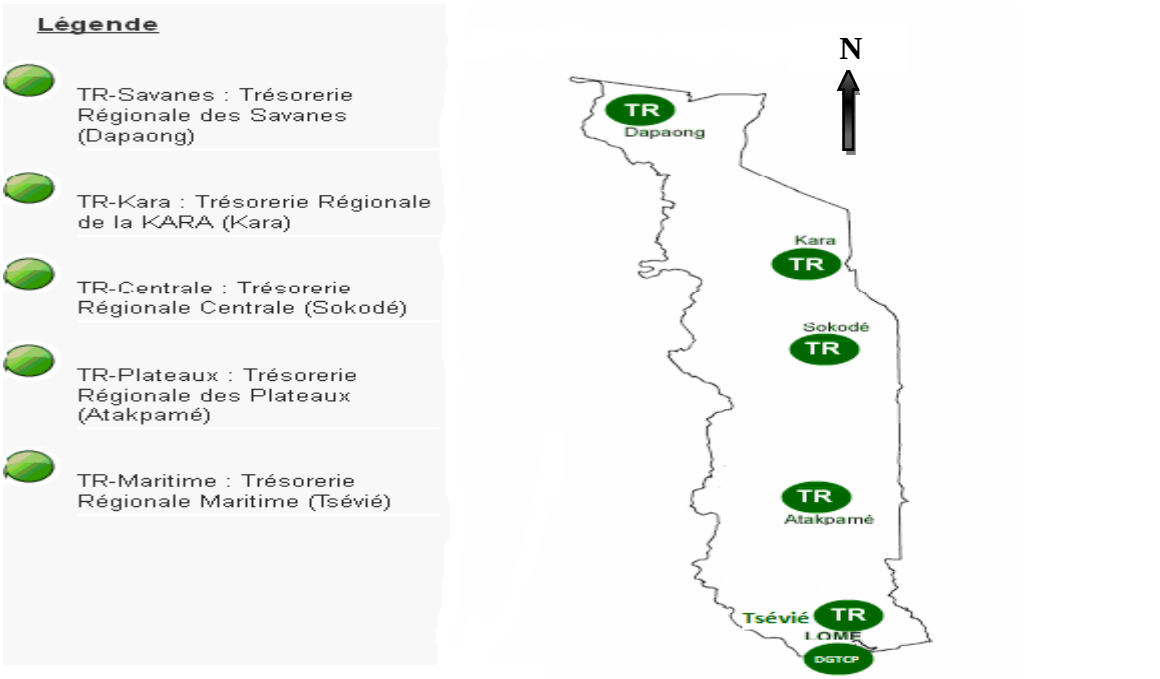
En déconcentré, SIGFiP Comptabilité est opérationnel uniquement dans les Trésoreries Régionales (TR) et à la Trésorerie Principale des Missions Diplomatiques et Consulaires (TPMDC). Cette extension a permis aux utilisateurs d'effectuer de façon interactive les Bordereaux de Transfert des Opérations Comptables (BTOC).

Les Trésoriers (T) après traitement de leurs opérations (budgétaires ou de trésorerie), les transfèrent à leur Trésorier Régional (TR). Cependant SIGFiP n'étant pas encore fonctionnel dans les postes de Trésorerie, les trésoriers envoient leurs opérations au TR de la circonscription financière. A la Trésorerie Régionale, des agents sont désignés pour tenir les postes des T. Ces derniers procèdent à la saisie des opérations avant de les transférer au TR. Le TR, après couverture du T, intègre ou transfère l'opération aux Comptables Principaux de l'Etat (CPE) selon la nature de celle-ci. Pour ce qui concerne les opérations des payeurs, elles sont envoyées à la TPMDC. A ce poste, il y a des teneurs de poste qui saisissent les opérations des payeurs et agissent au nom et pour le compte de ces derniers.

Exceptionnellement, il est autorisé à la TPMDC, à la TP Golfe, et à la TP Lomé Commune de transférer directement leurs opérations aux CPE.

La figure II.15 à la page 38 illustre la présentation schématique de l'extension SIGFiP en déconcentré

Résumé schématique du réseau informatique des TR



Source : http //www.tresor-togo.org

Figure II.15: Schéma Présentation schématique de l'extension SIGFiP en déconcentré [9]

En définitive, il est à remarquer que les postes de trésoreries principales, des paieries des ambassades et les trésoreries dans les préfectures et communes ne sont pas encore couverts par le SIGFiP.

Bien que cette couverture soit insuffisante, elle présente les résultats encourageants dans la gestion des finances publiques.

2.4. Les résultats encourageants du SIGFiP

La mise en place du SIGFiP a eu pour conséquence des améliorations notables dans la gestion des finances publiques. Ce système, tout en assurant un meilleur suivi des

dépenses publiques, a permis l'automatisation de la gestion des finances publiques avec une célérité dans le traitement des opérations d'exécution budgétaire.

Le progiciel offre aux utilisateurs la facilité de travail et la rapidité dans le traitement quotidien des dossiers comptables. Ce qui permet de respecter le délai de production des documents comptables. L'exploitation du progiciel est donc moins fatiguant.
Avec le système actuel, il y a moins d'erreurs dans le traitement des données. Ce dernier propose aux utilisateurs les choix possibles à réaliser contre l'ancien système dans lequel il fallait taper les écritures. Le progiciel permet également aux utilisateurs de vite reconnaître l'opération faite par chaque teneur de comptes. A chaque utilisateur, il est attribué un identifiant et un mot de passe.

Par rapport à l'application FOX - PROW, SIGFiP offre la possibilité d'interconnexion des postes comptables. Chaque utilisateur est désormais identifié par son mot de passe. Au regard des améliorations et de la satisfaction qu'il apporte à la gestion des finances publiques, le SIGFiP est, sans conteste, un outil de gestion efficace et évolutif.

La facilité de gérer les privilèges des utilisateurs permet non seulement d'éviter les éventuelles fraudes dans le traitement des données mais aussi de garantir la traçabilité des opérations comptables. Cette traçabilité permet à l'administrateur du progiciel de savoir qui a fait quoi dans le système et à quel moment ?

A ces avantages, il faut ajouter la déconcentration du réseau pour rapprocher l'outil de gestion des finances publiques aux trésoreries régionales (intranet). Ainsi, toute écriture comptable est actuellement interactive, ce qui entraîne une incidence positive sur le gain de temps de traitement des données comptables et sur la rapidité d'exécution des tâches.

2.5. Environnement du matériel

2.5.1. Les défauts de climatisation

Il n'y a pas une salle informatique pour héberger le matériel informatique. Les serveurs, modem sont placés dans un bureau bien climatisé, l'accès à ce bureau n'est pas restreint. L'armoire informatique n'est pas climatisé.

- ✓ Appréciation

Les équipements informatiques sont conçus pour travailler dans un environnement spécifique pour respecter les conditions normales de fonctionnement. Alors que ces conditions sont partiellement respectées.

- Recommandation

Il est recommandé de :

- ✓ spécifier un local protégé comme salle informatique;
- ✓ placer un climatiseur dans le local où se trouve l'armoire informatique.

2.5.2. Détection des dégâts d'eau

Le ministère ne dispose pas un détecteur contre l'humidité et les dégâts d'eau.

- ✓ Appréciation

Il y a risque de propagation de l'eau dans la salle connectique ce qui peut causer des incidents à citer :

- ✓ divers cours-circuits entrainant la rupture de service des équipements;
- ✓ détérioration des équipements;
- ✓ corrosion des câbles et connecteurs.
- ✓ Recommandation

Il est conseillé d'utiliser des tubes pour isolés pour le câblage d'alimentation, ainsi que pour le câblage réseaux. **[10]**

Malgré toutes ces opportunités, l'exploitation de SIGFiP Comptabilité est confrontée à certaines difficultés que nous présenterons dans la partie suivante avec les approches de solutions.

2.5.3. Détection des dégâts du feu

Il n y a pas une présence physique contre les dégâts de feu.

- ✓ Appréciation

Ce type d'incident peut mener à la destruction partielle du ministère et particulièrement des équipements informatiques.

- Recommandation

Il est recommandé de :

- ✓ éviter le stockage de produits inflammables dans le bureau où se trouve le matériel informatique;
- ✓ vérifier régulièrement les circuits électriques. **[11]**

2.5.4. Les dégâts d'électricité

Les serveurs, les Switch, ainsi que quelques postes utilisateurs sont protégés par les onduleurs contre les coupures électriques.

- ✓ Appréciation

L'utilisation d'un onduleur est un point fondamental pour protéger le matériel informatique contre :

- ✓ coupure électrique;
- ✓ surtension, c'est-à-dire une valeur nominale supérieure à la valeur maximale prévue pour le fonctionnement normal;
- ✓ sous-tension, c'est-à-dire une valeur nominale inférieure à la valeur maximale prévue pour le fonctionnement normal.

- Recommandation

Il est recommandé de brancher les onduleurs avec tous les équipements informatiques, afin de commander proprement l'extinction de données en cas de coupure de courant.

2.6. Environnement des logiciels de base

Les différents systèmes d'exploitation installés au niveau des différents postes sont :

- ✓ Windows Xp;
- ✓ Windows Vista;
- ✓ Windows 7;
- ✓ Windows 8.

2.6.1. Les Patchs

Les patchs de sécurité "service Pack" ne sont pas installés au niveau des postes de travail. La majorité des patchs de sécurité relatifs au système d'exploitation ne sont pas appliqués. Cette faille offre aux intrus la possibilité d'exploiter les vulnérabilités non corrigées.

- Recommandation

Il est conseillé d'installer un serveur de mise à jour Windows afin de distribuer les patchs sur le réseau vers les postes de travail. **[12]**

2.6.2. Les systèmes de fichier

Le système de fichier détecté au niveau des postes utilisateurs est le FAT et le NTFS.

- ✓ Appréciation

Le système de fichier FAT n'offre pas de mécanisme de sécurité qui peuvent être appliqués aux fichiers stockés sur le disque tel que :

- ✓ La sécurité des fichiers : les droits d'accès peuvent être assignés aux fichiers et répertoires.
- ✓ Le cryptage : les fichiers peuvent être stockés sur le disque sous forme crypté.

- Recommandations

Il vaut mieux réinstaller les postes utilisateurs en FAT par le système de fichier en NTFS, ceux qui peuvent offrir :

- ✓ une sécurité au niveau des fichiers et des dossiers;

- ✓ une compression des fichiers;
- ✓ un quota des disques;
- ✓ un cryptage de fichiers.

2.7. Configuration du réseau

2.7.1. La segmentation

Il existe une séparation logique au niveau du réseau et tous les postes connectés sont placés sur des segments différents.

- ✓ Appréciation

Les données échangées disposent d'un niveau de confidentialité différent. Ce qui réduit le risque de perdre la confidence dans les données échangées.

2.7.2. L'affectation des adresses IP

Il existe le serveur DHCP qui permet d'attribuer automatiquement des adresses IP à la station de travail.

- ✓ Appréciation

Les adresses IP sont attribuées de manière dynamique. Ce qui permet d'éviter l'identification des adresses des équipements et accéder à ses ressources.

2.7.3. Les postes utilisateurs

La plus part des postes utilisateurs ne possèdent pas de session, mais il y a d'autres qui possèdent la configuration de deux sessions :

Un pour l'administrateur informatique, et l'autre pour l'utilisateur.

- ✓ Appréciation

L'absence de session offre à l'intrus la possibilité de collecter un ensemble d'information sur la cible (nom utilisateur, partage).

L'audit des postes de travail connectés au réseau a relevé la présence de cette vulnérabilité pour plusieurs postes.

- Recommandation

L'exigence d'avoir au moins deux sessions pour chaque poste, une pour l'utilisateur avec privilège restreint de préférence pour ne pas modifier la configuration initiale et la deuxième pour l'administrateur qui est le seul à pouvoir modifier les paramètres de base. **[13]**

Une authentification par nom de l'utilisateur et son mot de passe est obligatoire.

2.8. Les risques techniques

La majorité des postes de travail dispose d'un antivirus installé (Kaspersky) qui vérifie en permanence les fichiers de l'ordinateur, mais il y a quelques un qui sont mal configurés et qui ont une mise à jour ancienne.

- Recommandation

Il faut configurer le programme antivirus convenablement pour les postes afin d'avoir une protection une protection fiable, une mise à jour automatique et un scan régulier.

2.8.1. Attaque sur le réseau

Absence d'un système de détection d'intrusion contre tout accès non autorisé depuis l'extérieur.

✓ Appréciation

Le système de détection d'intrusion sera un composant primordial pour les mécanismes de sécurité des réseaux.

- Recommandation

Il est conseillé d'implanter système de détection d'intrusion sécurisé :

✓ NIDS (Network Intrusion Détection System): est un détecteur d'intrusion réseau qui détecte les attaques réseau en se basant sur une base de signatures très à jour;

✓ HIDS (Host intrusion Détection System) : ces ondes s'incèrent entre les applications et le cœur du système d'exploitation pour protéger des applications ou des serveurs critiques.

Les solutions IDS (Intrusion Détection System) pour réseau garantie une surveillance permanente du réseau.

2.8.2. Attaque sur le mot de passe

Aucun mécanisme n'est pris en considération pour lutter contre les attaques sur les mots de passe.

- ✓ Appréciation

Un intrus peut mener une attaque pour collecter les mots de passe afin d'accéder aux ressources matériels mises en question.

- Recommandation

L'administrateur doit respecter les exigences de la stratégie de mot de passe :

- ✓ durée limité de la conservation de l'historique;
- ✓ durée de vie maximale;
- ✓ durée de vie minimale;
- ✓ exigence de complexité;
- ✓ cryptage.

2.9. La sécurité du système

2.9.1. déploiement complet d'Active directory

Une véritable solution quelconque n'est pas encore fonctionnelle avec Active directory. Le contrôle d'accès n'est pas suffisant pour empêcher l'intrusion du système informatique. Active Directory fournit à la fois le magasin et l'étendue de l'application pour les stratégies de sécurité.

Une stratégie de sécurité peut inclure des informations de compte, telles que des restrictions de mot de passe applicables sur l'ensemble du domaine ou des droits pour les ressources de domaines spécifiques. Les stratégies de sécurité sont mises en place par le biais des paramètres de stratégie de groupe. Ainsi les avantages de Active Directory sont :

- ✓ amélioration de la productivité des utilisateurs;

- ✓ réduction des taches d'administration informatique;
- ✓ amélioration de la tolérance de pannes pour réduire les périodes d'indisponibilité;
- ✓ amélioration de la sécurité. **[14]**

2.9.2. Station antivirale

La protection antivirale consiste à appliquer une solution antivirus client/serveur. Cette solution consiste à installer un serveur antivirus sur le réseau, et de déployer sur chaque machine le client associé. Une telle solution permet de centraliser la tache d'administration : mise à jour des fichiers de signature et déploiement automatique sur les postes clients. L'antivirus proposé implémente les fonctionnalités suivantes : exécution en tache de fond, détection automatique, récupération des fichiers indésirables et mise à jour automatique. Cette solution n'est pas encore effective.

2.9.3. Le serveur de mise à jour

Microsoft software update services (SUS) est un maillon essentiel dans la nouvelle politique de sécurité de Microsoft. Le fonctionnement de SUS est relativement simple. Pour déployer, deux modules doivent être mis en place, un client et un serveur :

- ✓ le module serveur télécharge les informations à partir du site Windows update de Microsoft et vous laisse à choisir les mises à jour à installer sur les postes clients;
- ✓ le module client quant à lui communique périodiquement avec le serveur pour savoir si les mises à jour disponibles, si oui il les installe.

Cette solution offre un avantage de réduction de la bande passante internet et une simplification d'administration et de déploiement. Il est donc nécessaire de renforcer la sécurité du système à travers le serveur de mise à jour.

2.9.4. Le Firewall

La solution de filtrage consiste à déployer trois niveaux de filtrage sur les ressources du réseau, comme écrit ci-dessous :

2.9.4.1. Firewall à filtrage de paquets

La majorité des équipements de routage actuels disposent d'une fonctionnalité de firewalling basé sur le filtrage de paquets. Cette technique permet de filtrer les protocoles, les sessions, les adresses sources, les ports sources et destination et même l'adresse MAC.

2.9.4.2. Firewall Statefull Inspection

Cette solution sera implémentée par un équipement firewall matériel qui agit en tant que passerelle, afin de garantir la sécurité entre le trafic du réseau interne. La technologie "statefull inspection" permet de contrôler les couches applicatives sans nécessité de proxy applicatif pour chaque service, en cherchant une session correspondante pour les paquets analysés.

Au niveau architecture du réseau, le firewall proposé définira trois domaines de sécurité :

- ✓ zone interne : représente le réseau local et contient le plus haut niveau de sécurité;
- ✓ zone externe : représente la zone publique par laquelle passe tout le trafic de destination internet;
- ✓ zone démilitarisée : représente la zone contenant les serveurs visibles de l'extérieur dont l'accès est public. **[15]**

2.9.4.3. Firewall applicatif

Un firewall applicatif sera installé sur tous les postes clients et serveurs afin de protéger en premier lieu les tentatives d'intrusion interne. En deuxième lieu, l'utilisation d'un firewall applicatif permet de contrôler les connections depuis et vers ces machines, de renforcer la confidentialité des données et de se protéger contre les programmes malveillants. On peut citer par exemple un firewall : mode_ Security et mode proxy.

2.9.4.4. Annuaire

Un annuaire permet de stocker les données légèrement typées, organisées selon des classes particulières et présentées dans un arbre. Un annuaire se présente comme une base de données, c'est à dire qu'on peut y mettre des informations et les consulter. Ses principales caractéristiques sont d'accéder à des données par des recherches multicritères. **[16]**

On peut trouver des solutions d'annuaire comme Lightweight Directory Access Protocol (LDAP), permettant d'effectuer :

- ✓ les opérations d'interrogation : on y trouve deux fonctions l'une permettant la recherche et l'autre la comparaison;
- ✓ les opérations de mise à jour : on y trouve quatre opérations qui sont l'ajout, la suppression, la modification et le changement de nom;
- ✓ les opérations d'identification et de contrôle de la session : on y trouve trois fonctions qui sont l'ouverture de la session et l'identification, la fermeture de la session, et l'abandon d'une requête en cours.

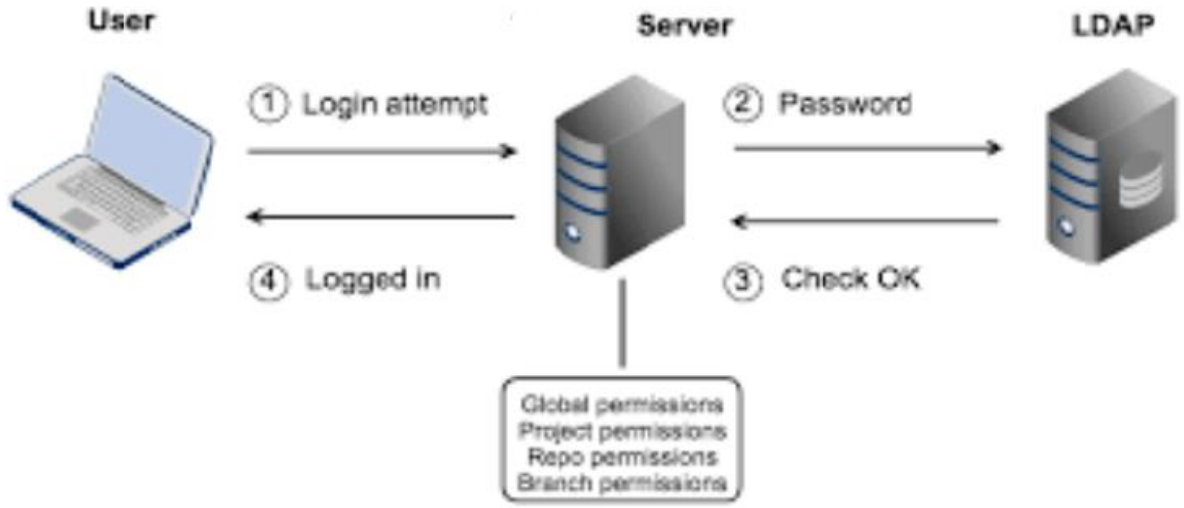


Figure II.16 : Schéma de gestion et de contrôle d'accès aux ressources.

2.10. L'analyse de l'existant

Dans le souci d'apporter un tant soit peu des solutions aux différents maux qui minent l'informatisation de la comptabilité de l'État, nous avons le devoir de décrire les difficultés liées au système informatique actuel et de contribuer à son amélioration.

