Centre Africain d'Etudes Supérieures en Gestion

CESAG BF – CCA
Banque, Finance, Comptabilité, Contrôle & Audit

Master Professionnel en Audit et Contrôle de Gestion (MPACG)

Promotion 8
(2013 - 2015)

CESAG - BIBLIOTHEQUE

Mémoire de fin d'étude

THEME:

AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE DE LA LOTERIE NATIONALE SENEGALAISE (LONASE).

Présenté par :

AMEDJOKPO Kodjo Adjéwoda

Dirigé par :

BLE Koffi Charles
Auditeur à la BCEAO et
Enseignant associé au CESAG

AVRIL 2015

DEDICACE

Je dédie ce travail :

- à mes frères et sœurs, spécialement à mon frère ABOTCHI Koffi Sokada ;
- à la mémoire de mes chers parents défunts.

CESAG - BIBLIOTHEQUE

REMERCIEMENTS

Je rends grâce à Dieu le tout-puissant, car il a fait des merveilles, éternel est son amour. Par lui je puis tout, parce qu'il me fortifie. Saint est son nom.

Mes remerciements vont également à :

- M. BLE Charles, mon directeur de mémoire pour ses conseils, le temps consacré pour l'encadrement de cette étude et de m'avoir donné le goût d'évoluer dans ce domaine ;
- M. BAIDARI, Directeur Général du CESAG et à tout le personnel administratif ;
- M. YAZI Moussa, Directeur du Département Banque, Finance, Comptabilité, Contrôle et Audit du CESAG, pour ses conseils et à tout le corps professoral pour la qualité de leurs enseignements et conseils ;
- M. GUEYE Mamadou, pour son aide dans la recherche de stage et son soutien sans faille ;
- M. GUEYE Mouhamadou, Directeur des Ressources Humaines de la LONASE, pour m'avoir accordé le stage ;
- M. BADIANE, Directeur de l'Audit Interne de la LONASE, pour sa disponibilité ;
- Mme GBAGUIDI Anoko, Directrice Financière et Comptable de la LONASE, pour m'avoir ouvert ces portes ;
- M. SYLLA Fadel, Chef du Service Assistance et Formation de la LONASE, pour ses apports multiformes ;
- tout le personnel de la LONASE pour l'accueil chaleureux et le soutien qu'il m'a apporté durant notre stage ;
- la famille HIEN, pour son soutien ;
- tous mes camarades de la 8ème promotion du Master Professionnel Audit et Contrôle de Gestion ;
- Panafrican Risks Managers (PRM) pour les belles valeurs que nous partageons ;
- tous ceux et celles qui ont participé d'une manière ou d'une autre à la réalisation de ce travail et qui ont voulu que je passe sous silence leur nom.

CESAG - BIBLIOTHEQUE

SIGLES ET ABREVIATIONS

AFAI	Association Française de l'Audit et du Conseil Informatique
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CLUSIF	Club de la Sécurité de l'Information Français
COBIT	Control Objectives for Business and Related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DSI	Direction du Système d'Information
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
EDI	Echange de Données Informatisées
IFACI	Institut Français de l'Audit et du Contrôle Internes
IIA	Institute of Internal Auditors
ISACA	Information Systems Audit and Control Association
ISO	Organisation Internationale de Normalisation
ITAF	Information Technology Assurance Framework
ITGI	Information Technology and Governance Institute
ITSEC	Information Technology Security Evaluation Criteria
LONASE	Loterie Nationale Sénégalaise
MEHARI	Méthode Harmonisée d'Analyse de Risques
OHADA	Organisation pour l'Harmonisation en Afrique des Droits des Affaires
PSSI	Politique de Sécurité des Systèmes d'Information
RSSI	Responsable de la Sécurité des Systèmes d'Information
RTO/RPO	Recovery Time Objective / Recovery Point Objective
SIC	Système d'Information Comptable
SMSI	Système de Management de la Sécurité de l'Information
SoA	Statement of Applicability
SSI	Sécurité des Systèmes d'Information

CESAG - BIBLIOTHEQUE

LISTES DES TABLEAUX ET FIGURES

LISTE DES TABLEAUX

LISTE DES FIGURES

CESAG BIBLIOTHEQUE

LISTE DES ANNEXES

CESAG - BIBLIOTHEQUE

TABLE DES MATIERES

CESAG - BIBLIOTHEQUE

CESAG - BIBLIOTHEQUE

CESAG - BIBLIOTHEQUE

CESAG - BIBLIOTHEQUE

INTRODUCTION GENERALE

CESAG - BIBLIOTHEQUE

L'information est l'une des ressources essentielles pour toute organisation. Elle représente par conséquent un patrimoine à forte valeur. Sa protection doit donc constituer un élément fondamental de la stratégie globale de toute organisation publique ou privée.

En effet, avec le développement fulgurant des technologies de l'information et de la communication de ces dernières années, nombreux sont des organismes qui investissent de fortes sommes afin de disposer d'un système d'information adapté à leur activité. Ce qui a créé une forte dépendance de ceux-ci par rapport aux SI pour leur bon fonctionnement, alors que ces derniers ne cessent d'engendrer de nouvelles vulnérabilités.

Par ailleurs, les multiples menaces qui pèsent sur ces systèmes ont conduit les organisations à réfléchir sur la manière de se protéger. Ainsi, la notion de sécurité des systèmes d'information est devenue un enjeu crucial ; sans doute l'une des actuelles problématiques dont les organisations doivent faire face. De même, il s'est développé au début de ce XXI^{ème} siècle, le concept de « gouvernance des systèmes d'information », qui fédère un ensemble de réflexions et de bonnes pratiques sur plusieurs thèmes concernant le pilotage des SI y compris leur sécurité. Cette dernière s'intéresse à l'intégrité, à la confidentialité et à la disponibilité des actifs informationnels, en particulier les plus critiques et sensibles.

Les types d'incidents rencontrés par les organisations repartent fortement à la hausse par rapport à l'étude 2012. Avec le trio de tête : les pertes de services essentiels qui passent de 26 % à 39 % ; les vols qui passent de 19 % à 37 % ; les pannes d'origine interne passent de 25 % à 35 % (CLUSIF, 2014 : 6).

Les organisations qui offrent des produits liés aux jeux de hasard ne sont pas à l'abri de ces menaces. Le déni de service, dont a été victime la loterie nationale danoise pour la période d'août 2009, et qui a rendu indisponible son système d'information, est une illustration des dangers encourus par ce secteur d'activité.

Face à ces menaces, certains pays sont allés jusqu'à se doter d'entités dont la mission est d'assurer la sécurité de l'information notamment, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) en France et de la National Security Agency (NSA) aux Etats-Unis d'Amérique.

Les différentes réglementations tendant à l'organisation du contrôle interne dans les organisations ne sont pas de même restées silencieuses sur le sujet. La loi Sarbanes-Oxley, concernant la Sécurité du Système d'Information (SSI), impose aux entreprises des procédures

CESAG - BIBLIOTHEQUE

de contrôle interne, de conservation des informations, et de garantie de leur exactitude. Elle fait également le point sur la nécessité de la continuité des opérations ; la sauvegarde et l'archivage des données ; l'externalisation et son contrôle.

Dans l'espace OHADA (Organisation pour l'Harmonisation en Afrique des Droits des Affaires), l'Acte Uniforme portant Organisation et Harmonisation des Comptabilités des entreprises exige selon les termes de l'article 3 de son chapitre I, des organisations publiques et privées de tenir des comptes réguliers, sincères et fidèles de leur situation.

Ainsi, le Système d'Information Comptable (SIC), est devenu le garant du traitement et de l'obtention d'informations sincères, fiables et pertinentes pour toutes les parties prenantes. Du fait du volume important des opérations à traiter, le SIC à gagner une place prépondérante dans les organisations. Il est le principal circuit de diffusion des informations au sein d'une organisation. A côté de ce rôle important, il va falloir prendre en compte ses éventuelles vulnérabilités.

Au Sénégal, la Loterie Nationale Sénégalaise (LONASE), détient le monopole d'organisation dans l'intérêt public et suivant des méthodes commerciales, des loteries publiques, paris, concours et jeux de hasard, conformément aux dispositions de la loi n° 87-43 du 28 décembre 1987. Elle utilise un SI automatisé pour ses opérations comptables et financières.

La sécurité du SIC représente donc pour la LONASE une priorité stratégique et incontournable. Sa démarche vers la certification à la norme ISO 27001 renforce cette idée.

Malgré son importance, le SIC de la LONASE n'a jamais fait l'objet d'un audit interne ou externe de sécurité afin, de documenter de son niveau de vulnérabilité. Cette situation résulte de plusieurs facteurs dont :

- la méconnaissance des risques liés aux actifs informationnels ;
- la perception que la sécurité des SI est un travail uniquement dévolu à la Direction des Systèmes d'Information ;
- la perception limitée au coût élevé de la sécurité des SI ;
- l'appréhension difficile de la valeur du système d'information comptable ;
- l'absence de politique formalisée de sécurité des systèmes d'information ;
- la difficulté d'évaluation du retour sur les investissements en sécurité.

CESAG BIBLIOTHEQUE

Les conséquences du problème sont entre autres :

- l'accès non autorisé aux actifs informationnels, pouvant entraîner l'altération ou la destruction de ceux-ci ;
- l'enregistrement de transactions frauduleuses ou d'écritures comptables erronées ;
- la violation du principe de séparation des tâches ;
- le coût énorme de gestion des sinistres ;
- la non crédibilité des informations comptables et financières ;
- la divulgation des informations comptables et financières confidentielles ;

Pour minimiser l'impact des risques et ou réduire leur fréquence de réalisation, les solutions suivantes peuvent être envisagées :

- former et sensibiliser les utilisateurs sur la sécurité du SIC ;
- élaborer une politique de sécurité des systèmes d'information et l'intégrer dans les plans stratégiques ;
- élaborer et communiquer la cartographie des risques de sécurité des SI ;
- définir une politique de réaffectation des coûts de sécurité au différent centre métier ;
- définir une charte de sécurité utilisateur ;
- auditer la sécurité du système d'information comptable.

La dernière solution nous semble être la meilleure dans la mesure où elle permettra à la LONASE de connaître son niveau de vulnérabilité aux risques liés à son SIC et est un jalon dans sa démarche vers la certification à la norme ISO 27001.

Au regard de la solution retenue, la question que nous posons principalement dans le cadre de cette étude est de savoir quel est le niveau de vulnérabilité du SIC de la LONASE ?

Il convient de considérer les questions spécifiques suivantes :

- qu'est-ce qu'un système d'information comptable?
- quels sont les risques liés à la sécurité des systèmes d'information ?
- comment se déroule une mission d'audit de sécurité des SI ?
- comment la LONASE assure-t-elle la sécurité de son SIC ?
- quels sont les axes d'amélioration à proposer pour aider la LONASE à améliorer ses dispositifs de sécurité ?

CESAG BIBLIOTHEQUE

Mieux répondre à ces préoccupations et amener la LONASE à améliorer ces pratiques de sécurité, sont des raisons qui nous ont motivé à choisir comme thème d'étude : **Audit de la sécurité du Système d'Information Comptable de la LONASE.**

Notre étude est articulée autour d'un objectif principal qui est celui de documenter le niveau de vulnérabilité du SIC de la LONASE. Plus spécifiquement il s'agira de :

- appréhender la notion de système d'information comptable ;
- identifier les risques liés à la sécurité des systèmes d'information comptable ;
- présenter les différentes étapes d'un audit de sécurité des systèmes d'information ;
- identifier les contrôles et les dispositifs de sécurité mise en place par la LONASE ;
- vérifier si les dispositifs et procédures de sécurité du SIC sont conformes aux contraintes légales, réglementaires et aux bonnes pratiques ;
- proposer des axes d'amélioration pour renforcer le dispositif de contrôle interne du Système d'Information Comptable.

Notre étude se limitera aux aspects fonctionnels et organisationnels liés à la sécurité du SIC de la LONASE sans prendre en compte les aspects techniques.

Elle revêt un double intérêt. Le premier bénéficiaire est la LONASE car elle pourra l'aider à avoir une idée sur le niveau de sécurité de son SIC afin de décider des actions à mettre en œuvre pour son amélioration.

Nous en tirons de même un profit dans la mesure où cette étude nous permettra d'approfondir nos connaissances jusque-là théoriques en audit des systèmes d'information. C'est également une occasion d'explorer ce domaine dans lequel nous voulons bien faire carrière.

Cette étude est structurée en deux parties avec chacune trois chapitres.

La première partie traitera des notions théoriques de système d'information comptable (chapitre 1), d'audit de la sécurité des systèmes d'information (chapitre 2) ainsi que la méthodologie (chapitre 3) que nous avons retenue pour l'étude.

La deuxième partie concernera la pratique de l'étude à travers la présentation de la LONASE (chapitre 4) et de l'état actuel des pratiques de sécurité de celle-ci (chapitre 5). Pour finir, nous présenterons les résultats de l'audit (chapitre 6).

CESAG BIBLIOTHEQUE

PREMIERE PARTIE : CADRE THEORIQUE DE L'AUDIT DE LA SECURITE D'UN SYSTEME D'INFORMATION COMPTABLE

CESAG BIBLIOTHEQUE

Introduction de la première partie

La sécurité des SI est un facteur de productivité, de compétitivité et donc de croissance pour les organisations. En effet, quelle que soit sa taille, une organisation doit prendre conscience qu'elle peut être à tout moment confrontée une menace. Qu'il s'agisse par exemple, d'erreurs ou de malveillances visant à l'altération des données ou de déni de service, les conséquences des réalisations des risques liés aux SI pour les organisations, sont souvent désastreuses et peuvent remettre en cause leur pérennité.

Se pose alors la question de savoir comment s'assurer raisonnablement que son système d'information est sécurisé sachant que la sécurité à 100% demeure une utopie ?

Nous partageons l'avis de certains organismes comme l'ISACA (Information Systems Audit and Control Association) qui pensent qu'il faut passer par l'évaluation des dispositifs et politiques de sécurité de cette organisation. En effet, dans son référentiel COBIT (Control Objectives for Business and Related Technology), ISACA a réservée un domaine (surveillance et évaluation) qui décrit la nécessité et les objectifs de l'évaluation de la sécurité des SI (MOISAND, 2009 : 179-193).

Nous avons bien voulu approfondir le sujet en retournant dans cette partie, aux écrits académiques et professionnels sur la notion d'audit de la sécurité d'un système d'information.

Par conséquent, le premier chapitre de cette partie a pour objectif de nous situer sur ce qu'est un système d'information et plus particulièrement un SIC. De même, nous allons aborder la question concernant la relation entre un système d'information et un système informatique. Le deuxième chapitre traitera des notions théoriques de l'audit de la sécurité du SIC à travers les méthodes, les normes et les bonnes pratiques en la matière. Comme une étude pertinente doit être menée avec une méthodologie cohérente, nous consacrerons le troisième chapitre et le dernier de cette première partie à la description de la méthodologie d'audit des SI que nous avons retenue pour l'étude.

CESAG BIBLIOTHEQUE

CHAPITRE 1 : SYSTEME D'INFORMATION COMPTABLE

Introduction

Les dirigeants en vue de prendre des meilleures décisions conduisant à la création de la valeur, doivent disposer des informations fiables, facilement vérifiables et surtout en temps opportun. Le SIC se veut un système cohérent d'information et de communication au service des organisations. Selon REIX & al. (2011 : 80), la comptabilité constitue l'exemple le plus ancien et le plus répandu d'un système d'information formalisé et organisé. C'est un domaine où les éléments significatifs sont bien définis, les règles de traitement claires, les résultats à obtenir rigoureusement établis. Avec le recours étendu aux techniques informatiques, le SIC croît mais devient plus vulnérable.

Dans ce chapitre, il s'agira de chercher à mieux cerner la notion du système d'information comptable ; d'analyser les impératifs de sécurité pour un bon système d'information comptable. Aussi, nous aborderons la démarche de gestion des risques qu'encours le SIC et enfin nous identifierons les bonnes pratiques associées à la responsabilité de chaque acteur de l'entreprise.

CESAG - BIBLIOTHEQUE

1.1. Notion de Système d'Information

Pour mieux cerner la notion « Système d'Information Comptable », nous allons l'aborder dans cette section à travers celle de SI. En effet, le SIC est un sous ensemble d'un SI.

Selon REIX & al. (2011 : 4), le SI est « un ensemble organisé de ressources : matériel, logiciel, personnel, données, procédures… permettant d'acquérir, de traiter, de stocker des informations (sous forme de données, textes, images, sons, etc.) dans et entre des organisations. »

Nous retrouvons dans cette définition les principales caractéristiques et les fonctions d'un système d'information. Elle souligne également une organisation conséquente des ressources humaines et informatiques pour la gestion des informations.

Un SI peut être aussi défini comme un ensemble de composantes inter reliées. Celles-ci recueillent, traitent, stockent et diffusent de l'information afin d'aider à la prise de décision, à la coordination, au contrôle, à l'analyse et aux capacités de représentation de situations au sein d'une entreprise (LAUDON & al, 2013 : 22).

Cette définition rappeler le rôle fondamental d'un SI qui est celui de fournir des informations susceptibles d'aider à prendre des décisions stratégiques, budgétaires et opérationnelles.

1.1.1. Définition du Système d'information comptable

Selon JACQUOT & al. (2011 : 59), un Système d'Information Comptable est la partie du système d'information de l'entreprise consacrée à la collecte, à la saisie, au traitement et à la diffusion des données susceptibles d'alimenter les modèles comptables.

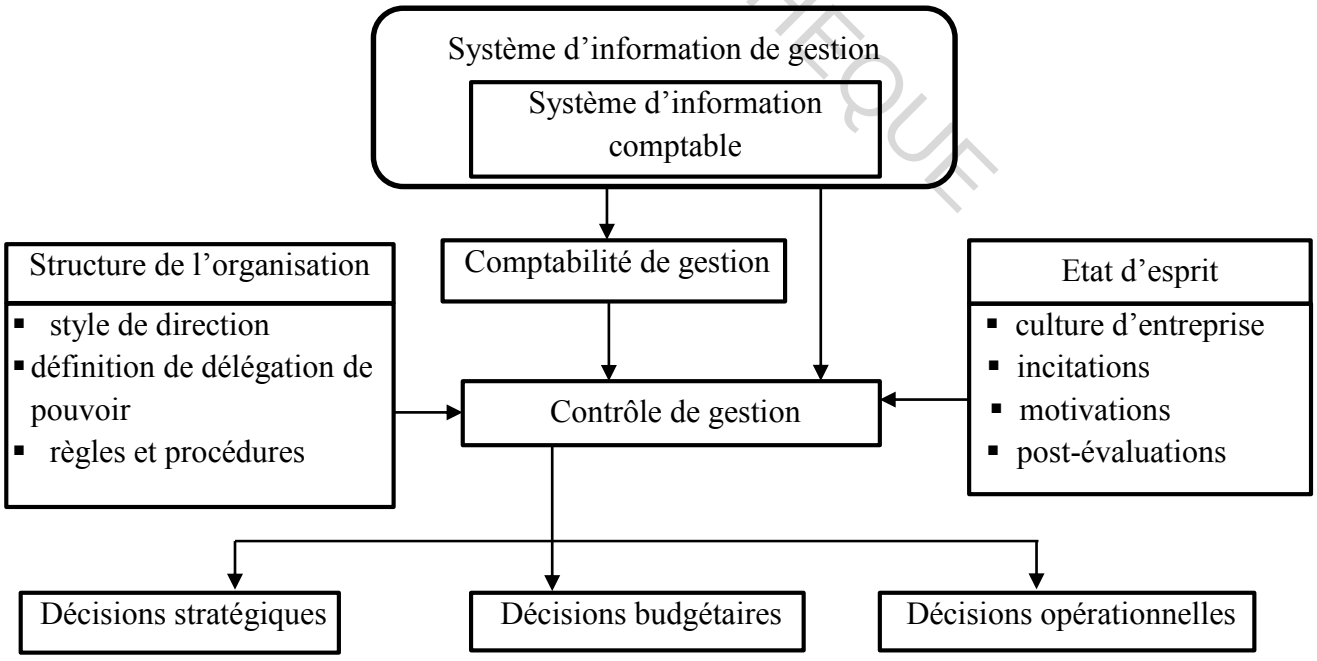
Etant un sous ensemble du SI de l'entreprise, il convient de noter que fournir des informations pour des soins comptables ne doit pas être le seul objectif du SIC.

Ainsi, pour BOUVIER & al. (2008 : 1) le SIC fournit une information intelligible, significative, fiable et pertinente sur la réalité économique de l'entreprise. Elle permet notamment de rendre compte des relations de l'entreprise avec ses partenaires et d'informer sur la situation patrimoniale et les performances de l'entreprise. Les informations fournies sont des indicateurs qui aident les opérationnels à exercer avec efficacité et efficience leur activité.

La production des données comptables par le SIC met en étroite relation, la comptabilité générale, la comptabilité analytique et le contrôle de gestion en tenant compte des facteurs de contingence de l'organisation. La figure 1 résume les liens qui existent entre le système d'information comptable, le contrôle de gestion et les valeurs propres à l'organisation-type.

CESAG - BIBLIOTHEQUE

Figure 1: Relation entre le système d'information, la comptabilité de gestion et le contrôle de gestion et les valeurs de l'organisation.



Source : Nous-mêmes à partir de COSSU & al. (2005 : 87).

La qualité et la pertinence des informations de gestion qui seront mises à la disposition des différents acteurs de l'entreprise au moment opportun dépendent de cette relation.
La notion SIC sera appréhendée dans la suite de l'étude à travers la notion générale « Système d'Information » tout en mettant un accent particulier sur les spécificités du SIC. Pour dire, le SIC est un sous-système indissociable du système d'information de toute organisation.

1.1.2. Organisation et fonctionnement du SIC

Le rôle joué par le système d'information dans l'entreprise se manifeste à travers ses fonctions, correspondant aux différentes étapes de transformation et de sauvegarde de l'information. Pour mettre en place un système d'information efficace et efficient, il faut l'adapter aux spécificités de l'entreprise ; en d'autres termes cela nécessite une organisation adéquate.

1.1.2.1. Organisation du SIC

Une obligation est faite aux entreprises publiques ou privées assujetties au droit OHADA de se conformer aux dispositions réglementaires en ce qui concerne l'organisation du SIC. L'OHADA, à l'article 14 du chapitre 2 du titre premier de l'Acte Uniforme portant Organisation et Harmonisation des Comptabilités des Entreprises dispose que : « l'organisation comptable mise en place dans l'entreprise doit satisfaire aux exigences de régularité et de sécurité pour assurer l'authenticité des écritures de façon à ce que la comptabilité puisse servir à la fois d'instrument de mesure des droits et obligations des partenaires de l'entreprise, d'instrument de preuve, d'information des tiers et de gestion »[1] (OHADA, 2000 : 4).

De cet article, on peut noter que l'organisation comptable (notion qui se rattache à la mise en place d'un système comptable dans une entreprise) doit prendre en compte les questions de sécurité. Cette organisation (en système informatisé ou manuel) se déroule en tenant les livres comptables (le journal; le grand livre, la balance générale des comptes) ; qui servent à la présentation des états financiers.

On rencontre généralement trois niveaux d'organisation en tenant compte de différents paramètres de l'entreprise (l'architecture informatique, l'organisation de l'activité comptable et la taille). Ainsi, à chaque groupe de facteurs va correspondre un système d'information comptable approprié.

[1]Titre I. Chapitre 2.Article 14 de l'Acte Uniforme portant Organisation et Harmonisation des Comptabilités des Entreprises adopté le 22 février 2000 et publié au Journal Officiel N° 10 du 20 nov. 2000.

CESAG - BIBLIOTHEQUE

Tableau 1: Différentes architectures et niveaux d'intégration des SIC

Types de SIC	Architecture informatique	Organisation de la comptabilité	Taille de l'entité
Comptabilité autonome	❖ Micro-ordinateur autonome ❖ Progiciel comptable	❖ Saisie manuelle centralisée ❖ Axe réglementaire (juridique et fiscal)	Petite
Comptabilité semi-intégrée	❖ Réseau local ❖ Applications fonctionnelles interfacées	❖ Génération automatique des écritures comptables ❖ Axe réglementaire et axe gestion	Moyenne
Comptabilité intégrée	❖ Architecture client-serveur ❖ Applications « intégrées »	❖ Saisie unique des évènements ❖ Axes d'analyse multiples	Grande et Très grande

Source : Adapté de GRENIER & al. (2004 : 301).

L'organisation comptable en environnement informatisé doit, selon VERNHET (2008 : 8), permettre néanmoins de satisfaire aux exigences de rapidité, de contrôle et de sécurité (la vérification des conditions d'enregistrement et de conservation des données entrées qui doivent être intelligibles et intègres, l'irréversibilité des traitements effectués qui doit interdire toute suppression, addition ou modification ultérieure de l'enregistrement).

Le traitement des données comptables peut être effectué selon deux modes d'organisation :

- **le système classique**

Le système classique (annexe 1, page 103) est adapté aux entreprises de petite taille qui traitent des informations de quantité moins importante. Il consiste à l'authentification des opérations par le journal, au classement méthodique par le grand livre et la vérification par la balance et l'établissement en fin de période des états financiers (GOUADAIN, 2002 : 75).

Cependant, ce système présente des insuffisances du fait de l'existence d'un journal unique qui ne peut être tenu par une seule personne, quels que soient le volume des pièces comptables à enregistrer et le nombre de personnes travaillant au service comptable.

CESAG - BIBLIOTHEQUE

Par ailleurs, la nécessité de réduire les délais de traitement des informations comptables afin d'améliorer la gestion des entreprises et l'importance de la division du travail dès le dépassement du stade artisanal ont conduit les comptables à imaginer un autre système (le système centralisateur) qui permet de pallier aux inconvénients du système classique.

- **le système centralisateur**

Le système centralisateur préconise selon DOBILL (2013 : 27), la création de plusieurs journaux auxiliaires en fonction du très grand nombre d'opérations réalisées et de l'informatisation généralisée des procédures d'enregistrement comptable pouvant être tenus simultanément par plusieurs personnes. Adapté aux grandes entreprises, il a pour but d'améliorer l'organisation comptable.