Nous avions posé différentes hypothèses et réalisé des enquêtes via les questionnaires et interview en vue de la vérification de ces hypothèses, utilisé les outils d'audit informatique et établi un diagnostic pour identifier les différentes difficultés spécifiques relatives à l'actuel progiciel.

Le diagnostic établi nous a permis d'examiner les problèmes rencontrés et de proposer des solutions. Notons que certaines recommandations ont été déjà faites dans le troisième chapitre relatif à l'étude de l'existant.

2.10.1. Les difficultés relatives au progiciel SIGFiP

Au vu des résultats de notre technique de collecte d'information (questionnaire et interview) sur l'exploitation du système actuel, nous avons constaté que des difficultés y persistent malgré les améliorations que celui-ci a apportées à la gestion des finances publiques en général et à la qualité de l'information comptable en particulier.
Ces difficultés peuvent être classées en deux grandes parties à savoir le problème d'ordre réglementaire et humain d'une part et le problème d'ordre matériel et technique d'autre part.

2.10.2. Les difficultés d'ordre réglementaire et humain

Ces problèmes sont relatifs aux textes qui régissent le fonctionnement du réseau des comptables directs du Trésor et aux acteurs (administrateurs et utilisateurs) du SIGFiP Comptabilité. Nous traiterons d'abord les problèmes relatifs aux textes puis ceux d'ordre humain.

2.10.2.1. Les difficultés d'ordre réglementaire

Les textes réglementaires sont la traduction juridique d'une orientation ou d'une volonté des décideurs. Or la mise en œuvre de ces derniers n'est pas sans influence sur

l'outil informatique. L'application des textes juridiques devrait nécessairement prendre en compte la réalité technique du progiciel.

Un règlement peut demander à la DGTCP de revoir ses procédures comptables. Dans ce cadre, il est indispensable que le système informatique présente un ensemble de traitement qui réponde au cadre réglementaire.

Le fonctionnement de la direction générale du Trésor et de la comptabilité publique est régit par le décret n° 2001-155 du 20 août 2001 portant organisation de la Direction Générale du Trésor et de la Comptabilité Publique.

Toutefois, il faut souligner qu'aucune disposition ne régit l'exploitation du SIGTA et son extension en déconcentré. Aucune instruction comptable ne définit les niveaux d'intervention de chaque utilisateur de SIGFiP Comptabilité.

C'est le cas par exemple des chefs divisions et sections qui sont tacitement responsabilisés sans aucun texte juridique. Or techniquement ces derniers interviennent dans le progiciel avec leur identifiant et leur mot de passe. Il serait judicieux que les arrêtés soient élaborés pour nommer et responsabiliser chaque utilisateur de l'application. Le manque de textes nominatifs fait que la DGTCP ne pourrait pas imputer la responsabilité à un utilisateur en cas d'un problème donné.

De même, les textes (arrêtés ou décisions) que prennent les autorités pour le fonctionnement de la DGTCP ne tiennent pas compte de la réalité informatique. Ce n'est que dans l'application de ces textes qu'on rencontre les difficultés interactives. Cela déstabilise l'exploitation du progiciel[13].

Par ailleurs, aucun arrêté ministériel ne précise les tâches spécifiques des informaticiens et administrateurs du système informatique. Aucun texte ne définit la création de la Direction Informatique au sein de la Direction Générale du Trésor et de la Comptabilité Publique.

[13]Exemple de l'arrêté n°131/MEF/SG/DGTCP/DCP portant organisation, fonctionnement et attributions de la paierie générale du Trésor du 16 mai 2012.

L'incidence de ces inquiétudes est qu'on ne peut pas juridiquement engager la responsabilité d'un utilisateur quelconque du progiciel. Aucun texte ne précise les tâches réservées aux informaticiens du Trésor.

La direction informatique est totalement absente dans l'organigramme de la DGTCP. A ce titre, il est également difficile de situer la responsabilité des informaticiens de ladite direction.

Parfois, les textes sont pris sans l'implication des différents acteurs de l'exploitation du progiciel SIGFiP. On se rend compte à l'application de ces textes que le système ne répond pas. Ce qui rend difficile la traçabilité des opérations comptables.

Actuellement, le circuit administratif est trop long lorsqu'il s'agit de corriger une erreur dans le système. Ce long parcourt s'explique du fait que l'utilisateur en cas de problème ne peut pas directement s'adresser à la structure informatique de SIGFiP qui n'est autre qu'un cabinet.

C'est ce dernier qui a installé le système informatique. En réalité après le travail, il devrait transmettre la compétence aux informaticiens de l'administration publique. Cela n'a pas été fait. Le cabinet est donc devenu un maillon de la structure de l'Etat. Ce qui ne devrait pas être le cas.

Prenons par exemple le cas d'un problème né au niveau de la division comptabilité du RGT, le chef division comptabilité adresse la demande qui passe d'abord par le Receveur Général ensuite celle-ci transite au niveau de l'ACCT et enfin arrive chez l'administrateur de SIGFiP au Centre Administratif des Services Economiques et Financiers (CASEF). Ce dernier affecte le même dossier au responsable de la cellule informatique qui, à son tour l'affecte aux informaticiens du cabinet. Si l'un des acteurs est absent, l'erreur perdure et ceci bloque l'effectivité du travail à faire.

Lorsque les utilisateurs contactent les informaticiens, quelquefois ces derniers répondent qu'ils n'ont pas reçu la demande. Ceci constitue un véritable blocage dans le déroulement normal des activités quotidiennes des utilisateurs. Les dispositions

réglementaires non adaptées aux exigences techniques entravent la gestion informatisée des données comptables.

Il n'y a pas que le problème réglementaire, il existe aussi les inquiétudes d'ordre humain.

2.10.2.2. Les difficultés d'ordre humain

Les ressources humaines constituent une préoccupation majeure dans la gestion du SIGFiP Comptabilité de la DGTCP (SIGTA). Les difficultés se situent à deux niveaux à savoir :

- au niveau des utilisateurs ;
- et au niveau des informaticiens et administrateurs du SIGFiP Comptabilité

2.10.2.2.a. Les utilisateurs

Un utilisateur est une personne qui fait usage de l'outil informatique pour traiter les données comptables dans le progiciel. L'on se pose des questions relatives aux problèmes d'ordre humain. Est-ce que le choix des utilisateurs du système informatique est approprié ? Est-ce qu'ils sont bien formés ? Est-ce que l'effectif du personnel est suffisant ?

Lorsqu'un agent est affecté à une autre fonction, il est souvent difficile de trouver une autre personne qui réponde à l'ancien poste. L'absence d'un utilisateur influence négativement l'exécution de la tâche confiée à l'agent affecté. L'affectation d'un agent ne tient pas compte de la maîtrise de la tenue de la comptabilité de l'État ni de l'outil informatique.

Il ne suffit pas seulement de créer les postes comptables, mais il faut aussi les doter d'agents compétents et formés. Il se pose donc un problème de gestion du plan de carrière des utilisateurs dû au manque de responsabilisation réglementaire des agents et à l'insuffisance d'adéquation entre les qualifications professionnelles et les postes occupés.

Par nos observations, nous avons identifié qu'il manque d'évaluation de l'efficacité des formations, de prise en compte des aspects de compétence et de qualification des agents, du processus de sensibilisation sur l'impact de la contribution individuelle des acteurs à l'obtention de la qualité de l'information financière et comptable de l'État.

En réalité, l'insuffisance du capital humain constitue un blocage au déroulement normal des activités quotidiennes de la DGTCP. Cette insuffisance oblige les agents à reporter plus tard le traitement de certains dossiers. Au jour le jour, l'on constate une accumulation des dossiers non traités.

Par ailleurs, selon nos analyses, un des défis à relever est celui du recrutement conséquent du personnel et sa valorisation. Non seulement il y a insuffisance du personnel, mais aussi ce dernier ne bénéficie pas d'une formation permanente sur l'utilisation du module SIGTA (SIGFiP Comptabilité).

La professionnalisation des comptables, exige une réforme de la formation initiale avec l'implication des agents sur le déroulement de la formation et sur l'utilisation de l'outil informatique pour passer les écritures comptables. Cette formation continue devrait bénéficier de procédures fonctionnelles et techniques durables pour répondre aux immenses besoins de la DGTCP.

Un autre aspect est que les utilisateurs ne sont pas suffisamment outillés pour répondre aux exigences informatiques (utilisation d'outil informatique). Certains problèmes surviennent dans le système informatique par erreur de manipulation de l'ordinateur.

2.10.2.2.b. Les informaticiens et administrateurs du système

Un informaticien ou une informaticienne est une personne qui exerce un métier dans l'étude, la conception, la production, la gestion et la maintenance des systèmes de traitement de l'information.

En informatique, le titre d'administrateur système désigne la personne responsable des serveurs du système informatique (ensemble organisé de ressources matérielles et logicielles)

et qui veille à ce que tous les utilisateurs aient un accès rapide au système d'information d'une organisation. Ce dernier porte la responsabilité de l'intégrité du système et de sa bonne marche.

L'équipe informatique du SIGFiP est souvent dépassée par les problèmes quotidiens des utilisateurs et est donc obligée de reporter certaines interventions. Pendant tout ce temps, l'utilisateur est désœuvré.

De même, souvent l'administrateur du SIGFiP Comptabilité est obligé de se déplacer et aller résoudre les problèmes des services en déconcentré. En ce moment lorsqu'un problème survient à la DGTCP, les utilisateurs sont obligés d'espérer son retour. Ceci pose d'énormes difficultés aux utilisateurs dans l'exécution de leurs tâches quotidiennes.

Il y a des moments, l'administrateur effectue le déplacement avec certains informaticiens. Pourtant ce sont les mêmes personnes qui assistent les utilisateurs en cas d'éventuels problèmes. La bonne exploitation de l'application est donc tributaire de ressources humaines conséquentes. Jusqu'à ce que l'équipe informatique ne revienne à la centrale, les problèmes à résoudre sont déjà énormes. Cette situation explique l'indisponibilité des techniciens de pouvoir satisfaire tous les utilisateurs en temps réel.

A toutes ces difficultés liées aux ressources humaines, s'ajoutent les problèmes matériel et technique.

2.10.2. Les difficultés d'ordre matériel et technique

Les trésoriers ne passent pas directement leur écriture dans l'application. Ils les transmettent aux trésoriers régionaux de leur circonscription administrative pour traitement interactif. Quelles en sont donc les entraves matérielles ?

2.10.3. Les difficultés d'ordre matériel

Actuellement, tous les postes comptables ne sont pas équipés du matériel informatique et réseau. Ce manque de matériel rend pénible le travail des agents placés à ces postes. Ces agents n'ont pas un accès direct au progiciel.

Non seulement certains postes comptables ne sont pas connectés au réseau SIGFiP Comptabilité, mais aussi il y a des insuffisances relatives à l'aménagement des bureaux et au matériel informatique dans les postes connectés.

2.10.3.1. Difficultés relatives à l'aménagement des bureaux

Certains bureaux des utilisateurs sont contigus et non conformes pour favoriser le travail. C'est le cas par exemple de la Trésorerie Principale d'Aného où il existe seulement deux bureaux pour six personnes : l'un pour le trésorier avec son coffre-fort et l'autre pour le reste du personnel.

Outre les dimensions physiques de l'espace de travail et le mobilier qui ne sont pas respectés, d'autres aspects ne sont pas pris en considération, comme par exemple :

- l'espace de travail ne permet pas de préserver la confidentialité (par exemple les personnes peuvent-elles parler sans être entendues, compte tenu du niveau de confidentialité requis ? les bruits et les conversations ne nuisent-ils pas à la concentration ou ne font-ils pas obstacle à la compréhension des interlocuteurs, lorsque l'utilisation du téléphone occupe une grande part du travail ?) ;

- l'espace de travail ne permet pas à l'agent d'être à l'aise dans son bureau ;
- l'employé n'arrive pas à personnaliser son poste de travail compte tenu de l'espace qui lui est réservé ;
- l'aménagement du lieu de travail ne facilite pas les relations interpersonnelles.
- l'espace n'est pas suffisant pour que chacun puisse s'y mouvoir librement, de façon sécuritaire, et s'acquitter de ses tâches ;

- les aspects des locaux ne permettent pas d'accueillir des visiteurs au besoin et de disposer le matériel requis pour le travail ;

- les dimensions physiques ne respectent pas la norme recommandée qui est de 10 m² pour une personne (la norme NF X 35-102)[14].

Le manque d'ergonomie informatique dans certains bureaux rend difficile la mise en place des équipements informatiques. La plupart des structures déconcentrées abritent des installations apparentes. Les différents bureaux de ces structures sont facilement exposés à l'insécurité électrique[15]. La moindre erreur ou le frottement entre les fils peut entraîner de lourds dégâts dans les lieux de travail.

Il n'y a pas que les bureaux qui manquent d'ergonomie informatique, on peut noter aussi l'insuffisance du matériel informatique.

2.10.3.2. Difficultés relatives au matériel informatique

On note également le manque ou l'insuffisance d'ordinateurs, d'imprimantes et de consommables informatiques pour les utilisateurs. Certains trésoriers sont parfois obligés de venir à la Trésorerie Régionale pour acquérir du consommable informatique (cartouche d'encre par exemple).

L'insuffisance du matériel (sur 82 enquêtés, 15 personnes n'ont pas d'ordinateurs) oblige certains utilisateurs du système informatique à attendre afin de permettre aux autres de finir d'abord leur travail avant d'avoir accès à l'ordinateur. Il y a nécessité d'équiper suffisamment tous les postes comptables et de les interconnecter.

En principe avec le nouveau système, la DGTCP devrait renouveler son parc informatique dans le respect de la compatibilité du progiciel avec les ordinateurs utilisés. Ceci peut être également source de lenteur du réseau. Le nouveau système est plus puissant en termes d'exécution des requêtes des utilisateurs alors que le matériel utilisateur n'est pas adéquat avec la capacité de traitement de ce dernier.

[14] Source : http //www.google.tg/search ?sclient
[15] Il s'agit de quelques images relatives aux aspects de certains bureaux en déconcentré. Voir annexe 7
Source : Comité Technique SIGFiP/ Mission Extension SIGFiP dans les TR, TP et T (du 06 au 22 février 2012)

Le matériel informatique étant insuffisant, une division quelconque qui utilisait 10 ordinateurs par exemple, lorsqu'on affecte un nouvel agent dans ladite division, il faudrait également mettre à sa disposition un ordinateur. Ce qui n'est pas le cas. Les ressources informatiques ne sont donc pas attribuées à certains nouveaux utilisateurs pour qu'ils puissent exercer leur travail.

Aux problèmes matériels, s'ajoutent les faiblesses techniques.

2.10.4. Les difficultés d'ordre technique

Les problèmes d'ordre technique se rapportent :

- à la base de données (structure de stockage et de manipulation des données) ;
- au réseau (emplacement physique des équipements de communication et de partage des ressources de l'ordinateur et des données) ;
- à l'application (le progiciel SIGFiP) ;
- à la maintenance du système informatique ;
- à la sécurité des données.

2.10.4.1. La base de données

On remarque très souvent en entreprise des bases de données mal structurées. A la conception rien d'anormal n'est détecté et l'on est rapidement confronté à plusieurs problèmes lorsque la base de données est mise en exploitation.

En effet, il existe certaines requêtes que SIGFiP n'arrive pas à générer facilement. C'est le cas par exemple des encaissements des ordres de recettes. Le système édite difficilement les états comptables par période et par ligne (type de recette), par contre FOX - PROW restitue facilement ces éditions. L'utilisateur est donc obligé de faire une double saisie ; une dans FOX - PROW et une autre dans SIGFiP Comptabilité pour un même ordre de recette. Ceci rend pénible l'exécution de la tâche à réaliser.

De même, toutes les informations du progiciel FOX - PROW dont la récupération n'est pas effective par le progiciel actuel, sont produites par l'ancien système. L'utilisateur est obligé d'utiliser l'application FOX - PROW lorsqu'il veut sortir la

balance ou lorsqu'il a besoin d'une information relative à la gestion antérieure (gestion 2008 par exemple).

Cela voudrait dire que la base de données actuelle n'a pas pu prendre en compte certaines données de l'ancien système.

Ce défaut de fonctionnement est souvent causé par une insuffisance d'expertise dans l'analyse, la conception de bases de données et la programmation informatique. La lourdeur des requêtes pourrait être due au manque d'index[16] sur certaines colonnes impliquées dans l'exécution de ces dernières. La base de données souffrirait donc d'une insuffisance d'indexation et d'optimisation.

Ce qui fait que le temps d'exécution de la requête devient très long. Une base de données non optimisée ne peut pas facilement servir plusieurs dizaines de requêtes à la fois. Il serait donc important de détecter les sources de problème de lenteur, et de proposer les recommandations pour pallier à certains problèmes récurrents.

2.10.4.2. Le réseau

Le système est également confronté à la lenteur du réseau et parfois à l'absence de connexion. Pour la fibre optique comme pour la paire torsadée, le problème de débit fait partie du même constat : le passage de l'information dans la bande passante est souvent lent.

Actuellement il existe deux types de câblage réseau au niveau de la DGTCP. Un ancien doté du câble catégorie 5 et un nouveau doté du câble catégorie 6. Tous les utilisateurs connectés à l'ancien réseau passent par le nouveau réseau via un pont réseau (Switch) pour avoir accès à l'application SIGFiP Comptabilité. L'échec de connexion au réseau devient donc récurrent.

La transmission électronique d'informations comptables entre les Trésoriers et les Trésoriers Régionaux fait toujours défaut en raison du non achèvement des travaux d'extension de l'application.

[16] C'est une manière de faciliter la recherche d'information dans une base de données

2.10.4.3. L'application

Avec le système actuel, lorsqu'une erreur survient, il est difficile de la corriger en temps réel. En effet, l'on constate souvent la non apparition des comptes de contrepartie après la couverture des opérations de transfert reçues des autres comptables.

Au niveau de l'édition des déclarations de recettes (DR), SIGFiP n'offre pas une facilité de pouvoir classer ces DR par comptes de dépôts ni reporter les soldes de ces derniers pour la gestion suivante. Au niveau du bordereau des déclarations de recettes, le classement des numéros par compte de dépôts et par date de validation n'est pas pris en compte.

Actuellement, le progiciel n'a pas pris en compte le vrai libellé pour la couverture des timbres fiscaux des trésoreries. Les montants de ces derniers sont jusqu'ici couverts par le libellé : Impôts sur le Revenu des Personnes Physiques.

Dans la gestion des produits financiers, le choix de liste de valeurs de l'écran ci-après ne permet pas de distinguer le type de produit financier (dividende, gain de change, commission sur transfert, intérêt sur placement).

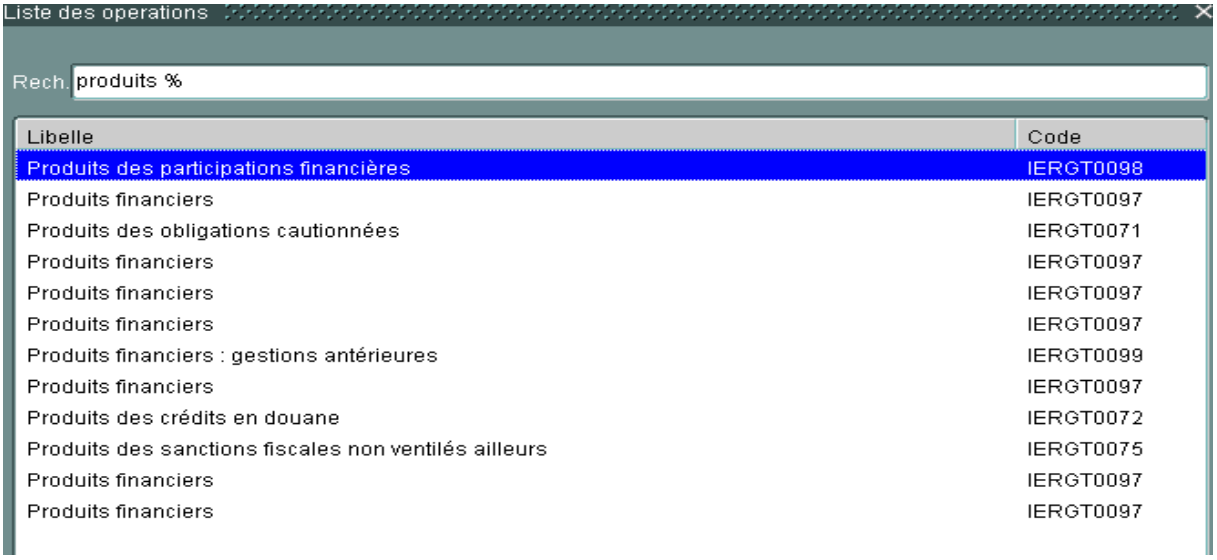


Figure II.17 : Ecran de couverture des déclarations de recettes

L'utilisateur est obligé de choisir un à un les libellés produits financiers sur la liste. A

chaque sélection, il regarde si le choix correspond au dividende, au gain de change, à la commission sur transfert ou à l'intérêt sur placement avant de continuer son travail. Cette façon de faire devient très fastidieuse.

On note également des difficultés relatives à l'introduction des numéros d'imputation, d'ordre pour la prise en charge des ordres de recettes et la saisie des déclarations des recettes.

La plainte des utilisateurs ne cesse de s'accroître face à la non fluidité (instabilité) du progiciel. Ce qui crée parfois des doublons d'écritures comptables lors du traitement interactif des données.

Les utilisateurs rencontrent également des difficultés pour éditer certaines situations comptables. C'est le cas par exemple de la situation du montant total recouvré sur un ordre de recette d'une période donnée ou de la gestion par type de recette des régies financières.

Avec le SIGFiP, l'utilisateur n'a pas la possibilité de corriger lui-même une quelconque erreur relative à une opération déjà validée. La correction ne peut être faite que par les informaticiens sur demande.

Le manque de module de messagerie système (alerte de transmission automatique des documents comptables ou d'une action effectuée par un utilisateur) constitue aussi un problème applicatif. Par exemple lorsque l'utilisateur fait un clic sur le bouton ''enregistrer'', il manque sur certains écrans l'information '' enregistrement effectué''. Pour ce dernier rien ne s'est produit et lorsqu'il refait un nouveau clic, cela crée des doublons dans le système. Il y a aussi le temps de réponse des requêtes utilisateurs qui est parfois trop long.

La plupart des écrans de saisie nécessitent des améliorations surtout au niveau du choix des listes de valeurs (paramètre de recherche d'information). Une saisie faite en amont ne devrait plus être reprise dans son circuit normal. La reprise de saisie pourrait générer des erreurs de traitement parfois difficiles à répertorier.

Il y a également les écrans pour effectuer les déclarations de recettes qui posent des difficultés. Le système édite ces dernières, ligne par ligne pour une même nature d'opération (TVA par exemple) au lieu de sortir cela en bloc.

L'écran de paramétrage d'édition de la balance illustré dans le paragraphe II du chapitre II de la première partie manque de programmes de contrôles à certains niveaux. En principe, une fois que la période de gestion est précisée, les dates début et fin doivent être conformes à celle-ci ; ce qui n'est pas le cas.

Le progiciel n'est pas aussi ouvert. Par "ouverture d'un progiciel" on entend sa faculté à récupérer, pour son propre compte, les données en provenance d'autres programmes non conçus pour fonctionner en relation avec celui-ci. On désigne cette opération sous le terme d'importation de données.

Il faut ajouter que l'application SIGFiP n'a pas pris en compte la gestion de la trésorerie. Ce qui rend difficile l'élaboration du plan de trésorerie au niveau de l'Agence Comptable Centrale du Trésor.

2.10.4.4. La maintenance

La maintenance vise à maintenir ou à rétablir un bien dans un état spécifié afin que celui-ci soit en mesure d'assurer un service déterminé. Elle regroupe ainsi les actions de dépannage, de réparation, de réglage, de révision, de contrôle et de vérification des équipements matériels (ordinateur et ses périphériques) ou même immatériels (logiciels informatiques).

Une maintenance régulière est essentielle pour préserver la sécurité et la fiabilité de l'équipement, des machines et de l'environnement de travail. L'absence de maintenance ou une maintenance inadéquate peut engendrer des situations dangereuses sur les données comptables. La maintenance est indispensable pour garantir une productivité continue. Elle a toutefois une incidence sur la santé et la sécurité du travail.

Des pannes surviennent dans l'application parce que les appareils ne font pas l'objet d'une inspection et d'un entretien régulier. L'entretien de l'équipement au

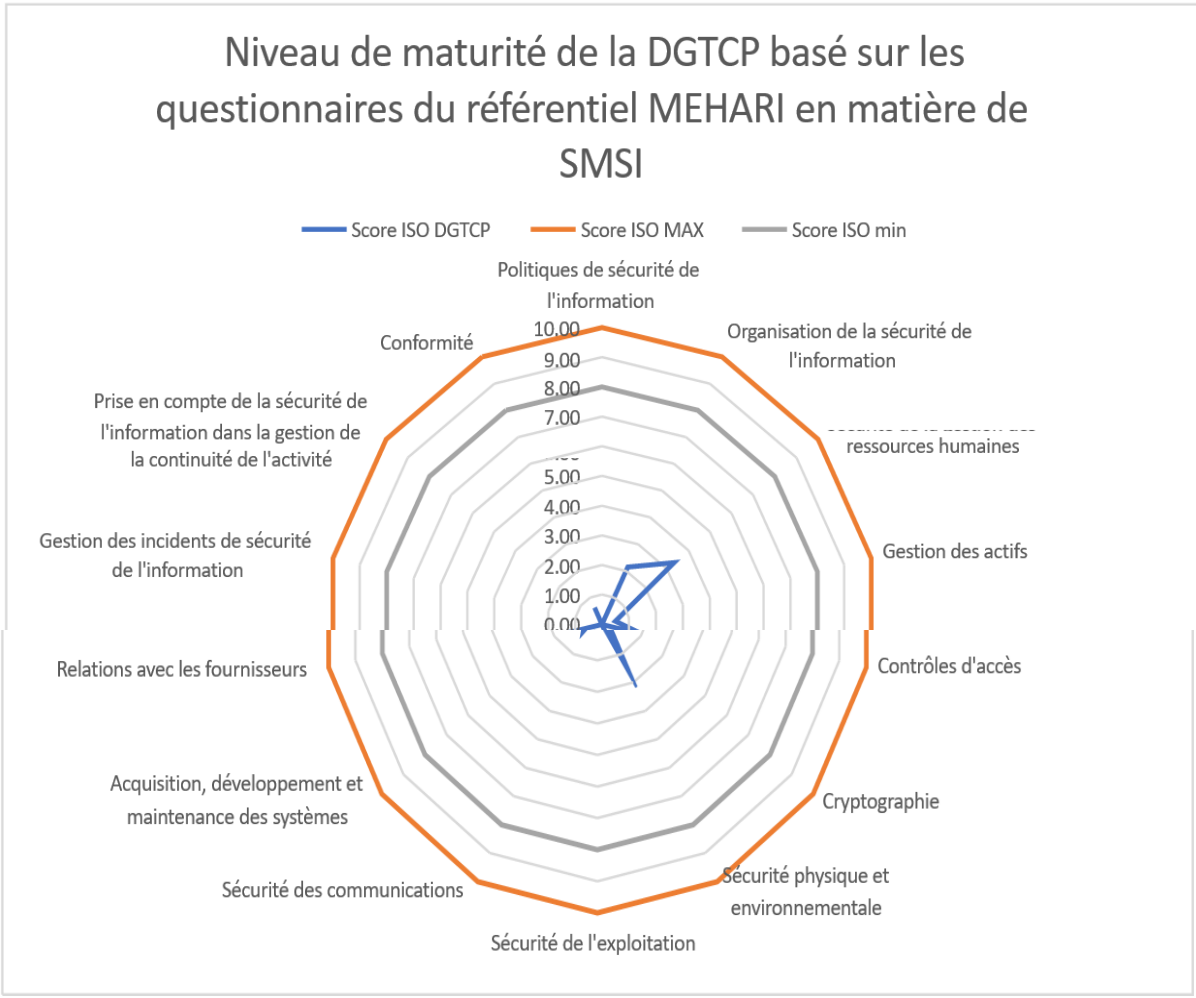
dépoussiérage est crucial dans tous les processus générateurs de poussières pour empêcher l'exposition des travailleurs et des équipements utilisés aux poussières. Les conduites de ventilation ne sont pas dégagées en permanence et réparées si elles sont endommagées. Les filtres ne sont pas entretenus régulièrement suivant les recommandations du fabricant.

Le fait d'avoir sur chaque poste un antivirus peut être aussi une source de lenteur du réseau. Le manque d'antivirus "réseau" rend difficile la mise à jour des ordinateurs. Le parc informatique est souvent envahi par la poussière et ne bénéficie pas d'une climatisation suffisante.

A toutes ces insuffisances, l'on constate également le mauvais fonctionnement de certaines prises réseaux, d'ordinateurs et de concentrateurs (équipement réseau qui permet de relier les ordinateurs). Il faut souligner également que l'amortissement des équipements n'est pas respecté. Ceci diminue leur performance.

Somme toute, il y a nécessité de penser aux approches de solutions pour l'amélioration du système informatique actuel.

2.10.5. Niveau de maturité de la DGTCP basé sur les questionnaires du référentiel MEHARI en matière de Système de management de la sécurité de l'information (SMSI)



D'après la figure, on remarque que le niveau de la DGTCP est très bas par rapport à la demande de MEHARI qui est au minimum de 8 sur 10.

Le tableau ci-dessous nous montre le détail des notes et les recommandations faites.

N°	Domaine étudié	Recommandations
1	Politiques de sécurité de l'information	Établir une politique de sécurité de l'information en conformité avec les exigences métiers et les recommandations ISO 27001 et le faire approuver par la direction
N°	Domaine étudié	Recommandations
2	Organisation de la sécurité de l'information	Établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information au sein

		de l'organisation
3	Sécurité de la gestion des ressources humaines	S'assurer que les salariés et les contractants comprennent leurs responsabilités et qu'ils sont compétents pour remplir les fonctions que l'organisation envisage de leur confier
4	Gestion des actifs	Identifier les actifs de l'organisation et définir les responsabilités appropriées en matière de protection
5	Contrôles d'accès	Limiter l'accès à l'information et aux moyens de traitement de l'information.
6	Cryptographie	Garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité,l'authenticité et/ou l'intégrité de information.
7	Sécurité physique et environnementale	Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'organisation.
8	Sécurité liée à l'exploitation	S'assurer de l'exploitation correcte et sécurisée des moyens de traitement de l'information.
9	Sécurité des communications	Garantir la protection de l'information sur les réseaux et des moyens de traitement de l'information sur lesquels elle s'appuie.
10	Acquisition, développement et maintenance des systèmes	Veiller à ce que la sécurité de l'information fasse partie intégrante des ystèmes d'information tout au long de leur cycle de vie. Cela inclut notamment des exigences spécifiques pour les systèmes d'information fournissant des services sur les réseaux publics.
11	Relations avec les fournisseurs	Garantir la protection des actifs de l'organisation accessibles aux fournisseurs.
12	Gestion des incidents de sécurité de l'information	Garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité del'information, incluant la communication des événements et des failles liés à la sécurité.
13	Prise en compte de la sécurité de l'information dans la gestion de la continuité de l'activité	S'assurer que la continuité de la sécurité de l'information fasse partie intégrante des systèmes de gestion de la continuité de l'activité
14	Conformité	Éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l'information, éviter toute violation des exigences de sécurité.

Les plans d'actions suivantes s'imposent pour améliorer le niveau de sécurité du système d'information :

- Chiffrement des données applicatives stockées
- Contrôle de l'utilisation de droits privilégiés

- Contrôle d'accès aux systèmes et applications
- Sécurité des mails et des messages électroniques
- Contrôle des configurations
- Chiffrement des données bureautiques
- Protection de l'intégrité des fichiers de données bureautiques
- Protection contre les risques environnementaux divers
- Protection du poste de travail
- Sûreté de fonctionnement des éléments de l'infrastructure

De l'analyse du système existant pour la gestion des données financières et comptables, nous allons proposer les approches de solutions à travers la technologie blockchain et terminer notre développement avec les discussions et perspectives relatives à la gestion efficace des finances publiques.

DEUXIEME PARTIE : SOLUTION BLOCKCHAIN PROPOSEE, RESULTATS ET DISCUSSIONS

CHAPITRE III : SOLUTION BLOCKCHAIN PROPOSEE POUR AMELIORER LA GESTION DU SYSTEME FINANCIER ET COMPTABLE

La blockchain est une forme de technologie de registre distribué, dans laquelle les données sont regroupées en chaines de blocs successifs. L'ensemble des blocs vise à cristalliser le contenue des transactions. Le bloc est positionné dans la blockchain de manière à rendre impossible toute modification accidentelle. Cette cristallisation repose sur un lien cryptographique venant à souder tous les éléments entre eux. Dans la blockchain, les procédures de consensus permettent de définir la manière dont les nœuds doivent interagir, la façon de transmettre les données entre ces derniers et les exigences pour une validation de bloc réussie.

Dans le déroulement de la solution proposée, nous allons parcourir toute la chaine de la dépense publique et apporter les améliorations dans le but de sécuriser l'information comptable et financière du système étudié. Les approches de solutions de l'application actuelle peuvent être classées comme suit : les solutions d'ordre réglementaire et humain d'une part et les solutions relatives à l'aspect matériel et technique d'autre part.

3.1. Les solutions d'ordre réglementaire et humain

L'absence des textes pour régir l'exploitation du SIGFiP Comptabilité dans son ensemble et l'insuffisance du personnel qualifié posent d'énormes problèmes dans l'exécution du système informatique mis en place.

Il est donc nécessaire de présenter des approches de solutions adéquates et applicables à l'exécution de l'application. Nous avons donc opté de présenter les solutions réglementaires (3.1.1) avant d'aborder celles qui se rapportent à l'aspect humain (3.1.2).

3.1.1. Les solutions d'ordre réglementaire

Il conviendrait de rédiger les textes qui devraient régir l'exploitation du module SIGFiP Comptabilité (SIGTA) et son extension en déconcentré. Il faudrait également

élaborer les instructions comptables pour définir les niveaux d'intervention de chaque utilisateur. Nous avons mis en place, les éléments structurant la technologie de blockchain comme suit :

- le registre et son contenu : le registre étant une forme de stockage distribué, il est possible de centraliser toutes les demandes à la direction informatique afin de réduire le circuit administratif des sollicitations utilisateurs des différentes directions.
- l'accès au registre pour les différents acteurs (utilisateurs et valideurs) de la chaine de dépense. Le processus de demande et de validation sera désormais géré au niveau du registre pour minimiser le délai de traitement des demandes.
- la validation du registre par consensus en fonction des mécanismes de validation choisis, la possibilité pour l'ensemble des acteurs de contribuer à l'émergence du consensus (ou celle d'exprimer un désaccord) ne peut être garantie. L'ensemble des acteurs partage cependant un accord sur l'état du registre.
- la régulation des acteurs afin d'inciter les acteurs à contribuer à la rapidité de traitement des dossiers, mais également afin d'obtenir un équilibre du système, il est nécessaire de mettre en place un mécanisme de régulation dans le circuit informatique.

Le schéma présenté à la page suivante résume la solution blockchain proposée :

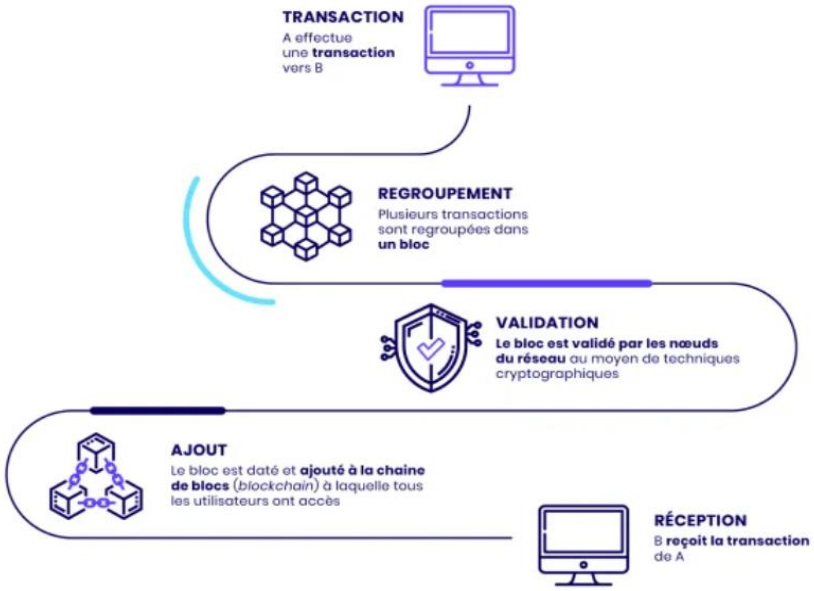


Figure III.1 : Schéma résumé de la solution blockchain

Il serait souhaitable que la DGTCP œuvre à la création d'une Direction Informatique pour faciliter la gestion et l'exploitation du module SIGFiP Comptabilité. Le cabinet qui a installé le système informatique devrait par voie réglementaire transmettre la compétence technique aux informaticiens de l'administration publique.

La lourdeur du circuit pour corriger les éventuelles erreurs dans le système n'existerait pas si la DGTCP était dotée d'une Direction Informatique. Toutes les demandes de correction passeraient par ladite direction. Le circuit des demandes deviendrait court et l'intervention des informaticiens serait rapide pour assister les utilisateurs. Le travail évoluerait et l'on gagnerait du temps dans l'exécution des tâches quotidiennes.

Il faudrait également que l'élaboration des textes tienne compte de l'incidence technique sur le système. Le fait que toutes les opérations effectuées par la DGTCP soient retracées dans l'application, il est souhaitable qu'on associe les informaticiens et administrateurs du système aux prises de décisions réglementaires.

La DGTCP pourrait aussi définir par notes de services les tâches spécifiques des informaticiens (réseau, développement, maintenance, assistant utilisateur et administration base de données). Toutes ces préoccupations devraient faire l'objet d'une réglementation.

Il serait judicieux d'établir les textes réglementaires pour réorganiser la structure informatique afin de doter à cette dernière une autonomie de gestion des dossiers relatifs aux problèmes techniques des services centraux et des structures en déconcentré de la DGTCP.

3.1.1.a. Organisation de la structure informatique

Cette organisation devrait commencer par la création de la Direction Informatique à la DGTCP avec la mise en place des équipes informatiques suivantes :

- les administrateurs systèmes et réseaux informatiques ;
- les développeurs d'applications ;
- les maintenanciers ;
- les administrateurs de base de données.

Ceci permettrait de situer les responsabilités en cas d'éventuels problèmes et de savoir à quelle équipe s'adresser pour tel ou tel dysfonctionnement.

A défaut de créer la direction informatique, la DGTCP pourrait mettre en place un correspondant permanent au sujet du SIGFiP Comptabilité. Ce dernier s'occupera uniquement du traitement des dossiers relatifs à la gestion et à l'administration du module comptabilité de l'application.

Il est également souhaitable d'introduire des mesures juridiques adéquates pour asseoir une base efficace et équitable des actions à mener à l'endroit de la modernisation et de définir le niveau d'intervention de chaque utilisateur de l'application. C'est dans ce cadre qu'il faudrait élaborer les textes qui organisent l'exploitation de l'application.

Toute structure informatique, pour être viable, devrait avoir des principes généraux soutenus par une base juridique. Rappelons que les solutions proposées ne peuvent être mises en œuvre qu'à travers une action concertée entre les responsables à divers niveaux de la DGTCP. Outre les solutions organisationnelles, il faut aussi élaborer les textes pour étendre le réseau dans les services en déconcentré.

3.1.1.b. L'extension du réseau aux structures en déconcentré

La Blockchain est apparue avec la monnaie cryptographique et le système de paiement peer-to-peer Bitcoin en 2008. Il s'agit d'une technologie cryptologique qui permet la tenue d'un registre public de transactions, organisé par ordre chronologique, et qui s'appuie sur un réseau décentralisé d'utilisateurs.

La Blockchain que nous avons proposé prend en compte trois caractéristiques principales que sont la transparence de l'information financière et comptable entre les utilisateurs ; la protection des données (non falsification, vérification des informations par les nœuds du réseau, absence d'effacement des données, anonymisation) ; et la décentralisation (fonctionnement sans organe central de confiance chargé de l'administration, du contrôle, et plus généralement de la gouvernance du système).