Le schéma comptable de ce système (annexe 2, page 104) consiste à la tenue les journaux auxiliaires, le report dans les grands livres auxiliaires, à la tenue de la comptabilité générale ou centralisatrice, à l'établissement du journal général à partir des totaux des journaux auxiliaires; aux reports dans le grand livre général, à l'établissement de la balance et enfin à l'établissement des comptes financiers.

Le choix de l'un ou l'autre de ces systèmes dépendra, d'une part, des méthodes et des moyens utilisés et, d'autre part, de l'importance des informations traitées par l'entreprise. Néanmoins, le système choisi doit assurer l'efficacité et l'efficience des différentes fonctionnalités du SIC sans pour autant faire obstacle au respect des obligations légales et réglementaires.

CESAG BIBLIOTHEQUE

1.1.2.2. Fonctionnalités du SIC

Un SI doit répondre, selon BOHNKE (2010 : 3), aux besoins de stockage, de préservation, d'exploitation et d'échange des informations afin d'automatiser les tâches réplicables de façon plus sécurisée que n'en le pourrait une intervention humaine ou fournir à des utilisateurs les informations indispensables pour leur permettre d'agir à bon escient et plus vite.

DAYAN & al. (2008 : 977) et DORIATH & al. (2008 : 2) y ajoutent la tâche d'acquisition que nous jugeons importante, car elle traite de la capacité du SI à disposer d'informations pertinentes. Ainsi, nous pouvons retenir comme fonctions du SI au regard de l'information :

- son acquisition : elle se fait grâce aux deux sources dont dispose l'organisation à savoir la source interne (informations issues des activités de l'entreprise) et la source externe (informations provenant de l'environnement externe de l'entreprise) ;

- son stockage : il consiste à garder l'information de manière stable et durable ;
- son exploitation: l'information mémorisée doit pouvoir être sélectionnée, consultée, triée, fusionnée, mise à jour ou supprimée le cas échéant ;
- sa diffusion : il s'agit de la mise à disposition des utilisateurs de l'information.

Pour assurer ces différentes fonctions, le SIC utilise des moyens compte tenu des besoins de l'entreprise. Ces moyens constituent en d'autres termes ses composantes.

1.1.3. Composantes du Système d'Information Comptable

Comme tout SI, le SIC est un système constitué de ressources qui évoluent dans une organisation et dont le fonctionnement coordonné vise l'atteinte d'un but commun : fournir des informations pour les prises de décision. Il est donc nécessaire d'identifier les ressources du SI et de définir celles qui doivent être protégées afin de garantir une exploitation maîtrisée et raisonnée. Pour un système d'information, DAYAN & al. (2008 : 977) ont identifié les personnes, les matériels, les logiciels, les processus et les données comme des ressources indispensables.

1.1.3.1. Les personnes.

La composante « personne » d'un SI, selon DORIATH & al. (2008 : 2), est l'ensemble constitué d'analystes, de programmeurs et d'utilisateurs.

Selon REIX & al. (2011 : 4), il n'a y pas de système d'information sans personnes, sans acteurs. Ce sont soit des utilisateurs du système, employés, cadres qui, pour la réalisation de leurs tâches, utilisent l'information produite par le système et ses possibilités d'automatisation ou qui alimentent le système en données nouvelles ; soit encore des spécialistes de la construction des systèmes (analystes, programmeurs…) dont le travail consiste à concevoir, développer, implanter les bases technologiques du système et assurer son fonctionnement.

Cette dernière définition nous convient plus, car elle est plus détaillée.

Les personnes constituent donc l'élément principal du SIC. Néanmoins, la conception et le maintien de ce dernier nécessitent parfois des matériels avec des procédures formalisées ou non.

1.1.3.2. Les matériels

Selon MONACO (2014 : 18), c'est l'ensemble constitué de dispositifs physiques (photocopieurs, scanners, ordinateurs, moyens de communication) plus ou moins techniques.

CESAG - BIBLIOTHEQUE

On note également les supports de l'information comme les disques durs, les clés USB (Universel Serial Bus), etc.

Ces matériels doivent permettre le transport, le stockage et la manipulation des données. Même si l'on peut avoir un système d'information avec des matériels modestes, être équipé de matériels performants en termes de réponse serait un atout considérable.

1.1.3.3. Les logiciels et les procédures

Selon DORIATH (2008 : 2), le SI comporte également les logiciels, les procédures, les règlements. En effet, le système d'information peut être manuel ou automatisé. Ce dernier aspect du SI, le plus fréquent d'ailleurs nécessite des logiciels qui sont des programmes articulés entre eux et utilisés pour automatiser les tâches de traitement de l'information.

Très souvent, il y a imbrication des tâches automatisées assurées, par l'ordinateur et des tâches manuelles confiées aux employés. Les procédures constituent la partie dynamique d'un système d'information. Elle explicite dans un langage directement accessible, qui fait quoi ? Où il le fait ? Quand il le fait ? Comment et à quelle fin ? (c'est l'exemple du manuel des procédures comptables, qui sert de référence pour les tâches comptables).

Quant aux règlements, ils permettent d'orienter les actions des acteurs du système d'information pour la réalisation des objectifs stratégiques et opérationnels de l'organisation.

1.1.3.4. Les données

L'AFNOR (Association Française de Normalisation) définit une donnée comme un fait, une notion ou une instruction représentée sous forme conventionnelle convenant à la communication, à l'interprétation ou au traitement par des moyens humains ou automatiques.

Elles matérialisent les informations détenues par une organisation et peuvent se présenter sous différentes formes (chiffres, textes, images, etc.). Elles constituent généralement le bien le plus précieux pour certaines organisations et, de ce fait elles sont la principale cible des attaques.

La simple juxtaposition de ces ressources humaines, informatiques et organisationnelles ne constitue pas un SI. Il faut une bonne structuration pour qu'elles puissent mieux répondre aux besoins. De même, il va falloir tenir compte de leurs vulnérabilités ; qui peuvent être exploitées par des menaces susceptibles d'impacter considérablement les objectifs de sécurité. Alors, une gestion efficace des risques s'impose.

CESAG - BIBLIOTHEQUE

1.2. Gestion des risques de sécurité des systèmes d'information.

Les systèmes d'information dont dépendent fortement l'activité opérationnelle et la fiabilité de l'information comptable et financière, rendent incontournable leur prise en compte dans une démarche sérieuse d'analyse des risques.

HASSID (2008 : 138) définit la gestion des risques comme un processus matriciel itératif de prise de décision et de mise en œuvre des instruments qui permettent de réduire à un niveau acceptable l'impact des vulnérabilités pesant sur toute entité.

Nous pouvons déduire de cette définition que la sécurité d'un SI revient à essayer de se protéger contre les menaces intentionnelles ou non, et d'une manière plus générale contre tous les risques pouvant avoir un impact sur le SI, ou sur des informations qu'il traite. Alors, qu'est-ce qu'un risque ? Comment peut-on garantir une sécurité raisonnable du SIC ?

CESAG - BIBLIOTHEQUE

1.2.1. La notion de risque

La notion de risque est définie par IFACI (in RENARD, 2013 : 137) comme étant « un ensemble d'aléas susceptibles d'avoir des conséquences négatives sur une entité et dont le contrôle interne et l'audit ont notamment pour mission d'assurer autant que faire se peut la maîtrise. »

Le risque résulte donc, de tout événement, comportement ou situation susceptible de provoquer un dommage à l'organisation et/ou de l'empêcher de réaliser ses objectifs ou de maximiser ses performances ou encore de saisir une opportunité. On distingue plusieurs types de risques. Ceux liés au SIC sont qualifiés de risques opérationnels car découlant de l'activité comptable, auxquels l'on associe les risques liés aux moyens mis en œuvre pour produire l'information.

En effet, le risque opérationnel selon Bâle 2 (in JIMENEZ, 2008 : 19) est un risque de perte résultant d'une inadaptation ou d'une défaillance attribuables à des procédures, personnes et systèmes internes ou à des événements externes.

Cette définition recouvre les erreurs humaines, les fraudes et malveillances, les défaillances des systèmes d'information, les problèmes liés à la gestion du personnel, les litiges commerciaux, les accidents, incendies, inondations, etc.

Se référant à la sécurité des systèmes d'information, le risque serait la possibilité qu'une menace donnée exploite une ou plusieurs vulnérabilités d'un actif ou d'un groupe d'actif et cause ainsi un préjudice à l'organisation (ISACA, 2013 : 74).

Cette dernière définition est celle qui retiendra notre attention dans la suite de cette étude. Alors qu'est-ce qu'une vulnérabilité ? Une menace ?

1.2.1.1. La vulnérabilité

La vulnérabilité est considérée par CARPENTIER (2009 : 31) comme une faiblesse des procédures de sécurité techniques et physiques ou encore d'une absence de protection qui peuvent être exploités par une menace.

Cette définition se limite aux mesures de sécurité alors qu'un actif informationnel peut présenter des faiblesses intrinsèques. En effet, ISO/CEI 27000 (in CLUSIF, 2010 : 5) donne une définition plus complète en ces termes : « la vulnérabilité est une faille dans un actif ou mesure de sécurité qui peut être exploitée par une ou plusieurs menaces ».

La réalisation du risque se manifeste donc par l'exploitation d'une ou des vulnérabilités par une ou plusieurs menaces.

1.2.1.2. La menace

La notion de menace est, selon PILLOU & al. (2011 : 33), toute action susceptible de nuire dans l'absolu.

En d'autres termes, il s'agit de tout évènement dont la survenance est susceptible de compromettre l'atteinte des objectifs. On distingue les menaces à caractère non intentionnel qui peuvent globalement se scinder en deux catégories notamment les accidents (inondation, incendie etc.) et les erreurs et les menaces à caractère intentionnel (vol de données, modification ou altération des données, déni de service, émission de programme malveillant) qui sont essentiellement dues à de la malveillance qui peuvent être d'origine interne ou externe.

Les facteurs « probabilité » et « impact » caractérisent le risque et déterminent sa criticité. Le risque est susceptible de se produire et d'avoir un impact négatif sur la réalisation des objectifs. La gestion des risques est donc d'une très grande importance pour assurer la continuité des activités de l'entreprise.

1.2.2. Définition du cadre de gestion des risques de SSI.

La gestion des risques de SSI pour emprunter les mots à FEVRIER (2013 : 25) est un sous ensemble du vaste domaine de la gestion globale des risques (risk-management).

CESAG - BIBLIOTHEQUE

En effet, les apporteurs de capitaux exigent souvent des garanties quant à la sécurité de leurs investissements. Ainsi, nombreux sont ceux qui investissent dès lors qu'une politique efficace de gestion de risques est mise en place au sein de l'organisation. Alors, qu'est-ce que la gestion des risques spécialement la gestion de ceux qui entravent la sécurité des SI ?

Au premier volet de cette question, COSO II[2] (in CORDEL & al., 2013 : 25) répond en ces termes : la gestion des risques est un processus mis en œuvre par le conseil d'administration, la direction générale, et l'ensemble des collaborateurs de l'organisation. Il est conçu pour identifier les événements potentiels susceptibles d'affecter l'organisation dans les limites de son appétence pour le risque afin de fournir une assurance raisonnable quant à la réalisation des objectifs.

La gestion des risques des SI étant un processus continu, il convient de définir précisément le cadre, c'est-à-dire les ressources, les moyens, ainsi que les responsabilités pour chacun des aspects suivants : classification des actifs informationnels, identification des vulnérabilités et menaces, évaluation et traitement des risques et la mise en place d'une bonne politique de gestion de ces risques. Ce processus comprend également des mesures de préventions, de détection et de correction à mettre en place pour réduire les risques à un niveau acceptable.

CESAG - BIBLIOTHEQUE

1.2.3. Classification des actifs informationnels

Il est important d'identifier et de catégoriser les actifs que l'on veut protéger car selon ANDRESS (2014 : 12) si l'on ne peut pas énumérer les actifs qu'on a et évaluer l'importance de chacun d'eux, les protéger peut devenir une tâche très difficile.

On attend par actif informationnel une banque d'information (numérique, un système ou un support d'information, une TI, une installation ou encore un ensemble de ces éléments acquis ou constitués par un organisme) et ayant de la valeur (ISO 27002, 2005 : 19).

Par ricochet, le risque est lié à l'existence de valeurs ou d'actifs qui représentent pour un organisme un enjeu. Il s'agit donc, d'élaborer un plan de classification et d'hiérarchisation des actifs informationnels selon les besoins, les priorités et le degré souhaité de protection. L'objectif est de garantir un niveau de protection approprié aux actifs informationnels et de permettre une meilleure identification des risques inhérents à ces actifs.

[2] Committee of Sponsoring Organizations of the Treadway Commission est un référentiel de gestion des risques de l'entreprise (« ERM : Enterprise Risk Management Framework »).

1.2.4. Identification des risques de sécurité des systèmes d'information

Cette phase est la plus importante dans le processus de gestion des risques. Elle a pour but selon MENTHONNEX (1995 : 119), d'aider à connaître et à analyser les événements pouvant être à l'origine de la non-réalisation des objectifs poursuivis notamment par le SIC.

Même s'il est difficile, voire impossible d'identifier de façon exhaustive tous les risques auxquels serait exposé le SIC, il s'agira tout au moins, d'identifier ceux susceptibles de compromettre la continuité des activités.

Selon BERRADA (2012 : 70), identifier un risque ou un objet de risque revient à recenser l'ensemble des ressources dont l'entreprise a besoin pour fonctionner et à les rapprocher de tous les événements aléatoires, à localiser leur source.

En effet, un risque non identifié ne pourra jamais être traité. Plusieurs approches permettent d'identifier les risques. En se référant à JIMENEZ & al. (2008 : 63), nous pouvons noter à titre d'exemple les approches « brainstorming », « Top down », « Bottom-up », etc.

1.2.5. Évaluation des risques de SSI

L'évaluation des risques est selon LINLAUD (2003 : 43), le préalable indispensable à l'élaboration du système de gestion de la sécurité de l'information.

L'objectif est d'obtenir, pour chaque risque identifié, une évaluation du niveau auquel l'organisation serait exposée. Ce niveau dépend de deux facteurs que sont l'impact et la potentialité (ou probabilité) du risque. CORDEL (2013 : 19) illustre le risque par la formule suivante : Risque = Probabilité d'occurrence × Impact.

BLOCH & al. (2011 : 252) expriment l'impact comme étant le produit d'une ou des menaces et d'une ou des vulnérabilités.

En d'autres termes, les menaces exploitent les vulnérabilités pour provoquer un dommage ou la perte d'un actif informationnel. Nous pouvons en déduire par transitivité que :

Risque = Probabilité d'occurrence × Menace × Vulnérabilité.

Dans un contexte où des mesures de sécurité ont déjà été prises, il faudra en outre tenir compte de la qualité de ces mesures ou de leur maturité. Alors le risque sera selon l'expression suivante :

CESAG - BIBLIOTHEQUE

$$\text{Risque} = \frac{\text{Probabilité d'occurrence} \times \text{Menace} \times \text{Vulnérabilité}}{\text{Contre-mesures}}$$

Selon PINET (2012 : 47-48), l'impact (produit de la menace et de la vulnérabilité) et la probabilité d'apparition d'un risque s'évaluent à travers la définition d'une échelle faisant apparaître des différents niveaux d'appréciation. Le niveau des impacts doit être apprécié pour chacun des trois facteurs : disponibilité, intégrité et confidentialité des actifs sélectionnés.

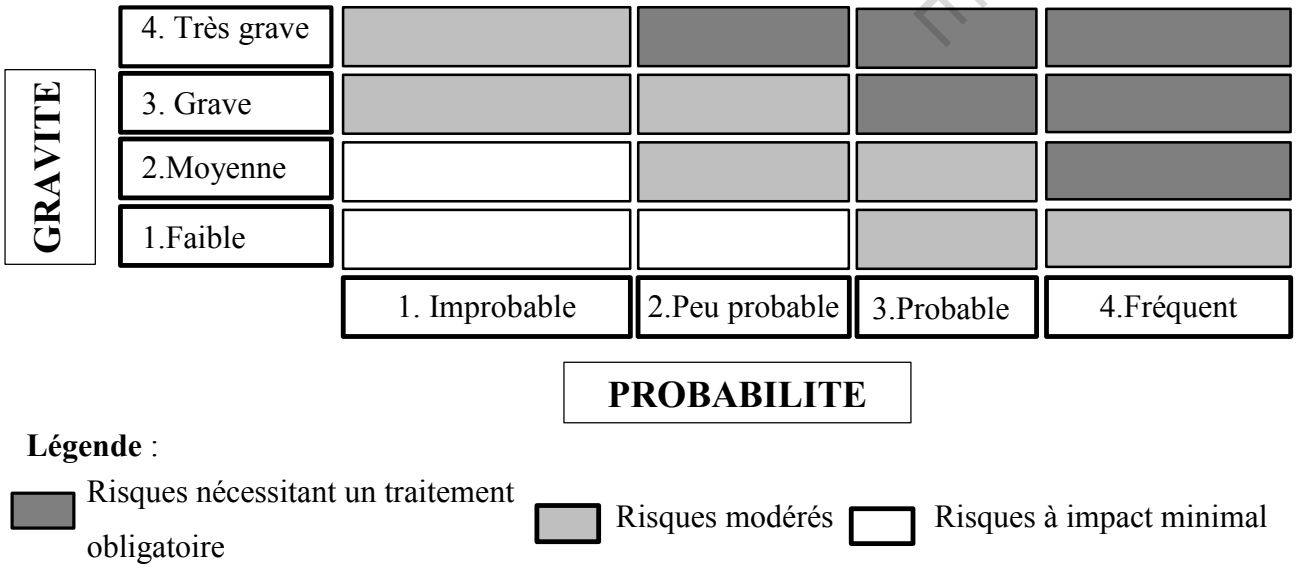
La probabilité, selon CORDEL (2013 : 143) est déterminée soit par extrapolation (utilisation des données historiques disponibles et fiables), soit par prédilection (lorsque les données ne sont pas disponibles) ou en faisant le recours structuré aux experts.

Par ailleurs, les contre-mesures s'apprécient selon leur capacité à réduire l'impact et ou la probabilité d'un ou de plusieurs risques.

Une fois l'évaluation faite, une hiérarchisation consistant à attribuer une priorité aux différents risques identifiés et évalués est nécessaire. L'identification, l'évaluation et la hiérarchisation des risques, permettront d'établir la matrice des risques qui, pour reprendre HASSID (2008 : 139) est une forme de mesure et de priorisation des risques en une seule étape afin de déterminer le niveau de danger particulier, à l'aide des critères objectifs de probabilité et de gravité.

Nous notons qu'elle constitue, un outil d'aide à la prise de décision dans la gestion des risques en ce sens qu'un traitement approprié est réservé à chaque risque conformément à l'appétence aux risques de l'organisation. La figure 8 montre un exemple de matrice de risques.

Figure 2: Matrice des risques (cotation des risques en termes de gravité et de probabilité)



Source : Nous-mêmes à partir de FERNANDEZ (2013 : 5).

CESAG - BIBLIOTHEQUE

Toutefois, les différents niveaux d'appréciation des risques restent relatifs. Les finalités de cette matrice sont : de définir les risques les plus importants à maîtriser et de permettre de se baser sur un schéma commun pouvant aider à identifier et coter les risques.

1.2.6. Traitements des risques de sécurité du SIC

Le traitement des risques de SSI consiste à trouver une réponse à chacun des risques identifiés, évalués et hiérarchisés. En d'autres termes il s'agit de prendre les mesures appropriées pour les ramener à un niveau acceptable ou de les rendre plus supportables pour l'organisation. Selon la norme ISO 27002 (2005 : 5), on distingue quatre manières de gérer le risque, par ordre croissant de coût : l'acceptation, l'évitement, le transfert ou le partage et la réduction.

- **l'acceptation du risque**

Elle consiste, selon COSO II (in CORDEL, 2013 : 153), à « ne prendre aucune mesure susceptible de modifier la probabilité d'occurrence d'un risque et ou son impact ». Elle peut être justifiée si une réalisation du risque n'aura pas d'impact significatif sur l'entreprise c'est-à-dire si le risque est déjà en-dessous du seuil de tolérance de l'entreprise.

- **l'évitement du risque**

Selon KEREBEL (2009 : 65), éviter un risque consiste à renoncer par exemple à lancer une nouvelle activité ou à supprimer une activité existante, source de ce risque.

- **la réduction du risque**

Réduire le risque consiste à prendre des mesures afin de réduire la probabilité d'occurrence ou l'impact du risque, ou les deux à la fois ; ce qui implique tout un ensemble de décisions opérationnelles courantes (PwC[3] & al, 2014 : 127).

L'objectif est donc, de définir des mesures techniques et organisationnelles pour ramener le risque à un niveau acceptable. C'est le traitement le plus courant.

- **le transfert du risque**

Selon WITHMAN (2011 : 147), le transfert d'un risque consiste à sous-traiter l'activité, source de risque ou en souscrivant à une assurance.

[3] PwC : PricewaterhouseCoopers

CESAG - BIBLIOTHEQUE

C'est une stratégie qui est donc nécessaire lorsque l'entreprise n'est pas en mesure de mettre en place des dispositifs de sécurité qui permettraient de réduire le risque. On parle aussi du partage du risque si elle décide d'externaliser une partie ou l'ensemble de l'activité qui présente des risques.

Chacun de ces traitements a un coût ; et pour être rationnel l'entreprise doit veiller à ce que ce coût ne dépasse pas l'impact d'une survenance du risque. Il serait donc nécessaire de procéder à un arbitrage entre le coût du traitement du risque et l'impact de la survenance dudit risque.

La gestion des risques du SIC, a donc pour finalité la sécurité de ce dernier afin de mettre en confiance les destinataires de l'information comptable.

1.3. Notion de sécurité du système d'information comptable

La sécurité du SIC constitue un domaine depuis et encore plus de nos jours déterminant pour la survie de l'entreprise. Pour que la gouvernance des SI atteigne ses objectifs, il est indispensable de tenir compte de la sécurité du système d'information comptable.

1.3.1. Définition de la notion de sécurité du système d'information

Nombreuses sont les définitions données à la notion de sécurité du système d'information. Nous portons notre attention sur quelques-unes susceptibles de nous aider à la comprendre.

Pour reprendre MENTHONNEX (1995 : 74), la sécurité d'un SI est un ensemble de moyens techniques ou non, de protection, permettant à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des équipements et/ou des données traitées ou transmises et des services connexes offerts ou rendus accessibles par le système.

Selon la norme ISO 27002 (2005 : 14), la sécurité de l'information est l'état de protection face aux risques identifiés et résultant de l'ensemble des mesures de sécurité prises par une entreprise pour préserver : la confidentialité, l'intégrité et la disponibilité de l'information que détient l'entreprise, quel que soit le support (papier, électronique, etc.).

Ces deux définitions identifient clairement les principaux critères de sécurité à prendre en compte dans la gouvernance de la sécurité des SI tout en proposant les moyens à mettre en œuvre afin d'atteindre les objectifs de sécurité que nous aborderons plus loin.

CESAG - BIBLIOTHEQUE

1.3.2. La gouvernance de la sécurité du SIC

Selon ITGI[4] (in WHITMAN & al, 2011 : 176), la gouvernance de la sécurité de l'information comprend toutes les responsabilités et les méthodes prises par la haute direction afin de fournir des orientations stratégiques pour la définition des objectifs de sécurité.

Elle est donc une activité continuelle qui doit tenir compte des besoins de l'organisation, tout en assurant son alignement par rapport aux objectifs généraux. En outre, il s'agit de mobiliser un ensemble de mesures de sécurité organisationnelles, procédurales et techniques, sans toutefois négliger l'importance de l'adhésion du personnel de l'organisation afin de s'assurer de la continuité des services et de la protection des actifs informationnels.

1.3.2.1. L'organisation de la sécurité du SIC

L'organisation et plus largement la gestion de la SSI repose sur un ensemble d'actions, lesquelles doivent être alignées sur le plan stratégique de l'entité. Ainsi, pour IFACI (1993 : 57), l'efficacité de la SSI repose également sur les procédures et les plans stratégiques.

Un service ou un individu doit être responsable de cette sécurité afin de la faire comprendre à l'ensemble du personnel. L'organisation à mettre en place implique également un partage des responsabilités (annexe 3, page 105) entre les différents niveaux, notamment les niveaux décisionnels, de pilotage et opérationnel. Les chaînes de responsabilité doivent réagir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux menaces. L'objectif étant de faciliter la mise en place des mesures de sécurité physique et logique.

1.3.2.2. La sécurité physique et la sécurité logique

La sécurité physique consiste à protéger les actifs informationnels contre les menaces éventuelles : erreurs humaines, actes délibérés (sabotage, vandalisme, vol, déni de service, etc.), de même que des catastrophes naturelles (incendie, inondation, etc.). Elle se manifeste par le choix et le déploiement d'un ensemble de dispositifs pouvant protéger physiquement les éléments du SI.

C'est ce que WHITMAN & al. (2011 : 399) souligne dans sa définition de la sécurité physique. Selon lui, elle englobe la conception, la mise en œuvre et le contrôle des dispositifs qui protègent les ressources physiques d'une organisation, y compris les personnes, les matériels,

[4] Information Technology Governance Institute.

CESAG BIBLIOTHEQUE

les éléments de support et les ressources qui contrôlent les informations dans tous ses états (transport, stockage et traitement de l'information).

Cependant, les dispositifs physiques n'assurent qu'une protection limitée de ces actifs, car leur seule existence ne suffit pas. Il va falloir penser à limiter les accès du moins, aux actifs sensibles, d'où la nécessite de penser à la sécurité logique.

Selon l'IFACI (1993 : 27), la sécurité logique consiste à protéger les données et programmes contre les erreurs et les malveillances à travers la gestion des accès. Elle permet d'identifier individuellement les utilisateurs des données et des ressources, de limiter l'accès à des données et/ou ressources sensibles, de produire des pistes d'audit de l'activité du SI.

Il faudra donc mettre en place des dispositifs de protection de type pare-feu, de logiciels (antivirus par exemple), pour contrer les logiciels malveillants, des contrôles d'identification et d'authentification ou encore de chiffrement de données. Il conviendrait par ailleurs de protéger les données à caractère personnel. L'objectif est d'anticiper les effets de menaces fortuites ou délibérées et de satisfaire les impératifs de sécurité.