Ainsi, il faut s'imaginer « un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible entre les acteurs de la chaine. Le schéma ci-dessous illustre la solution blockchain proposée :

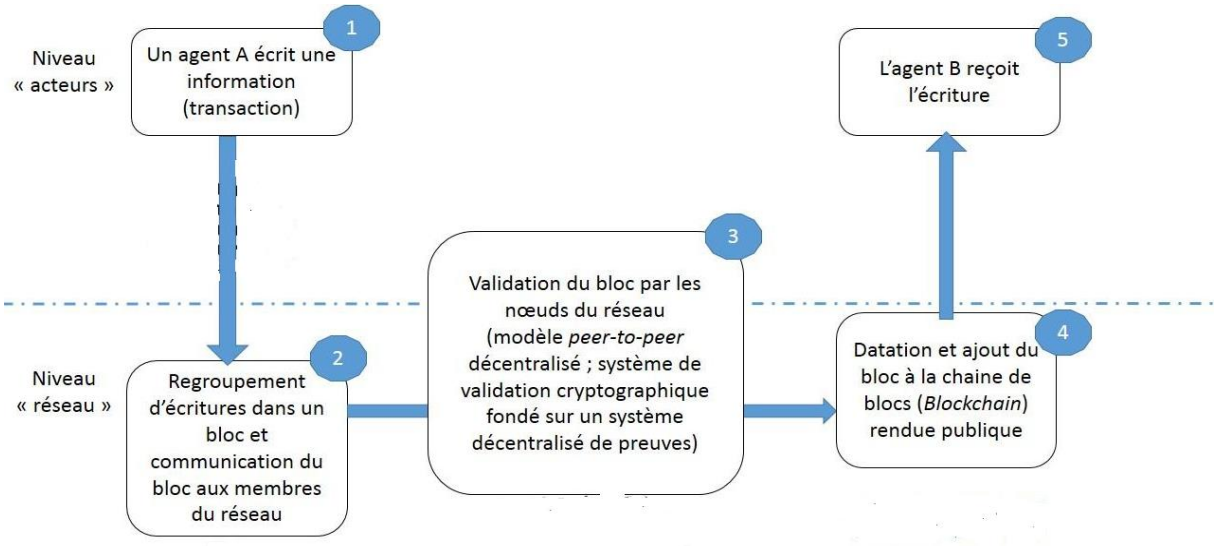


Figure III.2 : processus de fonctionnement de la Blockchain financière et comptable

La première étape (1) s'apparente à la demande d'écriture comptable ou transaction financière par un agent A à destination d'un agent B dans le registre de la Blockchain. L'agent A formule sa demande via une interface logicielle spécifique connectée au réseau. La demande d'écriture est ajoutée à un chapitre ou "bloc" d'informations recueillies sur un laps de temps défini auprès de l'ensemble des utilisateurs du réseau, et le bloc est désormais placé dans une "file d'attente" (2). Le bloc va attendre d'être validé par un consensus des utilisateurs (ou nœuds) du réseau pour pouvoir être ajouté de manière ordonnée, irréversible à la chaîne de blocs, registre répliqué à travers tout le réseau.

La validation par consensus d'un bloc (3) est l'étape clef de la technologie Blockchain. Chaque bloc est soumis à un protocole cryptographique qui décidera l'ajout ou non du bloc à la chaîne de blocs. Ce protocole cryptographique est réalisé par des acteurs (ou groupes d'utilisateurs) volontaires du système appelés "mineurs".

Les mineurs mettent à disposition du réseau la capacité de calcul d'ordinateurs ou de serveurs informatiques pour procéder à l'étape du minage, c'est à dire la réalisation de solutions cryptographiques nécessaires à la sécurisation du réseau. Cette cryptographie permettra par la suite d'identifier un bloc, sans en révéler le contenu, et donc de vérifier l'intégrité d'un document. Cette étape mathématique mobilise traditionnellement le principe de la "preuve de travail" (proof of work) qui est une validation par les pairs membres du réseau.

Lorsque les utilisateurs de la Blockchain ont validé l'exactitude de l'opération, le bloc est validé, horodaté, et ajouté à la chaîne de blocs (Etape 4). Au final, tous les membres du réseau ont la même copie des informations enregistrées au sein de la Blockchain (étape 5). Les blocs sont ajoutés un par un, à intervalle régulier pour garantir la transaction.

Il demeure urgent de consolider les réformes structurelles engagées au sein de la Direction Générale du Trésor et de la Comptabilité Publique (DGTCP).

Il serait encourageant d'achever les travaux d'extension de l'application pour faciliter la transmission de l'information comptable entre les postes comptables en déconcentré et les services centraux de la DGTCP. Cette extension va permettre aussi au Trésor public de produire les comptes de gestion des comptables dans de bons délais et les soumettre à la Cour des comptes.

Il faudrait également connecter tous les postes comptables au site SIGFiP Comptabilité afin de réduire les délais de production de la balance générale des comptes du Trésor et de régulariser dans le système, les comptes d'attente et d'avance.

Pour ce faire, il serait souhaitable que la DGTCP œuvre à l'extension de l'application dans des délais raisonnables pour faciliter le partage d'informations entre tous les acteurs du réseau des comptables directs du Trésor.

Une fois l'extension établie, il ne restera qu'à choisir le personnel qualifié pour réaliser les différentes fonctions définies dans les postes comptables.

3.1.2. Les solutions d'ordre humain

Le manque d'actions régulières de renforcement des capacités des agents chargés de la tenue interactive de la comptabilité de l'Etat est à la base de la non maîtrise des procédures de comptabilisation dans le progiciel. Il serait souhaitable que la DGTCP organise des séances de formation à l'endroit du personnel. La DGTCP pourrait également faire un recrutement des agents qualifiés en renforcement du personnel et veiller aussi à sa formation périodique.

3.1.2. a. Le recrutement conséquent du personnel qualifié

Ce recrutement devrait prendre en compte le personnel informatique et comptable. Il ne s'agit pas de recruter le personnel parce que les postes sont vacants. Il faudrait que le choix soit bien approprié et il faudrait définir au départ les profils de recrutement du personnel.

Si les différentes mesures que nous venons de proposer sont de nature à améliorer les prestations de la qualité de l'information financière et comptable de l'Etat, celles-ci ne

pourraient atteindre une véritable efficience sans une action efficace sur les ressources humaines qui animent les structures du réseau des comptables directs du Trésor.

Introduire de nouvelles techniques au sein de la gestion des finances publiques exigerait que des actions préalables soient entreprises dans le recrutement conséquent du personnel compétent. Les actions d'adaptation et de modernisation de la tenue de la comptabilité de l'Etat devraient pour la plupart être orientées vers les ressources humaines compétentes.

Ainsi, il est souhaitable de recruter et surtout d'élaborer un plan de carrière des utilisateurs qui respecterait une bonne politique de ressource humaine.

En outre, pour une meilleure amélioration de la production de l'information financière et comptable, il serait souhaitable que la formation (renforcement périodique des utilisateurs) accompagne le recrutement du personnel.

3.1.2.b. La mise en place d'un programme de formation du personnel

Ce système de formation devrait prendre en compte les informaticiens et les comptables. L'informaticien pourrait périodiquement suivre des formations pour être à la hauteur de l'évolution technologique. Ces formations prendraient en compte l'optimisation de la base de données, l'application et la maintenance du système informatique (certification tuning).

Base de toutes connaissances véritables, la formation et la communication s'imposent à toute organisation moderne qui se veut forte et durable. Seule la formation continue des utilisateurs du progiciel peut améliorer la qualité de l'information financière et comptable de l'État. La formation en tant que facteur de motivation du fonctionnaire, améliore également la qualité du service de l'État.

Les utilisateurs devraient être bien formés pour mieux utiliser l'outil informatique. La formation est un élément important. Sans formation, le comptable ne peut rien faire dans le progiciel.

La technologie évolue et il faudrait que la formation suive pour permettre aux utilisateurs d'être à jour. Il y a lieu de former également les personnes responsables des mesures sécuritaires du système informatique.

Cette formation ou mise à niveau devrait se faire aussi bien au niveau des comptables que des informaticiens pour maintenir le système plus évolutif. Elle devrait porter sur l'utilisation du progiciel pour les comptables et sur l'administration du réseau, l'administration de la base de données, la maintenance matérielle ou logicielle pour les informaticiens.

Ainsi, les recyclages et formations n'auraient plus un caractère sélectif et discriminatoire qui sont souvent à l'origine des frustrations, de la démotivation et de rancœur dans les services administratifs.

En tout état de cause et eu égard à l'importance de la formation, il est souhaitable qu'on renforce le volet de l'information et de la communication. C'est en ces termes que M. Derek Bok, ancien Président de l'Université HAVARD aux Etats-Unis d'Amérique disait : « S'il vous semble que l'information coûte cher, essayez donc l'ignorance ».

Le système de formation permettrait de mieux outiller le personnel sur l'évolution technologique. Le renforcement du personnel dans les postes comptables à travers l'affectation de cadres compétents et la multiplication des séminaires de formation à leur intention permettraient de mieux répondre aux exigences informatiques et comptables. Il faudrait également qu'on mette sur pied un plan de carrière des utilisateurs.

Le suivi permanent ou l'assistance aux utilisateurs permettrait de renforcer le degré de sécurité du SIGFiP Comptabilité. Il faudrait aussi mettre à la disposition du personnel les manuels de procédures d'utilisation du système informatique.

Dans le souci d'améliorer davantage l'information financière et comptable de l'État, des approches de solutions relatives au matériel d'une part et d'ordre technique d'autre part doivent être appréhendées.

3.1.3. Les solutions d'ordre matériel et technique.

Face aux problèmes énumérés plus haut, il serait judicieux de renforcer les équipements du système informatique en place. Dans cette section, nous allons aborder d'abord les approches de solutions au niveau matériel (paragraphe I) et ensuite celles du volet technique (paragraphe II) du système informatique.

3.1.3.1. Les solutions d'ordre matériel

Ces solutions concernent les différents matériels indispensables au bon fonctionnement du système informatique. On ne peut parler de l'évolution technologique sans matériel informatique. Il est donc nécessaire de doter le système informatique actuel du matériel bureautique et informatique.

3.1.3.1.a. Dotation du système informatique en matériel de bureau

Les bureaux des techniciens et des utilisateurs devraient être bien équipés en mobiliers de bureau et instruments de travail. L'ergonomie informatique exige qu'un poste de travail soit mieux équipé pour permettre à l'utilisateur d'être à l'aise. Ainsi, tous les bureaux devraient être dotés en fourniture et installation de tables ordinateurs et de chaises.

Outre les dimensions physiques de l'espace de travail et le mobilier, d'autres aspects devraient également être pris en considération tels que l'aménagement du lieu de travail, l'entreposage ou l'espace requis pour les équipements.

Du service central aux structures en déconcentré, les acteurs du réseau des comptables directs du Trésor ne devraient pas souffrir du matériel de bureau. Ce matériel devrait être adapté à l'environnement informatique. Chaque bureau pourrait se conformer à l'ergonomie informatique.

Les bureaux des utilisateurs devraient aussi respecter la norme exigée. Celle-ci recommande 10 m² pour une seule personne, 11 m² par personne dans un bureau collectif (soit 22 m² pour 2 personnes ou 33 m² pour 3, etc.…) et 15 m² par personne dans un espace collectif bruyant (si les tâches nécessitent des communications téléphoniques par exemple). S'il s'agit d'un bureau collectif, il est recommandé de ne

pas dépasser 5 personnes exécutant un travail homogène (objectifs et commandement communs, type de tâches proches, stabilité du groupe...) [17].

On devrait éviter de mettre dans un endroit restreint plusieurs personnes. Les bureaux devraient être aérés et non contigus.

L'insuffisance du matériel de travail pourrait être à l'origine du mauvais rendement de l'utilisateur.

Le matériel de bureau seul ne suffit pas. Il faut lui associer l'équipement informatique adapté afin de faciliter l'utilisation de l'application.

3.1.3.1.b. Dotation du système en matériel informatique

Le système informatique devrait être bien équipé. Chaque utilisateur devrait avoir un ordinateur (PC) pour le travail. Les bureaux ne devraient pas souffrir de prise réseau d'accès au SIGFiP Comptabilité.

Ce n'est pas intéressant de voir certains utilisateurs attendre leur collègue finir leur tâche sur un même poste avant qu'ils n'accèdent à l'ordinateur. Si actuellement certains postes comptables ne sont pas connectés au site central, c'est dû au manque d'équipements informatiques et réseaux.

Chaque utilisateur devrait avoir tous les équipements indispensables à la réalisation du travail qui l'incombe. Pour l'exploitation du progiciel, il faudrait donc fournir aux utilisateurs des éléments nécessaires à savoir l'ordinateur, l'imprimante, le scanner, l'onduleur etc… Les installations électriques, et installations de groupes électrogènes devraient aussi accompagner les équipements informatiques et réseau.

Il serait également souhaitable de mettre en place dans les différents bureaux une bonne climatisation pour maintenir le matériel informatique dans de bonnes conditions de température et de sécurité.

Pour plus de performance du système, il faudrait forcement associer au matériel informatique, les moyens techniques.

[17] Cours Méthode et Organisation
http //www.google.tg/search ?sclient

3.1.3.2. Les solutions d'ordre technique

Ces solutions sont additionnelles aux solutions précédentes. Les différentes approches de solutions sont de deux ordres :

- les solutions relatives à l'application et à la base de données ;
- les solutions liées au réseau câblé et à la maintenance du système informatique.

3.1.3.2.a. Les approches de solutions relatives à l'application et à la base de données

Nous aborderons dans ce titre les solutions liées à l'application avant d'exposer celles qui concernent la base de données.

3.1.3.2.a.1. Au niveau de l'application

La non souplesse de l'application[18] explique le problème de la rectification difficile des écritures comptables clôturées dans le progiciel. Il faut rendre souple l'application en corrigeant de temps en temps les insuffisances constatées.

Les développeurs d'applications devraient revoir l'algorithme des scripts de traitement interactif. Par exemple dans la fenêtre d'édition de la balance ou du grand livre, il pourrait y avoir un contrôle de saisie des dates début et fin de période relative à l'année de gestion. Nous avons constaté que lorsque l'utilisateur sélectionne l'année de gestion et saisit des dates début et fin de période qui ne sont conformes à celle-ci, l'ordinateur n'affiche aucune boîte de dialogue pour attirer l'attention de l'utilisateur. Lorsque ce dernier clique sur le bouton ''imprimer'', il remarque que les informations qui s'affichent sont erronées.

Il serait important de mettre en place le module de messagerie système pour gérer les alertes de transmission de documents comptables (bordereaux de transmission par exemple) entre les acteurs du SIGFiP Comptabilité.

[18] Algorithme des procédures et fonctions qui permettent d'exécuter les requêtes des utilisateurs dans l'application plus le problème d'analyse conceptuelle du domaine d'informatisation

Il faudrait également faciliter la saisie sur certains écrans en mettant les boutons à choix multiple tout en évitant de surcharger ces écrans. Les informaticiens devraient assister en temps réel les utilisateurs du progiciel. Il devrait avoir également un suivi continu de l'utilisation du module SIGTA du réseau des comptables directs du Trésor.

Nous suggérons également à ce que l'archivage électronique des pièces comptables soit pris en compte dans le progiciel SIGFiP. Ceci faciliterait non seulement la recherche d'informations relatives aux pièces justificatives en cas d'éventuels problèmes mais aussi éviterait l'encombrement de la paperasse dans les bureaux.

Il faudrait aussi réorienter les outils de programmation du système actuel vers le JAVA 2E (langage de programmation entreprise édition) pour faciliter le partage d'informations, améliorer le problème de lenteur du réseau et pouvoir produire les graphiques et diagrammes à partir des données comptables. **[17, 21,25]** Avec JAVA EE, l'utilisateur peut à partir de son téléphone portable accéder à l'application SIGFiP.

Ce langage de programmation pourrait permettre de mettre en place une application web (Internet). De nos jours, personne ne peut se passer du web. L'utilisateur qui est à la maison peut se connecter au serveur comme s'il était au bureau et faire son travail. Le JAVA EE est un langage moins lourd et portatif, c'est-à-dire peut s'exécuter sur n'importe quel système d'exploitation.

On pourrait également mettre en place le système ''tuning''[19] pour simplifier les codes sources de l'application. Ce système permettrait de réduire la lourdeur des procédures pour faciliter l'exécution des requêtes et éviter la lenteur du réseau.

Il faudrait aussi prendre en compte dans le progiciel, la gestion de la trésorerie pour faciliter l'élaboration du plan de trésorerie de l'État.

Il serait souhaitable qu'on évalue régulièrement le progiciel mis en place (audit informatique). Cette évaluation périodique permettrait de corriger de temps en temps les difficultés des utilisateurs.

[19] Ce système permet aux administrateurs de diagnostiquer, optimiser et gérer les performances relatives à l'application, la base de données et la maintenance

Pour une bonne pratique de l'hygiène numérique, la DGTCP devrait prendre en compte les aspects suivants pour sécuriser le système applicatif :

- utiliser les mots de passe robuste (minimum 8 caractères) ;
- sensibiliser les utilisateurs de se méfier avant de cliquer (WhatsApp, Réseaux sociaux, Réseaux Wi-Fi inconnus, mail etc…) ;
- mettre à jour les appareils connectés ;
- sensibiliser les utilisateurs sur l'utilisation de la messagerie professionnelle ;
- installer des applications et logiciels officiels.

Un proverbe dit : « Mieux vaut prévenir que guérir. » Au terme du parcours des divers aspects de la sécurité des systèmes d'information, nous pouvons dire qu'en ce domaine prévenir est impératif, parce que guérir est impossible et de toute façon ne sert à rien. Lorsqu'un accident ou un pirate a détruit les données comptables, c'est toute l'administration qui tombe.

Face au volume important des requêtes, la conception de l'application nécessite l'optimisation de la base de données pour réduire le temps de réponse entre les serveurs d'application et les utilisateurs.

3.1.3.2.a.2. Au niveau de la base de données

Nous n'allons pas passer sous silence l'optimisation de la base de données. L'administrateur de la base veillera à l'amélioration de celle-ci en supprimant de temps en temps les fichiers temporaires que génère le système. Il devrait également mettre constamment à jour les tables et les données tout en supprimant les doublons pour éviter la lourdeur d'exécution des requêtes.

Grâce aux index adéquats, le système de gestion de base de données relationnelle (Oracle) est en mesure d'exécuter des requêtes sur des tables très rapidement et sans faire de lecture complète.

En considérant que la table suivante possède un million de lignes avec des valeurs différentes :

```
CREATE TABLE PAIEMENT (
  NUM_PAY NUMBER PRIMARY KEY,
  MONT_PAY NUMBER (15),
   DESCRIPTION VARCHAR2 (30),
   OBJET_PAY VARCHAR2 (15)
TABLESPACE PERFORMANCE);
```

Supposons deux situations : situation1 - La colonne OBJET_PAY n'est pas indexée, situation2 - La colonne OBJET_PAY est indexée. (CREATE INDEX objet_idx ON PAIEMENT (OBJET_PAY)) ;

Et la requête suivante :

```
SELECT COUNT (*) FROM PAIEMENT WHERE OBJET_PAY LIKE 'M%';
```

Dans la situation 1, la requête s'est exécutée en quatre secondes. Dans la situation 2, puisque la colonne OBJET_PAY est indexée, la requête s'est exécutée en une seconde. On remarque une différence très avantageuse. L'administrateur de la base de données SIGFiP devrait forcément indexer les colonnes utilisées dans les différentes requêtes. Ceci faciliterait l'exécution rapide de tous les scripts SQL (langage de manipulation des données).

Nous avons également constaté la présence de « grosses » requêtes n'utilisant pas ou peu les index et provoquant des balayages de tables de plusieurs millions (dizaine de millions) de rangs pour finalement n'en récupérer que quelques dizaines de milliers.
Lors des tests, et à base des rapports Automatic Workload Repository (AWR), nous avons remarqué qu'un certain nombre des requêtes lourdes utilisaient des balayages de tables plutôt que des accès indexés. Les origines de ce phénomène sont multiples :

- ✓ absence d'une clé primaire au niveau de la table temporaire « TOSTOCK » qui fait plus de 6.000.000 enregistrement, et qui est sollicitée par la majorité des

requêtes. Le manque de cette contrainte, oblige Oracle de faire des balayages complets de la table. (source principale de lenteur);

- ✓ mauvaise formulation de certaines requêtes. Ce qui ne permet pas à l'optimiseur de requêtes de faire un « bon » choix puisqu'il se fonde sur des informations erronées ou incomplètes ;
- ✓ d'autres cas sont visiblement dus à une inadéquation des index aux requêtes que nous avons analysées, chose qui permet de générer certains événements d'attentes « waits et verrous ».

Exemple de requêtes sources du problème, avec leurs plans d'exécution avant et

```
Plan hash value: 2614032313
PLAN_TABLE_OUTPUT
-----------------------------------------------------------------------------------------------------------------------------
| Id  | Operation                     | Name         | Starts | E-Rows | A-Rows |   A-Time   | Buffers | Reads  |
-----------------------------------------------------------------------------------------------------------------------------
|   1 |  SORT AGGREGATE               |              |      1 |      1 |      1 |00:46:46.91 |     705K|    146K|
-----------------------------------------------------------------------------------------------------------------------------
|*  2 |   FILTER                      |              |      1 |        |   1363 |00:40:04.21 |     705K|    146K|
|*  3 |    TABLE ACCESS FULL          | TOEMPLAC     |      1 |  26183 |   1900 |00:00:00.03 |    1287 |     34 |
|*  4 |    FILTER                     |              |   1900 |        |   1363 |00:46:46.77 |     704K|    146K|
-----------------------------------------------------------------------------------------------------------------------------
|   5 |     SORT AGGREGATE            |              |   1900 |      1 |   1900 |00:46:46.74 |     704K|    146K|
|*  6 |      TABLE ACCESS BY INDEX ROWID| TOSTOCK      |   1900 |      1 |  61871 |01:36:08.48 |     704K|    146K|
|*  7 |       INDEX RANGE SCAN        | TOSTOCK_IDX2 |   1900 |    150 |    920K|00:25:03.33 |   10144 |   6351 |
-----------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Predicate Information (identified by operation id):
--------------------------------------------------------------------------------
   2 - filter( IS NOT NULL)
   3 - filter("TOEMPLAC"."TYP_EMPLAC"='P')
   4 - filter(SYSDATE@!-MAX("DAT_STOCK")>2)
   6 - filter(("TOSTOCK"."COD_ARTICLE"=:B1 AND "TOSTOCK"."COD_STOCKEUR"=:B2 AND "TOSTOCK"."TYP_MVT"='PIC'))
   7 - access("TOSTOCK"."COD_DEPOT"=:B1 AND "TOSTOCK"."COD_ZONE"=:B2 AND "TOSTOCK"."COD_RACK"=:B3
   AND "TOSTOCK"."COD_MEUBLE"=:B4 AND "TOSTOCK"."COD_NIVEAU"=:B5)
  TOARTICLE.HAUTEUR_MIN, TOARTICLE.HAUTEUR_MAX, TOARTICLE.GEST_LOT, TOARTICLE.POIDS_NET_UVC,
  TOARTICLE.POIDS_BRUT_UVC, TOSTOCK.COD_DEPOT, TOSTOCK.COD_ZONE, TOSTOCK.COD_RACK,
  TOSTOCK.COD_MEUBLE, TOSTOCK.COD_NIVEAU, TOSTOCK.LETTRAGE, TOSTOCK.PCB,
  TOSTOCK.NB_COLIS_COUCHE, TOSTOCK.NB_COUCHE_PAL, TOARTICLE.DALLE,
  TOARTICLE.APPRO_DALLE, TOARTICLE.QER, TOARTICLE.UER,
  DECODE(TOARTICLE.METHODE_STK, 'O', 'D', TOARTICLE.METHODE_STK)
```

après l'intervention :

Constat :

- ✓ au niveau de l'opération N° 6 : Pour récupérer en fin de compte un seul enregistrement, Oracle met 01h36min pour accéder à la Table « TOSTOCK » via l'index « TOSTOCK_IDX2 », ce dernier n'est pas le meilleur choix. Cette opération a généré : 127 KO de lecture physique et 707 KO de lecture Logique ;

- ✓ au niveau de l'opération N° 3 : Un FULL SCAN de la table « TOEMPLAC » avait un effet désastreux, et il a influencé négativement sur l'opération N : 2.

Recommandations urgentes :

- Création d'un index « TOSTOCK_IDX8 » au niveau de la table « TOSTOCK » sur les colonnes de la clause WHERE de la requête.
- Création d'un index « TOEMPLAC_IDX7 » au niveau de la table « TOEMPLAC» pour éviter un balayage complet de la table.

Plan d'exécution après implémentation des recommandations :

```
Plan hash value: 2614032313
PLAN_TABLE_OUTPUT
-----------------------------------------------------------------------------------------------------------------------
| Id  | Operation                     | Name          | Starts | E-Rows | A-Rows |   A-Time   | Buffers | Reads  |
-----------------------------------------------------------------------------------------------------------------------
|   1 |  SORT AGGREGATE               |               |      1 |      1 |      1 |00:00:37.54 |     705K|     13K|
-----------------------------------------------------------------------------------------------------------------------
|*  2 |   FILTER                      |               |      1 |        |   1363 |00:02:04.36 |     705K|     13K|
|*  3 |    INDEX RABG SCAN            | TOEMPLAC_IDX7 |      1 |   2100 |   1900 |00:00:00.01 |    1287 |     34 |
|*  4 |    FILTER                     |               |    800 |        |   1363 |00:06:18.77 |     704K|     13K|
-----------------------------------------------------------------------------------------------------------------------
|   5 |     SORT AGGREGATE            |               |    800 |      1 |   1900 |00:06:17.20 |     704K|     13K|
|*  6 |      TABLE ACCESS BY INDEX ROWID| TOSTOCK       |    800 |      1 |  61871 |00:06:05.01 |     704K|     13K|
|*  7 |       INDEX SCIP SCAN SCAN    | TOSTOCK_IDX8  |    800 |   1300 |   1200 |00:00:02.19 |    1024 |    151 |
-----------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Predicate Information (identified by operation id):
--------------------------------------------------------------------------------
   2 - filter( IS NOT NULL)
   3 - filter("TOEMPLAC"."TYP_EMPLAC"='P')
   4 - filter(SYSDATE@!-MAX("DAT_STOCK")>2)
   6 - filter(("TOSTOCK"."COD_ARTICLE"=:B1 AND "TOSTOCK"."COD_STOCKEUR"=:B2 AND "TOSTOCK"."TYP_MVT"='PIC'))
   7 - access("TOSTOCK"."COD_DEPOT"=:B1 AND "TOSTOCK"."COD_ZONE"=:B2 AND "TOSTOCK"."COD_RACK"=:B3
   AND "TOSTOCK"."COD_MEUBLE"=:B4 AND "TOSTOCK"."COD_NIVEAU"=:B5)
```

Effet : Le temps total de cette requête passe de 01h36min à 0h0minh38s.

Il faudrait également renforcer le système de sauvegarde des données comptables en dupliquant les sites de sauvegardes et les serveurs de stockage internes et externes du lieu d'exploitation du progiciel.

Il serait souhaitable de prendre en compte certains principes de sécurité des données. Ces principes portent sur le codage de la donnée qui consiste à rendre celle-ci incompréhensible (la cryptologie) et l'authentification relative au nom utilisateur et son mot de passe.

Le même principe de sécurité prend également en compte l'adresse MAC (Média Access Control) unique de l'ordinateur qui se connecte au serveur. Ceci permettrait à l'administrateur du système d'identifier les machines qui ne sont pas autorisées à se connecter au réseau et de contrôler l'accès pour lutter contre des volontés malveillantes. **[18, 23, 28]**

Autres pistes d'approches de solutions relatives à la gestion de la mémoire, des entrées / sorties, et aux statistiques de la base de données. Nous avons vu que l'on peut « récupérer » de la mémoire réservée par le système d'exploitation et inutilisée.

On peut booster l'utilisation de la mémoire au maximum. Après plusieurs essais avec sauvegarde du fichier spfile, nous avons pu atteindre le System Global Area (SGA) au maximum à 1750Mo, la partie de la mémoire qui est partagée par tous les processus appartenant à l'instance Oracle. Nous avons augmenté la mémoire comme suit : la taille du database buffer cache à 1280Mo pour ainsi gagner en termes de performance à hauteur de 70% par rapport à l'état actuel en se basant sur la vue v$db_cache_view.
Nous avons également augmenté la taille de la keep buffer cache à 10% du data buffer cache c'est-à-dire à 120Mo pour gagner toujours en performance puisque nous avons remarqué que certaines tables sont de petite taille (TOMOUVEMENT, TOOPTION, …) et donc il sera préférable de les charger une seule fois dans le cache et de s'en servir pour toutes les requêtes les utilisant. **[18, 20]**

Les effets attendus sont :

- ✓ meilleure efficacité du cache débouchant sur une transaction plus rapide;
- ✓ meilleure « résistance » du cache aux grosses requêtes occasionnant les transactions plus régulières et temps de réponse utilisateur plus constant. Au lieu de varier de 1 à 4 les temps de réponse ne varieront plus que de 1 à 2 (ces chiffres ne sont qu'un exemple);
- ✓ meilleure efficacité du cache entrainant un peu moins d'entrées / sorties.

Malgré les bons résultats attendus lors du réglage de la mémoire, la taille actuelle de la SGA, ne permet pas de charger les données demandées par les requêtes de tous les

utilisateurs surtout s'ils sollicitent la même table. Ce qui provoque un swapping désastreux pour les performances et aussi des events wait de type lock. Une augmentation de la rapidité des entrées sorties sera très nécessaire.

Les actions pour baisser le nombre d'entrées / sorties sont :

- ✓ augmenter la valeur du paramètre « DB_FILE_MULTIBOLCK_READ » de 16 à 64 afin de diminuer le nombre d'entrées / sorties;
- ✓ changer la valeur du paramètre « OPTIMIZER_INDEX_COST_ADJ » de 25 à une valeur entre 15 et 20, et ce afin qu'Oracle privilège l'utilisation des index sur les FULL SCAN.

Il a été constaté que certains fichiers (« data files » Oracle) sont beaucoup plus sollicités que les autres : une répartition plus optimisée dans la baie de disques pourrait participer à l'amélioration des performances. Il faudra pour cela disposer d'informations et de statistiques sur le fonctionnement de la baie de disques.

Les effets attendus sont :

- ✓ meilleur « rendement » global des entrées / sorties;
- ✓ diminution du temps de lecture / écriture entraînant une amélioration des performances ressenties pas les utilisateurs.

L'optimiseur de requêtes d'Oracle utilise des statistiques sur la répartition de la valeur des données au sein des tables et index pour « choisir » un « bon » plan d'exécution de la requête demandée.

Les effets attendus sont :

- ✓ meilleurs plan d'exécution des demandes;
- ✓ diminution des temps de réponse;
- ✓ légère diminution des entrées / sorties.

Quelques autres éléments peuvent être contrôlés et éventuellement modifiés. On a constaté que le système est programmé pour un redémarrage quotidien (02h15) sans arrêt correcte de la BD, ce qui oblige Oracle de recharger l'ensemble des données lors du prochain démarrage.

Oracle utilise un nombre de processus pour servir l'ensemble des sessions utilisateurs de la base de données. Ce nombre était suffisant avant les réglages réalisés puisque le nombre de requêtes exécutés était faible par rapport à l'état actuel. Actuellement presque 53Go sont lu par heure et presque 450Mo sont écrite par heure donc Oracle utilise plus de processus. C'est pourquoi nous avons augmenté le nombre de processus à 250.

3.1.3.2.a.3 Les aspects sécuritaires de la base de données et l'application

Avec l'outil de sécurité informatique, 'Nessus' a signalé les faiblesses potentielles ou avérées sur les machines testées. Ceci inclut, entre autres : les services vulnérables à des attaques permettant la prise de contrôle de la machine, l'accès à des informations sensibles. Nessus est un logiciel qui effectue de réelles attaques, comme pourrait le faire un hacker essayant de pirater la solution étudiée par exemple. Une fois le scan effectué, Nessus présente les résultats du test sous forme d'un rapport. Le tableau ci-dessous illustre les résultats après scannage du système d'information :

Vulnérabilités	**Hôtes**	**Remédiations**	**Classement des risques**	**Type de contrôle**
Détection de serveur Web Apache non prise en charge	x.x.x.x	Supprimer le serveur Web s'il n'est plus nécessaire. Sinon, mettre à niveau vers une version prise en charge si possible ou passer à un autre serveur.	Critique	Corrective
Détection de version PHP non prise en charge, Vulnérabilités multiples de PHP	x.x.x.x	Mettez à niveau vers une version de PHP actuellement prise en charge.	Critique	Corrective
Détection de version non prise en charge de la base de données Oracle	x.x.x.x	Effectuer une mise à niveau vers une version d'Oracle Data base actuellement prise en charge.	Critique	Corrective

Détection d'installation non prise en charge par Microsoft Windows 8	x.x.x.x	Effectuer une mise à niveau vers une version de Microsoft Windows actuellement prise en charge.	Critique	Corrective
Détection de version non prise en charge par Microsoft SQL Serveur	x.x.x.x	Effectuer une mise à niveau vers une version de Microsoft SQL Serveur actuellement prise en charge.	Critique	Corrective
Accès non authentifié au serveur X : capture d'écran, Accès non authentifié au serveur X11	x.x.x.x	Restreindre l'accès à ce port avec la commande 'xhost'. Si la fonction client/serveur X n'est pas utilisée, désactiver complètement les connexions TCP au serveur X.	Critique	Corrective
Plusieurs vulnérabilités d'Apache Tomcat	x.x.x.x	Mettrz à niveau vers la version ultérieure d'Apache Tomcat.	Critique	Corrective
Vulnérabilités multiples d'Oracle GlassFish Serveur	x.x.x.x	Effectuer une mise à niveau vers la version ultérieure d'Oracle GlassFish Serveur, comme indiqué dans l'avis de mise à jour des correctifs critiques Oracle de juillet 2016.	Critique	Corrective
Système d'exploitation Windows non pris en charge	x.x.x.x	Mise à niveau vers un service pack ou un système d'exploitation pris en charge	Critique	Corrective
Plusieurs ports de gestions sont ouverts sur les serveurs publics.	x.x.x.x	Procéder au durcissement du système et suivre les bonnes pratiques. Installation d'antivirus.	Critique	Préventif
Interface Tomcat Manager / Host Manager par défaut trouvée	http:// x.x.x.x /WebClearing/ http:// x.x.x.x /didoc	Proceder au durcissement du système	Majeur	Préventif
Apache/2.4.29 semble être obsolète	http:// x.x.x.x /WebClearing/ http:// x.x.x.x /didoc	Mettre à niveau vers la dernière version	Majeur	Corrective
JQuery 1.2 < 3.5.0 Multiple XSS	10.155.1.116	Mettre à niveau vers la version ultérieure de JQuery.	Mineur	Corrective

Il n'y a pas que l'optimisation de la base de données. Il faudrait aussi apporter des améliorations au niveau du réseau et de la maintenance de tout le système.

3.1.3.2.b. Les approches de solutions relatives au câblage réseau et à la maintenance du système

Nous proposerons ici en premier lieu les solutions liées au réseau et en second lieu celles relatives à la maintenance.

3.1.3.2.b.1. Les solutions liées au câblage réseau

Le réseau câblé devrait faire l'objet de maintenance périodique pour éviter la perte d'information ou la mauvaise connexion au niveau des utilisateurs. Il serait donc nécessaire de revoir la configuration physique du système réseau. L'audit relatif au réseau informatique actuel serait la bienvenue pour palier le problème de lenteur au niveau des utilisateurs.

Il faudrait également multiplier les prises réseaux (multiplicateur de prise) dans les bureaux pour permettre à chaque utilisateur de se connecter à l'application. Pour rendre plus rapide la connexion, il serait souhaitable de doter tout le système réseau en fibre optique.

En permettant à chaque individu d'accéder au réseau, les occasions de le fragiliser sont multiples. Puisque la sécurisation de l'intégralité du maillage informatique passe par la responsabilisation de l'ensemble de ses utilisateurs.

Il convient de diffuser une culture de la cyber sécurité auprès de l'opinion publique
Non pas pour transformer chaque citoyen en informaticien, mais bien pour en faire un consommateur de technologies responsable, conscient de l'ampleur de la menace potentielle et de la valeur de l'information, dans un monde où les données circulent à la vitesse de la lumière.

La sécurité ne doit pas être l'apanage des seuls militaires ou des policiers. Elle doit au contraire être partagée entre le plus grand nombre. C'est en sachant ce que l'on risque de perdre sur la toile que l'on peut entreprendre une démarche de sécurisation des données sensibles et commencer à s'interroger sur le juste équilibre entre une politique de surveillance très aboutie, et le droit à préserver une vie privée.

Chaque organisation a la responsabilité de renforcer la confiance des utilisateurs, de protéger l'intégrité des données et des réseaux et d'envisager les menaces existantes et potentielles

L'administrateur du système pourrait pallier aux éventuels virus dans le réseau en limitant ou en empêchant l'accès des utilisateurs sur l'utilisation des clés USB lorsqu'ils effectuent des travaux dans le SIGFiP Comptabilité. Il est également souhaitable de mettre en place les liaisons VSAT par hub satellite (équipement réseau satellitaire)[20] pour la maîtrise de l'effet climatique dans certaines zones montagneuses (Badou par exemple).

On pourrait aussi éviter l'échec de connexion qui survient parfois et rendre rapide la connexion du réseau informatique de tout le système à l'aide de la technologie VSAT.

Il serait souhaitable d'étendre le réseau SIGFiP en déconcentré et au niveau des payeurs pour optimiser son utilisation (extranet). Ceci permettrait de garantir la disponibilité du réseau et le partage d'informations.

Pour améliorer les performances, il faudrait qu'on utilise la paire torsadée blindée plus résistante aux perturbations électromagnétiques et qui autorise un débit pouvant aller jusqu'à 1000Mbits/s.

<u>Image III.1</u> : câble à paire torsadée type 5E blindé

Voici les différentes normes de l'Ethernet en matière de câble à paire torsadée :

- 10 Base T : sur 100 mètres maximum, vitesse de 10 Mbps, chaque extrémité d'un tel câble étant munie d'une prise RJ45 ;
- 100 Base TX : sur 100 mètres maximum, vitesse de 100 Mbps, chaque extrémité d'un tel câble étant munie d'une prise RJ45 ;

[20] Les terminaux VSAT possèdent des slots permettant d'accueillir des cartes réseaux (X25, ATM, Ethernet), multimédia (Visioconférence, Streaming vidéo) et de communication (lignes analogiques, lignes numériques) : VSAT n'est plus seulement un réseau de données, mais aussi un réseau téléphonique et de diffusion vidéo.

- 1000 Base T : sur 100 mètres maximum, vitesse de 1000 Mbps, chaque extrémité d'un tel câble étant munie d'une prise RJ45.

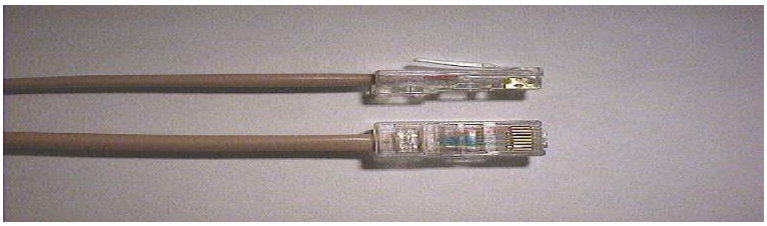


Image III.2 : Prise RJ45

On pourrait également utiliser la fibre optique entre les concentrateurs et le circuit réseau câblé pour rendre plus rapide la transmission des données. Il suffit de prévoir le module transiva. Ce module permettra de convertir le signal lumineux en signal électrique.

Image III.3 : Fibre optique en silice

Les grands avantages de la fibre optique par rapport aux autres supports filaires sont : peu de perte de signal, vitesse de transmission élevée, faible poids, immunité aux interférences électromagnétiques, pas d'échauffement etc…

La bande passante d'une fibre optique étant très large (plusieurs MHz), il est aisé de faire du multiplexage fréquentiel[21] pour faire transiter simultanément plusieurs communications.

Voici les différentes normes de l'Ethernet en matière de fibre optique :

- FOIRL (Fiber Optic Inter Repeater Link / lien inter-répéteur sur fibre optique) : le standard original pour l'Ethernet sur la fibre optique. Vitesse de 10 Mbps ;
- 10 Base-FL : mise à jour du standard FOIRL, vitesse de 10 Mbps ;
- 100 Base-FX : vitesse de 100 Mbps ;
- 1000 Base-LX : monomode, vitesse de 1000 Mbps, portée de 3 km ;

[21] Permet de gérer la bande passante afin d'optimiser celle-ci. Selon le débit définit, un point peut avoir accès à plusieurs canaux en même temps.