CESAG BIBLIOTHEQUE

1.3.3. Les critères de sécurité

Selon FEVRIER (2013 : 29), le niveau de sécurité d'un SI peut s'interpréter comme sa capacité à demeurer inaccessible à l'ensemble des risques auxquels il est exposé, que ce soit en termes de contenant (structure) ou de contenu (données).

Pour connaître ce niveau de sécurité il faut pouvoir l'évaluer par des indicateurs. Ces derniers constituent les exigences fondamentales en matière de sécurité des SI. Ils caractérisent ceux à quoi s'attendent les utilisateurs vis-à-vis du SI.

Ainsi, selon LAFITTE (2003 : 31), LINLAUD (2011 : 11) et GHERNAOUTI (2013 : 1), la sécurité des systèmes d'information repose principalement sur trois critères que sont la Disponibilité (D), l'Intégrité (I), et la Confidentialité (C) décrits comme suit :

- **la disponibilité**

Elle garantit que les éléments considérés sont accessibles autant que besoin aux personnes autorisées. En d'autres termes, elle conditionne le fait que le système puisse fonctionner sans défaillance, durant les plages d'utilisation prévues, garantit l'accès aux services et ressources installées avec le temps de réponse attendu.

- **l'intégrité**

La norme ISO/CEI 27002 définit l'intégrité comme la propriété de protection de l'exactitude et de l'exhaustivité des actifs informationnels.

Selon PINET (2012 : 44), l'intégrité d'un équipement, d'un système ou des données est obtenue lorsque ceux-ci ne subissent aucune altération ou destruction accidentelle ou volontaire.

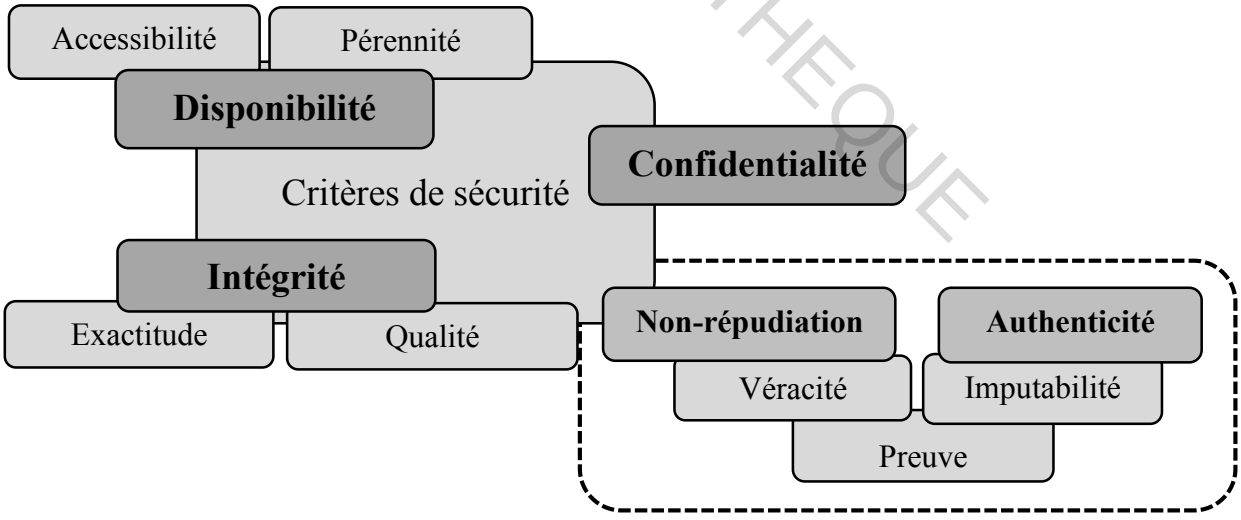
- **la confidentialité**

Elle est la propriété qu'une information ne soit disponible, divulguée qu'aux personnes, entités ou processus autorisés. C'est également la garantie qu'une information n'est connue que de ceux qui sont habilités à en disposer (ANDRESS, 2014 : 6).

A ces trois critères primitifs et essentiels de la sécurité dits « critères DIC », nous pouvons également considérer selon ISO 27002 (2005 : 2) d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation, etc.

Il reviendra aux responsables de chaque entité de les hiérarchisés par rapport aux objectifs de sécurité. La figure 3 ci-après résume les critères et fonctions permettant de mesurer le niveau de sécurité du SI d'une organisation.

Figure 3: Critères de sécurité



Source : GHERNAOUTI (2013 : 2).

Nous pouvons retenir qu'un système d'information ou une application, pour être considéré comme « sécurisé », doit au minimum disposer les qualités suivantes :

- empêcher les accès et la consultation de données aux personnes non autorisées ;

CESAG - BIBLIOTHEQUE

- ❖ conserver et restituer les données dans l'état où elles ont été saisies ;
- ❖ fournir les données ou services requis lorsque les utilisateurs autorisés en ont besoin ;
- ❖ identifier et authentifier les utilisateurs sur le système d'information ;
- ❖ permettre de retracer chaque opération.

Dans le cadre de la gestion de la sécurité, outre la définition des objectifs de sécurité, il faut néanmoins rappeler les rôles des différents acteurs afin que les différentes politiques de sécurité puissent être partagées par toute l'organisation.

1.3.4. Les rôles et les responsabilités des acteurs de la sécurité du SIC

La sécurité du patrimoine informationnel est, certes l'affaire de « TOUS », repérer les rôles et responsabilités des différents acteurs de la SSI est un plus. A contrario, la politique sécuritaire de l'organisation serait vouée à l'échec.

1.3.4.1. Le Comité de Sécurité

Selon la norme ISO 27002 (2005 : 8), compte tenue de la taille de l'organisation le comité de sécurité aura à soutenir activement la politique de sécurité au moyen de directives claires, d'un engagement franc, d'attribution de fonctions explicites et d'une reconnaissance des responsabilités liées à la sécurité de l'information.

Il devra notamment recommander les orientations, approuver les standards, les pratiques et le plan d'action de la sécurité de l'entreprise.

1.3.4.2. La Direction Générale

Selon IFACI (1993 : 2), en matière de sécurité des systèmes d'information, la Direction Générale n'est pas seulement impliquée mais elle en détient la responsabilité ultime. L'évaluation des risques, l'établissement de la politique de sécurité et la mise en place d'une structure organisationnelle adéquate, sont de son ressort.

On pourrait y ajouter qu'elle est l'acteur de la culture de la sécurité au sein de l'organisation.

Par ailleurs, pour atteindre les objectifs de sécurité du SI, elle doit allouer des ressources. De même, elle peut être amenée à déléguer certaines responsabilités. Elle doit néanmoins disposer des moyens de contrôle et de pilotage de l'ensemble des actions de son équipe.

CESAG - BIBLIOTHEQUE

1.3.4.3. La Direction du Système d'Information (DSI)

La DSI a été longtemps une direction chargée essentiellement de la technologie, de la maîtrise des coûts des projets informatiques. Avec la place actuelle qu'occupe le SI, la fonction de DSI est devenue stratégique.

La nouvelle DSI est selon MONACO (2014 : 21), celle qui doit posséder les compétences technologiques, communicationnelles, organisationnelles et managériales. Elle doit s'assurer de l'adéquation du SI à la stratégie de l'entreprise.

En matière de sécurité des SI, elle doit veiller à ce que l'ensemble des composants matériels et logiciels dont elle est responsable soient utilisés conformément aux directives décrites dans la charte de sécurité de l'organisation.

CESAG - BIBLIOTHEQUE

1.3.4.4. Le Responsable de la Sécurité du Système d'Information

Le Responsable de la Sécurité des Systèmes d'Information (RSSI), est le garant de la sécurité des SI de l'organisme. Il intervient dans des domaines multiples avec un seul objectif : assurer l'intégrité, la confidentialité et la disponibilité des données et des matériels qui les supportent (ISO 17799 in LINLAUD, 2003 : 83).

Sa mission est donc de concevoir et d'animer la démarche de SSI en veillant à ce que, les niveaux de sécurité soient conformes aux prescriptions légales, aux bonnes pratiques et aux standards. Il est le responsable de la sensibilisation et de la formation des responsables opérationnels sur leurs rôles et leurs devoirs dans le domaine de la sécurité des SI de l'organisation.

Comme le souligne MONACO (2014 : 24), il doit conseiller, assister, informer, former et alerter sur les questions de sécurité.

Ainsi, avec le gestionnaire des risques, il prend part à la définition de la stratégie de sécurité et sous l'autorité directe de la Direction Générale, aux activités suivantes :

- exploiter et relayer les informations relatives à la sécurité ;
- définir les dispositifs de sécurité physiques et de contrôle des accès aux actifs informationnels tout en veillant à leur efficacité ;

Ces messages doivent informer les utilisateurs sur les enjeux de sécurité ; les principales menaces ; les lois et les règlements ; les comportements à adopter.

1.3.4.5. Le Risk Manager

Le Risk Manager (RM) ou le gestionnaire des risques est le coordonnateur du processus de gestion globale des risques d'une organisation. Selon IFA[5] (2010 : 8), il est responsable du recensement et du suivi des risques de celle-ci en mettant en place notamment une cartographie des risques qui est déployée au niveau de chaque direction de l'organisation. Il définira la méthodologie, fournira un support et mobilisera les entités opérationnelles pour la mise en œuvre de la politique de gestion des risques.

Il doit donc intégrer la gestion des risques des systèmes d'information aux pratiques existantes de gestion des risques et en rendre compte périodiquement à la Direction Générale. Selon HORN & al. (in HASSID, 2008 : 74), le risk manager a pour mission de :

- assister les dirigeants dans l'élaboration de la politique de gestion des risques ;
- planifier, d'organiser, d'animer et de contrôler les ressources de son service ;
- assister les responsables opérationnels pour la mise en œuvre locale de la politique de gestion des risques ainsi que pour la définition des responsabilités et actions de leurs subordonnés en matière de sécurité des informations.

1.3.4.6. L'Audit Interne

L'Audit Interne (AI), par ses missions d'assurance, joue un rôle capital en matière de sécurité des SI. En effet, les auditeurs internes sont appelés à fournir à la direction, une assurance indépendante et raisonnable de la pertinence et de l'efficacité des objectifs de sécurité et des contrôles connexes à ces objectifs. Ils doivent se prononcer sur l'état de la sécurité de l'information et rapporter les anomalies significatives à la DG (ISO 27002, 2005 : 13).

Ils doivent également, selon JIMENEZ & al. (2008 : 100) et IFA (2010 : 8), s'assurer que les structures sont claires et bien adaptées, que les procédures comportent les sécurités suffisantes, que les opérations ne présentent pas d'irrégularités et que les informations diffusées sont sincères. Ce qui permettra à la Direction Générale de connaître le niveau de maîtrise des risques.

Ainsi, ils doivent identifier les menaces et ou vulnérabilités qui peuvent causer un préjudice à l'organisation ; évaluer les dispositifs de maîtrise des risques et proposer des mesures d'amélioration tout en s'assurant de leur mise en œuvre.

[5] Institut Français des Administrateurs.

CESAG - BIBLIOTHEQUE

1.3.4.7. Le personnel opérationnel

Selon MENTHONNEX (1995 : 174), dans le domaine de la sécurité des SI, le succès de l'ensemble des mesures de sécurité dépend des actions du personnel opérationnel.

En effet, les opérationnels sont appelés à exécuter les instructions de sécurité de l'organisation dans l'exécution de leurs tâches quotidiennes car ils sont dans la plupart des attaques les maillons faibles de la stratégie de prévention contre les risques liés aux SI.

Il doit respecter les procédures en cas de danger réel ou potentiel. Le personnel doit également signaler toute anomalie rencontrée lors de l'exercice de leurs activités.

1.4. Relation entre le système d'information et le système informatique

CESAG - BIBLIOTHEQUE

Les concepts de système d'information et de système informatique (technologie d'information) doivent être bien distingués. Depuis l'avènement des TIC, une grande confusion est née dans l'appréhension des deux notions. Certains auteurs nous permettent de les discerner.

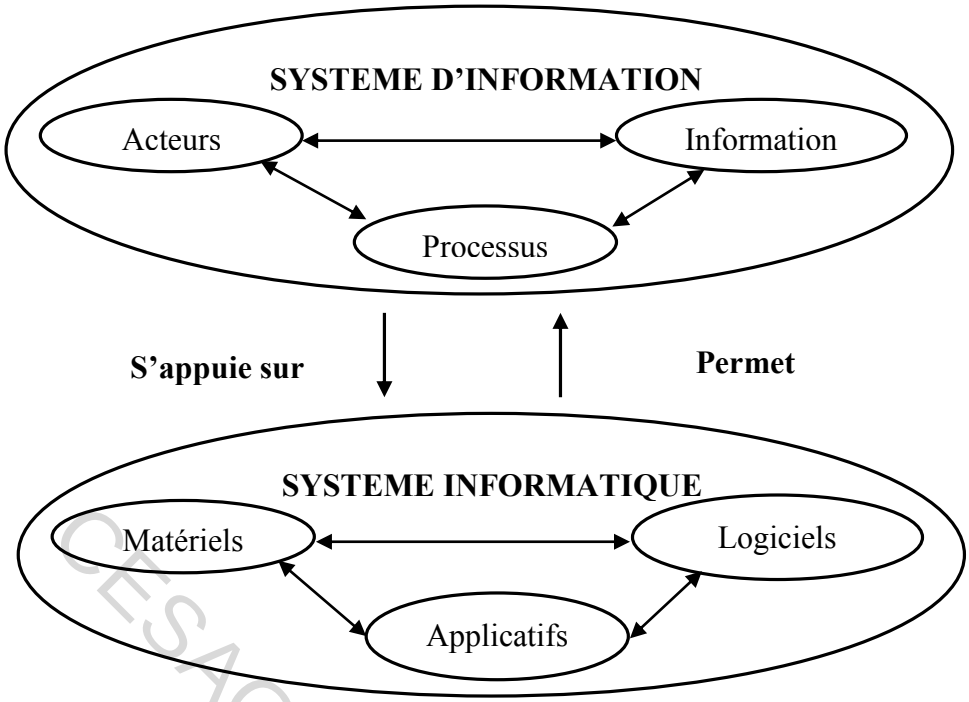
En effet, les précédentes définitions d'un SI (voir pages 8-9) nous permettent d'identifier la différence entre un système d'information et un système informatique ainsi que les relations qui existent entre ces deux systèmes. Alors que le système informatique est un sous ensemble du système d'information, il doit être soutenu par une organisation suffisante.

AUTISSIER & al. (2008 : 48-49) soutiennent que le SI est celui qui traite de l'utilisation de la technologie informatique (système informatique) en entreprise.

En d'autres termes, le système d'information fait le lien entre la technologie informatique et le fonctionnement de l'entreprise alors que le système informatique désigne des machines (ordinateurs, réseaux) et des logiciels.

Nous pouvons ainsi résumer le système d'information à un ensemble intégré de « technologies » et d'« organisation ». La technologie (sa robustesse) dépendra de l'importance des données traitées et des besoins (temps de réponse). L'organisation serait la manière de gérer le SI en mettant en place un ensemble de procédures, de directives, etc. Egalement, le constat qui corrobore la distinction entre le système d'information et le système informatique, c'est qu'un système d'information peut être manuel ou même informel. La figure 4 ci-dessous, reprise de MORLEY & al. (2011 : 26), fait le lien entre le SI et le système informatique.

Figure 4: Système d'Information et Système d'Informatique



Source : MORLEY & al. (2011 : 26).

CESAG - BIBLIOTHEQUE

Donc, le système d'information, pour fournir ou traiter l'information, s'appuie sur le système informatique qui est un ensemble organisé d'objets techniques matériels ou immatériels (logiciels, applicatifs, etc.). Cependant, les technologies de l'information font partie intégrante du système d'information en ce sens qu'il l'aide à atteindre ses objectifs. Elles représentent en d'autres termes l'infrastructure du système d'information.

Conclusion du premier chapitre

La bonne gestion de l'information est source de gains pour toute organisation. À ce titre, la sécurité de l'information est une nécessité. Se protéger de nombreuses menaces qui pèsent sur les actifs informationnels et dont les conséquences peuvent compromettre la continuité de l'activité de l'organisation devient un objectif. Des mesures doivent donc être définies, mises en œuvre, suivies, réexaminées et améliorées afin d'atteindre les objectifs de sécurité. Toutefois, ces mesures doivent s'intégrer harmonieusement avec les autres processus dans le cadre du système de management global de l'organisation. Afin de préciser les exigences de sécurité relatives à l'information, un référentiel normatif doit être élaboré : la politique de SSI.

Ce premier chapitre nous a permis d'avoir des notions sur la SSI, lesquelles nous permettront de mieux appréhender l'audit de la SSI que nous aborderons dans le chapitre suivant.

CHAPITRE 2 : AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE

Introduction

Le contrôle de la conformité des pratiques de sécurité des SI existantes dans une entreprise, d'une part par rapport aux normes, standards et bonnes pratiques en la matière et, d'autre part, par rapport à une éventuelle politique de sécurité propre à l'entreprise, permet d'atteindre les objectifs de disponibilité, d'intégrité et de confidentialité. Il permettra de même de connaître la maturité des processus de sécurité et de savoir qu'elles sont les actions à mener pour une amélioration continue de la sécurité.

L'objectif de ce chapitre est de nous permettre de comprendre les différentes étapes du déroulement d'une mission d'audit de la sécurité des SI. Nous allons aussi focaliser notre attention sur les bonnes pratiques, les normes, les standards et les méthodes en la matière.

CESAG - BIBLIOTHEQUE

2.1. Définition et objectifs de l'audit de la SSI comptable.

A travers cette section, nous aborderons la notion de l'audit de la sécurité des SI. L'examen des objectifs de cet audit nous intéresse de même afin de comprendre, l'importance de telles missions pour les organisations.

2.1.1. Définition de l'audit de Sécurité du SIC

L'audit de la sécurité du SI est l'un des audits appartenant à la famille de l'audit des SI.

Selon l'ISACA (2013 : 53), « l'audit des SI est un processus qui recueille et évalue les preuves afin de déterminer si les SI et les ressources connexes protègent adéquatement les actifs, maintiennent la confidentialité, l'intégrité et la disponibilité des données et des systèmes, fournissent des renseignements pertinents et fiables, atteignent les buts organisationnels de façon efficace, utilisent les ressources efficacement et possèdent des contrôles internes qui offrent, une assurance raisonnable que les objectifs opérationnels, d'entreprise et de contrôle seront atteints et que les évènements indésirables seront évités, ou détectés et corrigés ».

Il ressort que l'audit des SI donne une réponse aux perspectives comme : l'efficacité, l'efficience, la fiabilité, la conformité, la disponibilité, l'intégrité et la confidentialité. Celui de la SSI donne plutôt, une réponse aux trois dernières assertions de sécurité.

2.1.2. Objectifs de l'audit de la sécurité du SIC

Les objectifs de cet audit se distinguent très peu des objectifs classiques d'audit des systèmes d'information et consistent essentiellement à :

- déterminer les déviations par rapport aux bonnes pratiques de sécurité, au fonctionnement opérationnel des procédures et de la cohérence de ces dernières ;
- proposer des actions visant l'amélioration du niveau de sécurité du SIC.

La conformité aux normes internationales, l'utilisation des méthodes de sécurité, de même que l'observation des bonnes pratiques de sécurité conduisent à l'atteinte de ces objectifs.

2.2. Normes, méthodes et outils de l'audit de la SSI

Dans le domaine de la SSI, il existe plusieurs normes, méthodes et référentiels de bonnes pratiques qui permettent aux organisations de disposer d'un ensemble de procédures et de règles afin d'assurer une meilleure sécurisation de leur patrimoine informationnel. Ils constituent donc, des guides méthodologiques, des moyens pour la gestion efficace de la sécurité. Ils servent également d'arsenal pour les praticiens de l'audit de la sécurité des SI.

Dans le cadre de cette étude, nous sommes intéressés à la famille des normes internationales ISO 2700X qui est utilisée soit pour gérer la sécurité de l'information, soit au vu d'une éventuelle certification ou pour l'évaluation des pratiques existantes et à quelques méthodes.

2.2.1. La famille de normes internationales ISO 2700X

Intitulée ''Technologies de l'information-Techniques de sécurité-Systèmes de management de la sécurité de l'information : Vue d'ensemble et vocabulaire'', la famille des normes ISO 27000 est le fruit des réflexions menées sur la sécurité de l'information par de groupes de travail internationaux. Elle est publiée par l'ISO depuis 2005 et présente une vue d'ensemble des Systèmes de Management de la Sécurité de l'Information (SMSI), et aide indéniablement tout type d'entreprise à atteindre les objectifs de sécurité (WHITMAN & al, 2011 : 191).

La version 2012 de cette famille de normes a pour objectifs de proposer des termes et définitions et d'introduire la famille des normes du SMSI. Elle est composée d'une série de normes dédiées à la sécurité de l'information. Sans être exhaustifs, nous allons présenter quelques-unes de ces normes en considérant celle certifiante et celles non certifiantes.

CESAG - BIBLIOTHEQUE

2.2.1.1. Norme certifiante : ISO 27001 « Système de gestion de la sécurité de l'information »

Selon BLOCH & al. (2011 : 23), elle constitue la première pierre de la grande famille de normes internationales ISO consacrées à la sécurité des systèmes d'information. Publiée en 2005 et mise à jour en 2013, la norme ISO 27001 est issue des travaux de l'organisme de normalisation anglais, British Standard Institution (BSI), plus précisément de la norme BS 7799-2 : 1999, intitulé en anglais, Information Security Management Systems - Specifications with guidance. Elle s'appuie sur la méthode PDCA (Plan-Do-Check-Act) ou roue de Deming, avec une formulation « établir, implémenter, maintenir, améliorer ». Elle compte six familles de processus à savoir :

- définir une politique de sécurité des informations ;
- définir le périmètre du système de gestion de la sécurité de l'information ;
- réaliser une évaluation des risques liés à la sécurité ;
- gérer les risques identifiés ;
- choisir et mettre en œuvre les contrôles ;
- préparer un SoA (Statement of Applicability ou DdA pour Déclaration d'Applicabilité en français). Ce document est selon MOISAND & al. (2009 : 15), un cadre de référence qui permet de tracer les mesures qui ont été retenues et celles qui ont été écartées.

Par ailleurs, elle formalise les exigences pour la mise en place d'un SMSI qui est selon CLUSIF (2004 : 2), un ensemble d'éléments interactifs permettant à un organisme d'établir une politique et des objectifs en matière de sécurité de l'information en inventoriant les mesures de sécurité, dans un périmètre défini, afin de garantir la protection des actifs informationnels.

Le SMSI constitue donc un dispositif global de gouvernance de la sécurité de l'information dont l'objectif est de protéger les informations de toute perte, vol ou altération et les systèmes informatiques de toute intrusion afin de donner la confiance aux parties prenantes.

2.2.1.2. Normes non certifiantes

- **ISO 27002 : Code de bonnes pratiques pour la gestion de sécurité de l'information**

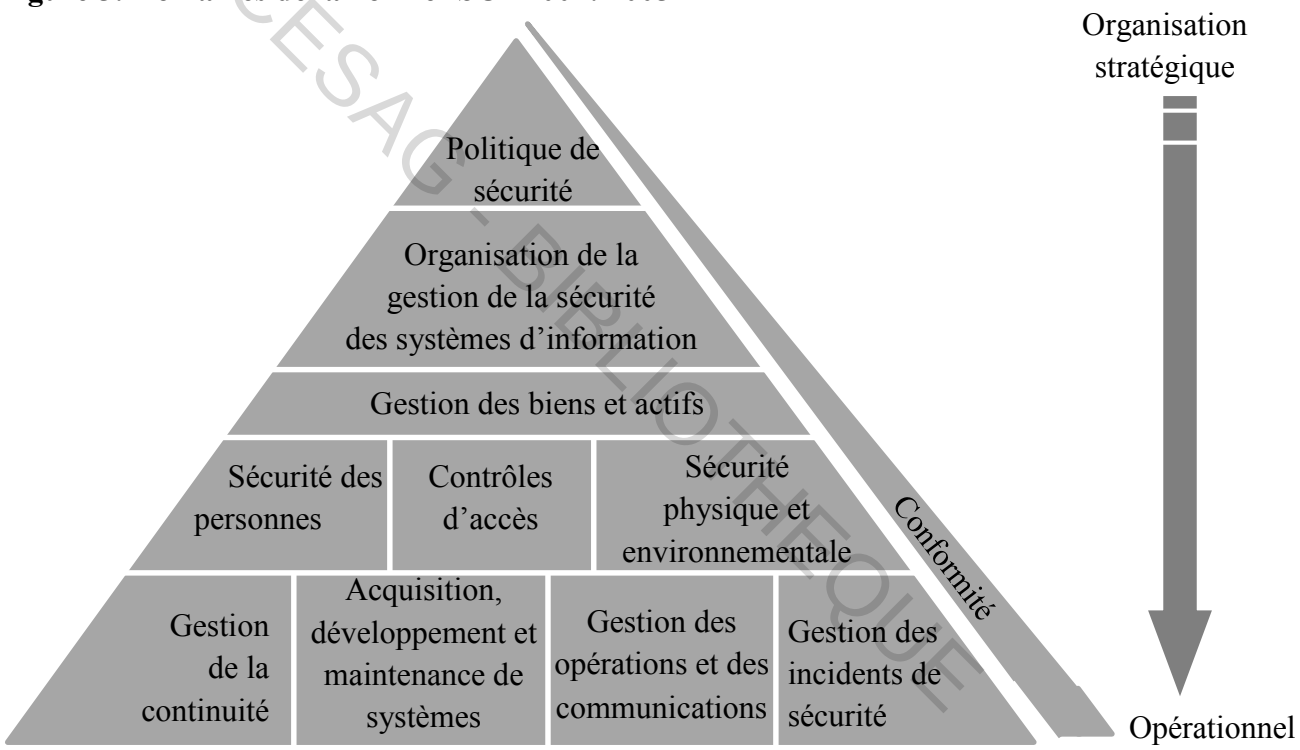
Selon TENEAU & al. (2009 : 75), elle remplace depuis 2005 l'ISO 17799 : Technologies de l'information - Techniques de sécurité - Code de bonnes pratiques pour la gestion de la sécurité

CESAG - BIBLIOTHEQUE

de l'information. Il s'agit selon CARPENTIER (2009 : 22), de la description des bonnes pratiques décrivant les principaux objectifs de contrôle de l'ensemble de la sécurité de l'information.