-1000 Base-LX : multimode, vitesse de 1000 Mbps, portée de 550 m ;

Que ce soit l'optimisation de la base de données ou l'amélioration du câblage réseau, il serait opportun de faire la maintenance périodique du système.

3.1.3.2.b.2. Les approches de solutions relatives à la maintenance du système

Il serait souhaitable que l'équipe de maintenance informatique fasse régulièrement la maintenance matérielle et logicielle. Ceci permettrait d'éviter des pannes techniques du système.

On pourrait également installer un antivirus "réseau" pour faciliter la mise à jour automatique des PC utilisateurs et doter tous les postes utilisateurs des versions actualisées du système d'exploitation Windows.

Il faudrait harmoniser le système du réseau actuel afin d'avoir un seul câblage pour rendre plus rapide la transmission des données comptables. Le réseau câblé nécessite également une maintenance régulière. A ce titre, il serait judicieux de veiller à la résolution des problèmes techniques dans les meilleurs délais pour éviter les pannes de connexion.

Il y a lieu de sensibiliser les utilisateurs sur l'abus de l'internet lorsqu'ils effectuent un travail dans le progiciel. On pourrait aussi mettre les routeurs de relai à chaque nœud du réseau câblé pour amplifier sa bande passante. Il faudrait également éviter le gaspillage de câble lors du câblage du réseau et veiller à la protection physique des installations (prévoir les risques d'incendie, fournir une alimentation permanente).

Dans le souci d'améliorer la sécurité et la réduction du temps de maintenance, il est souhaitable de mettre en place le système Simple Network Management Protocol (SNMP), ou « protocole simple de gestion du réseau » pour garantir la non interruption du service. C'est un protocole de communication qui permet aux administrateurs de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes "réseau" et matériel (PC utilisateur) à distance.

Les objectifs du protocole SNMP sont :

- connaître l'état global d'un équipement (actif, inactif, partiellement opérationnel...) ;
- gérer les événements exceptionnels (perte d'un lien réseau, arrêt brutal d'un équipement...) ;
- analyser les différentes métriques afin d'anticiper sur les problèmes futurs (engorgement réseau...) ;
- agir sur certains éléments de la configuration des équipements ;
- résoudre le problème à distance d'un ordinateur connecté au central.

Présentation schématique de la technologie SNMP :

Le schéma ci-après comporte toute une technologie informatique qui prend en compte tous les éléments du système concerné. La configuration SNMP gère non seulement la partie logicielle mais aussi la partie matérielle de toute l'installation.

Figure III.3 : Schéma technologie SNMP

Dans la terminologie SNMP, le synonyme manager est plus souvent employé que superviseur. Le superviseur est la console qui permet à l'administrateur d'exécuter des requêtes de management.

Devant la véritable explosion des réseaux (que ce soient des réseaux internes à l'entreprise ou bien l'internet lui-même) et leur importance primordiale dans une

infrastructure, les besoins de superviser et surtout de diagnostiquer rapidement les problèmes sont devenus des préoccupations majeures.

La technologie SNMP permettant de se connecter directement à la console de l'équipement, offre une vue synthétique de l'infrastructure séparant ainsi les deux métiers différents que sont la supervision et l'administration matérielle et logicielle.

Les différents éléments que l'on peut identifier avec le protocole SNMP sont synthétisés par le schéma ci-dessus.

Entre autres mesures de sécurité, nous pouvons mentionnés les approches de solutions suivantes :

- Identifier les actifs du système d'information de l'entité et s'assurer que les responsabilités sont définies pour la protection des actifs ;
- Sécuriser les informations qui sont stockées sur les supports numériques ;
- Limiter l'accès aux systèmes d'information aux seules personnes autorisées ;
- Empêcher tout accès physique non autorisé, tout dommage ou toute intrusion dans les environnements des SI ;
- Garantir la protection de l'information sur les réseaux informatiques de l'entité ;
- Fournir aux utilisateurs, les postes de travail sécurisés pour leurs activités professionnelles ;
- Intégrer la sécurité dans le cycle de vie des systèmes d'information qu'ils soient acquis ou développés par l'entité ;
- Sécuriser les applications web exposées sur internet ;
- Garantir l'utilisation correcte et efficace de la cryptographie afin de protéger l'intégrité, la confidentialité et l'authenticité des informations ;

Etant donné que le Système Intégré de Gestion des Finances Publiques aide la DGTCP dans la production de l'information financière et comptable de l'Etat, il serait donc

souhaitable que les approches de solutions évoquées soient prises en compte pour son amélioration.

CHAPITRE IV : INTERPRETATION DES RESULTATS ET DISCUSSIONS

Une fois que nous avons terminé nos analyses d'audit du système comptable et financier de la DGTCP, il est question pour nous dans cette dernière partie de présenter les résultats de recherche, et puis d'interpréter les principaux aboutissements des solutions proposées afin de confirmer ou infirmer nos hypothèses.

La discussion du présent document est le lieu pour une rédaction plus poussée et plus interprétative des résultats. Cette partie est importante pour la crédibilité de notre travail. Elle valorise notamment nos approches de solutions en exposant le sens de l'argumentation et de la réflexion. C'est une preuve que nos recherches n'émergent pas du néant et reflète en effet la pertinence de notre travail.

Cela suppose également un sens du réalisme et de l'autocritique. Afin de la mener à bien, il est nécessaire de faire preuve de réflexion, d'analyse, de comparaison et de synthèse. Dans ce chapitre, nous allons parcourir les solutions d'ordre réglementaire et humain d'une part et les solutions relatives à l'aspect matériel et technique d'autre part afin de dégager les résultats et discussions.

4.1. Les résultats d'ordre réglementaire et humain

Nous avons jugé opportun de commencer avec la présentation de notre résultat par identification des transactions effectuées en tenant compte des textes qui régissent désormais, l'exploitation du SIGFiP Comptabilité constituant le socle des activités comptables de la DGTCP. Ce résultat encourageant à favoriser l'exécution du système informatique mis en place sur toute la chaine de la dépense publique.

4.1.1. Les résultats d'ordre réglementaire

Les textes qui devraient régir l'exploitation du module SIGFiP Comptabilité (SIGTA) et son extension en déconcentré sont rédigés et misent en application. De même, les instructions comptables pour définir les niveaux d'intervention de chaque utilisateur ont été élaborés afin de facilité le traitement de l'information financière et comptable.

La DGTCP a également définit par des notes de services les tâches spécifiques des informaticiens (réseau, développement, maintenance, assistance utilisateur et administration de la base de données).

4.1.1.a. Organisation de la structure informatique

La direction informatique a été créée pour faciliter la gestion et l'exploitation du module SIGFiP Comptabilité. Ce qui a permis d'éviter la lourdeur du circuit pour corriger les éventuelles erreurs dans le système informatique. Toutes les demandes de correction passeraient par ladite direction. Le circuit des demandes est devenu court et l'intervention des informaticiens est plus rapide pour assister les utilisateurs. Le travail est amélioré et l'on a gagné du temps dans l'exécution des tâches quotidiennes. La Blockchain permettant de situer les responsabilités en cas d'éventuels problèmes et de savoir à quelle équipe s'adresser pour tel ou tel dysfonctionnement a été constituée.

4.1.1.b. L'extension du réseau aux structures en déconcentré

Les travaux d'extension Blockchain de l'application pour faciliter la transmission de l'information comptable entre les postes comptables en déconcentré et les services centraux de la DGTCP ont contribué à la performance de la production de l'information financière et comptable. Les comptes de gestion des comptables sont désormais produits dans de bons délais pour la Cour des comptes.

Tous les postes comptables sont actuellement connectés au site SIGFiP Comptabilité, facilitant la production de la balance générale des comptes du Trésor.

Une fois l'extension établie, la Blockchain a pris en compte le choix du personnel qualifié pour réaliser les différentes fonctions définies dans les postes comptables.

4.1.2. Les résultats d'ordre humain

Les acteurs de la Blockchain sont régulièrement formés de la tenue interactive de la comptabilité de l'État et de la maîtrise des procédures de comptabilisation dans le progiciel. Le recrutement des agents qualifiés en renforcement du personnel est également effectué.

4.1.2. a. Le recrutement conséquent du personnel qualifié

La Blockchain du recrutement est constituée du personnel informatique et comptable. Les profils ont été définis au départ afin d'éviter de recruter parce que les postes sont vacants. La Blockchain a tenu compte de l'adéquation de la qualification à la fonction occupée.

Si les différentes mesures que nous venons de proposer sont de nature à améliorer les prestations de la qualité de l'information financière et comptable de l'État, celles-ci ne pourraient atteindre une véritable efficience sans une action efficace sur les ressources humaines qui animent les structures du réseau des comptables directs du Trésor.

Ainsi, le plan de carrière des agents a été élaboré et tient compte de la bonne politique de mobilité du personnel dans la gestion des ressources humaines.

4.1.2.b. La mise en place d'un programme de formation du personnel

La Blockchain de formation regorge les informaticiens et les comptables. Le personnel connait désormais les modules de formations inscrites dans le plan de travail annuel et est régulièrement formé.

La formation en tant que facteur de motivation du fonctionnaire, a considérablement amélioré la qualité du service de l'État et a permis au personnel d'être à jour.

Le système de formation a également facilité de mieux outiller le personnel sur l'évolution technologique et l'impact de la tenue de la comptabilité afin de renforcer le degré de sécurité du SIGFiP Comptabilité.

Les manuels de procédures d'utilisation du système informatique et comptable ont été élaborés dans le souci d'améliorer davantage l'information financière et comptable de l'État. Les résultats relatifs au matériel d'une part et technique d'autre part n'ont pas été négligeables.

4.1.3. Les résultats sur le plan matériel et technique.

La Blockchain a renforcé les équipements du système informatique en place. Dans cette section, nous allons aborder d'abord les résultats au niveau matériel et ceux du volet technique.

4.1.3.1. Les résultats d'ordre matériel

La Blockchain a recensé les différents matériels indispensables au bon fonctionnement du système informatique. On ne peut parler de l'évolution technologique sans matériel informatique. Le système informatique actuel a été doté du matériel bureautique et informatique.

4.1.3.1.a. Dotation du système informatique en matériel de bureau

Les bureaux des techniciens et des utilisateurs ont été bien équipés en mobiliers de bureau et instruments de travail. Ainsi, tous les bureaux ont été dotés en fourniture et installation de tables ordinateurs et de chaises. Les bureaux sont désormais bien aérés facilitant le rendement de l'utilisateur.

Le matériel de bureau seul ne suffit pas. Il faut lui associer l'équipement informatique adapté afin d'optimiser l'utilisation de l'application.

4.1.3.1.b. Dotation du système en matériel informatique

Le système informatique a été bien équipé. Chaque utilisateur possède un ordinateur (PC) pour le travail. Les bureaux ne souffrent plus de prise réseau d'accès au SIGFiP Comptabilité.

Chaque a tous les équipements indispensables à la réalisation du travail qui l'incombe. Pour l'exploitation du progiciel, les utilisateurs ont à leur disposition des éléments nécessaires à savoir l'ordinateur, l'imprimante, le scanner, l'onduleur etc… Les installations électriques, et installations de groupes électrogènes ont aussi accompagnés les équipements informatiques et réseau.

Dans bureau, une bonne climatisation est installée pour maintenir le matériel informatique dans de bonnes conditions de température et de sécurité.

Pour plus de performance du système, la Blockchain a associée au matériel informatique, les moyens techniques.

4.1.3.2. Les résultats d'ordre technique

Ces résultats sont de deux ordres :

- les résultats relatifs à l'application et à la base de données ;
- les résultats liés au réseau câblé et à la maintenance du système informatique.

4.1.3.2.a. Les résultats relatifs à l'application et à la base de données

Toutes entités souhaitent la transparence, la fiabilité de ses documents de synthèses pour aboutir à l'image fidèle. Pour ce faire, la Blockchain est venue améliorer et protéger les informations produites contre les manipulations de compte comptable et financier. Le critère de la fiabilité est placé en premier lieu dans le groupe thématique que nous avons eu à analyser. Toutes les opérations enregistrées sont cryptées et décentralisées dans tout le réseau au niveau applicatif et au niveau de la base de données du système d'information comptable.

4.1.3.2.a.1. Au niveau de l'application

La Blockchain a contribué très significativement à la réduction des erreurs dans les transactions financières et à la protection de l'information comptable. Le résultat de notre travail permet d'être dans le délai de production de documents de synthèses. Ceci, nous fait savoir que la fiabilité et la sécurité sont parmi les critères d'appréciation des informations de la Blockchain. D'ailleurs, dans le cadre de la chaine de dépense publique, la Blockchain permet une meilleure maitrise des risques de perte de données dans le processus de traitement des données comptables.

Le module de messagerie système pour gérer les alertes de transmission de documents comptables (bordereaux de transmission par exemple) entre les acteurs du SIGFiP Comptabilité a été mis en place afin de sécuriser toute la chaine financière.

Toujours dans la Blockchain, l'archivage électronique des pièces comptables est pris en compte dans le progiciel SIGFiP. Ceci a facilité non seulement la recherche d'informations relatives aux pièces justificatives en cas d'éventuels problèmes mais aussi éviterait l'encombrement de la paperasse dans les bureaux.

Face au volume important des requêtes, la conception de l'application nécessite l'optimisation de la base de données pour réduire le temps de réponse entre les serveurs d'application et les utilisateurs.

4.1.3.2.a.2. Au niveau de la base de données

La base de données a été optimisée en supprimant de temps en temps les fichiers temporaires que génère le système et les données doublons afin d'éviter la lourdeur d'exécution des requêtes.

Grâce aux index adéquats, le système de gestion de base de données relationnelle (Oracle) est en mesure d'exécuter des requêtes sur des tables très rapidement et sans faire de lecture complète.

Dans la Blockchain, le système de sauvegarde des données comptables a été renforcer en dupliquant les sites de sauvegardes et les serveurs de stockage internes et externes du lieu d'exploitation du progiciel.

Le principe de la cryptologie et d'authentification relative au nom utilisateur et son mot de passe a été renforcé en incorporant dans la Blockchain l'adresse MAC (Média Access Control) unique de l'ordinateur qui se connecte au serveur.

Ceci a permis à l'administrateur du système d'identifier les machines qui ne sont pas autorisées à se connecter au réseau et de contrôler l'accès pour lutter contre des volontés malveillantes.

4.1.3.2.a.3. La sécurité de la base de données et de l'application

La Blockchain a intégré l'outil de sécurité « Nessus » qui a signalé les faiblesses potentielles ou avérées sur les machines testées. Ceci inclut, entre autres : les services vulnérables à des attaques permettant la prise de contrôle de la machine, l'accès à des

informations sensibles. Nessus est un logiciel qui effectue de réelles attaques, comme pourrait le faire un hacker essayant de pirater la solution étudiée par exemple. Une fois le scan effectué, Nessus présente les résultats du test sous forme d'un rapport dans la Blockchain afin de mettre à jour les éventuels risques détectés.

Il n'y a pas que l'optimisation de la base de données. Les résultats probants ont été remarquables dans la Blockchain du réseau et de la maintenance de tout le système.

4.1.3.2. b. Les résultats relatifs au câblage réseau et à la maintenance du système

Nous proposerons ici en premier lieu les résultats liés au réseau et en second lieu celles relatives à la maintenance.

4.1.3.2. b.1. Les résultats liés au câblage réseau

Dans la Blockchain, une maintenance périodique de tout le système a été mise en place pour éviter la perte d'information ou la mauvaise connexion au niveau des utilisateurs.

Les prises réseaux (multiplicateur de prise) ont été multipliées dans les bureaux pour permettre à chaque utilisateur de se connecter à l'application. Pour rendre plus rapide la connexion, tout le système réseau a été doté en fibre optique.

Que ce soit l'optimisation de la base de données ou l'amélioration du câblage réseau, nous avons constaté également des résultats dans la maintenance périodique du système.

4.1.3.2.b.2. Les résultats relatifs à la maintenance du système

La solution de Blockchain a pris en compte la maintenance matérielle et logicielle régulière pour éviter des pannes techniques du système. L'antivirus "réseau" a été installé pour faciliter la mise à jour automatique des PC utilisateurs et doter tous les postes utilisateurs des versions actualisées du système d'exploitation Windows.

Le système du réseau actuel a été harmonisé afin d'avoir un seul câblage pour rendre plus rapide la transmission des données comptables et de veiller à la résolution des problèmes techniques dans les meilleurs délais.

Dans le souci d'améliorer la sécurité et la réduction du temps de maintenance, le système Simple Network Management Protocol (SNMP), ou « protocole simple de gestion du réseau » a été développé dans la Blockchain pour garantir la non interruption du service.

4.2. Discussions des résultats interprétés

Afin d'affiner notre discussion, nous allons procéder par une analyse point par point, des différents résultats que nous venons d'interpréter plus haut. Les différents résultats de transactions effectuées par la Blockchain nous a permis de constater que la DGTCP génère de manière automatique des différents documents comptables dans le progiciel de gestion intégré des finances publiques.

L'automatisation et la rapidité des opérations comptables et financières de la DGTCP, nous ont permis de confirmer les résultats réalisés dans la Blockchain proposée. On constate qu'aujourd'hui, avec la multiplication des logiciels et les applications dans les pratiques comptables, obligent les entités à paramétrer toutes ses opérations dans l'optique d'une amélioration de la façon de tenir la comptabilité. Le reporting pourrait se faire plus facilement et plus rapidement, répondant aux problèmes de délais de production des informations comptables.

Avec la solution Blockchain proposée, La fiabilité et la sécurisation des documents comptables a été renforcée et a donné la certitude sur les documents comptables. De même, Blockchain nous a rassuré que toutes modification ou altération d'un compte est impossible. En résumé, les transactions sont ajoutées au bloc et scellés interdisant ainsi la manipulation de toutes sortes par une tierce personne. Ce qui n'était pas le cas avec les résultats antérieurs.

Au terme de notre travail orienté sur la Contribution de la Blockchain à l'amélioration de la qualité de l'information comptable de la DGTCP, notre question d'évaluation du système intégré de gestion des finances publiques est la suivante : comment les acteurs de la chaine de dépense apprécient ils les documents de synthèse diffusés par la technologie Blockchain ? Partant d'un premier constat selon lequel, on assiste depuis

plusieurs années déjà, à une série de scandales financiers mettant en cause la certification des documents comptables.

Et d'un second constat, l'implémentation de la Blockchain permet de réduire ce risque de scandales financiers et faciliter la génération automatique des documents de synthèse de bonne qualité. La présente étude avait donc une double ambition, d'abord identifier les différents types des opérations comptables effectuées par la Blockchain et en fin de mettre en évidence les informations comptables issues de la technologie Blockchain.

Afin d'apporter des éléments de réponse à notre question de recherche, nous avons adopté une démarche qualitative dans laquelle nous avons réalisé le questionnaire en annexe du document. L'analyse des éléments de réponses obtenus à partir du dit questionnaire nous a permis de formuler les propositions suivantes :

- proposition 1 : Toutes les transactions effectuées par la Blockchain sont des opérations comptables ;
- proposition 2 : La Blockchain fonctionnant sur les comptes numériques, protège les documents comptables contre sa modification ou altération d'aucune sorte ;
- proposition 3 : La pratique managériale de la Blockchain permet de réduire les temps de saisi d'une opération et la génération automatique des documents de synthèse de bonne qualité.

Cependant, ce travail comporte certaines limites, notamment : la faiblesse de l'échantillon, car nous nous sommes limités dans les locaux de la direction générale. Ce travail pourrait donc être complété par une enquête par questionnaire, susceptible de mettre les répondants plus à l'aise et de garantir la valeur prédictive des éléments de réponses mis en avant précédemment.

Il faudrait aussi prendre en compte dans le progiciel, la gestion de la trésorerie pour faciliter l'élaboration du plan de trésorerie de l'État. Il serait souhaitable qu'on évalue régulièrement le progiciel mis en place (audit informatique). Cette évaluation périodique permettrait de corriger de temps en temps les difficultés des utilisateurs.

L'objectif étant de voir la possibilité de sécuriser l'information financière sur la chaine de la dépense publique, nous avons mis en lumière l'importance de mettre en place la technologie de la Blockchain. Un autre champ d'investigation sera donc la conception d'un système capable de contourner les limites liées à l'influence des facteurs externes afin de garantir l'intégrité des données comptables. Un accent particulier doit être mis sur les algorithmes de détection des intrusions.

En perspectives, nous comptons étudier le lien entre la comptabilité de l'État et celle des structures en déconcentré. Ainsi, l'une des perspectives de notre travail est d'explorer l'impact de la comptabilité des collectivités sur la performance des systèmes informatiques de la DGTCP afin de retracer les opérations comptables de celles-ci dans la balance générale de l'État.

CONCLUSION ET PERSPECTIVES

Les travaux effectués dans le cadre de ce mémoire ont trait aux audits des systèmes informatiques et plus particulièrement l'évaluation du réseau des comptables directs du trésor avec pour finalité d'améliorer la gestion des données comptables et financières. Nous avons commencé par présenter un état de l'art détaillé des activités de la DGTCP à ce jour.
Nous avons ainsi contribué à enrichir la gestion financière de la chaine de la dépense publique à travers l'audit du système informatique. Nous avons également proposé des approches de solutions aux emprises de la blockchain.

Nous nous sommes intéressés ensuite à la sécurité des données comptables et financières du domaine étudié avant de proposer une nouvelle architecture de prise en compte des faiblesses détectées afin de mieux adapter le système informatique.

Les résultats obtenus montrent une amélioration de gestion du réseau des comptables directs du trésor public togolais qui ouvrent la voie à un certain nombre de perspectives. Au terme de notre étude, il y a lieu de constater que beaucoup reste encore à faire. Le système Intégré de Gestion des Finances Publiques nécessite de gré ou de force une amélioration automatisée dans la tenue de la comptabilité de l'Etat.

Un autre phénomène marquant dans cette analyse reste le problème réglementaire et humain. Pour surmonter les difficultés actuelles dans la gestion informatisée de la tenue de la comptabilité de l'Etat, il faudrait que les pouvoirs publics togolais expriment une volonté réelle de changer le visage interactif de celle-ci.

La modernisation dans la gestion des finances publiques constitue une préoccupation essentielle pour tous les États. Cette préoccupation est plus accentuée dans les pays en développement vu les enjeux auxquels ils font face : améliorer la qualité de

l'information financière et comptable de l'Etat et engager des projets de développement.

A cet égard, il faudrait que les nouvelles orientations tendent vers le contexte environnemental actuel. Les exemples des pays voisins par rapport à l'évolution de la technologie ne sont pas à négliger, mais devraient être étudiés et reconnus comme pouvant s'appliquer à notre administration.

Aujourd'hui, il faudrait un peu plus d'ouverture vers les administrations d'autres pays, car la globalisation de l'informatique et la transformation du monde en un village planétaire, nous y contraignent.

Par ailleurs, pour ce qui concerne les modèles existants de progiciels de gestion des finances publiques, les nuances sont introduites selon la réalité de chaque pays. Le Togo pourrait expérimenter sa découverte sans perdre de vue les grands repères du modèle de référence choisi ‘’tout génie étant imitateur’’.

Du reste, la gestion interactive des finances publiques se voulant plus forte et plus unie en Afrique, des efforts soutenus devraient se poursuivre pour réussir ce pari qu'est la transparence et surtout le partage des informations.

La modernisation de la gestion des finances publiques de nos Etats ne pourrait être efficiente qu'en s'appuyant sur des applications plus viables et plus enrichissantes de par leurs variétés.

L'ordinateur occupe donc une place importante dans la production de l'information financière et comptable de l'Etat. Toutes les tâches relatives à celle-ci nécessiteraient une amélioration permanente. L'administration ayant à sa charge l'organisation des services comptables, veut toujours rendre plus efficace le système de gestion de cette activité.

Les difficultés d'ordre financier et matériel influencent aussi négativement la mise en œuvre du système informatique. La Direction Générale du Trésor et de la Comptabilité Publique (DGTCP) s'étant vue assigner au titre de ses attributions, la

Phase comptable de l'exécution budgétaire, il s'agira alors pour cette direction d'assurer une bonne qualité de l'information financière et comptable de l'Etat à travers l'outil informatique.

A l'instar de tous les pays du monde, l'Etat Togolais doit pour son fonctionnement faire face à des charges de plusieurs natures à partir de ses ressources. D'où la nécessité de moderniser la gestion des finances publiques pour mieux répartir le peu de ressources disponibles et renforcer le contrôle dans l'exécution des dépenses budgétaires.

Les solutions préconisées pour résoudre les différents problèmes que soulève l'exploitation du SIGFiP Comptabilité reposent essentiellement sur le manque de ressources techniques, humaines, financières et sur la détermination des autorités à changer positivement le visage de la gestion interactive des finances publiques.

Toutefois, l'introduction d'un tel système informatique devrait nécessairement aboutir à une gestion transparente et saine des finances publiques. Les défis de notre temps nous obligent d'adopter des comportements non plus isolés mais intégré à l'instar de la mondialisation.

Etant donné que l'hypothèse formulée dans notre introduction est justifiée, nos propositions de solutions pourraient être prises en compte par les autorités pour que l'exploitation du progiciel connaisse une amélioration. Il faudrait donc que les moyens financiers soient suffisamment alloués à la DGTCP à cet effet, de même que ceux humains et matériels.

Le choix du Système Intégré de Gestion des Finances Publiques avec ses différentes fonctionnalités a permis l'amélioration de la gestion informatique de l'activité et répond aux attentes de la DGTCP. Néanmoins il est question d'œuvrer à faire évoluer l'exploitation dudit progiciel et de le conduire jusqu'à terme pour bénéficier pleinement de ses nombreux avantages.

Le nouveau système informatique devra permettre à la DGTCP de faire un bond significatif vers la performance tant recherchée à travers l'amélioration de

l'information financière et comptable de l'Etat produite au niveau des services centraux et des structures en déconcentré.

Notre travail a seulement pris en compte l'aspect informatique de la comptabilité de l'Etat. Il serait souhaitable que des études futures soient menées sur d'autres problèmes relatifs à l'organisation et à la tenue de la comptabilité de l'Etat en vue de rendre performant le système comptable togolais et de dynamiser à nouveau de ce fait l'action publique. En plus, ce travail m'a été profitable en termes d'acquisition d'une bonne expérience professionnelle, à travers laquelle j'ai eu l'occasion d'appliquer mes connaissances scientifiques et de confronter la notion théorique à la pratique.

En perspectives, nous comptons étudier et mettre en place un modèle de blockchain adapté à toute la chaine de la dépense publique du système d'information comptable et financier de la DGTCP. Nous pouvons dire que l'objectif global n'est pas atteint par un seul projet, mais par une succession de projets afin d'établir une évaluation plausible selon une méthode et norme standard. Nous nous posons la question de savoir quel modèle faut-il mettre en place pour corriger les difficultés de nos jours.

REFERENCES

[1] Décret n°2008-092/PR portant régime juridique applicable aux comptables publics du 29 juillet 2008.

[2] Décret n°2001-155/PR portant organisation et attributions de la DGTCP du 20 août 2001.

[3] Recueil de textes relatifs à la gestion des Finances Publiques.

[3] DGTCP du Bénin, (1999) : << instruction c1 relative à la réforme de la comptabilité de l'Etat (phase 1) >>.

[4] Décret n°2008-097/PR portant définition des structures déconcentrées de la DGTCP du 29 juillet 2008.

[5] MEDE, Nicaise, (2007) : << L'établissement d'une comptabilité patrimoniale de l'Etat au Bénin : Avancées et contraintes >>, Revue Française de Finances Publiques n°98 Pages 109-118.

[6] Projet d'Informatisation de la comptabilité des EPN et des collectivités locales. Informatisation des Postes Comptables rattachés [16-08-2012] de l'INTERVIEW DE M. WAHOUM JEAN PIERRE NKONGSAMBA (trésorier payeur général de la Côte d'Ivoire).

[7] L'histoire des Services du Trésor Public au Gabon (Fait à Libreville, le 25 avril 2002) par Louis ALEKA- RYBERT sur les points suivants : - L'organisation des Services du Trésor sous la colonisation - L'enseignement du décret du 30/12/1912 sur le régime financier des colonies (1912-1945).

[8] Arrêté n°249/MEF/SP-PRPF du 22 octobre 2009 portant création, attributions et organisation d'une cellule d'administration du Système Intégré de Gestion des Finances Publiques au sein du Ministère de l'Economie et des Finances en attendant la création d'une direction du SIGFiP.

[9] http:// WWW.tresor-togo.org.

[10] http:// WWW.google.com.

[11] http:// www.memoireonline.com.

[12] http://easi.wallonie.beLexique.

[13] http:// WWW.togoregforme.com.

[14] http://vosdroits.service-public.fr/professionnels-entreprises/F24505.xhtml.

[15] http:// WWW.service.public.fr.

[16] http:// www.fondafip.org.

[17] AVAHOUNDJE Fiacre Jésugnon Judicaël, (2008) : <<Contribution à l'amélioration de la tenue de la comptabilité de l'Etat au Bénin>>, Mémoire de fin de Cycle III à l'Ecole Nationale d'Administration et de Magistrature (ENAM) au Bénin.

[18] SESSINOU Amour Fleurus, (2008) : << Contribution à une gestion performante de la trésorerie de l'Etat >>, Mémoire de fin de Cycle II à l'Ecole Nationale d'Administration et de Magistrature (ENAM) au Bénin.

[19] Cours (Ecole Doctorale des Sciences de l'Ingénieur (ED-SDI) ABOMEY-CALAVI) Internet et Sécurité : **ANSSI_PSSIE_BENIN.**

[20] Http:// CERT.tg : centre national de réponse aux incidents de cyber sécurité au Togo en collaboration avec la société CDA (Cyber Défense Africa)**.**

[21] Hervé Boulanger « Les institutions supérieures de contrôle à l'heure de la maitrise des dépenses publiques », Editions choiseau « Géoéconomie », 2013/4 N° 67 Pages 207-221.

[22] Jean –Michel HUET, DIANNE DE Pompignan et Julien BATT « Les pionniers de la nouvelle gestion publique », l'expansion Management Review, 2013/2, Pages 113-121.

[23] Laurent PAUL, Jeanne PAVOT « La maitrise de la croissance des dépenses publiques : un facteur clé pour des finances publiques saines », bulletin de la Banque de France, N° 154, octobre 2006

[24] Michel BOUVIER « La maitrise de la dépense publique au cœur d'un projet de Société ? », RFFP N° 125-Février 2014

[25] Régis LANNEAU, « QU'entend-on par la maitrise de la dépense publique », RGFP N° 11/2013, pages 16-20.

[26] Robert Hertzog « Les ressources publiques sous tension : victimes ou causes de la crise des finances publiques » RFAP, 2012/4 N° 144, P 915 à 928.

[27] Banque Mondiale, -« Revue de la dépense publique et de la gestion budgétaire-Union des Comores », 2015 -« Evaluation de la gestion des finances publiques dans l'Union des Comores pour la période 2013-2015 selon la méthodologie PEFA », Mai 2016.

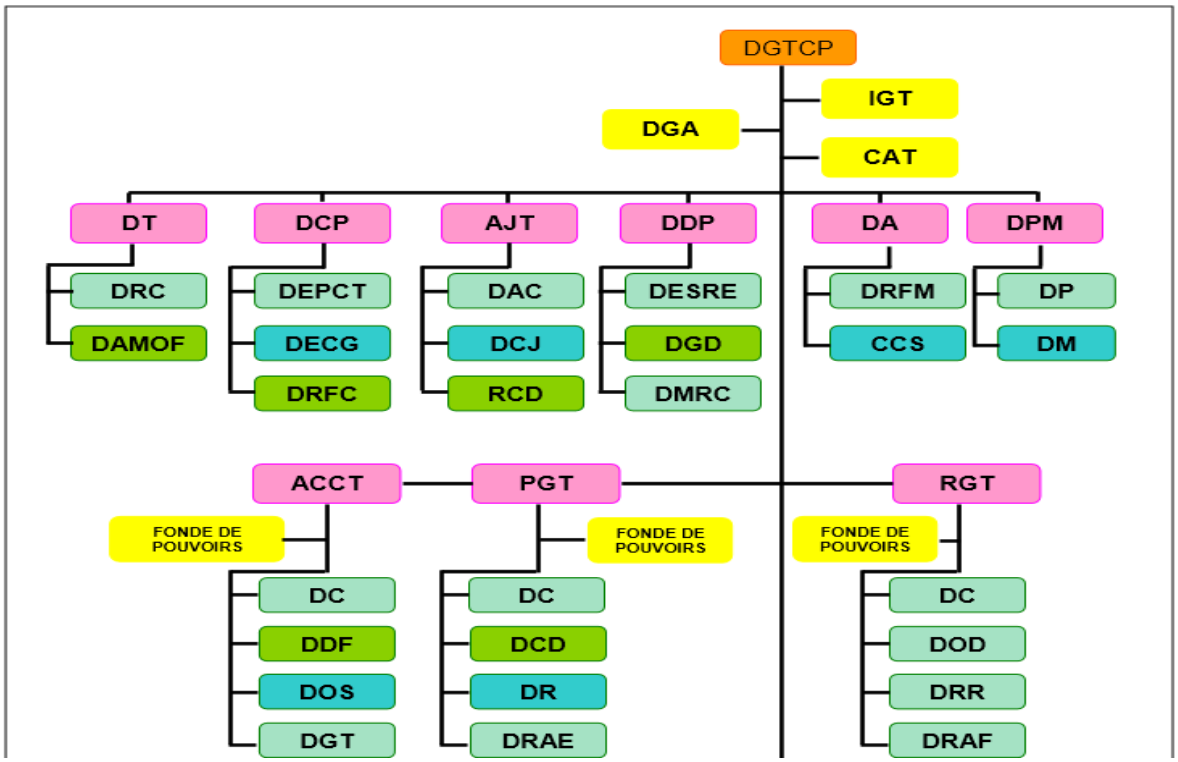
[28] Fond Monétaire International -« les dépenses publiques improductives : Analyse pragmatique de l'action des pouvoirs publics », Département des Finances publiques, Washington, 1996 -« Cadrage macro-budgétaire à moyen terme 2015-2017 », Département des finances publiques, Afritac-sud, 8-22 Mai 2014 -TADAT « Outil d'évaluation de l'administration fiscale : Union des Comores, rapport d'évaluation de la performance », Janvier 2016 -Consultation du FMI au titre de l'article IV, N° 16/393, Décembre 2016 -« Consolider les finances publiques pour accompagner la stratégie de développement de l'Union des Comores : conditions de réussite et actions prioritaires », Afritac-sud, janvier 2017 -Perspectives économiques régionales « Afrique subsaharienne : ajustement budgétaire et diversification économique », Etudes économiques et Financières, octobre 2017.

ANNEXES

1- Organigramme
2- Questionnaire
3- Résultat du questionnaire
4- Schéma fonctionnel du SIGFiP
5- Images bureaux
6- Fonctionnement de l'architecture SNMP

<u>Annexe 1</u> : Organigramme de la DGTCP

ORGANIGRAMME GENERAL DE LA DGTCP



ACCT : **A**gence **C**omptable **C**entrale du **T**résor

AJT : **A**gence **J**udiciaire du **T**résor

DGTCP : **D**irection **G**énérale du **T**résor et de la **C**omptabilité **P**ublique

CAT : **C**ellule d'**A**ppui **T**echnique

IGT : **I**nspection **G**énérale du **T**résor

DT : **D**irection du **T**résor

DRC : **D**ivision **R**églementation et **C**ontrôle

DAMOF : **D**ivision des **A**ffaires **M**onétaires et **F**inancières

DCP : **D**irection de la **C**omptabilité **P**ublique

DEPCT : **D**ivision **E**tablissements **P**ublics et **C**ollectivités **T**erritoriales

DECG : **D**ivision **E**tudes et **C**omptes de **G**estion

DRFC : **D**ivision **R**églementation **F**inancière et **C**omptable

DAC : **D**ivision des **A**ffaires **C**ontentieuses

DCJ : **D**ivision **C**onseil **J**uridique

RCD : **R**ecette des **C**réances **D**iverses

DDP : **D**irection de la **D**ette **P**ublique

DESRE : **D**ivision **E**tudes, **S**ynthèse et **R**elations **E**xtérieures

DGD : **D**ivision **G**estion de la **D**ette

DMRC : **D**ivision **M**obilisation, **R**emboursement et **C**ontrôle

DNA : **D**irection **N**ationale des **A**ssurances

DRFM : **D**ivision **R**églementation et **F**ormation du **M**arché

CCS : **C**ellule de **C**ontrôle et des **S**tatistiques

DPM : **D**irection du **P**ersonnel et du **M**atériel

DP : **D**ivision du **P**ersonnel

DM : **D**ivision du **M**atériel

DC : **D**ivision **C**omptabilité

DDF : **D**ivision des **D**épôts de **F**onds

DOS : **D**ivision des **O**pérations **S**pécifiques

DGT : **D**ivision **G**estion de la **T**résorerie

PGT : **P**aierie **G**énérale du **T**résor

DCD : **D**ivision **C**ontrôle de **D**épense

DR : **D**ivision des **R**èglements

DRAE : **D**ivision des **R**ègles d'**A**vance et des **E**xonérations

RGT : **R**ecette **G**énérale du **T**résor

DOD : **D**ivision des **O**pérations **D**iverses

DRR : **D**ivision des **R**égies de **R**ecettes

DRAF : **D**ivision des **R**ecettes des **A**dministrations **F**inancières

TR : **T**résorerie **R**égionale

DR : **D**ivision **R**ecouvrement

DD : **D**ivision **D**épense

DCT : **D**ivision **C**ollectivités **T**erritoriales

DAF : **D**ivision de l'**A**ction **F**inancière

TPMDC : **T**résorerie **P**rincipale des **M**issions **D**iplomatiques et **C**onsulaires

TP : **T**résorerie **P**rincipale

T : **T**résorerie

P : **P**aierie

Annexe 2 : Questionnaire

Questionnaire : Fiche de collecte des données

Toute organisation qui se veut transparent dans sa gestion, doit mettre en place des systèmes de sécurité et de viabilités forts et efficaces. En ce qui concerne le Ministère des Finances au Togo, la mise en place du système intégré de gestion des finances publiques (SIGFiP) se justifie par la nécessité de mener à bien les réformes en cours dans tous les secteurs de l'administration.

Plus précisément la partie comptabilité assurée par le module SIGTA (SIGFiP comptabilité) reste préoccupante pour l'Etat togolais. Cependant, le problème qui se pose est de savoir si SIGFiP suffit à lui seul, à garantir la sécurité des deniers publics et l'exécution efficace et efficiente des budgets publics.

Pour tenter de répondre à cette question, nous avons choisi de traiter le thème suivant : « **Evaluation de l'informatisation du réseau des comptables directs du Trésor au Togo** »

En votre qualité d'Agent Comptable Central du Trésor (ACCT), votre avis sur le sujet nous parait indispensable. Nous vous remercions pour votre disponibilité et vous sommes reconnaissant pour l'objectivité de votre opinion sur la question. Veuillez cocher les affirmations correspondantes à vos réponses parmi les propositions suivantes :

1. Existe-t-il une instruction comptable relative à l'extension de SIGFiP Comptabilité en structure déconcentrée?
   a. Oui □
   b. Non □

   Si oui est-elle opérationnelle? ☐
   Donner vos impressions :

……...
……....
……

2. Existe-t-il une instruction comptable relative à l'exploitation de l'application SIGFiP au niveau des postes comptables connectés au réseau?
   a. Oui □
   b. Non □

   Si oui est-elle opérationnelle? ☐
   Donner vos impressions :

……
……

……

3. Existe-t-il un schéma technique qui précise le périmètre du réseau SIGFiP ?

a. Oui □
b. Non □

Si oui est-elle opérationnelle? ☐

Donner vos impressions :

……...
……....
……

4. Nous souhaitons, avec votre permission, avoir copie du schéma réseau existant

……
……
……

5. Excuser nous, de nous décrire, l'ensemble des équipements et matériels réseau :

……
……
……

6. Votre appréciation sur le réseau existant

……
……
……

7. Pouvons nous avoir des informations relatives aux services de sécurité :

a. les locaux

……
……
……

b. réseau étendu

……
……
……

c. à la sécurité

……
……
……

d. contrôle d'accès applicatif

……
……
……

e. contrôle intégrité des données

……
……

……

f. disponibilité des données

……
……
……

g. sécurité logique des équipements

……
……
……

h. les plans de secours

……
……
……

i. les plans de sauvegarde

……
……
……

j. la maintenance réseau

……
……
……

8. Existe t-il un système de détection d'intrusion contre tout accès non autorisé ?

…….....
.....……
……...……

9. Existe t-il un mécanisme de lutte contre les attaques sur les mots de passe ?

…….....
...…….....
.....……

10. Existe-t-il une politique de sécurité sur l'infrastructure ?

…….....……
…….....……...
……

11. Tableau : Liste de contrôle d'audit de sécurité

Le référentiel MEHARI (Méthode Harmonisée d'Analyse des Risques) permet d'avoir une vue d'ensemblesur la gestion de la sécurité de l'information telle que spécifiée dans la norme ISO/IEC 27001 : 2013.