De façon schématique, la démarche de sécurisation du système d'information selon la norme ISO/CEI 27002 passe par quatre étapes à savoir : la définition du périmètre à protéger (liste des biens sensibles) ; l'identification de la nature des menaces ; l'évaluation de leur impact sur le système d'information et la détection de mesures de protection à mettre en place pour réduire les impacts. Elle comporte ainsi 39 catégories de contrôle et 133 points de vérification répartis en 11 domaines tels qu'illustre la figure ci-dessus.

Figure 5: Domaines de la norme ISO 27002: 2005



CESAG - BIBLIOTHEQUE

Source : EURIWARE (2010 : 9).

❖ L'ISO 27005 : Gestion du risque en sécurité de l'information

La première norme de gestion des risques de la SSI est l'ISO 27005. Cette norme est un guide de mise en œuvre du processus de gestion des risques liés à la sécurité de l'information (PINET, 2012 : 18).

Par une explication détaillée du comment conduire l'appréciation des risques et le traitement des risques, elle aide à la mise en œuvre de la norme ISO 27001. Au-delà des apports

méthodologiques qu'elle représente pour la gestion des risques, elle est enrichie d'annexes qui constituent un outil conséquent pour leur appréciation et leur analyse.

Pour autant, l'ISO 27005 ne constitue probablement pas aujourd'hui une base de scénarios de risques suffisamment exhaustive pour être utilisée. L'aide d'une véritable méthodologie d'analyse de risques (comme EBIOS, MEHARI, COBIT, etc.) et une expertise avancée restent nécessaires.

- **L'ISO 27007 : Guide d'audit du Système de Management des Systèmes d'Information (SMSI)**

La norme ISO 27007 fournit selon ISO (in WHITMAN & al, 2011 : 195) les lignes directrices pour les audits des SMSI ainsi que, des conseils sur la compétence des auditeurs de ces derniers.

Elle inclut aussi les lignes directrices contenues dans la norme ISO 19011 : Lignes directrices pour l'audit des systèmes de management.

Outre la famille des normes ISO 2700X, d'autres méthodes et outils sont utilisés pour gérer de la sécurité des SI.

2.2.2. Méthodes et outils de l'audit de la SSI.

Les méthodes et outils utilisés dans le domaine de la sécurité des SI ont pour auteurs les associations, les groupes de travail, etc. Ces derniers sont souvent composés d'experts internationaux qui fournissent à l'échelle mondiale des méthodes et des outils pouvant aider à évaluer les risques, à contrôler mais également à gérer la sécurité des systèmes d'information.

Nous allons faire un focus sur trois référentiels qui nous paraissent être les plus représentatifs.

2.2.2.1. MEHARI

La MEHARI (Méthode Harmonisée d'Analyse de Risques) est issue de la fusion de deux méthodes que sont MELISA (Méthode d'évaluation de la vulnérabilité résiduelle des SI) et MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux) (MENTHONNEX, 1995 : 361).

Elle est la propriété de CLUSIF. Cette méthode apporte des conseils, fait référence à un cadre méthodologique cohérent et fournit un ensemble d'outils et de bases de connaissance sur des

CESAG - BIBLIOTHEQUE

domaines spécifiques tels que l'analyses des enjeux, l'étude des vulnérabilités, les scénarii de risques, le pilotage de la sécurité de l'information (CLUSIF, 2010).

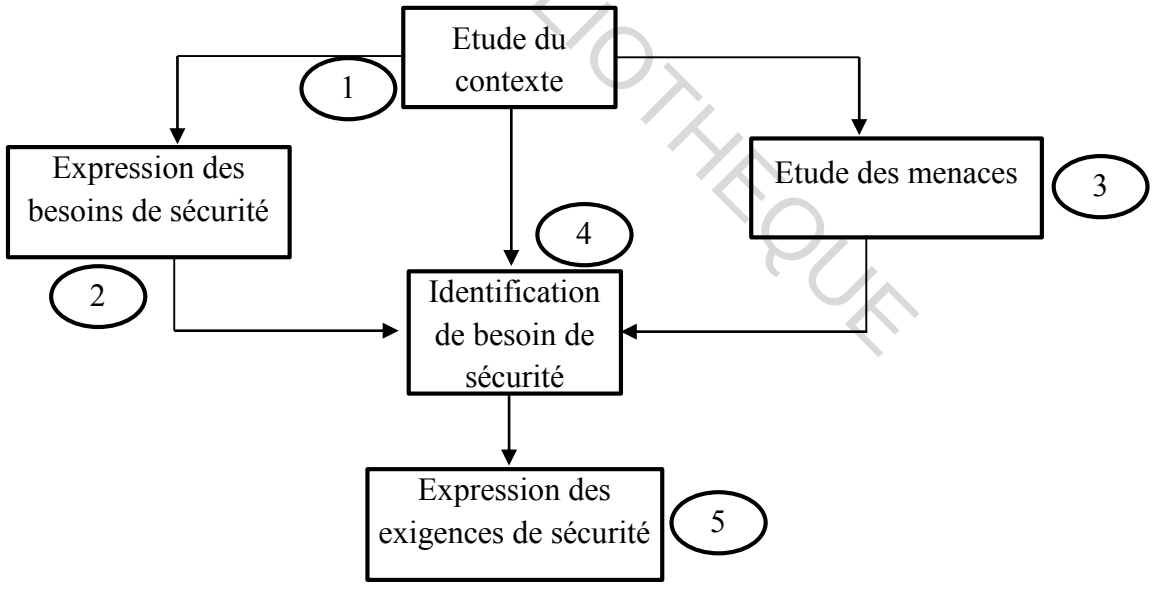
2.2.2.2. EBIOS

La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), est également l'une des méthodes d'analyse des risques SI. Elle est d'origine française. L'ANSSI qui en est l'auteur la présente sous forme de document et de logiciel gratuit. Pour reprendre BLOCH & al. (2011 : 23), EBIOS permet d'apprécier et de traiter les risques relatifs à la SSI et de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires afin de contribuer au processus de gestion des risques de SSI.

Cette méthode apporte toute l'aide nécessaire et indispensable pour juger des mesures de sécurité fonctionnelles et techniques qu'il faudra mettre en place autour du système d'information dans sa démarche de gestion des risques en cinq étapes (figure 7). Elle est aussi un recueil de bonnes pratiques pour élaboration du schéma directeur de la SSI.

CESAG - BIBLIOTHEQUE

Figure 6: Démarche globale de EBIOS



Source : ANSSI (2010 : 13).

La phase principale concerne la méthode d'analyse de l'existant (contexte). Après avoir mené ces différentes analyses, des actions appropriées doivent être mises en œuvre afin de réduire les risques à un niveau acceptable.

2.2.2.3. COBIT

Le COBIT (Control Objectives for Business and Related Technology), est un référentiel complet de principes, de pratiques, d'outils d'analyse et de modèles généralement reconnu qui aident les organisations et les professionnels des SI à aborder efficacement les enjeux critiques en lien avec la gestion et la gouvernance de l'information et de la technologie.

Publié pour la première fois par l'ISACA en 1996 et mis à jour régulièrement (Information Systems Audit and Control Association), ce référentiel se positionne comme une référence en matière de la gouvernance et d'audit des SI. COBIT version 4.1, contient 34 objectifs de contrôle déclinés en processus organisés permettant d'atteindre les objectifs tels que la performance, la confidentialité, l'intégrité et la disponibilité en quatre niveaux ou domaines.

En se référant à TENEAU & al. (2009 :121) et à MOISAND & al. (2009), nous pouvons noter:

- la Planification et l'Orientation (PO) ;

Les objectifs des processus de ce domaine consistent à officialiser l'identification des moyens permettant à l'informatique de contribuer le plus efficacement possible à la réalisation des « objectifs métiers » de l'organisation et de renforcer sa position, c'est-à-dire de s'assurer de l'alignement stratégique des politiques informatiques.

- l'Acquisition et l'Implémentation (AI) :

Le domaine « AI » rassemble tous les processus qui impactent les ressources (applications, informations, infrastructures, personnes). Il va de l'acquisition à la mise en œuvre des solutions informatiques. Il concerne également la réalisation de la stratégie informatique.

- la Distribution et le Support (DS) :

Le domaine « DS » concerne la livraison aux utilisateurs des prestations informatiques requises (gestion de la sécurité, gestion de la continuité de service, assistance aux utilisateurs, etc.). L'auditeur de la SSI se servira particulièrement de la DS5 : Assurer la sécurité des systèmes.

- la Surveillance et l'Evaluation (SE) :

Les processus de ce domaine permettent aux managers d'évaluer la qualité et la conformité des processus informatiques aux exigences de contrôle, ce qui fera appel aux équipes d'audit pour des audits organisationnels, techniques, de qualité, etc.

CESAG BIBLIOTHEQUE

Une analyse de ce référentiel montre que ces domaines constituent des champs de responsabilité et dans chacun d'eux, sont définis : des objectifs de contrôle ; un schéma acteur/tâches qui permet de préciser les différentes responsabilités des acteurs du SI. L'annexe 5 (page 106) résume l'ensemble des processus du CobiT.

L'ensemble des normes, méthodes et outils étudiés ont des objectifs communs, ceux de :

- identifier les besoins de sécurité des SI ;
- étudier le contexte à sécuriser et d'identifier les risques liés aux SI ;
- élaborer des procédures et de mettre en place des dispositifs pour couvrir les risques identifiés ;
- surveiller et de détecter des éventuelles vulnérabilités du système d'information et de mettre en place un système de veille des vulnérabilités ainsi que de définir des actions à entreprendre en cas de détection de menace réelle sur le SI.

Cependant, l'adoption de ces normes, méthodes et outils ne garantit pas systématiquement un meilleur niveau de sécurité. Les managers doivent savoir qu'une sensibilisation des utilisateurs aux bonnes pratiques de sécurité reste incontournable face aux problèmes de sécurité.

2.3. Bonnes pratiques de sécurité

Une entreprise peut se prémunir contre les risques liés à son système d'information et garantir les objectifs de sécurité en prenant en compte en amont l'aspect sécurité.

2.3.1. Définition d'une charte de SSI

Selon LINLAUD (2003 : 45&49), la charte de SSI constitue la traduction concrète des règles décrites dans la Politique de Sécurité des SI (PSSI). Elle a pour objectifs de définir clairement les droits et les devoirs des utilisateurs, d'informer les utilisateurs sur les comportements à risque devant être évités, de les sensibiliser aux enjeux de la sécurité de l'information.

Elle constitue donc un « code de bonne conduite » qui décrit des pratiques comportementales essentielles devant être connues et appliquées par l'ensemble du personnel afin d'assurer l'usage correct et sécurisé du SI de l'organisation. Pour cela, elle doit être établie en respectant les règles de bases telles que : la transparence, la discussion collective, la proportionnalité (mettre en place des dispositifs de sécurité sans pour autant porter atteinte aux libertés individuelles sur le lieux de travail), la sensibilisation et la formation. Elle fait partie intégrante de la stratégie de protection des informations contre toute altération volontaire ou fortuite.

CESAG - BIBLIOTHEQUE

2.3.2. Prise en compte de la sécurité dans les projets SI

Pour BLOCH & al. (2011 : 222), la sécurité doit être prise en compte à toutes les étapes d'un projet (interne ou externe) SI. Pour cela, un dossier de sécurité doit accompagner chaque projet et préciser les enjeux, les méthodes, les mesures préconisées, les jalonnements et les tableaux de bord éventuels.

Il s'agit donc d'intégrer, la sécurité aux besoins fonctionnels que vise à satisfaire le système ou l'application. Pour les projets de conception des programmes propres à l'entreprise la sécurité doit être prise en compte lors de la conception, du développement et du déploiement. En ce qui concerne l'acquisition des solutions sur le marché, les garanties de sécurité doivent être clairement indiquées dans le cahier de charges et réviser lors des différentes phases du projet. Cela est nécessaire car le risque d'avoir des logiciels ou des systèmes qui ne répondent plus d'un jour à l'autre aux besoins ou qui deviennent vulnérables est très élevé avec la course à mettre sur le marché de nouveaux logiciels et l'accélération technologique.

Ainsi, il convient pour l'entreprise de mener des analyses de risques dès la phase de conception et non d'appliquer des « patchs » de sécurité une fois les spécificités fonctionnelles et techniques écrites et validées. Il s'agira pour elle d'être proactif en adoptant la méthode dite de « Security by Design » (adresser les problématiques de sécurité à leur source).

2.3.3. La mise en place d'une Politique de Sécurité des SI

Bien que cela soit difficile à évaluer, l'insécurité a un coût qui se manifeste lors des incidents ou des dysfonctionnements. Face aux risques encourus, il importe de formuler des objectifs de sécurité, d'identifier, d'arbitrer et de mettre en œuvre les parades adaptées au juste niveau de sécurité retenu. Ces actions passent prioritairement par la définition et la mise en place au sein de l'organisation d'une « Politique de Sécurité des Systèmes d'Information (PSSI) »

2.3.3.1. Définition d'une PSSI

La PSSI est, selon PILLOU & al. (2011 : 36), un ensemble d'orientations suivies par une organisation en termes de sécurité des systèmes d'information.

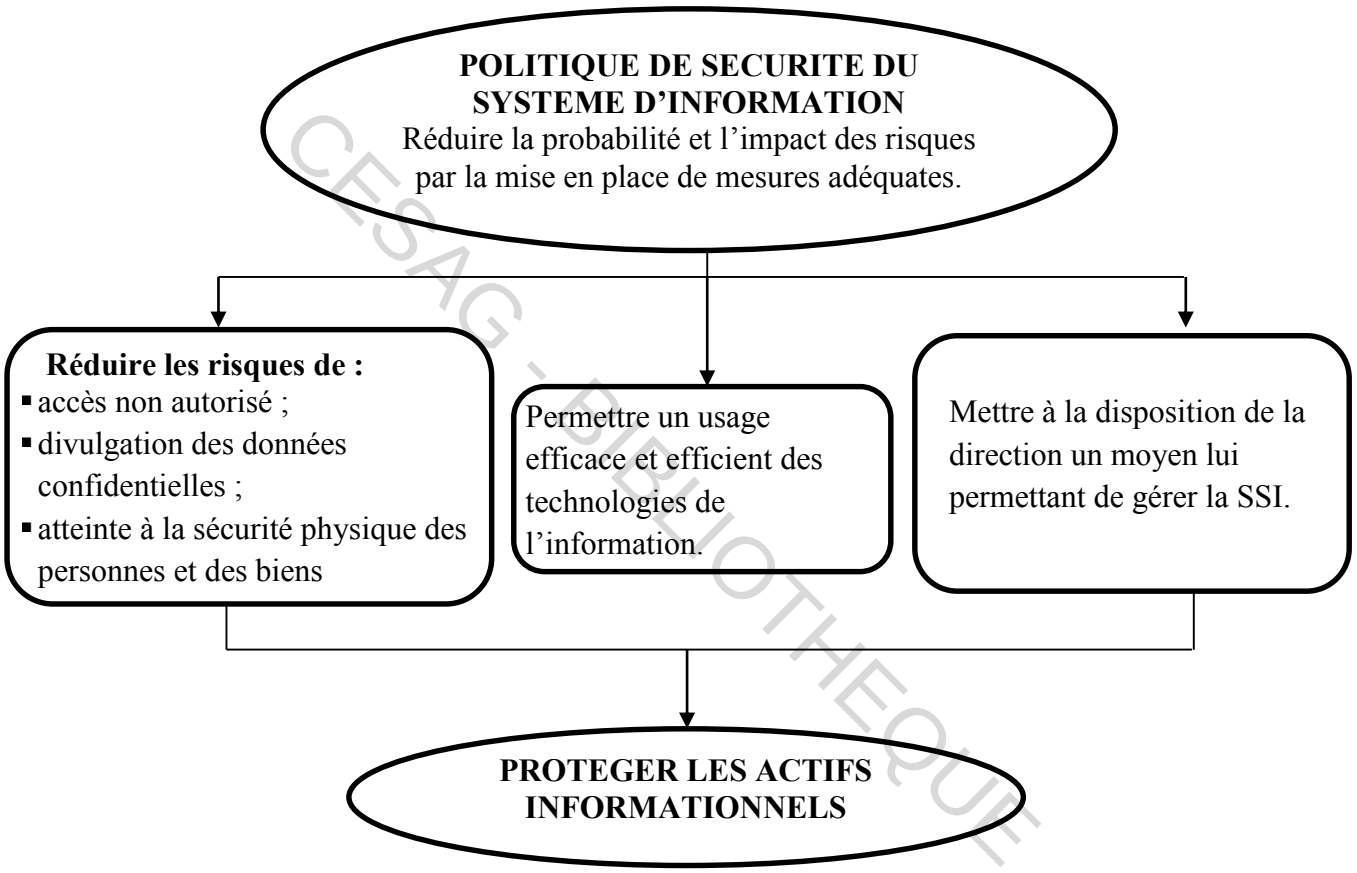
Elle nécessite par conséquent, des actions spécifiques comme nous pouvons l'identifier dans la définition selon laquelle une PSSI est une série d'énoncés qui classifient les risques, identifient les objectifs de sécurité raisonnables en matière de sécurité et indiquent les moyens permettant d'atteindre ces objectifs (LAUDON & al, 2013 : 329).

CESAG BIBLIOTHEQUE

2.3.3.2. Objectifs d'une Politique de SSI

La PSSI a pour objectifs de permettre à une organisation de se doter d'un ensemble de règles organisationnelles, techniques, de codes de conduite et de bonnes pratiques visant à protéger ses biens (infrastructures et actifs critiques). Elle se veut être un document dans lequel la Direction Générale et toute l'organisation manifestent leur engagement clair et ferme en ce qui concerne la gestion de la sécurité. La figure 8 ci-dessous illustre les objectifs d'une PSSI.

Figure 7: Les objectifs d'une Politique de SSI



CESAG - BIBLIOTHEQUE

Source : Nous-mêmes à partir de ISO 27002 (2005 : 6).

Les besoins de sécurité s'appliquent aussi bien aux ressources du SI qu'aux données. Cependant, il serait inutile, utopique et coûteux de protéger avec les mêmes niveaux de sécurité toutes les informations de l'organisation. La hiérarchisation des informations est donc la base de leur sécurisation. La PSSI est spécifique à chaque organisation.

Selon IFACI (1993 : 9), il est important que les préoccupations propres à l'organisation soient reflétées dans les politiques et conformes aux normes de sécurité. Il est enfin important qu'une communication suffisante soit faite au personnel en ce qui concerne les clauses de la PSSI afin de lui donner un impact considérable.

2.3.4. Sensibilisation et formation des utilisateurs

La clé de voûte d'une politique de sécurité efficace reste la dimension humaine (maillon le plus faible) de l'entreprise car la méconnaissance ou la non application des procédures, les erreurs ou la malveillance peuvent être à elles seules la cause de dysfonctionnement ou de vulnérabilités (CARPENTIER, 2009 : 41).

Ainsi, lorsque les comportements sont inadaptés, toutes les mesures techniques et organisationnelles seront vaines parce que contournées et pour reprendre l'adage anglais «There is no patch for human stupidity ».

Il est donc primordial que les utilisateurs comprennent l'importance des informations qu'ils manipulent et ou des ressources qu'ils utilisent. Ils doivent aussi disposer d'une documentation suffisante et mise à jour régulièrement décrivant les politiques et les procédures de sécurité. De même, leurs responsabilités doivent être clairement définies.

2.3.5. Mise en place d'un plan de reprise d'activités

Selon DAYAN & al. (2004 : 1038), le plan de reprise permet généralement de minimiser fortement les effets dommageables des évènements constatés (pannes, attaques, accidents, etc.).

Il a donc pour objectif de permettre à une organisation de continuer à offrir ses services essentiels, advenant une perturbation. Cependant, il dépend des besoins en information de l'organisation pour ses activités. Ces besoins sont exprimés en fonction de la RTO (Recovery Time Objective) et de la RPO (Recovery Point Objective) de l'organisation (annexe 4, page 105). Le premier traduit la durée maximale d'interruption admissible. Il s'agit du temps maximal acceptable pendant lequel une ressource informatique (serveur, réseau, ordinateur, application, etc.) peut ne pas être fonctionnelle suite à son interruption. Implicitement, le RTO indique selon KEREBEL (2009 : 64), le niveau d'impact que le métier accepte de supporter.

Le second désigne la durée maximale d'enregistrements des données qu'il est acceptable de perdre lors d'une panne. La quantification du RPO aide à définir les objectifs de sauvegarde.

Les auditeurs de la SSI ne peuvent valablement se prononcer sur la conformité ou la non-conformité des pratiques d'une organisation par rapport à ces bonnes pratiques que par une mission d'audit de la SSI suivant un processus bien défini.

CESAG - BIBLIOTHEQUE

2.4. Processus de conduite d'une mission d'audit de sécurité d'un SIC

Comme tout audit, celui de la SSI, suit généralement trois phases à savoir celle de la planification, d'exécution et de conclusion de la mission.

2.4.1. Phase de planification de la mission d'audit

Cette phase est celle qui marque le début de la mission. Les actions sont régies par la norme d'audit et d'assurance des SI 1201 : planification de la mission de l'ITAF (Information Technology Assurance Framework). Elle constitue une phase importante qui est enclenchée dès la réception par l'auditeur de la lettre de mission s'il s'agit d'un intervenant externe et de l'ordre de mission s'il s'agit d'une mission d'audit interne.

En effet, dans le cadre d'une mission d'audit interne de la SSI, la planification est régie par la norme 2200 de l'IIA (in IFACI, 2013 : 52) selon laquelle : « les auditeurs internes doivent concevoir et documenter un plan pour chaque mission. Ce plan de mission précise les objectifs, le champ d'intervention, la date et la durée de la mission, ainsi que les ressources allouées ».

L'auditeur de la SSI aura donc à définir un plan d'approche en tenant compte des tâches de prise de connaissance du système à auditer ; de décomposition du système en éléments plus facile à conceptualiser, d'identification des risques et de définition des objectifs de la mission. Ces tâches lui permettront d'élaborer le référentiel de la mission.

2.4.1.1. Prise de connaissance de l'entité ou de la structure auditée.

Elle est l'une des plus importantes étapes d'une mission d'audit de la SSI, car elle permet d'avoir une vue d'ensemble de la structure objet de la mission, des dispositifs de contrôle mis en place, d'identifier les risques et de définir les objectifs.

Pour RENARD (2013 : 206-207), l'auditeur doit préparer sa prise de connaissance en élaborant un Questionnaire de Prise de Connaissance (QPC).

L'auditeur aura à se faire communiquer les documents à jour sur les méthodes et procédures de travail, les rapports et les comptes rendus antérieurs, les notes relatives à des modifications récentes ou à venir dans l'organisation, les responsabilités et l'environnement informatique. Il procédera, si nécessaire à des entretiens et interviews préliminaires avec les responsables du domaine audité.

CESAG - BIBLIOTHEQUE

In fine, la prise de connaissance permet à l'auditeur de la SSI de décomposer le sujet en « objets auditables », d'identifier et d'évaluer les risques, de rédiger le rapport d'orientation de la mission et par la suite le programme de vérification (LEMANT, 2003 : 24-25).

2.4.1.2. Décomposition du SIC en « objets auditables »

Il s'agit de découper le processus SIC en activités ou opérations élémentaires plus simple à appréhender et à étudier comme le recommande DESCARTES (in SCHICK, 2010 : 99) : « diviser chacune des difficultés…en autant de parcelles…qu'il serait requis pour mieux les résoudre ».

Les objets auditables constituent donc la base d'élaboration du référentiel d'audit.

2.4.1.3. Identification et évaluation des risques : élaboration du tableau de risques

Selon les normes 2201 de l'IIA (in IFACI, 2013 : 52) et 1202 de l'ITAF, l'auditeur interne doit identifier et évaluer les risques pertinents liés à l'activité à auditer en planifiant sa mission.

Ces tâches sont également indispensables en audit de la sécurité des SI. En se référant à RENARD (2013 : 220), pour l'élaboration de ce référentiel, il s'agira pour l'auditeur de la sécurité des SI d'identifier selon la décomposition qui est fait du système d'information en objets auditables, et pour chacun d'eux : les objectifs de contrôle interne et les risques inhérents associés à chaque objectif.

Pour discerner les risques, l'auditeur interviewera les principaux responsables pour comprendre les spécificités et les fonctionnements sans vérifications sauf pour s'assurer qu'il a bien compris. Souvent il établira des « diagrammes de circulation » des informations ou des documents, et les validera avec les responsables concernés (LEMANT, 2003 : 25).

Par ailleurs, pour chaque risque (inhérent) identifié, il va falloir :

- déterminer sa criticité par une appréciation de ses impacts et de sa probabilité ;
- identifier les dispositifs de sécurité existante ou que l'on devrait trouver en bonne logique (bonnes pratiques) et qui garantiraient l'atteinte des objectifs de sécurité.

L'analyse de l'existence des dispositifs ou de bonnes pratiques de sécurité dédiés à la maîtrise de chacun des risques permet à l'auditeur de déterminer les tests ou les points sur lesquels il

CESAG - BIBLIOTHEQUE

doit mener des diligences. Elle constitue ainsi, le point de départ de l'élaboration de son rapport d'orientation.

2.4.1.4. Rapport d'orientation ou référentiel d'audit

Selon SCHICK & al. (2010 : 115), l'auditeur doit élaborer un rapport d'orientation ou référentiel d'audit présentant les objectifs et les zones à risques qu'il doit examiner. Le but de ce document n'est donc pas de décrire les travaux ou techniques spécifiques, mais de préciser les points qui feront l'objet d'analyse au cours de la mission. Il constitue donc une sorte de contrat entre les audités et l'auditeur.

Le rapport d'orientation permet dans la phase de planification de définir et de formaliser les axes ou les grandes lignes d'investigation de la mission et ses limites en les exprimant en objectifs à atteindre par l'audit. Ces objectifs doivent être discutés avec les responsables du SI.

Les objectifs se déclinent selon ISACA (2013 : 58) en objectifs généraux (s'assurer de la sécurité des actifs informationnels, de la fiabilité des informations comptables, du respect des règles et des directives, ainsi que de l'optimisation des ressources) et en objectifs spécifiques (il s'agit de préciser de façon concrète les différents points de contrôle qui vont être analysés, qui tous contribuent à la réalisation des objectifs généraux et qui tous se rapportent aux zones à risques ultérieurement identifiées).

Ainsi, le rapport d'orientation doit faire l'objet d'une validation par les responsables de la sécurité du SI, et ce, afin de canaliser leur adhésion. Il constitue de ce fait, la base l'élaboration du programme de vérification.

2.4.1.5. Elaboration du programme de vérification

Selon la norme 2240 de l'IIA (in IFACI, 2013 : 55), les auditeurs internes doivent élaborer et documenter un programme de travail permettant d'atteindre les objectifs de la mission.

Ce programme doit faire référence aux procédures à appliquer pour identifier, analyser, évaluer et documenter les informations lors de la mission. Le programme de travail doit être approuvé avant sa mise en œuvre. Les ajustements éventuels doivent être approuvés rapidement (norme 2240.A1 et MPA[6] 2240-1 de l'IIA).

[6] Modalités pratiques d'Application

CESAG BIBLIOTHEQUE

Le programme de vérification représente donc, la base de la phase d'exécution de la mission en ce sens qu'il décrit les travaux d'audit à accomplir et qui permettront à l'auditeur d'atteindre les objectifs décrits dans le rapport d'orientation. L'auditeur procédera également à la détermination des techniques et outils notamment l'entretien, le sondage statistique, etc.

2.4.2. Phase d'exécution de la mission d'audit : mise en œuvre du programme de vérification

Elle consiste au déroulement effectif de la mission sur le terrain. La réunion de lancement avec les audités marque son début. Au cours de cette phase l'auditeur de la SSI mettra en œuvre son programme de vérification et si besoin l'actualiser.

Selon la norme 2300 de l'IIA (in IFACI, 2013 : 55), dans la phase d'accomplissement de la mission, les auditeurs internes doivent identifier les informations suffisantes, fiables, pertinentes et utiles pour atteindre les objectifs de la mission.

Il s'agit donc de dérouler les points de contrôle du référentiel validé en évaluant les pratiques de l'organisme sur la base des règles, des procédures et des bonnes pratiques du référentiel. Cette étape se manifeste par l'évaluation du contrôle interne, la réalisation des tests ; lesquelles aboutiront à la collecte des éléments probants, base de la formalisation des constats dans des Feuilles d'Analyse de Risques (FAR) et dans des feuilles de couverture de test.

2.4.2.1. Evaluation du contrôle interne

L'évaluation du contrôle interne permet à l'auditeur de compléter sa prise de connaissance de l'environnement de contrôle et des procédures de contrôle, d'évaluer les risques d'échec des contrôles et de non détection. L'objectif consiste à vérifier l'existence et l'efficacité des contrôles définis dans le référentiel d'audit et de s'assurer que les audités sont conscients des risques liés aux SI (ISACA, 2013 : 58).

Afin de fonder leurs conclusions et les résultats de leur mission sur des analyses et évaluations appropriées, les auditeurs internes et ceux de la SSI en occurrence peuvent recourir à des procédures analytiques, à des analyses causales, etc. qui constituent souvent des moyens efficients et efficaces pour obtenir des preuves d'audit. L'évaluation résulte de la comparaison d'une information avec des résultats attendus ou définis par l'auditeur interne alors que l'analyse causale consiste à rechercher l'origine d'un problème, au lieu de simplement le constater ou en rendre compte (MPA 2320 de l'IIA (in IFACI, 2013 : 199-200).

CESAG - BIBLIOTHEQUE

Bien que les normes ne décrivent pas clairement les outils à utiliser, nous considérons que les entretiens, l'analyse documentaire et le Questionnaire de Contrôle Interne (QCI) pourront également servir à l'auditeur des SI.

2.4.2.2. Tests de confirmation et de corroboration

Ils sont nécessaires du fait de la dématérialisation des écritures ou des documents comptables. Les tests de conformité (tests de procédures) permettent de recueillir des preuves en identifiant primo, les contrôles clés qui doivent faire l'objet de tests et secundo, effectuer les tests proprement dits sur la fiabilité, la prévention des risques et le respect des politiques et des procédures de l'organisation (ISACA, 2013 : 57&59).

Ils permettent ainsi, d'appréhender le chemin de l'information, de s'assurer de l'exhaustivité, de la réalité et de la fiabilité des données. Par contre, les tests de corroboration consistent à recueillir les preuves pour évaluer l'intégrité des transactions individuelles, de données ou d'autres renseignements. Les tests de corroboration fournissent des preuves de la validité et de l'intégrité des données contenues dans le système d'information.

Selon CANNON (2008 : 99), pour cette étape, l'auditeur peut se servir des techniques comme l'échantillonnage, les recoupements des données, etc. afin d'obtenir des éléments probants.

2.4.2.3. Obtention des éléments probants

L'obtention des éléments probants au cours de la mission d'audit de la sécurité des SI constitue un défi pour l'auditeur, car il ne peut jamais baser ses constats sur des hypothèses ou des intuitions. Il doit disposer de la preuve pour chacune de ses déclarations.

Selon ISO/CEI 27002 (2005 : 99), il convient que l'auditeur de la sécurité des SI obtienne un nombre suffisant et adéquat d'éléments probants en mettant au point et en appliquant des procédures afin de tirer des conclusions raisonnables sur lesquelles il basera les résultats de l'audit.

L'obtention de ces éléments probants repose sur la compréhension et l'évaluation des contrôles internes ainsi que des résultats des tests de confirmation et de corroboration. Avec les résultats de l'évaluation du contrôle interne et des tests, l'auditeur formalise son travail dans des FAR et des feuilles de couverture de tests.

CESAG BIBLIOTHEQUE

2.4.2.4. Formalisation des travaux : établissement des FAR et des feuilles de couverture de tests.

Selon LEMANT (2003 : 26), au fur et à mesure que l'auditeur effectue ses vérifications, il doit les conclure. Ses vérifications révèlent soit qu'il n'y a pas de problème (risque ou dysfonctionnement), soit qu'il y en a un et il va alors établir une FAR (Feuille d'Analyse de Risque). De même il doit renseigner ses fiches de couverture de test. Ces documents seront présentées aux principaux responsables concernés afin d'enregistrer leurs réactions.

Cependant, contrairement aux FAR qui sont établis au fur et à mesure qu'un risque est identifié, les feuilles de couverture sont établi en deux temps : il s'agit de décrire dans un premier temps les modalités de mise en œuvre du test défini dans le programme de vérification et dans un second, mettre en évidence les conclusions qui en ont été tirées. L'ensemble de ces documents constituera la base du projet de rapport de l'auditeur. Pour cela, ils doivent être suffisants, fiables, pertinents et utiles pour fournir une base saine et sûre aux constats et aux recommandations (SCHICK & al, 2010 : 118&125).

2.4.3. Phase de conclusion ou de rédaction de rapport

Selon la norme 1401.1 de l'ITAF, les professionnels de l'audit et de l'assurance des SI doivent produire un rapport à l'achèvement de la mission, leur permettant de communiquer les résultats. Les activités de cette phase consistent à ordonner les résultats des évaluations sous forme de rapport.

Dans le cadre d'une mission d'audit interne de la sécurité des SI, elle est régie par la norme 2400 de l'IIA. En effet, selon MPA 2400-1 de l'IIA (in IFACI, 2013 : 217) les auditeurs internes rassemblent des preuves, émettent des jugements fondés sur des analyses, rendent compte des résultats.

L'auditeur à la fin de sa mission élaborera donc un projet de rapport puis un rapport final. Alors qu'elle est la différence entre un projet de rapport et un rapport final d'audit?

2.4.3.1. Le projet de rapport

Le « projet de rapport » est le document qui formalise les constats et recommandations de l'auditeur. Il constitue un relevé des lacunes, des faiblesses, des dysfonctionnements constatés au cours de la mission, évalués et hiérarchisés en fonction du degré de gravité des conséquences qu'ils induisent mais également les forces.

CESAG - BIBLIOTHEQUE

Le projet de rapport doit son nom du fait que l'auditeur n'a pas encore fait valider ses constats aux audités, du fait de l'absence de réponse de la part des audités par rapports aux différentes recommandations et du fait de l'absence de plan d'action. Il peut se présenter soit sous forme d'un simple relevé des FAR classées de façon logique et par ordre d'importance soit selon le format du rapport final (SCHICK & al, 2010 : 136).

2.4.3.2. Le rapport final

Selon RENARD (2013 : 275), le rapport final d'audit est celui qui prend en compte les constats, les recommandations validées et éventuellement les commentaires des audités.

A cet effet, il représente un document d'information à l'attention des commanditaires de la mission quant au degré de la sécurité du système d'information objet d'audit, et un outil de travail pour les audités du fait qu'il constitue la base d'élaboration du plan d'actions.

2.4.4. Activités de suivi

La norme d'audit et d'assurance S8 de l'ISACA stipule, « après édition d'un rapport sur les conclusions et les recommandations, l'auditeur des SI doit solliciter et analyser des informations pertinentes pour les évaluer si les mesures adéquates ont été prises par les dirigeants dans les délais impartis ».

Les auditeurs en SI doivent s'assurer de la mise en œuvre des actions ayant trait aux différentes recommandations formulées dans le rapport d'audit.

2.5. Les différents aspects d'audit de la sécurité des SI

L'audit de la SSI peut être mené sous différents angles selon les objectifs que les commanditaires veulent atteindre. Le CLUSIF (in LAUDON & al. 2013 : 324) a identifié dans son rapport de 2010, trois principaux types d'audit et ou de contrôle visant à tester et à améliorer la sécurité des SI : les vérifications de l'organisation et des procédures de sécurité, vérification des configurations techniques et les tests d'intrusion des réseaux.

2.5.1. Audit organisationnel et physique

Cet audit a pour objet d'évaluer les pratiques de la sécurité de l'entreprise sur le plan organisationnel et physique. Egalement, il concerne l'évaluation de la maturité des mesures mises en place pour assurer la sécurité du personnel et des biens.

CESAG - BIBLIOTHEQUE

2.5.2. Audit technique

Cet aspect de l'audit de la SSI tient compte de la capacité du système d'information à permettre l'atteinte des objectifs de sécurité à travers l'identification des vulnérabilités. Pour cela l'auditeur se servira des outils techniques qu'il maîtrise. Son objectif est de permettre à l'auditeur SI, de confirmer ou d'infirmer les propos recueillis lors de l'audit organisationnel et physique afin de déceler les écarts sur lesquels il pourrait formuler ces recommandations.

2.5.3. Audit intrusif

L'audit intrusif encore appelé test d'intrusion ou piratage éthique constitue un aspect particulier de l'audit des SI. Selon ISACA (2013 : 422) et BLOCH & al. (2011 : 252), il s'agit pour l'auditeur de la sécurité des SI d'utiliser les mêmes techniques qu'un pirate pour perpétrer une intrusion afin de détecter les failles du système à protéger. En d'autres termes, il consiste à attaquer son système de protection (pare-feu, antivirus, réseau, etc.) puis à obturer les brèches que l'on aura détectées.

En effet, il nécessite une compétence très pointue notamment en réseau, car son objectif est de stimuler une intrusion possible dans le SI de l'entreprise. La compétence demandée concerne le fait que ce test ne doit pas empêcher l'entreprise de fonctionner. Les auditeurs doivent tenir également compte du respect des limites de la mission sous peine de sanction.

CESAG - BIBLIOTHEQUE

Conclusion du deuxième chapitre

L'audit de la sécurité d'un SI permet à une organisation d'avoir des informations sur les menaces qui pèsent sur ses actifs informationnels et dont leur réalisation peut impacter ses finances et/ou son image et de disposer des actions à mettre en œuvre pour renforcer sa sécurité.

Nous avons appréhendé à travers ce chapitre les objectifs d'un audit de sécurité des SI, les normes, outils et méthodes qui servent à l'auditeur de la sécurité des SI et dont les plus utilisés sont : la famille des normes 2700X, les méthodes EBIOS, MEHARI et COBIT. Ces derniers permettent de faire des évaluations périodiques des mesures de sécurité physiques et logiques en tenant compte sans doute de la cohérence de la PSSI afin de garantir la disponibilité, l'intégrité, la confidentialité, la non répudiation et la traçabilité des informations sensibles.

Nous avons également, passé en revue les bonnes pratiques et les types d'audit de sécurité des SI. Par ailleurs, nous avons analysé les différentes étapes d'une mission d'audit de la SSI lesquelles nous aideront à décliner la méthodologie de notre étude.

CHAPITRE 3 : METHODOLOGIE DE L'ETUDE

Introduction

L'audit de la sécurité des systèmes d'information est une mission dont la condition sine qua none pour sa réussite est la définition d'une méthodologie cohérente. Cette dernière constitue le cadre de référence sur lequel l'auditeur doit s'appuyer. Elle permet d'établir une suite d'actions à effectuer, de questions à se poser, de choix à faire, etc. Ce cadre aide également l'auditeur à obtenir des résultats démontrables et qui peuvent être reproduits ou vérifiés par une tierce personne externe à la mission. Autrement, c'est la systématisation de la mission afin de la mener de la manière la plus efficace possible.

Ce chapitre est consacré à la présentation du modèle d'analyse ainsi que la description des différents outils et techniques que nous aurons à utiliser.

CESAG - BIBLIOTHEQUE

3.1. Modèle d'analyse

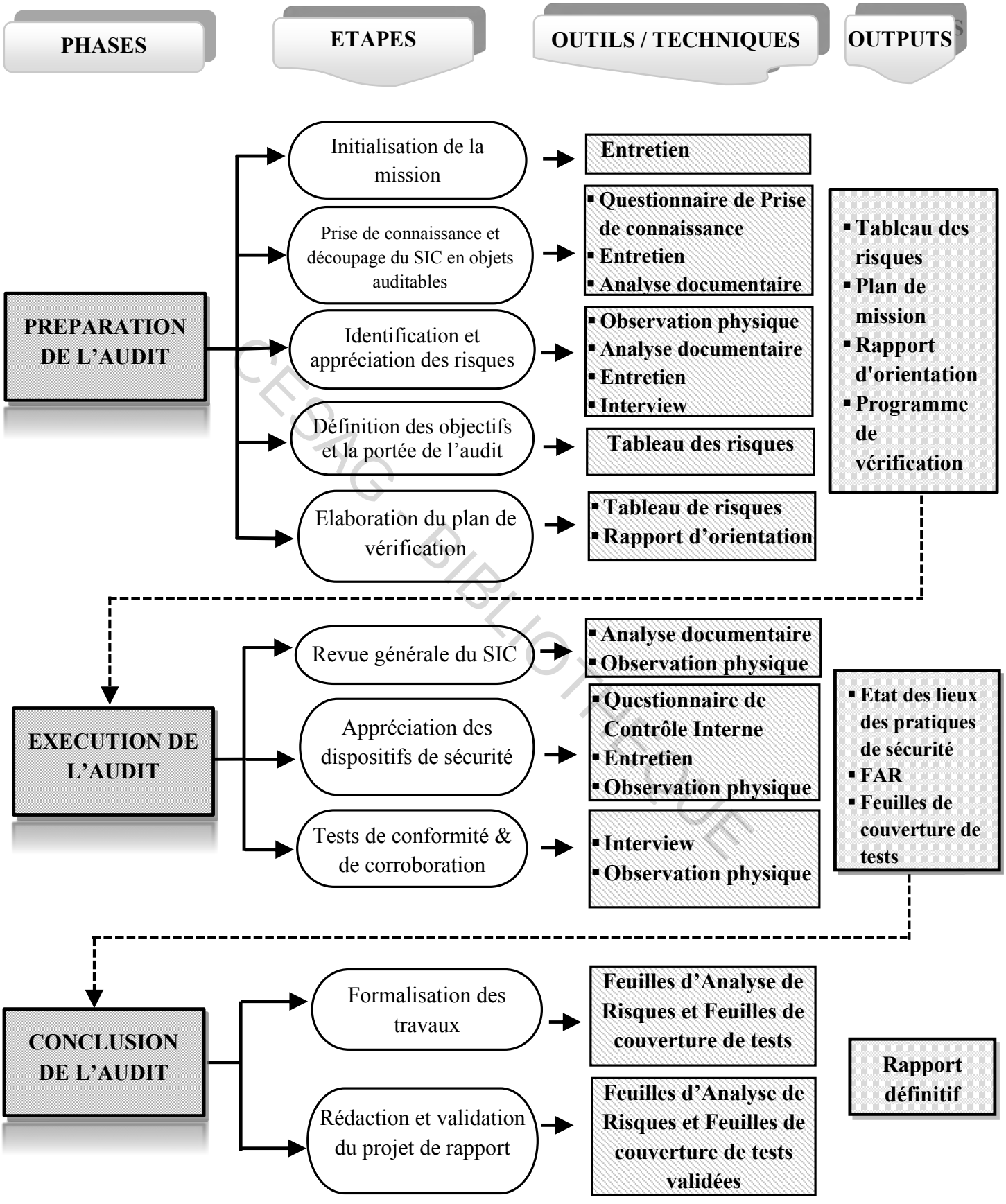
Le modèle d'analyse est pour nous une représentation schématique des différentes étapes méthodologiques à respecter pour l'efficacité de notre étude sur l'audit de la sécurité du système d'information comptable.

Nous le déclinons en trois phases : phase de la planification de l'audit, de son exécution et celle de sa conclusion. Chacune de ces phases est subdivisée en étapes auxquelles nous associons des outils et/ou techniques permettant la collecte et l'analyse des données.

Dans la panoplie de méthodes qui aident le praticien de l'audit de la sécurité de l'information, nous avons opté pour l'approche basée sur l'analyse des risques liés à la sécurité des SI de la norme ISO 27005 que nous allons coupler avec la méthodologie de la sécurité des systèmes d'information, telle décrite par l'ISACA.

De manière schématique, notre modèle d'analyse se présente comme suit :

Figure 8: Modèle d'analyse



Source : Nous-mêmes.

3.2. Les outils de collecte et d'analyse de données

Cette section décrit les outils que nous allons utiliser au cours des différentes étapes de notre démarche d'étude aussi bien pour la collecte des données que pour leur l'analyse.

3.2.1. Etape d'initiation de la mission

Pour cette étape il s'agira pour nous d'entretenir avec les responsables de la LONASE et du SIC notamment le Directeur des Ressource Humaines (DRH), le Directeur de l'Audit Interne et de la Qualité (DAIQ), la Directrice Financière et Comptable (DFC) et le Directeur des Systèmes d'Information et de l'Exploitation (DSIE). L'intérêt est de porter à leur connaissance l'objet de notre étude afin d'avoir leur approbation avant le démarrage de la mission.

3.2.2. Etape de prise de connaissance de la LONASE et de son SIC

L'objectif de cette étape est d'avoir des informations sur la LONASE en général et d'appréhender le SIC en particulier afin d'organiser nos travaux. Pour cela, nous utiliserons des outils comme le questionnaire de prise de connaissance, l'entretien et l'analyse documentaire.

3.2.2.1. Le questionnaire de prise de connaissance

Nous utiliserons le QCP (annexe 7, page 108), pour avoir une bonne compréhension du fonctionnement général de la LONASE et de l'environnement de la sécurité du SIC. Il nous servira de socle pour les questions que nous aurons à poser dans le cadre de l'évaluation du contrôle interne du SIC. Ce questionnaire sera administré face à face auprès de la DFC, du DAIQ et du DSIE et du DRH.

3.2.2.2. L'entretien

L'entretien est une technique qui nous aidera à échanger avec la DFC, le DSIE et les chefs des services de la Direction Financière et Comptable. Pour reprendre IFACI (2013 : 50), ces échanges nous permettront de construire une relation de travail positive avec les audités. En effet, au cours de ces entretiens et à l'aide d'un guide d'entretien (annexe 9, page 115), nous allons poser des questions susceptibles de nous aider à comprendre le SIC.

3.2.2.3. L'analyse documentaire

Il s'agit pour nous de consulter des documents internes (le règlement intérieur, le manuel de procédures administratives, financières et comptables, la politique de sécurité des SI, les notes

CESAG - BIBLIOTHEQUE

relatives à des modifications récentes ou à venir dans l'organisation du SIC, les rapports des audits antérieurs, etc.) ou externes (les articles, les lois et règlements qui régissent le secteur, etc.) à la LONASE en vue de recueillir des informations qui peuvent nous permettre de faire le rapprochement entre les écrits et les pratiques à la LONASE.

Nous aurons à consulter également, les écrits théoriques et les travaux des experts dans le domaine de la SSI ainsi que les normes et les bonnes pratiques en la matière.

3.2.3. Etape d'identification et d'appréciation des risques liés au SIC

Cette étape est prépondérante pour notre étude non seulement à cause de l'approche que nous avons retenue, mais aussi parce qu'elle nous permettra d'avoir une idée sur le niveau de vulnérabilité du SIC et d'identifier les zones sur lesquelles nous aurons à porter plus d'attention. Ainsi, pour l'analyse des informations que recueillerons au cours de cette étape, nous nous servirons : de l'observation physique, de l'interview et de l'analyse documentaire. Les informations seront synthétisées dans un tableau (de risques) (voir annexe 10, page 117).

3.2.3.1. L'analyse documentaire

Nous procéderons à l'aide de cette technique à l'identification des objectifs fixés en ce qui concerne le SIC. Cette analyse nous permettra d'identifier sans assurer leur exhaustivité, les événements susceptibles de compromettre l'atteinte de les objectifs de sécurité du SIC. Elle portera spécialement sur la cartographie des risques, le manuel de procédures administratives, financières et comptable, le plan de continuité des activités, le plan de reprise et éventuellement tout document interne ou externe (lois et règlements en vigueur) qui nous sera accessible.

3.2.3.2. L'interview

L'interview a pour objectif d'une part de favoriser à travers des questions « ouvertes », l'appréhension des différents processus à travers leurs objectifs, la nature des tâches exécutées, les difficultés rencontrées, les documents utilisés dans l'organisation. D'autre part, l'interview selon SCHICK & al. (2010 : 185) permet à l'auditeur de se forger une première opinion sur le niveau de risque. Nous allons interviewer les agents « clés » du SIC en utilisant surtout les questions ouvertes de notre guide d'entretien (annexe 9, page 115). Spécifiquement nous interviewerons avec l'accord de leur responsable, au moins trois (3) agents de chacune des directions suivantes : la DFC, de la DAIQ, DSIE.

CESAG - BIBLIOTHEQUE

3.2.3.3. L'observation physique

L'audit de la SSI est une mission qui consiste à la recherche des faits et pour cela en plus d'écouter, nous jugeons aussi important d'observer les pratiques. Cette observation nous permettra d'identifier les problèmes qui ne sont pas connus, ou qui ne peuvent être déduits de l'analyse documentaire. Nos observations physiques seront directes et porteront sur les pratiques de sécurité des agents dans l'exécution de leurs tâches quotidiennes, par exemple les contrôle à l'entrée des locaux, le déroulement de l'opération d'attribution des droits d'accès, les dispositifs de sécurité, les comportements.

3.2.3.4. Le tableau de risques

Le tableau de risques (annexe 10, page 117) est un outil à l'aide duquel nous allons formaliser les risques liés à l'environnement du système d'information comptable ou aux opérations et qui sont identifiés avec les outils et techniques décrits précédemment. L'appréciation se fera en fonction du degré d'exposition (faible, moyen ou élevé) des actifs informationnels.

3.2.4. Etape d'élaboration du plan d'approche

Le plan d'approche ou plan de mission (tableau 6, page 79) est un document que nous aurons à élaborer après avoir mené les précédentes diligences. Il nous permettra de formaliser les grandes lignes des travaux et de rédiger le rapport d'orientation.

3.2.5. Etape de définition des objectifs : élaboration du rapport d'orientation

Le rapport d'orientation de la mission (tableau 7, page 80) est celui qui nous aidera à formaliser les différents objectifs, le champ et la durée de la mission. Sans toutefois décrire les actions à mener, il constitue une base essentielle pour la suite de la mission en ce sens qu'il est la feuille de route de l'audit. Les différentes tâches nécessaires à l'atteinte des objectifs seront enfin formalisées dans un programme ou plan de vérification.

3.2.6. Etape d'élaboration du plan de vérification

Le plan de vérification (annexe 11, page 122) est celui dans lequel nous allons décrire les tâches qui nous permettront d'atteindre les objectifs de l'audit. Il s'agit également de fixer l'étendue de notre revue générale du SIC de la LONASE et de définir la nature des tests que nous aurons à effectuer.

CESAG - BIBLIOTHEQUE

Nous nous servirons de l'analyse des risques (tableau d'analyse de risque) et du rapport d'orientation pour l'élaborer.

3.2.7. Etape de la revue générale

La revue générale se fera à l'aide d'un entretien avec le DSIE et la DFC. Nous incluons dans cette revue générale, celle de la politique de sécurité, de l'organisation de la fonction SI, de l'architecture technique et applicative. Nous prendrons connaissance et analyserons également les documents formalisés sur la gestion du SIC.

3.2.8. Etape d'appréciation des dispositifs de sécurité

Les outils dont nous nous servirons pour faire l'évaluation des dispositifs de contrôle interne sont le Questionnaire de Contrôle Interne (QCI) et l'observation physique.

3.2.8.1. Le questionnaire de contrôle interne

Selon LEMANT (1995 : 196), le QCI (annexe 8, page 110) permet à l'auditeur d'apprécier ou de porter un diagnostic sur le dispositif de contrôle interne de l'entité ou de la fonction auditée.