#	Liste de contrôle d'audit de sécurité	OUI	NON
	Disposition physique des bâtiments de l'organisation et des périmètres environnants		
1	La topographie de la propriété assure-t-elle la sécurité ou réduit-elle les moyens d'attaque ou d'accès ?		
2	L'aménagement paysager offre-t-il des emplacements pour se cacher ou des moyens d'accès aux toits ou à d'autres points d'accès ?		
3	Combien de points d'entrée y a-t-il dans le bâtiment? Ces entrées sont-elles surveillées ?		
4	Toutes les personnes entrant et sortant du bâtiment passent-elles par un point de contrôle de sécurité ?		
	Éclairage		
	Éclairage		
5	Y a-t-il un éclairage suffisant pour permettre aux gardes, aux employés ou à d'autres personnes de voir les lieux de dissimulation ou d'accès possibles ?		
6	Les points d'accès sont-ils masqués par une faible luminosité ?		
	Alarmes – y compris incendie, intrusion, sabotage, mouvement		
7	Les portes, fenêtres, portails, tourniquets sont-ils surveillés pour les sorties et les entrées ?		
8	Les moyens d'entrée peuvent-ils être audités pour identifier qui a accédé à ces zones ?		
9	Les locaux sont-ils surveillés en cas d'incendie ou de fumée ? Le système alerte-t-il le service d'incendie local ?		
10	En cas d'effraction, à qui le système d'alarme avertit-il ? Est-il surveillé par un tiers ou du personnel ?		
	Barrières physiques - y compris les clôtures, les bornes, les bandes de pneus, les portes		
11	Les clôtures sont-elles suffisamment hautes pour réduire l'accès non autorisé à la propriété ? La clôture est-elle vérifiée régulièrement par le personnel pour des trous, des dommages ou des points d'accès.		
12	Des bornes sont-elles en place pour éviter d'endommager les bâtiments ou les points d'accès par les véhicules ?		
13	Des bandes de pneus sont-elles installées et peuvent-elles être utilisées pour empêcher l'entrée non autorisée dans les zones sensibles autour de la propriété ? Parkings, quais de chargement, aires de ramassage.		
14	Les barrières sont-elles sécurisées et fonctionnent-elles correctement ?		
15	L'entrée dans les locaux est-elle protégée par des barrières ou la circulation des véhicules est-elle autorisée à entrer et sortir librement de la propriété ?		

	Points d'accès - y compris les portes, portails, tourniquets, fenêtres, quais, ascenseurs et cages d'escalier		
16	Les portes et portails sont-ils en bon état de fonctionnement ? Fonctionnent-ils correctement et se ferment-ils d'eux-mêmes ?		
17	Les tourniquets fonctionnent-ils correctement et des informations d'identification sont-elles nécessaires pour passer?		
18	Les fenêtres sont-elles verrouillées si elles peuvent être ouvertes ?		
19	Si de grandes vitres sont installées dans le bâtiment, sont-elles stratifiées avec un film de sécurité pour empêcher l'effraction ?		
20	Les quais et les portes de quai fonctionnent-ils correctement et sont-ils verrouillés lorsqu'ils ne sont pas utilisés ?		
21	Les ascenseurs et les cages d'escalier sont-ils vérifiés quotidiennement ou toutes les heures par le personnel de sécurité ?		
	Gardes		
22	La propriété de l'organisation utilise-t-elle un personnel de garde ?		
23	Les gardes vérifient-ils que les personnes venant sur la propriété sont autorisées à y accéder ? Comment vérifient-ils ? ID, vérifier auprès des membres du personnel, inspecter les véhicules, enregistrer les noms et les informations de licence ?		
24	Les gardiens font-ils des rondes dans la propriété pour vérifier les lieux d'accès ? Portes, fenêtres, ascenseurs, cages d'escalier, portes de quai ou de baie, zones sécurisées ?		
25	Les gardes remplissent-ils des feuilles de contrôle pendant leur service pour vérifier qu'ils ont vérifié comme indiqué ?		
26	Les gardes varient-ils leurs modèles de patrouille pour réduire le risque que leurs routines soient exploitées ?		
	Vidéosurveillance		
27	Le périmètre du bâtiment et le périmètre de la propriété sont-ils adéquatement couverts par des caméras ?		
28	Les caméras peuvent-elles passer automatiquement du jour à la nuit/faible luminosité ?		
29	Les entrées et sorties du bâtiment sont-elles surveillées par des caméras ?		
30	Les cages d'escalier et autres points d'accès sont-ils surveillés par des caméras ?		
31	Les caméras sont-elles surveillées 24 heures sur 24 ou ne sont-elles examinées qu'après qu'un incident s'est produit ?		

	Méthodes d'accès - y compris les serrures, les cartes de proximité/cartes magnétiques, les serrures à code ou à chiffre et d'autres méthodes d'identification.		
32	Les serrures et l'équipement de verrouillage sont-ils en bon état et fonctionnent-ils correctement ?		
33	Les anciens employés ont-ils encore des clés/cartes d'accès au bâtiment ?		
34	Les anciens employés/employés licenciés ont-ils été privés de l'accès à la propriété ?		
35	À quelle fréquence les codes sont-ils modifiés sur les serrures à code ou à chiffre ?		

	Méthodes de communication des violations découvertes lors de l'audit de sécurité aux personnes responsables de la sécurité de l'organisation. Y compris – alarmes/éclairage locaux, téléphone, SMS, e-mail, etc.		
36	Comment le personnel de sécurité est-il informé des atteintes à la sécurité et des accès non autorisés ? Gardes, alarmes locales, alarmes surveillées, appels téléphoniques ?		
37	Votre personnel de sécurité connaît-il les politiques de l'organisation pour informer la direction ou d'autres membres du personnel clé ?		

Annexe 3 : Résultats du questionnaire

Résultat n° 1 : Appréciation des enquêtés sur l'exploitation du progiciel SIGFiP

Réponses obtenues	Nombre	Fréquence Relative
Entièrement satisfait	25	30 %
Partiellement satisfait	48	**59 %**
Aucunement satisfait	02	02 %
Sans opinion	07	09 %
TOTAL	**82**	**100 %**

Source : Questionnaire

Résultat n° 2 : Connaissance du manuel utilisateur

Réponses obtenues	Nombre	Fréquence Relative
Oui	**02**	02 %
Non	**80**	**98 %**
Sans opinion	**00**	**00%**
TOTAL	**82**	**100 %**

Source : Questionnaire

Résultat n° 3 : Avis des enquêtés sur l'existence des difficultés dans la mise en œuvre de l'application SIGFiP

Réponses obtenues	Nombre	Fréquence Relative
Oui	72	**88 %**
Non	7	09 %
Sans opinion	3	04 %
TOTAL	**82**	**100 %**

Source : Questionnaire

Résultat n° 4 : Difficultés identifiées par les enquêtés dans la mise en œuvre de l'expérimentation de l'application SIGFiP en cours dans la direction

Réponses obtenues	Nombre	Fréquence Relative
La non maîtrise de l'utilisation de l'application SIGFiP	**7**	**09%**
Lenteur dans le traitement des dossiers au niveau du Trésor due au problème de connexion réseau	**72**	**88 %**
Les pannes fréquentes au cours de l'utilisation du SIGFiP	**3**	**04 %**
Sans opinion	**00**	**00%**
TOTAL	**82**	**100%**

Source : Questionnaire

Résultat n° 5 : Approche de solutions des enquêtés pour la correction des difficultés rencontrées dans la mise en œuvre de l'expérimentation du SIGFiP

Réponses obtenues	Nombre	Fréquence Relative
Mettre à la disposition des acteurs du réseau le guide utilisateur du progiciel	**48**	**59 %**
Former les acteurs sur les nouvelles procédures d'utilisation du SIGFiP	**25**	**30 %**
Sensibiliser les acteurs de la chaîne du réseau des comptables sur les réformes en cours	**02**	**02 %**
Faciliter les corrections des saisies faites dans le SIGFiP	**07**	**09 %**
Sans opinion	**00**	**00%**
	82	**100 %**

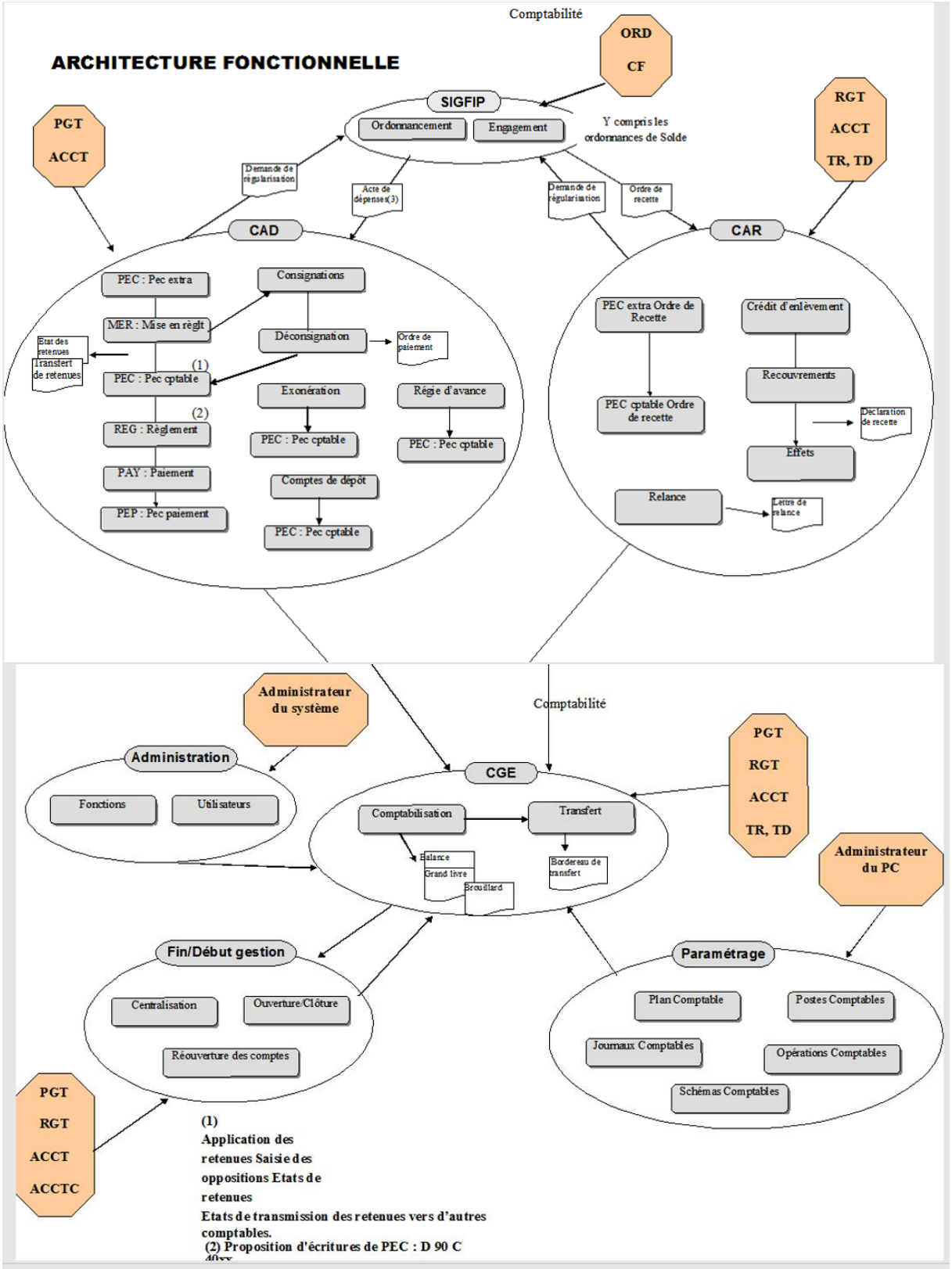
Source : Questionnaire

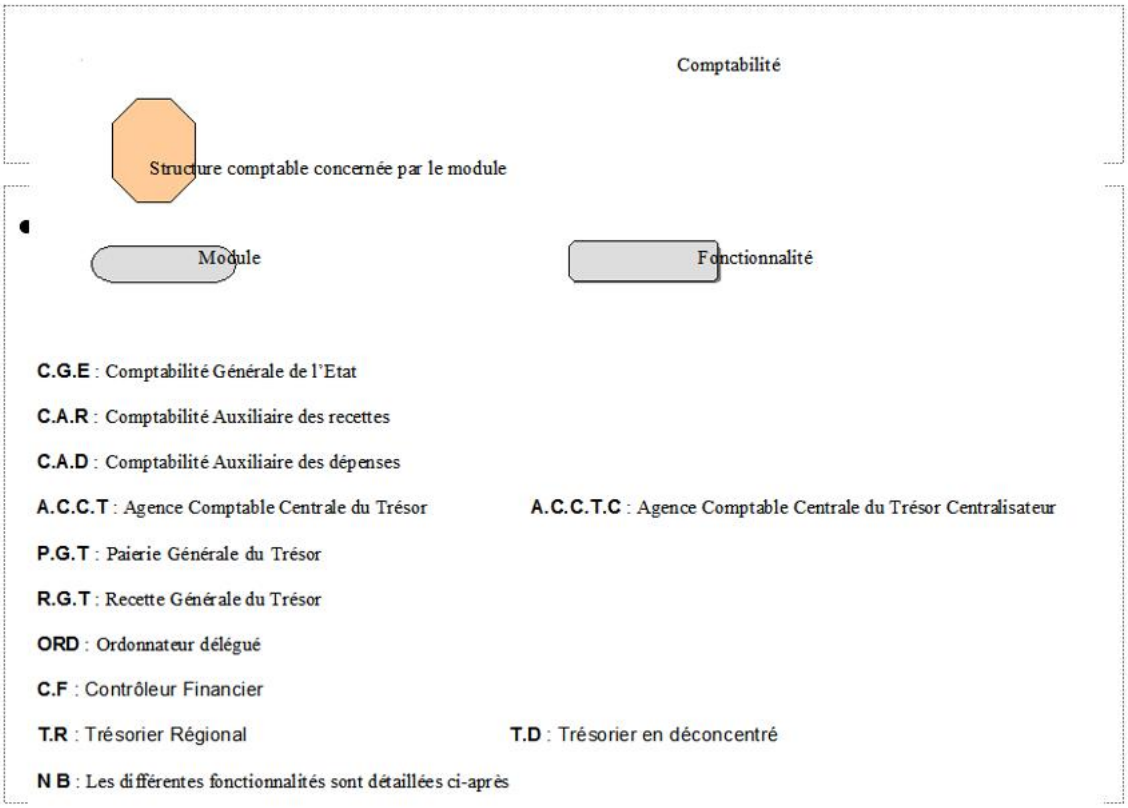
Résultat n° 6 : Liste de contrôle d'audit de sécurité du SI

Réponses obtenues	Nombre Oui	Nombre Non	TOTAL
Disposition physique des bâtiments et des périmètres environnants	**50**	**32**	**82**
Eclairage	**52**	**30**	**82**
Alarmes y compris incendie, intrusion, sabotage, mouvement	**00**	**82**	**82**
Barrières physiques y compris des clôtures, les bornes, les bandes de pneus, les portes	**10**	**72**	**82**
Points d'accès y compris les portes, les portails, tourniquets, fenêtres, quais, ascenseurs et cages d'escalier	**5**	**77**	**82**
Gardes	**50**	**32**	**82**
Vidéosurveillance	**45**	**37**	**82**
Méthodes d'accès y compris les serrures les cartes de proximité/cartes magnétiques, les serrures à code ou à chiffre et d'autres méthodes d'identification	**50**	**32**	**82**
Méthodes de communication des violations découvertes lors de l'audit de sécurité aux personnes responsables de la sécurité de l'organisation. Y compris alarmes/éclairage, téléphone, SMS, e-mail etc.	**45**	**37**	**82**

Source : Questionnaire

Annexe 4 : Schéma fonctionnel du SIGFiP





Source : DGTCP

Annexe 5 : Fonctionnement de l'architecture SNMP

L'architecture SNMP globale comprend :

- les agents SNMP : ce sont les équipements (réseau ou serveur) qu'il faut superviser ;
- le superviseur SNMP : c'est une machine centrale à partir de laquelle un opérateur peut superviser en temps réel toute son infrastructure, diagnostiquer les problèmes et finalement faire intervenir un technicien pour les résoudre ;
- le protocole SNMP : c'est le protocole utilisé par les agents SNMP et leur superviseur pour communiquer entre eux ;
- la MIB : ce sont les informations dynamiques instanciées par les différents agents SNMP et remontées en temps réel au superviseur ;
- les outils SNMP : ce sont les différents utilitaires utilisés par le superviseur pour l'aider à diagnostiquer un problème. Ces différents outils sont aussi utilisés lors de la configuration du superviseur pour prendre en compte les spécificités de l'infrastructure.

Le protocole SNMP est un protocole réseau qui comporte différentes requêtes. Ces requêtes sont regroupées en 3 familles :
- les messages du superviseur SNMP vers l'agent SNMP ;
- les messages de l'agent SNMP vers le superviseur SNMP ;
- les messages entre agents SNMP.

Le SNMP définit deux éléments. Il s'agit du protocole et des informations dynamiques. le protocole définit la façon dont est transportée l'information et les informations dynamiques sont fournies par les différents agents SNMP. Ces informations sont spécifiées dans ce que l'on appelle la MIB (Management Information Base).

La MIB est un ensemble structuré d'informations organisé sous la forme d'un arbre hiérarchisé de la même manière que l'arborescence des domaines Internet. Chaque information dans cette hiérarchie est identifiée par son OID (Object Identifier).

Un agent SNMP est un logiciel implanté sur un équipement à superviser. Il s'agit souvent d'un équipement réseau (switch, hub, routeur...) mais on trouve aussi des agents sur des serveurs.

Le rôle d'un agent SNMP est :
- d'instancier les différentes variables de la MIB spécifiques à cet équipement ;
- de mettre à jour les valeurs dynamiques de ces différentes variables ;
- de recevoir les requêtes SNMP envoyées par le superviseur SNMP et d'y répondre ;
- d'envoyer les messages SNMP "Trap" ou "Inform" au superviseur SNMP pour le prévenir d'un événement exceptionnel sur l'équipement ;
- de gérer la sécurité des accès aux variables de la MIB conformément au modèle de sécurité mis en place.

Le rôle d'un superviseur SNMP est de :

- présenter une vue de l'infrastructure supervisée avec l'état des différents équipements qui la composent. Dans les grosses infrastructures, il est courant que le superviseur SNMP affiche son écran sur un mur d'images dans la salle de supervision ;

- communiquer avec les différents agents SNMP pour récupérer régulièrement les différents états des équipements ;
- réagir en conséquence lorsqu'une variable de la MIB sort des limites définies par l'opérateur (engorgement du réseau, taux de remplissage du disque dur...). L'opérateur ou l'administrateur de la supervision peut définir les actions à réaliser en cas de réaction automatique (envoi d'un mail par exemple). Le comportement le plus courant d'un superviseur SNMP sera de modifier la couleur de l'équipement en cause pour alerter visuellement l'opérateur ;
- recevoir en temps réel les messages SNMP en provenance des équipements et modifier l'affichage général en conséquence pour refléter le nouvel état ;
- prendre en compte l'évolution de l'infrastructure en permettant l'ajout de nouveaux équipements dans le périmètre de supervision.

<u>Annexe 6</u> : Images aspects des bureaux en déconcentré

Trésorerie Adeta

Préfecture d'Assoli

Trésorerie Sinkassé

Trésorerie Kevé

Trésorerie Mango

Trésorerie Notse

TABLE DES MATIERES