Nous avons choisi cet outil afin de relever les contrôles existants, de constater les lacunes et les points forts des dispositifs et des procédures de sécurité de l'information mis en place. Les questions claires et objectives n'admettant en principe que les réponses « oui » ou « non » sont celles que nous privilégions. Il sera administré face à face auprès de la DFC (les chefs de services et leurs collaborateurs en occurrence); du DAIQ et du DSIE. Nous validerons les réponses obtenues par des observations physiques.

3.2.8.2. L'observation physique

Elle consiste à constater la réalité de la mise en œuvre des processus ou directives de sécurité. RENARD (2013 : 328) le qualifie « d'application universelle », dans la mesure où c'est un outil utilisé soit pour l'observation d'un processus, d'un site, d'un bien, des documents ou des comportements, etc.

Nous procéderons à une observation physique directe des dispositifs de prévention, de détection ou de correction déployés pour assurer la sécurité du SIC. Elle nous permettra de juger de l'effectivité et de l'application des mesures (physiques et logiques) de sécurité.

CESAG - BIBLIOTHEQUE

3.2.9. Etape des tests de conformité et de corroboration

Pour ces tests, nous ferons appel aux informaticiens du Département des Systèmes d'Information. Ils concerneront, d'une part, la gestion des profils et des habilitations et, d'autre part, la sécurité de l'application comptable.

3.2.10. Etape de formalisation des travaux et du projet de rapport

Nous allons utiliser les FAR (Feuilles d'Analyse de Risques) (pages 90-96) pour identifier les risques de sécurité, relater les faits, analyser les causes de ces faits et leurs conséquences et enfin faire des recommandations qui pourront permettre d'améliorer les pratiques de sécurité de la LONASE. Les fiches de tests (pages 85 et 86) seront également tenues.

Ainsi, elles nous serviront à formaliser les résultats des différentes étapes dans un projet de rapport.

CESAG - BIBLIOTHEQUE

Conclusion du troisième chapitre

L'audit de la SSI consiste à évaluer en toute indépendance l'efficacité de l'environnement de sécurité d'une organisation. Ce chapitre nous a permis de mettre en exergue les différentes étapes de notre étude à travers le modèle d'analyse. De même nous avons passé en revue les outils et techniques qui vont nous permettre de recueillir, d'analyser et d'évaluer les informations pour qu'un tiers auditeur prudent et bien informé puisse parvenir aux mêmes conclusions que les nôtres.

Conclusion de la partie théorique

L'objectif de cette première partie de notre étude est d'appréhender les notions et méthodes de base relatives à la sécurité des SI. En effet, le premier chapitre nous a permis de connaître les objectifs de la sécurité et les dispositifs à mettre en place pour assurer la sécurité du système d'information comptable. A travers le second chapitre, nous avons compris les notions de base de l'audit de la SSI. De même nous avons pu avoir un aperçu des normes, outils et méthodologies utilisés dans le cadre de l'audit de la SSI.

Par ailleurs, les outils et techniques présentés dans le troisième chapitre constituent notre arsenal pour entamer les phases proprement dites de notre modèle d'analyse. Comme mentionné plus haut cette mission est réalisée à Direction Financière et Comptable et à la Direction des Systèmes d'Information et de l'Exploitation de la LONASE.

CESAG - BIBLIOTHEQUE

DEUXIEME PARTIE: CADRE PRATIQUE DE L'AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE DE LA LONASE

CESAG - BIBLIOTHEQUE

Introduction de la deuxième partie

Ayant pris connaissance des différentes étapes de la conduite d'une mission d'audit de la sécurité des systèmes d'information, cette partie sera consacrée à la pratique dans une organisation publique sénégalaise : la LONASE. Pour rappel, notre objectif est de porter un œil critique sur les pratiques de sécurité au sein de cette organisation plus précisément sur celles de son système d'information comptable.

En effet, une mission d'audit de la sécurité des systèmes d'information outre que l'auditeur aura à faire un travail préalable en dehors de l'entité ou du domaine audité, il doit également aller sur le terrain afin de mener les diligences nécessaires à l'atteinte des objectifs prévus. Tel est l'intérêt de cette partie.

Toute comme la première, cette deuxième partie est structurée en trois (3) principaux chapitres. La présentation de la LONASE sera le premier point que nous aborderons, ensuite nous décrirons les pratiques de sécurité du système d'information comptable existantes et enfin nous présenterons les résultats de la mise en œuvre de l'audit.

CESAG - BIBLIOTHEQUE

CHAPITRE 4 : PRESENTATION DE LA LONASE

Introduction

Société appartenant à l'Etat sénégalais conformément à la loi n° 87-43 du 28 décembre 1987, la Loterie Nationale Sénégalaise (LONASE) détient le monopole de l'exploitation de toutes les formes de loteries, jeux de hasard, de pronostics et jeux assimilés avec un capital d'un milliard quatre-vingt-dix millions (1.090.000.000) de francs CFA.

Nous présenterons la LONASE à travers son historique, ses missions, sa nature juridique, ses activités ainsi que la structure organisationnelle qui lui permet de s'acquitter de ses missions.

4.1. Historique, missions et nature juridique

L'histoire de la LONASE de par les différents statuts juridiques qu'elle a pris au fil des temps, ses missions sont les points qui retiendront notre attention dans cette section.

4.1.1. L'historique

A sa création le 30 décembre 1966 en vertu de la loi n°66-58 du 30 juin 1966, portant organisation des jeux de hasard, la LONASE était une société anonyme privée à qui l'Etat avait déjà concédé l'exclusivité de l'exploitation des jeux de hasard. En contrepartie, le concessionnaire du nom de Jean Luc DEFAIT versait à l'Etat Sénégalais une redevance et s'engageait de même à investir un pourcentage de son bénéfice annuel dans les œuvres sociales.

En 1974, le pouvoir public a jugé opportun de déclencher le processus tendant à s'approprier de tout le capital de ladite société. Ainsi, il procéda à cette année d'abord par un rachat de 80% du capital de la société. Treize ans plus tard, c'est-à-dire en 1987, il racheta les autres 20% du capital. La LONASE devient dès lors une société nationale en vertu de la loi 87- 43 du 28 décembre 1987 avec les mêmes privilèges, ceux du monopole de l'exploitation des jeux de hasard, de pronostics et jeux assimilés au Sénégal.

4.1.2. Les missions

Les missions de la LONASE sont définies par la loi 87-43 du 28 décembre 1987. Elle a d'une part la mission d'exploiter toutes les formes de loteries, jeux de hasard, pronostics et jeux assimilés et d'en tirer des bénéfices. D'autre part, les bénéfices réalisés serviront à contribuer au développement économique et social. Le volet développement social fut intégré aux

CESAG - BIBLIOTHEQUE

missions de la LONASE par le plan social de 2000. Ces deux aspects se résument dans sa devise : «La fortune aux souscripteurs, les bénéfices à la Nation ».

4.1.3. Le statut juridique de la LONASE

La LONASE a connu de sa création à nos jours quatre (4) statuts juridiques qui se présentent comme suit :

- Société anonyme de 1966 à 1973 en vertu de la loi n°66-58 du 30 juin 1966 ;
- Société d'économie mixte de 1974 à 1977 ;
- Société de fait de 1977 à 1987 ;
- Société nationale de droit conformément à la loi N 87-43 du 28 décembre 1987.

Elle est placée sous la tutelle technique et financière du ministère chargé des finances.

CESAG - BIBLIOTHEQUE

4.2. Les activités de la LONASE

La LONASE mène deux principales activités :

- l'organisation des jeux de hasard sur lesquels ni elle, ni les joueurs n'ont pratiquement pas d'information pouvant influencer leur déroulement. Il s'agit des jeux de hasard à chiffres et des jeux instantanés (le Nopalé, le Tebbi) ;
- l'organisation, la promotion et la commercialisation des paris d'argent sur des courses de chevaux (réelles ou virtuelles) et sur des matchs de football. On distingue ainsi le Pari Mutuel Urbain (PMU) et les paris sportifs. Le PMU est composé de deux segments :
    - l'ALR (Avant la Réunion) : il enregistre le couplé, le tiercé, le quarté et le quinté tenant compte respectivement de l'ordre d'arriver des chevaux. Il est organisé tous les jours de la semaine (du lundi au dimanche) dans les agences et kiosques de la LONASE et se fait par un choix de combinaison à valider avant la course.
    - le PLR (Pendant La Réunion) : il est organisé en liaison télévisée directe avec la France sur les courses de chevaux. Pour ce pari, une salle est aménagée pour les parieurs. Contrairement à l'ALR, la prise de paris PLR se fait avant chaque course et à l'espace PLR uniquement.

Elle assure l'émission, l'exploitation et la commercialisation de ces différents jeux de hasard et de pronostics sur l'ensemble du territoire national sénégalais.

4.3. Les ressources de la LONASE

L'autorité de tutelle met à la disposition de la société, un ensemble de ressources à mettre en œuvre pour atteindre les objectifs qui lui sont assignés. Par ressources, nous entendons les moyens humains, financiers et matériels :

- **les ressources humaines**

Le développement des activités de la LONASE a conduit parallèlement à un accroissement considérable de son effectif. Le personnel a pour mission de contribuer de par leur compétence à l'atteinte des objectifs de la société. Elle compte 532 agents répartis comme suit :

Tableau 2: Répartition du personnel de la LONASE

Critères	Attributs	Répartition	
Genre	Hommes	321	
	Femmes	211	
Catégorie de personnel	Cadres	Hommes	96
		Femmes	42
	Non cadres	Hommes	225
		Femmes	169

Source : DRH LONASE (2014).

- **les ressources matérielles**

La LONASE dispose d'un patrimoine mobilier et immobilier qui est mis à la disposition de l'ensemble de ses Directions, Agences et bureaux. Ce patrimoine comprend entre autres, des biens meubles et immeubles, des véhicules de service, des matériels informatiques, etc.

- **les ressources financières**

Le capital, les réserves sur bénéfices, les subventions de l'Etat constituent les principales ressources financières de la LONASE. Néanmoins, elle obtient des institutions financières des emprunts à court, moyen et long terme selon les besoins.

CESAG - BIBLIOTHEQUE

4.4. La structure organisationnelle de la LONASE

L'organigramme de la LONASE (annexe 6, page 107), montre que l'ensemble des activités de celle-ci est piloté par un Conseil d'Administration, une Direction Générale aidée par des Conseillers (spéciaux et autres), des Directions fonctionnelles, des départements et des services.

Les activités sont relayées par les agences aussi bien à Dakar que dans les autres villes du Sénégal. Cette organisation fonctionnelle a pour objectif de s'assurer d'un travail harmonieux de l'ensemble des participants à la réalisation des missions de la LONASE.

4.4.1. Le Conseil d'Administration

Le Conseil d'Administration (CA) est un comité de gestion indépendante de la société et chargé de veiller à la bonne marche de celle-ci. Composé de sept (5) membres, le CA statue sur toutes les grandes décisions de l'administration, sur les programmes pluriannuels. Il s'agit entre et autres du :

- Président du CA (PCA) nommé par décret du Président de la République ;
- représentant du Secrétaire Général de la présidence ;
- représentant du Ministre de l'Economie et des Finances ;
- Trésorier Général ou son représentant ;
- représentant du département ministériel bénéficiant du concours de LONASE.

Ils ont un mandat de deux ans renouvelable. Toutefois leur mandat n'est pas limité.

Le CA statue sur le budget et compte prévisionnel, les acquisitions, les prises de participations financières, les comptes de fin d'exercice et également sur le rapport de gestion du DG.

Il définit le règlement intérieur, fixe les objectifs de la société, représente cette dernière auprès des pouvoirs étatiques et est informé des directives présidentielles issues des rapports des corps de contrôle sur la gestion de l'organisation.

4.4.2. La Direction Générale

Elle assure la direction et la gestion de la société et veille à la mise en œuvre des décisions prises par le Conseil d'Administration et les autorités de tutelle. On y trouve :

- un Directeur Général, nommé par le CA sur proposition du Président de la République pour un mandat de trois ans renouvelable ;

CESAG - BIBLIOTHEQUE

- un Secrétariat Général qui assure l'intérim en cas d'absence du Directeur Général ;
- des conseillers (spéciaux et autres) qui composent la structure en staff et donc ont pour rôle d'assister le Directeur Général dans sa mission.

4.4.3. Les Directions et Cellules fonctionnelles

La LONASE dispose de sept (7) directions fonctionnelles, de deux (2) cellules et d'un centre médico-social. Les directions et cellules sont subdivisées en dix-neuf (19) départements. Chacune de ces directions et cellules ont des missions spécifiques.

- **la Cellule de Contrôle de Gestion**

Elle est chargée d'élaborer, d'exécuter et de faire le suivi du budget de la société. Elle rend compte au Directeur Général de ses activités tout en aidant les autres directions fonctionnelles à mener leurs activités avec efficacité et efficience.

- **la cellule des affaires juridiques et du contentieux**

Cette cellule est l'instance chargée du règlement des affaires juridiques et des contentieux entre la LONASE et ses partenaires. Elle assure également la veille juridique pour aider l'organisation à se conformer aux différents lois et règlements en vigueur.

- **la Direction de l'Administration Générale et de l'Equipement (DAGE)**

La DAGE est chargée de la logistique et des approvisionnements de la LONASE. Elle assure sa mission par le biais de deux départements à savoir :

- le département des achats et des approvisionnements qui s'occupe de la centralisation des besoins d'achats, de la gestion des achats et de la réception des biens ;
- le département de l'administration générale qui gère le parc automobile et veille à la bonne exécution des contrats d'entretien, d'assurance et de bail.

- **la Direction des Ressources Humaines**

La Direction des Ressources Humaines (DRH) est chargée de la gestion du personnel permanent et à temps partiel. Elle participe également à la définition des orientations relatives à la gestion stratégique des ressources humaines. Elle est consultée par le Directeur General sur

CESAG - BIBLIOTHEQUE

l'évolution des structures et sur le choix des agents éligibles aux postes à pourvoir. La DRH est de même, chargée de la définition et de la mise en œuvre de la politique sanitaire et sociale.

❖ la Direction du Marketing et de la Communication

La Direction du Marketing et de la Communication (DMC) est chargée essentiellement de mener toutes les études nécessaires au lancement et à la promotion des produits, de la recherche et du développement de produits, de l'élaboration de plans d'actions et de communication.

❖ la Direction des Systèmes d'Information et de l'Exploitation (DSIE)

La DSIE, a pour mission d'assurer l'exploitation des jeux à travers un système automatisé, d'accompagner la LONASE dans sa stratégie de modernisation.

❖ la Direction Commerciale

La direction commerciale a pour mission la gestion de la vente et de la distribution des différents produits de la LONASE. Elle est chargée également de la procédure d'agrément destinée à l'exploitation des jeux SMS (Short Message Services) et aux concours téléphoniques.

❖ la Direction Financière et Comptable (DFC)

La DFC est responsable de l'enregistrement exact et exhaustif de toutes les transactions comptables et financières de la LONASE. Elle a pour mission de produire des états financiers suivant la périodicité retenue, de participer à la confession et la mise en œuvre de la politique financière et enfin d'organiser la gestion de la trésorerie. Elle est constituée du Département des Finances et du Département de la Comptabilité (annexe 6, page 107).

▪ le Département des Finances

Il a en charge la gestion financière de la LONASE et a pour mission de superviser et de piloter les services des finances, de participer à la recherche et de l'élaboration de la stratégie de financement. Il compte à son sein trois services dont le premier gère les prévisions, les analyses financières et les recherches de financement. Le second a pour mission la gestion de la trésorerie et le troisième de la gestion de la caisse.

CESAG - BIBLIOTHEQUE

- **le Département de la Comptabilité**

Ce département a pour mission de répertorier et d'enregistrer tous les mouvements et flux générés par des évènements commerciaux, matériels, juridiques et économiques de la LONASE. Il supervise et pilote également la comptabilité en s'assurant du respect des principes et procédures comptables. Il est constitué de quatre services à savoir le service caisse et banque, le service clients, le service fournisseurs et le service des valeurs inactives.

❖ **la Direction de l'Audit Interne et de la Qualité (DAIQ)**

La DAIQ a pour charge d'assister la direction générale et de l'aider à exercer efficacement ses missions en lui apportant des analyses, des appréciations, des recommandations de nature à lui permettre une meilleure maîtrise de ses activités. Elle a pour principale mission de contribuer à l'amélioration du système de contrôle interne de la LONASE. Elle est subdivisée en trois départements à savoir : le Département Qualité, le Département Inspection des Jeux et le Département Audit Interne.

❖ **le Centre Médico-Social (CMS)**

Le Centre Médico-social a pour mission la gestion du volet sanitaire et social de la LONASE. Dans ce cadre il a pour objectif de permettre aux agents d'atteindre le plus haut degré de bien-être physique et mental d'une part et d'autre part d'améliorer la qualité de vie et de travail.

4.4.4. Les agences

Les agences sont des unités multifonctionnelles qui relèvent hiérarchiquement de la Direction du Marketing et de la Communication.

Le chef d'agence est responsable de l'organisation, du fonctionnement et de la gestion de l'agence. A ce titre, il représente le Directeur Commercial au plan local. Il définit et évalue l'ensemble des activités, gère et administre l'ensemble du personnel ; gère la force de vente et le réseau commercial ; exécute au plan local la politique commerciale définie par la direction et assure la gestion financière de l'agence.

La LONASE dispose de quatorze (14) agences dont sept (7) à l'intérieur du pays, de six (6) bureaux, de seize (16) espaces sur l'ensemble du territoire national. Ce réseau commercial est récapitulé dans le tableau 3.

CESAG - BIBLIOTHEQUE

Tableau 3: Répartition des agences et bureaux appartenant à la LONASE sur le territoire National.

	Agences	Bureaux	Espaces PLR
1.	Dakar Plateau	Bambey	Plateau
2.	Medina	Fatick	Medina 1
3.	Grand-Dakar	Kolda	Medina 2
4.	Parcelles Assainies	Mbacké	Grand – Dakar
5.	Pikine	Richard Toll	Parcelles Assainies
6.	Rufisque	Kaffrine	Pikine
7.	Mbour	-	Rufisque
8.	Diourbel	-	Thiès
9.	Thies	-	Mbour
10.	Saint-Louis	-	Diourbel
11.	Kaolack	-	Kaolack
12.	Tambacounda	-	Louga
13.	Zinguinchor	-	Saint-Louis
14.	Louga		Richard Toll
15.	-	-	Tambacounda
16.	-	-	Zinguinchor

Source : DMC-LONASE (2014).

CESAG - BIBLIOTHEQUE

Conclusion du quatrième chapitre

La connaissance de l'environnement d'une organisation ou d'une structure faisant objet d'une quelconque évaluation est toujours capitale, car elle permet à l'auditeur d'orienter ses actions. Ce chapitre sur la présentation de la LONASE nous a permis de la découvrir, à travers ses missions, ses activités et son organisation. De même, il nous a aidé à faire une analyse préalable de ce que peut être la valeur d'un système d'information comptable sécurisé pour une telle organisation.

CHAPITRE 5 : DESCRIPTION DES PRATIQUES DE SECURITE DU SIC DE LA LONASE

Introduction

L'environnement général de la LONASE étant appréhendé, nous procéderons dans ce chapitre à la description de son Système d'Information Comptable ainsi que de ses pratiques de sécurité, tels que nous les avons observés et documentés. Pour le respect du champ de cette étude et dans le souci d'atteindre les objectifs fixés, nous allons mettre un accent sur les aspects organisationnels et procéduraux de la gestion de la sécurité du SIC mise en place par la LONASE. De même, la description de l'infrastructure du SIC retiendra notre attention.

5.1. La présentation du système d'information comptable

Nous présenterons dans cette section les objectifs du système d'information comptable de la LONASE et les différentes composantes de celui-ci.

5.1.1. Les objectifs du SIC

Pour la LONASE, le système d'information comptable est un instrument susceptible d'aider ses gestionnaires à planifier, contrôler et évaluer l'exécution et les résultats des opérations.

Il permet de répondre aux obligations comptables, fiscales et sociales. Pour cela, il doit pouvoir enregistrer les flux entre elle et son environnement (personnel, clients, fournisseurs, Etat, etc.), les classer et, périodiquement en faire une synthèse qui sera présentée aux responsables et aux partenaires financiers et sociaux. Comme corollaire, les informations fournies par ce système doivent :

- donner une image fidèle du patrimoine de la LONASE, de sa situation financière, de sa performance et des éventuelles variations de celles-ci ;
- permettre de prendre des décisions stratégiques et opérationnelles qui conviennent.

Ainsi, le SIC de la LONASE doit être un outil de communication et de coordination entre les différents services et domaines de gestion de l'organisation. Le SIC de la LONASE a également un objectif opérationnel en ce sens qu'il doit aider à traiter des informations nécessaires à l'exécution des tâches quotidiennes. Pour récapituler, les utilisateurs souhaitent pouvoir expliquer, contrôler, prévoir et informer à partir des informations produites par le SIC.

CESAG - BIBLIOTHEQUE

5.1.2. L'organisation du SIC

L'évolution de la technologie et le volume de plus en plus important des opérations à traiter sont des facteurs qui ont amené la direction de la LONASE à opter pour le système centralisateur.

En effet, le Département de la Comptabilité de la LONASE est composé de quatre (4) services : clients, fournisseurs, banque-caisse et valeurs inactives. Sous la responsabilité d'un chef de service, les comptables de chaque service tiennent un journal auxiliaire dans lequel ils enregistrent les opérations qui rentrent dans son champ.

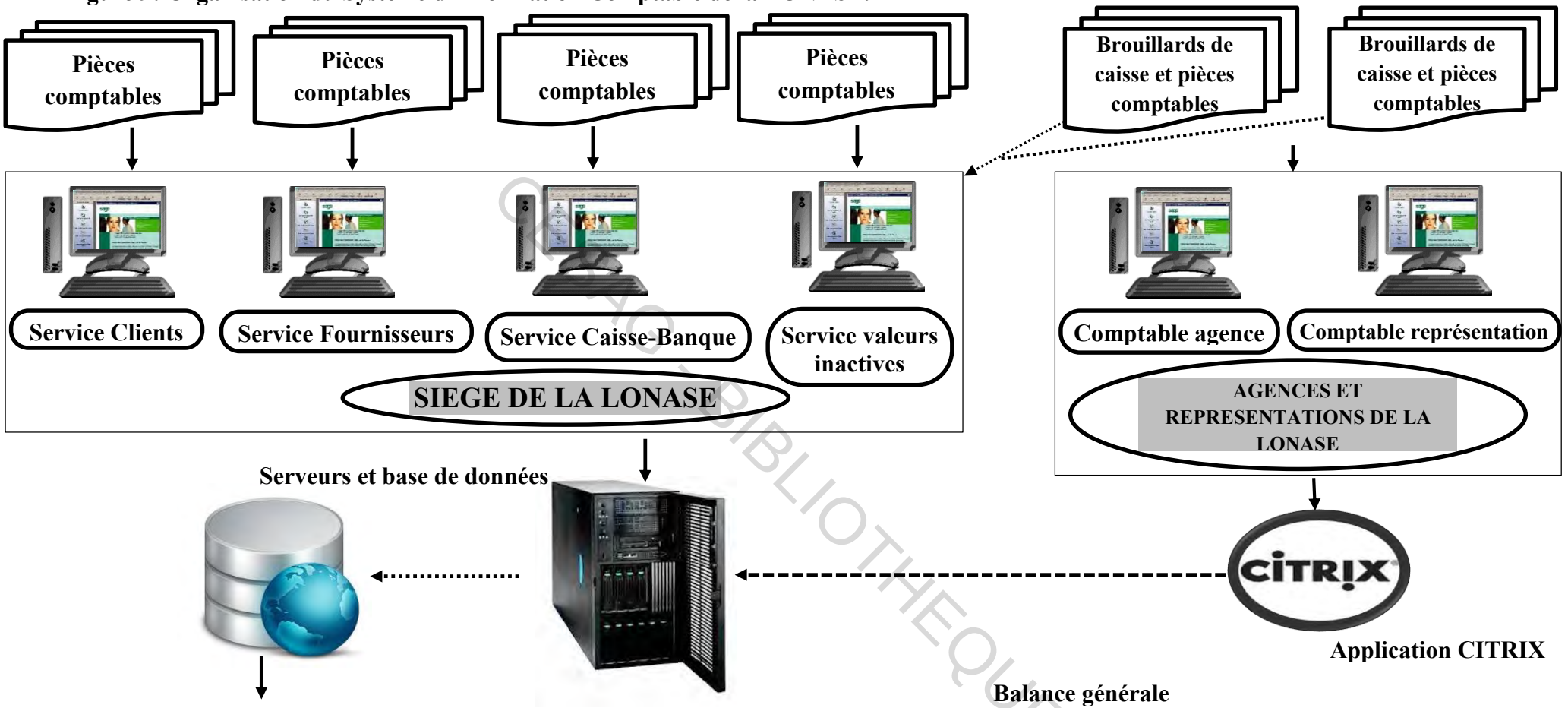
Les activités des comptables du siège consistent principalement au traitement des opérations réalisées par les différentes directions. Ces comptables vérifient également les opérations effectuées au niveau des différentes agences et représentations, sur la base des documents comptables et brouillards de caisse transmis à la DFC. Cela étant, les comptables des agences ne tiennent qu'une comptabilité de caisse. Par ailleurs, une écriture une fois enregistrée et validée est déversée systématiquement dans le grand livre.

Le SIC est également organisé en réseau et les différents responsables des services ont la possibilité de voir les opérations saisies par les comptables des autres agences et représentations de l'intérieur et qui concerne leurs domaines respectifs, à temps réel. Aucune partie de la comptabilité n'est externalisée.

L'organisation du système d'information comptable de la LONASE (figure 9) peut se schématiser comme suit :

CESAG - BIBLIOTHEQUE

Figure 9: Organisation du Système d'Information Comptable de la LONASE.



Source : Nous-mêmes.

5.1.3. Les composantes du SIC

Le SIC de la LONASE, pour assurer les fonctions de collecte, de traitement, de stockage et de diffusion des informations, utilise divers moyens notamment les moyens humains, matériels, pour n'en citer que ceux-là.

5.1.3.1. Les acteurs du Système d'Information Comptable

Deux principaux acteurs interviennent dans la gestion du SIC, l'un pour son maintien et l'autre pour son utilisation. Ce sont respectivement, la Direction des Systèmes d'Information et de l'Exploitation (DSIE) et les agents de la DFC.

La DSIE, plus précisément le Département des Systèmes d'Information (DSI), a pour mission de veiller, d'une part, au bon fonctionnement du SIC dans tout son aspect technique, c'est-à-dire de l'informatique, et à la sécurité des données comptables d'autre part. Elle est aussi chargée de la gestion du parc informatique qui soutient le SIC et de la maintenance. Le DSI est composé de trois services à savoir :

- **le service support et solution TI (Techniques Informatiques)**

Selon sa fiche de poste, ce service est chargé de la veille technologique et de conseils en informatique. Bien qu'il soit créé, il n'est pas encore pourvu en termes de ressources humaines.

- **le service administration réseau, de la sécurité et de la maintenance**

La mission de ce service est de gérer le réseau interne et externe à la LONASE. Il est également l'acteur principal de la sécurité des différents systèmes d'information. Il veille également au bon fonctionnement des matériels informatiques.

- **le service assistance et formation des utilisateurs**

C'est ce service qui est chargé d'organiser les formations sur l'utilisation d'une application ou sur les notions nécessaires à l'utilisation des matériels.

La deuxième catégorie d'acteurs du SIC sont les utilisateurs (comptables) qu'ils soient au siège ou dans les agences ou encore dans les représentations. Ils alimentent le SI en information et ils sont tenus au respect des règles, des procédures comptables et de sécurité des données et des équipements informatiques qu'ils utilisent.

CESAG - BIBLIOTHEQUE

5.1.3.2. L'architecture technique et applicative

La LONASE, pour la tenue de sa comptabilité, utilise des matériels (ordinateurs, réseaux, etc.) et des logiciels. En effet, la DFC utilise actuellement le logiciel « SAARI ligne 1000 » acquis courant 2008 en remplacement de la ligne 500.

Tous les postes de travail des différents services comptables sont dotés de ce logiciel sauf ceux des secrétaires. En plus du logiciel « SAARI ligne 1000 », qui permet de générer automatiquement des états de synthèse, la DFC dispose d'autres applications comme le logiciel CITRIX qui facilite la connexion entre le siège et les sites distants. Ce logiciel n'est utilisé que dans les agences.

La DFC dispose également de la suite office de Microsoft qui lui permet de gérer les besoins en bureautique. De même il est possible d'exporter les données du logiciel comptable vers l'application Excel.

Egalement, en cas de besoin des informations sur un exercice antérieur, un comptable habilité peut accéder à ces informations par interrogation du serveur. Cela, par l'entremise de l'outil d'interrogation des bases de données « Microsoft SQL (Structured Query Language) Server ».

Le parc technique et applicatif de la DFC peut se résumer dans le tableau 4 ci-après :

Tableau 4: Liste du parc informatique de la DFC de la LONASE

Eléments	Caractéristiques
Système d'exploitation	Windows 8.1
La suite Microsoft office	Version 2013
SAARI	Ligne 1000
CITRIX	Version 2013
Mac Afee	Version 2014 avec une architecture client-serveur
Postes de travail	Ils sont au nombre de 16 au département de la comptabilité, tous équipés d'un onduleur de 600 à 1000 KVA

Source : Nous-mêmes.

CESAG - BIBLIOTHEQUE

5.2. Processus d'évaluation et de gestion des risques liés au SIC

La gestion des risques susceptibles de compromettre la sécurité des SI fait partie d'un vaste programme de gestion des risques mené par la LONASE dans le cadre de son système de management de la qualité. Elle dispose d'une cartographie des risques établie par la DAIQ en 2013 couvrant tous les processus de la LONASE notamment celle de la gestion du SIC mais non encore validée par le Conseil d'Administration.

5.3. La gestion de la sécurité du système d'information comptable

Cette section est consacrée à la description de la manière dont la LONASE s'organise pour la gestion des menaces qui pèsent sur son SIC et ceci à travers les dispositions prises pour prévenir, détecter et corriger d'éventuelles vulnérabilités.

5.3.1. Organisation de la sécurité du système d'information

La LONASE ne dispose pas d'organe spécifique chargé de la gestion de la sécurité de son système d'information comptable. Cette gestion est plutôt laissée aux soins du service « administration réseau, maintenance et sécurité » de la DSIE qui s'assure de la disponibilité, de l'intégrité et de la confidentialité de l'information comptable. En d'autres termes, la DSIE est la direction responsable de la gestion de la sécurité du SIC de la LONASE.

5.3.2. Les dispositifs et les procédures de sécurité

Le premier dispositif de sécurité mis en place est l'obligation faite aux utilisateurs du respect des principes et des règles comptables en vigueur. Le manuel de procédures administratives et comptables retrace les différentes règles et procédures comptables.

Bien qu'ils ne soient pas documentés, d'autres dispositifs de sécurité sont déployés pour assurer la sécurité des personnes et des biens.

5.3.2.1. Les dispositifs de sécurité physique et leur gestion

Les locaux abritant le personnel et les matériels informatiques au siège sont gardés par quatre (4) vigiles, salariés d'une société de gardiennage SAGAM, sous contrat avec la LONASE. Ceux des agences sont gardés par deux vigiles (2) au moins.

CESAG - BIBLIOTHEQUE

Des imprimés expliquant les comportements à tenir en cas d'incendie sont affichés à l'entrée et au niveau de chaque étage. De même, trois extincteurs d'incendie sont disponibles à chaque étage. La salle des serveurs est fermée et c'est le chef du département des SI qui garde les clefs. Les serveurs sont gardés à une température maximale de 18° Celsius à l'aide de deux climatiseurs, en vue d'éviter qu'ils surchauffent.

5.3.2.2. La sécurité logique (la gestion des accès)

Les différents services comptables de la LONASE n'ont accès en général qu'aux paramètres de l'application comptable et informations nécessaires pour un déroulement harmonieux de leurs activités. Les privilèges vont de la saisie à la création de compte en passant par les phases de consultation et de modification.

Particulièrement pour un comptable donné, l'accès à un poste de travail est subordonné à la saisie préalable d'un nom d'utilisateur (login) et d'un mot de passe (lequel n'apparaît pas clairement lors de la saisie) fournis par le DSI. Toutefois, d'autres personnes peuvent travailler sur ce même poste de travail en utilisant une autre section dénommée « autres utilisateurs » ; un login et un mot de passe sont toutefois indispensables s'ils sont préalablement définis.

Par ailleurs, un mot de passe est exigé avant d'accéder aux paramètres de l'application comptable. Ces droits d'accès sont attribués par l'administrateur (le DSI) à la demande de la Directrice Financière et Comptable ou du chef comptable ; soit par téléphone ou par courriel. Bien que les droits d'accès soient créés en tenant compte des tâches de l'agent avec le programme, il n'existe pas une liste qui renseigne sur les droits d'accès octroyés.

En ce qui concerne l'accès au réseau local, un login ou code d'utilisateur et un mot de passe sont également nécessaires ; ce qui n'est pas le cas pour le réseau Internet. Tous les sites Internet sont accessibles aux agents.

Le « code utilisateur », une fois attribué, est géré par chaque utilisateur. Cependant, des prêts de mot passe sont interdits par la LONASE.

5.3.3. Formation et sensibilisation

A la LONASE, chaque utilisateur de l'application comptable doit avoir reçu une formation de base en la matière ou être formé sur place. Les formations sont organisées lorsque le besoin se fait sentir. En cas d'acquisition d'une nouvelle application ou de mise à jour d'une ancienne,

CESAG BIBLIOTHEQUE

les utilisateurs qui sont susceptibles de travailler avec cette application reçoivent des formations.

En matière de sensibilisation du personnel à la sécurité de l'information, la LONASE procède parfois par des affiches. De même la direction générale passe par les différents responsables pour sensibiliser le personnel affilié en ce qui concerne une nouvelle procédure ou une quelconque décision. L'objectif étant de faire comprendre à tous le personnel (utilisateurs, managers et informaticiens) les enjeux de la sécurité ainsi que la conduite à tenir vis-à-vis de l'information ou des ressources spécifiques qu'ils gèrent ou utilisent.

5.3.4. Sauvegardes et archivages des documents comptables

Les données comptables de la LONASE sont enregistrées automatiquement sur des « baies » de stockage. L'archivage s'applique aux livres comptables, aux pièces justificatives des opérations, aux documents électroniques et à toute autre pièce à valeur de preuve.

La Gestion Electronique des Documents (GED) de la LONASE se fait suivant un classement et un archivage des documents sur des supports magnétiques ou sur des CD-ROM (Compact Disc-Read Only Memory) par gravure de fichiers informatisés.
Le mode de classement et d'archivage physique est le plus utilisé à la LONASE. Les documents sont triés, classés et conservés de manière à faciliter leur accès selon trois catégories d'archive :

- les archives vivantes (ou courantes) conservées au moment de l'exécution des affaires ;
- les archives semi-vivantes (ou intermédiaires) dont l'usage est peu courant et qui sont stockées dans des endroits éloignés des lieux de travail ;
- les archives définitives (ou historiques) qui ont une valeur patrimoniale. Elles sont conservées indéfiniment. Si cette valeur n'est pas avérée, elles sont détruites à l'issue de la période légale de conservation.

Les matériels et fournitures d'archivage et de classement sont constitués essentiellement de chemises (simples, à rabat, pochettes, extensibles, élastiques, etc.), de classeurs à levier communément appelés "chrono", de dossiers suspendus à index vertical ou horizontal pour une lisibilité de face dans les classements d'armoires (ou de dessus dans les classements de tiroirs), de boîtes de classement et des boîtes ou caisses archives.

Le tableau 5 illustre le plan d'archivage de la LONASE :

CESAG - BIBLIOTHEQUE

Tableau 5: Plan de gestion des documents

Nature du document	Mode de classification	Support de classement	Durée de conservation
Marchés (contrats, dossier d'appel d'offre)	Numéro	Chemises à sangle	10 ans
Etats synthèse des titres de paiement	Numéro	Classeurs	10 ans
Facture ou décompte de fournisseur	Numéro	Classeurs	10 ans
Pièces de banque	Numéro	Classeurs	10 ans
Pièces de caisse	Numéro	Classeurs	10 ans
Déclarations fiscales	Date	Classeurs	10 ans
Déclarations sociales	Date	Classeurs	10 ans
Opérations diverses	Numéro	Classeurs	10 ans
Relevés de banque	Date	Classeurs	10 ans
Budget	Date	Chemises à sangle	10 ans
Balances	Date	Chemises à sangle	10 ans
Grand livre	Date	Boîtes à archive	10 ans
Bon de commande	Numéro	Classeurs	10 ans
Dossier du personnel et des immeubles	Date	Classeurs	Illimitée

Source : **DFC-LONASE (2013).**

Le système de sauvegarde mis en place par la LONASE permet également une sauvegarde sur ses serveurs et une duplication de ces données sur le site de secours.

5.3.5. Documentation

Cette section fait référence principalement au manuel des procédures comptables et financières et aux manuels « utilisateurs » de l'application comptable utilisée par la DFC.

L'exigence de fournir des informations comptables et financières et la nécessité de fournir un référentiel sont des raisons qui ont amené les dirigeants de la LONASE à élaborer un « manuel de procédures comptables ». Ce manuel décrit l'ensemble des règles et procédures d'enregistrement, de contrôle et d'organisation comptable retenues. Il y est mentionné des comptes utiles à chaque type d'opération.

CESAG - BIBLIOTHEQUE

L'extension des comptes admise par le plan comptable du SYSCOHADA (Système Comptable pour l'Organisation et l'Harmonisation en Afrique des Droits des Affaires), est utilisée pour ajouter des spécifications sur la nature d'une opération ou de l'acteur de l'opération. Les principes comptables de l'OHADA sont repris dans leur détail. Le manuel fixe également les règles d'arrêté des comptes et constitue à cet effet, la base à laquelle tous les services du département de la comptabilité doivent se référer pour l'exécution de leurs tâches.

Ce manuel existe en version numérique et en version papier et est facilement accessible aux comptables. La dernière mise à jour du manuel des procédures comptables de la LONASE remonte à septembre 2013.

En ce qui concerne les guides d'utilisation de l'application SAGE, ces derniers existent seulement en version numérique et les agents détiennent des supports fournis lors des différentes formations.

CESAG - BIBLIOTHEQUE

5.3.6. Gestion de la continuité des activités

Détenant le monopole de l'exploitation des jeux de hasard et produits assimilés sur le territoire national sénégalais; garantir la continuité de l'exploitation en cas de sinistre est pour les dirigeants un enjeu de taille.

Pour cela, en dehors du site du siège qui gère les principales activités, elle dispose d'un site de secours, prêt à accueillir les différentes directions « métier » en cas de sinistre. De même, pour assurer la sécurité de ses matériels informatiques et favoriser la continuité des activités en cas de délestage, la LONASE dispose d'un groupe électrogène à démarrage automatique à son siège et dans chacune de ses agences. Aussi, chaque poste de travail de la DFC est alimenté par le biais d'un onduleur à trente (30) minutes d'autonomie.

Conclusion du cinquième chapitre

L'objectif de ce cinquième chapitre de notre étude est de décrire la manière dont la LONASE assure la sécurité de son système d'information comptable. La revue du cadre organisationnel et des dispositifs de sécurité physiques et logiques constitue le grand point développé. Ce chapitre nous a également permis d'appréhender les pratiques actuelles ; lesquelles seront le socle de nos analyses et de nos éventuelles recommandations à travers la mise en œuvre de notre mission d'audit. Cette mise en œuvre de l'audit fera l'objet du prochain chapitre.

CHAPITRE 6 : MISE EN ŒUVRE DE L'AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE DE LA LONASE.

Introduction

L'audit de la sécurité d'un système d'information d'une organisation, comme nous l'avons souligné précédemment, a pour objectif de rapprocher les pratiques de celle-ci aux bonnes pratiques, d'analyser les écarts éventuels afin de proposer des actions pour renforcer les procédures et dispositifs de sécurité. Notre étude ne va pas déroger à cette démarche.

Conformément à notre modèle d'analyse, ce chapitre a pour objectif de décrire la mise en œuvre que nous avons faite de notre mission d'audit de la sécurité du SIC de la LONASE. En effet, nous avons réalisé l'audit selon un plan tripartite : la préparation, l'exécution et la conclusion.

Les différentes étapes de nos travaux avec les diligences menées seront présentées premièrement, ensuite nous présenterons sous forme de projet de rapport d'audit les résultats de la mission tout en faisant ressortir les forces et les faiblesses des procédures et des dispositifs mis en place par la LONASE afin de garantir la sécurité de son SIC. Nous terminerons par une hiérarchisation et une proposition de plan de mise en œuvre des différentes recommandations.

CESAG - BIBLIOTHEQUE

6.1. Préparation de la mission

Toute mission d'audit pour atteindre les objectifs, exige une bonne préparation. Cette préparation constitue en d'autres termes la phase d'étude de la mission où il importe de prendre des dispositions nécessaires au bon déroulement des travaux sur le terrain. Elle a consisté à initialiser la mission, à faire la prise de connaissance du domaine audité et à préparer les documents indispensables à la mission.

6.1.1. Initialisation de la mission et prise de connaissance de l'entité

Notre mission a été débutée avec une analyse documentaire sur l'audit de la sécurité des systèmes d'information. Par contre, à la LONASE, elle a commencé dès que nous avons reçu notre lettre de mise en stage au Département Audit Interne de la DAIQ.

Par la suite, nous avons porté à la connaissance des différents responsables (la DFC, le DRH, et le DAIQ) en relation avec le SIC, le thème de notre étude et les objectifs poursuivis. Des amendements ont été apportés par ces responsables.

Nous avons également élaboré un questionnaire de prise de connaissance (annexe 7, page 108) qui détaille les documents à consulter. Ainsi, nous avons pu prendre connaissance des activités, de l'histoire, de l'organisation de la LONASE en générale et de son SIC en particulier. Ces informations nous ont permis de présenter la LONASE (chapitre 4).

Une fois la prise de connaissance faite, nous avons procédé à un découpage de la mission en objets auditables ; à l'élaboration du tableau des risques, du plan de la mission, du rapport d'orientation et du programme de vérification.

6.1.2. Découpage du Système d'Information comptable en objets auditables et choix du référentiel de la mission.

CESAG BIBLIOTHEQUE

Les différents éléments composant le SIC n'exigeant pas un découpage en stade chronologique, nous avons opté pour le découpage par arborescence sémantique. Ainsi, nous avons découpé ce processus en activités ou opérations suivantes :

- politique et organisation de la sécurité de l'information ;
- gestion des actifs informationnels ;
- sécurité physique et environnementale ;
- gestion de la sécurité logique :
- sensibilisation et formation ;
- sauvegarde et archivage ;
- gestion de la continuité des activités ;

Ces différents domaines ou fonctions du SIC seront évalués au regard de la Politique de Sécurité des Systèmes d'Information de la LONASE, des bonnes pratiques de sécurité que proposent les normes ISO 27001 et 27002 et le processus « Délivrer et Supporter : DS.5 » du COBIT concernant la sécurité de l'information. Ces bonnes pratiques sont synthétisées dans le tableau des risques élaborés en fonction des objectifs de chaque objet auditable (annexe 10, page 117).

6.1.3. Plan de mission

L'auditeur de la sécurité des systèmes d'information doit établir un plan de mission. Selon la norme 2200 de l'IIA, ce plan doit comporter les objectifs, le champ d'intervention, la date et la durée de la mission, ainsi que les ressources allouées.

Dans le cadre de notre mission, notre plan de mission tiendra compte de l'objectif général de la mission, du champ de la mission, de sa date du début et de sa durée. Nous présenterons également l'approche retenue pour la mission et le calendrier y afférent.

Tableau 6: Plan de la mission

PLAN DE MISSION		
AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE	Entité : **LONASE** **Référence : PM/JD**	
OBJECTIF GENERAL DE LA MISSION : Documenter le niveau de vulnérabilité du système d'information comptable de la LONASE.		
Champ d'intervention	La mission portera sur l'audit des aspects organisationnels, physiques et procéduraux de la sécurité du SIC de la LONASE	
Date et durée de la mission	La mission débutera le 01 août 2014, et s'étendra jusqu'au 30 septembre 2014.	
Ressource :	La mission se fera par nous-même sous la supervision de notre directeur de mémoire.	
Approche retenue	Approche par les risques	
CALENDRIER DE LA MISSION		
02/08/2014 - 15/08/2014	2 semaines	Préparation de la mission et prise de connaissance de la LONASE et du SIC
16/08/2014- 22/08/2014	1 semaine	Préparation des documents de travail (QCP, Tableau des risques, QCI, Feuilles de test, etc.)
23/08/2014 – 27/08/2014	5 jours	Achèvement du programme de vérification
28/08/2014 – 15/09/2014	18 jours	Mise en œuvre du programme de vérification
16/09/2014 – 22/09/2014	7 jours	Préparation des conclusions
22/09/2014 – 25/09/2014	4 jours	Rédaction du projet de rapport
25/09/2014 – 30/09/2014	6 jours	Soumission du projet de rapport pour validation et intégrations des commentaires.

Source : Nous-mêmes.

CESAG - BIBLIOTHEQUE

A partir du plan de la mission, nous avons établi trois autres documents susceptibles de nous aider à atteindre l'objectif général de la mission. Il s'agit du tableau des risques inhérents (annexe 10, page 117) aux objets auditables; du rapport d'orientation (Tableau 7) et du programme de vérification (annexe 11, page 122).

6.1.4. Identification et analyse des risques : élaboration du tableau des risques

Conformément à la norme 2210 de l'IIA qui stipule qu'un auditeur interne doit procéder à une évaluation préliminaire des risques liés à l'activité soumise à l'audit, nous avons procédé à une première identification et analyse des risques du SIC ; laquelle a consisté particulièrement à identifier et à apprécier les risques inhérents à chacun des objets auditables. De même pour chaque risque, nous avons apprécié l'existence ou non des dispositifs et/ou bonnes pratiques qui peuvent aider à réduire leur fréquence et/ou leur impact comme l'illustre l'annexe 10 (page 117). Cette analyse préliminaire nous a permis d'élaborer le rapport d'orientation de la mission.

6.1.5. Rapport d'orientation de la mission

Le rapport d'orientation de la mission se présente comme suit :

Tableau 7: Rapport d'orientation de la mission

RAPPORT D'ORIENTATION DE LA MISSION	
MISSION : AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE	**ORGANISME : LONASE** **PERIODE : 01 août au 30 septembre 2014**
RAPPEL DE L'OBJECTIF GENERAL DE LA MISSION	
Documenter le niveau de vulnérabilité du système d'information comptable de la LONASE	
ELEMENTS IDENTIFIES LORS DE LA PHASE DE PRISE DE CONNAISSANCE	
❖ La comptabilité est tenue à l'aide de l'application SAARI ligne 1000 ; ❖ La DFC et la DSIE sont les principaux acteurs du SIC (pas de RSSI, ni de Risk Manager) ; ❖ La sécurité du SIC de la LONASE n'a jamais faite l'objet d'audit ; ❖ La LONASE se prépare à la certification à la norme ISO 27001 portant sur le Système de Management des Systèmes d'Information (SMSI) ; ❖ La LONASE est certifiée ISO 9001 : 2008 portant sur le Système de Management de la Qualité (SMQ).	

CESAG - BIBLIOTHEQUE

<table>
<tr><th colspan="2">Rapport d'orientation (suite)</th></tr>
<tr><th colspan="2">DESCRIPTION DES OBJECTIFS SPECIFIQUES DE LA MISSION</th></tr>
<tr><td colspan="2">Il s'agit spécifiquement de :
❖ s'assurer que la sécurité du SIC est organisée et gérée efficacement à travers la définition d'une politique de sécurité formalisée et diffusée ;
❖ s'assurer de la bonne protection des actifs informationnels ;
❖ s'assurer de la gestion efficace de la sécurité physique et environnementale du SIC ;
❖ s'assure de protection des données et matériels contre les accès non autorisés ;
❖ s'assurer que les données comptables sont sauvegardées de manière périodique sur différents supports à différents endroits ;
❖ s'assurer de la prise en compte de la sécurité dans la gestion des activités quotidiennes ;
❖ s'assurer de l'existence d'une documentation du SIC et de sa mise à jour régulière;
❖ s'assurer de la sensibilisation et de la formation périodique des utilisateurs aux risques de sécurité ;
❖ apprécier la politique de gestion des sinistres et le plan de continuité des activités ;
❖ faire des recommandations pour l'optimisation de la sécurité du SIC.</td></tr>
<tr><th colspan="2">CHAMP : AXES DE TRAVAIL ET D'INVESTIGATIONS DE L'AUDIT</th></tr>
<tr><td>Description du champ</td><td>La mission portera sur l'audit des aspects organisationnels, physiques et procéduraux de la sécurité du Système d'Information Comptable de la LONASE. Il s'agit spécifiquement de l'audit:
❖ de l'organisation et de la gestion de la sécurité ;
❖ des dispositifs de contrôle interne du SIC qui permettra d'identifier les forces et les faiblesses de la sécurité physique du SIC ;
❖ de la sécurité logique du SIC ;
❖ de la politique de sauvegarde et de l'archivage des données ;
❖ de la continuité des activités.</td></tr>
<tr><td>Exclusion du champ de l'audit</td><td>Nous excluons du champ de cet audit l'aspect technique à savoir le test d'intrusion.</td></tr>
</table>

Source : Nous-mêmes.

CESAG BIBLIOTHEQUE

6.1.6. Programme de vérification

Le programme de travail ou de vérification (annexe 11, page 122) décrit les diligences à mettre en œuvre (évaluation du contrôle interne, tests de conformité et de corroboration), les structures concernées par la mission, les personnes avec qui entretenir, les informations à collecter pour atteindre les objectifs de l'audit. Etant la suite logique du plan de mission et du rapport d'orientation, il reprend d'une part, le découpage qui est fait du SIC, les objectifs à atteindre et, d'autre part, les tâches à réaliser et la durée prévue pour leur exécution.

L'élaboration et la validation du programme de vérification ont mis fin à la phase d'étude de notre mission et ont marqué le début des travaux sur le terrain.

CESAG BIBLIOTHEQUE

6.2. Exécution de la mission : mise en œuvre du programme de vérification

Cette section est consacrée à la description de la mise en œuvre que nous avons faite du programme de travail. Seront décrites les diligences mises en œuvre, l'évaluation que nous avons faite du contrôle interne et les tests effectués.

6.2.1. Description de la mise en œuvre du programme de vérification

L'analyse des risques faite dans la première phase nous a permis d'adapter notre questionnaire de contrôle interne (annexe 7, page 108). Ainsi, nous nous sommes servis de cet outil pour évaluer les dispositifs et procédures de sécurité autour du SIC. Nous avons également effectué des entretiens avec quelques responsables dont le DAIQ, le chef du département de l'audit interne, les chefs des services comptables, le chef du département comptable et le DSIE. Nous avons pu également visiter la salle des serveurs en compagnie du DSI.

Les observations physiques directes que nous avons faites des pratiques nous ont aidées à confirmer ou infirmer les propos recueillis par le biais du questionnaire de contrôle interne.

Par ailleurs, les missions de contrôle des opérations comptables des agences auxquelles nous avons pris part nous ont permis également d'observer les pratiques de sécurités dans celles-ci.

Nous avons également fait des tests de confirmation (d'existence) et de corroboration sur l'application comptable et en ce qui concerne les accès logiques.

En résumé, nous avons procédé à une évaluation des dispositifs et des procédures de sécurité et à des tests afin de corroborer les informations recueillies lors de nos entretiens, revues documentaires, etc.

6.2.1.1. Evaluation des dispositifs et procédures de sécurité

L'évaluation des dispositifs et des procédures de la sécurité du SIC de la LONASE a consisté à analyser le degré de ces derniers à assurer la disponibilité, l'intégrité et la confidentialité des actifs informationnels. Cette évaluation s'est portée sur les domaines et procédures selon la déclinaison de la mission en objet auditable. Nous avons ainsi évalué :

- l'organisation et la gestion des risques de la sécurité du SIC ;
- la sécurité physique à travers :
  - l'évaluation des dispositifs d'accès physique aux locaux ;
  - l'évaluation des dispositifs de prévention et de détection de l'incendie.
- la sécurité logique (gestion des habilitations et des profils utilisateurs, gestion des mots de passe, l'accès au réseau local et à l'Internet) ;
- la politique de sauvegarde et d'archivage ;
- la politique de formation et de sensibilisation des utilisateurs ;
- le plan de continuité des activités.

Les résultats et les analyses de ces évaluations sont présentés dans le tableau 10 (voir page 87-89) en termes de forces et faiblesses et synthétiser dans des Feuilles d'Analyses de Risque (voir page 90-96) sous forme de projet de rapport.

6.2.1.2. Mise en œuvre des tests d'existence et de corroboration

Les tests de confirmation ont consisté essentiellement à s'assurer de l'existence des procédures documentées et relatives à la sécurité du SIC. Par contre, les tests de corroboration se sont portés sur les procédures d'accès logique à l'application comptable et sur le degré de sécurité que cette dernière offre en matière de disponibilité, de confidentialité, d'intégrité des données et de traçabilité des opérations comptables. Les fiches de couverture de ces tests sont présentées dans notre projet de rapport (voir page 85-86).

6.3. Conclusion de la mission

La phase de conclusion de la mission est celle au cours de laquelle nous avons à préparer et à diffuser les résultats des travaux de l'audit sous forme de projet de rapport aux différents responsables du SIC de la LONASE. En effet, ce projet de rapport fait la synthèse des travaux et contient une proposition de plan de mise en œuvre des recommandations (voir page 97).

CESAG - BIBLIOTHEQUE

6.3.1. Synthèse des travaux : le projet de rapport de la mission

La synthèse des travaux de l'audit est présentée sous forme de projet de rapport. Ce dernier prendra en compte les résultats des évaluations et des tests des dispositifs et des procédures de sécurité du SIC de la LONASE. Ces résultats seront analysés dans un tableau de forces et de faiblesses (tableau 10, page 87-89) et dans des Feuilles d'Analyse des Risques (FAR) suivant les différents domaines, procédures ou activités qui ont fait l'objet d'évaluation et ou de test.

6.3.1.1. Synthèse des résultats des tests et des évaluations des dispositifs

Nous allons présenter dans cette section les résultats des tests que nous avons effectués et l'analyse que nous avons faite des évaluations des dispositifs et des procédures de sécurité déployés autour du SIC pour assurer sa sécurité.

Le test d'existence nous a permis d'obtenir et d'analyser :

- la politique de sécurité des SI dont la publication dans ce mémoire a été refusée par les dirigeants ;
- la cartographie des risques qui a pris en compte certains risques des systèmes d'information ;
- le manuel de procédures administratives, comptables et financières ;

Cependant, nous n'avons pas pu obtenir la charte de sécurité et les fiches de poste par ce qu'elles ne sont pas documentées. De même le plan de continuité n'est pas documenté.

Pour ces manquements, les responsables nous ont fait savoir que ces procédures seront documentées dans le cadre du processus de certification à l'ISO 27001.

CESAG - BIBLIOTHEQUE

Tableau 8: Feuille de couverture de test n°1

AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE **Feuille de couverture de test**	**Date : 3 septembre 2014** **Etabli par : Nous-mêmes**	**Fiche 1/2**
	ORGANISME : LONASE **DIRECTION : DFC**	
Objectifs du test	❖ Examiner le processus d'accès à l'application comptable ; ❖ S'assurer que le processus d'authentification permet l'accès seulement aux personnes autorisées ; ❖ Suivre le processus de sauvegarde et d'accès aux informations de la base de données ; ❖ Vérifier la cohérence des droits aux responsabilités ; ❖ Vérifier le paramétrage et le fonctionnement de l'application	
Modalités d'exécution	❖ Se faire assister par l'administrateur des droits d'accès ; ❖ Simuler un accès à l'application et aux données comptables sur la baie réservée à celles-ci à partir d'un login ou un mot de passe arbitraire.	
Résultats	❖ Les droits d'accès sont cohérents aux responsabilités ; ❖ L'application permet la traçabilité des opérations à partir du code d'accès de l'opérateur ; ❖ Exigence d'un identifiant et d'un mot de passe avant l'accès aux différents paramètres ; ❖ La consultation de la base des données est limitée aux responsabilités.	
Conclusion	Les procédures d'accès telles que nous les avons testées, assurent raisonnablement l'intégrité et la confidentialité des informations comptables.	

CESAG BIBLIOTHEQUE

Source : Nous-mêmes.

Le second test s'est porté sur le niveau de sécurité de l'application comptable.

Tableau 9: Feuille de couverture de test n°2

AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE **Feuille de couverture de test 2/2**	**Date : 14 septembre 2014** **Etabli par : Nous-mêmes**	**Fiche 2/2**
	ORGANISME : LONASE **DIRECTION : DFC**	

Objectifs du test	Documenter le niveau de sécurité qu'offre l'application comptable SAGE 1000 qu'utilise la DFC.
Modalités d'exécution	❖ Se faire assister par le chef comptable ; ❖ Retracer une opération du début à la fin à partir d'un droit d'accès ; ❖ Stimuler la suppression et la modification d'une opération erronée.
Résultats	❖ On peut saisir un login et ou un mot de passe erroné au temps de fois ; ❖ Irréversibilité des traitements effectués (impossibilité de supprimer, de contrepasser, d'ajouter ou de faire des modifications ultérieures) ; ❖ Tout enregistrement comptable comporte l'indication de l'origine du journal, du contenu et de l'imputation de l'opération ; ❖ Les enregistrements sont classés par ordre chronologique, ❖ Seule la méthode « soustractive » est admise pour l'annulation d'un enregistrement comptable.
Conclusion	L'application utilisée ne permet pas une désactivation systématique après un certain nombre de tentations d'accès erronées. Toutefois, elle assure un niveau de sécurité satisfaisant des données comptables et financières.

Source : Nous-mêmes.

CESAG - BIBLIOTHEQUE

Tableau 10: Tableau des forces et faiblesses des dispositifs et des procédures de sécurité du SIC de la LONASE

POLITIQUES, PROCEDURES OU DISPOSITIFS DE SECURITE		FORCES	FAIBLESSES
Organisation de la sécurité		❖ L'existence d'une cellule chargée de la sécurité informatique ; ❖ L'engagement de la Direction Générale à protéger les informations de l'organisation par sa démarche à la certification à l'ISO 27001.	❖ Le système de gestion de la sécurité n'est pas clairement défini en termes de responsabilités ; ❖ L'absence de charte de sécurité du système d'information ; ❖ L'audit des systèmes d'information comptable n'est pas intégré dans le plan général d'audit.
La sécurité physique	**Contrôle physique des accès**	❖ Les locaux sont surveillés par des vigiles d'une société de gardiennage (SAGAM) ; ❖ La salle des serveurs est toujours fermée à clef ;	❖ Le personnel ne dispose pas d'un signe pouvant permettre de le distinguer des personnes étrangères ; ❖ Absence de registre des personnes qui accèdent à la salle des serveurs ; ❖ Pas de contrôle d'identité des personnes accédant au bâtiment du siège ; ❖ Pas de demande de confirmation sur les raisons ni sur la personne ou le service visité.
	Protection des actifs informationnels	❖ Chaque poste de travail est alimenté à partir d'un onduleur ; ❖ Chaque agence dispose un groupe électrogène à démarrage automatique en cas de délestage.	❖ Absence d'inventaire des actifs du SIC ; ❖ Aucune procédure de destruction des équipements de traitement et des données n'est documentée ; ❖ Absence de politique réglementant l'utilisation des supports amovibles.

CESAG - BIBLIOTHEQUE

	Protection contre les incendies	❖ L'existence des extincteurs ; ❖ La salle des serveurs n'abrite pas des éléments inflammables.	❖ Pas de formation ou de sensibilisation sur l'utilisation des extincteurs ; ❖ L'absence de détecteurs de fumée ou d'autres dispositifs de détection d'incendie.
Sécurité logique	**Gestion des habilitations et des profils**	❖ La personne qui recense les besoins et fait la demande des droits d'accès est différente de celle qui délivrent les autorisations ; ❖ Chaque utilisateur dispose un « compte » constitué d'un identifiant, d'un mot de passe par rapport à ses responsabilités ; ❖ L'attribution des privilèges d'accès est limitée et contrôlée ; ❖ L'application comptable permet de retracer les opérations de chaque agent à partir de son code.	❖ Les exigences de contrôle des accès logiques ne sont pas documentées ; ❖ Pas de revue périodique des droits d'accès accordés aux utilisateurs ; ❖ Les exigences de sécurité ne sont pas intégrées dans les contrats de travail des agents ni des stagiaires ; ❖ Les droits d'accès ne sont pas automatiquement désactivés en cas de cessation de fonction ou de mutation.
	Gestion des mots de passe	L'attribution des mots de passe fait l'objet d'une procédure précisant les responsabilités des utilisateurs.	❖ Aucun critère de qualité et de sécurité dans le choix des mots de passe n'est imposé ; ❖ Les mots de passe ne font pas l'objet de renouvellement selon une périodicité définie ; ❖ Pas de note de sensibilisation quant aux bonnes pratiques de gestion des mots de passe.

CESAG - BIBLIOTHEQUE

Sensibilisation et formation	Des formations sur les applications sont organisées au besoin.	❖ Le personnel n'est pas souvent sensibilisé en matière de sécurité des systèmes d'information ; ❖ La PSSI n'est pas diffusée à l'ensemble du personnel ;
Documentation	Les utilisateurs disposent d'un manuel de procédure spécifique à leurs fonctions et des guides d'utilisation de l'application comptable.	Absence de version papier des guides utilisateurs de l'application comptable.
Sauvegarde et archivage	❖ Le plan de conservation des documents et des données est documenté ; ❖ La sauvegarde régulière des données comptables ; ❖ La sauvegarde hors site des données comptables.	❖ Les tests de restauration sont faits seulement à la demande des utilisateurs ; ❖ Les procédures de sauvegarde et de restauration des données ne sont pas documentées.
Conformité avec les exigences légales	Des procédures de protection des données personnelles et de la vie privée des agents sont définies et documentées.	
Gestion de la continuité de l'activité	❖ L'existence d'un site de secours permettant la continuité des fonctions métiers en cas de sinistre ou de défaillances majeures ; ❖ L'étude d'impact des risques préalablement fait avant la mise en place du site de secours ; ❖ Des tests d'efficacité fait avec l'exploitation des jeux.	❖ La procédure de gestion de la continuité n'est pas documentée ; ❖ La non exhaustivité des tests.

CESAG - BIBLIOTHEQUE

6.3.1.2. Les Feuilles d'Analyse des Risques de la mission

Les FAR seront présentées selon les domaines ou procédures du SIC concernés par la mission.

❖ **Organisation de la sécurité et gestion des risques**

<table>
<tr><th colspan="3">FEUILLE D'ANALYSE DE RISQUE (FAR)</th></tr>
<tr><td colspan="2">MISSION : AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE DE LA LONASE</td><td>Référence : FAR N°1/7
Date 1er septembre 2014</td></tr>
<tr><td colspan="3">RISQUE
Stratégie de sécurité de la LONASE non adaptée aux objectifs pouvant entraîner leur non atteinte.</td></tr>
<tr><td>FAITS</td><td colspan="2">❖ Absence de schéma directeur informatique et de charte de sécurité ;
❖ La PSSI n'est pas connue de tout le personnel (voir QCI, page 114)
❖ Les auditeurs internes n'incluent pas dans leur plan d'audit les missions d'audit des SI.</td></tr>
<tr><td>CAUSES</td><td colspan="2">❖ Manque de compétence des auditeurs internes ;
❖ Poste de responsable de la sécurité des SI non pourvu ;
❖ Coût élevé des missions externes de sécurité.</td></tr>
<tr><td>CONSEQUENCES</td><td colspan="2">❖ Inefficacité des mesures de sécurité ;
❖ Acquisition de dispositif de sécurité non nécessaire.</td></tr>
<tr><td>RECOMMANDATIONS</td><td>R1 : Faire communiquer à tout le personnel la PSSI
R2 : Définir un schéma directeur informatique et une charte de sécurité ;
R3 : Intégrer l'audit de la sécurité des SI dans le plan annuel d'audit.</td><td><u>DIRECTIONS CONCERNEES</u>:

R1…DG et DRH
R2…DG et DSIE
R3……DAIQ</td></tr>
<tr><td>ETABLI PAR
Nous-même</td><td>APPROUVE PAR
Directeur du mémoire</td><td>VALIDE PAR
DSIE ET DAIQ</td></tr>
</table>

CESAG - BIBLIOTHEQUE

<table>
<tr><th colspan="3">FEUILLE D'ANALYSE DE RISQUE (FAR)</th></tr>
<tr><td colspan="2">MISSION : AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE DE LA LONASE</td><td>Référence : FAR N°2/7
Date : 2 septembre 2014</td></tr>
<tr><td colspan="3">RISQUE
Difficulté à trouver des solutions adaptées aux risques de sécurité du SIC.</td></tr>
<tr><td>FAITS</td><td colspan="2">❖ Absence de politique formalisée d'identification, d'évaluation et de traitement des risques SI ;
❖ Le Conseil d'Administration n'a pas encore validé la cartographie des risques.</td></tr>
<tr><td>CAUSES</td><td colspan="2">❖ Absence de responsable des risques ;
❖ Cartographie des risques incomplète ;
❖ Méconnaissance de l'utilité d'une cartographie des risques par le Conseil d'Administration.</td></tr>
<tr><td>CONSEQUENCES</td><td colspan="2">❖ Pilotage à vue ;
❖ Actions inappropriées des utilisateurs pouvant porter atteinte à la sécurité des actifs informationnels ;
❖ Réponse inefficace en cas de sinistre.</td></tr>
<tr><td>RECOMMANDATIONS</td><td>R4 : Définir une politique formalisée de gestion des risques ;
R5 : Faire valider la cartographie des risques afin de disposer d'un outil de gestion des risques de sécurité des SI ;
R6 : Rendre quelqu'un responsable de la gestion des risques de sécurité.</td><td><u>DIRECTIONS CONCERNEES</u>:
Direction Générale (DG)</td></tr>
<tr><td>ETABLI PAR
Nous-même</td><td>APPROUVE PAR
Directeur du mémoire</td><td>VALIDE PAR
----------</td></tr>
</table>

CESAG BIBLIOTHEQUE

❖ Gestion de la sécurité physique et protection des actifs informationnels

<table>
<tr><th colspan="3">FEUILLE D'ANALYSE DE RISQUE (FAR)</th></tr>
<tr><td colspan="2">MISSION : AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE DE LA LONASE</td><td>Référence : FAR N°3/7
Date : 5 septembre 2014</td></tr>
<tr><td colspan="3">RISQUE
Accès physiques non autorisés aux zones et aux documents sensibles.</td></tr>
<tr><td>FAITS</td><td colspan="2">❖ Le personnel ne dispose d'aucun signe pouvant permettre de les distinguer des étrangers ;
❖ Les personnes étrangères ne se font attribuer aucun signe et ne sont non plus accompagnées au cours de leur visite ;
❖ Absence de dispositifs de traçabilité des accès à la salle des serveurs.</td></tr>
<tr><td>CAUSES</td><td colspan="2">❖ La méconnaissance de l'importance de port de signe d'identification ;
❖ Absence de politique de gestion des accès physiques ;
❖ Manque de moyens.</td></tr>
<tr><td>CONSEQUENCES</td><td colspan="2">❖ Vol ;
❖ Divulgation d'informations confidentielles ;
❖ Atteinte à la sécurité physique des actifs informationnels.</td></tr>
<tr><td>RECOMMANDATIONS</td><td>R7 : Mettre à la disposition du personnel un badge nominatif et rendre le port obligatoire
R8 : Faire concevoir des badges pour les visiteurs et exiger d'eux une pièce d'identité avant leur accès aux locaux ;
R9 : Renforcer les dispositifs protégeant l'accès à la salle des serveurs (vidéosurveillance, ouverture par badges électroniques)</td><td><u>DIRECTIONS CONCERNEES</u>:
R7 ……DRH
R8…DSIE et DRH
R9….DG et DSIE</td></tr>
<tr><td>ETABLI PAR
Nous-même</td><td>APPROUVE PAR
Directeur du mémoire</td><td>VALIDE PAR :
DSIE</td></tr>
</table>

CESAG - BIBLIOTHEQUE

<table>
<tr><th colspan="3">FEUILLE D'ANALYSE DE RISQUE (FAR)</th></tr>
<tr><td colspan="2">MISSION : AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE DE LA LONASE</td><td>Référence : FAR N°4/7
Date : 5 septembre 2014</td></tr>
<tr><td colspan="3">RISQUE
Protection insuffisante des actifs informationnels.</td></tr>
<tr><td>FAITS</td><td colspan="2">❖ Les actifs informationnels ne sont pas classés selon leur criticité ;
❖ Difficulté à définir une protection appropriées à chaque actif du SIC.</td></tr>
<tr><td>CAUSES</td><td colspan="2">❖ Absence de procédures d'identification et de classement des actifs informationnels ;
❖ Protection des actifs laissée au seul soin du Département des SI</td></tr>
<tr><td>CONSEQUENCES</td><td colspan="2">❖ Vol ;
❖ Destruction des matériels informatiques ;
❖ Pertes de données comptables sensibles.</td></tr>
<tr><td>RECOMMANDATIONS</td><td>R10 : Etablir un inventaire des actifs du SIC et placer chaque ressource sous la responsabilité d'un propriétaire ;
R11 : Définir une politique formalisée de gestion des actifs informationnels ;
R12 : Former le personnel sur la nécessité de la protection des actifs informationnels mis à leur disposition.
R13 : Veiller à ce que les médias informatiques fassent l'objet d'une utilisation contrôlée.
R14 : Faire tenir un journal des activités</td><td><u>DIRECTIONS CONCERNEES</u>:
R10 ……DSIE et DFC
R11……DG et DSIE
R12……DG, DSIE et DFC
R13 et R14 …….DFC et DSIE</td></tr>
<tr><td>ETABLI PAR
Nous-même</td><td>APPROUVE PAR
Directeur du mémoire</td><td>VALIDE PAR
DSIE ET DFC</td></tr>
</table>

CESAG - BIBLIOTHEQUE

- **Gestion de la sécurité logique (habilitation et profil d'utilisateurs, accès à l'application et au réseau local et à l'internet)**

<table>
<tr><th colspan="3">FEUILLE D'ANALYSE DE RISQUE (FAR)</th></tr>
<tr><td colspan="2">MISSION : AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE DE LA LONASE</td><td>Référence : FAR N°5/7
Date : 8 septembre 2014</td></tr>
<tr><td colspan="3">RISQUE
Gestion inadéquate des habilitations et des droits d'accès (login et mot de passe).</td></tr>
<tr><td>FAITS</td><td colspan="2">❖ Après octroi du droit d'accès, sa gestion est laissée à l'utilisateur ;
❖ Pas de critères exigés pour le niveau de sécurité des mots de passe ;
❖ Tous les sites Internet sont accessibles aux agents ;
❖ Pas de renouvellement périodique des droits accordés.</td></tr>
<tr><td>CAUSES</td><td colspan="2">❖ Absence de politique formalisée liée à la gestion des accès logiques ;
❖ Méconnaissance des risques d'une mauvaise gestion des habilitations ;
❖ Les exigences de sécurité ne sont pas intégrées dans les contrats de travail des agents ni des stagiaires.</td></tr>
<tr><td>CONSEQUENCES</td><td colspan="2">❖ Déni de service et ou virus provenant de sites malveillants ;
❖ Usurpation de mots de passe ou de login ;
❖ Atteinte à l'intégrité et à la confidentialité des données.</td></tr>
<tr><td>RECOMMANDATIONS</td><td>R15 : Définir une politique de gestion des droits d'accès et sensibiliser le personnel sur les bonnes pratiques en matière de choix et de gestion des mots de passe ;
R16 : Limiter l'accès à certains sites Internet ;
R17 : Intégrer les exigences de sécurité dans les contrats des contrats de travail et de stage.</td><td><u>DIRECTIONS CONCERNEES</u>:
R15 et R16……..DG et DSIE
R17…….DRH</td></tr>
<tr><td>ETABLI PAR
Nous-même</td><td>APPROUVE PAR
Directeur du mémoire</td><td>VALIDE PAR
DSIE</td></tr>
</table>

CESAG - BIBLIOTHEQUE

❖ Gestion des sauvegardes et des archives

<table>
<tr><th colspan="3">FEUILLE D'ANALYSE DE RISQUE (FAR)</th></tr>
<tr><td colspan="2">MISSION : AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE DE LA LONASE</td><td>Référence : FAR N°6/7
Date : 10 septembre 2014</td></tr>
<tr><td colspan="3">RISQUE
Non exhaustivité des sauvegardes des données comptables.</td></tr>
<tr><td>FAITS</td><td colspan="2">❖ Il n'existe pas de procédures formalisées décrivant les sauvegardes périodiques et les opérations à effectuer (voir QCI, page 114)
❖ Les sauvegardes ne sont faites que sur les baies (site principal et site de secours) de sauvegardes réservées à cet effet.</td></tr>
<tr><td>CAUSES</td><td colspan="2">❖ Méconnaissance de l'utilité de formaliser les procédures de sauvegarde ;
❖ Confiance excessive aux dispositifs de sauvegarde ;</td></tr>
<tr><td>CONSEQUENCES</td><td colspan="2">❖ Supports de sauvegarde non adaptés ;
❖ Perte de données en cas de sinistre.</td></tr>
<tr><td>RECOMMANDATIONS</td><td>R18 : Définir une politique décrivant les fichiers à sauvegarder, la périodicité des sauvegardes et la technique de sauvegarde ;
R19 : Diversifier les supports de sauvegardes</td><td><u>DIRECTION CONCERNEE</u>:
DSIE</td></tr>
<tr><td>ETABLI PAR
Nous-même</td><td>APPROUVE PAR
Directeur du mémoire</td><td>VALIDE PAR
DSIE</td></tr>
</table>

CESAG-BIBLIOTHEQUE

❖ Gestion de la continuité des activités : plan de continuité des activités

<table>
<tr><th colspan="3">FEUILLE D'ANALYSE DE RISQUE (FAR)</th></tr>
<tr><td colspan="2">MISSION : AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE DE LA LONASE</td><td>Référence : FAR N°7/7
Date : 12 septembre 2014</td></tr>
<tr><td colspan="3">RISQUE
Non exhaustivité des données comptables après reprise en cas de sinistre sur le site principale</td></tr>
<tr><td>FAITS</td><td colspan="2">❖ Seule l'exploitation des jeux a fait l'objet d'un test au niveau du site de secours ;
❖ Les tests ne sont pas faits régulièrement pour juger de l'efficacité du plan de reprise d'activité (voir QCI, page 115) ;
❖ Le personnel manque d'informations sur la conduite à tenir en cas de sinistre sur le site principal (voir QCI, page 115).</td></tr>
<tr><td>CAUSES</td><td colspan="2">❖ Il n'existe pas de procédures formalisées décrivant le plan de reprise et la périodicité des tests de fiabilité ;
❖ Ignorance de la nécessité des tests du plan de reprise ;
❖ Confiance excessive aux dispositifs de sécurité mise en place au niveau du site de secours.</td></tr>
<tr><td>CONSEQUENCES</td><td colspan="2">❖ Réponses inadéquates en cas de sinistre ;
❖ Panique des agents en cas de sinistre ;
❖ Perte d'actifs informationnels suite à un sinistre.</td></tr>
<tr><td>RECOMMANDATIONS</td><td>R20 : Définir une politique décrivant les différentes étapes de reprise d'activité ;
R21 : Mettre en place un système de reporting des incidents ;
R22 : Tester régulièrement le plan de sauvegarde et de reprise.</td><td><u>DIRECTIONS CONCERNEES</u>:
R19……DG et DSIE
R20…… DSIE
R21…DAIQ et DSIE</td></tr>
<tr><td>ETABLI PAR
Nous-même</td><td>APPROUVE PAR
Directeur du mémoire</td><td>VALIDE PAR
DSIE ET DAIQ</td></tr>
</table>

CESAG - BIBLIOTHEQUE

6.3.2. Hiérarchisation et plan de mise en œuvre des recommandations

L'un des objectifs de notre étude et le plus ultime d'ailleurs consiste à proposer des axes susceptibles d'aider la LONASE à améliorer ou à renforcer ses dispositifs et procédures de sécurité existants ou à proposer ceux qui sont nécessaires et que la LONASE n'a pas encore mis en place.

Ces recommandations devront permettre à la LONASE de se préparer pour « l'audit à blanc » de la certification à la norme ISO 27001 comme le prévoient les dirigeants ainsi que tout le personnel.

Nous proposons également, un plan (tableau 11) pour la mise en œuvre des recommandations formulées. Nonobstant, nous n'assurerons pas leur suivi.

Tableau 11 : Plan de mise en œuvre des recommandations

Référence	Nature de la recommandation	Responsable de la mise en œuvre	Calendrier
FAR4 :R13 et R14	Gestion de la sécurité physique	DFC et DSIE	A partir de maintenant
FAR5 : R16	Gestion de la sécurité logique	DG, DSIE, DFC	
FAR 5 : R17	Gestion de la sécurité logique	DRH	
FAR 1 : R1	Organisation et gestion des risques de la sécurité	DRH	1 mois
FAR 4 : R10	Gestion de la sécurité physique	DSIE et DFC	
FAR 7 : R21	Gestion de la continuité des activités	DSIE DRH	
FAR 6 : R19	Gestion des sauvegardes et des archives	DSIE	
FAR 2: R4	Organisation et gestion des risques de la sécurité	DG	2 mois
FAR5 : R15	Gestion de la sécurité logique	DG et DSIE	
FAR 1 : R2	Organisation et gestion des risques de la sécurité	DG, DSIE	
FAR 4 : R11	Gestion de la sécurité physique	DG et DSIE	
FAR 6 : R18	Gestion des sauvegardes et des archives	DSIE	
FAR 2: R6	Organisation et gestion des risques de la sécurité	DG	
FAR 7 : R20	Gestion de la continuité des activités	DRH	
FAR 3 : R7	Gestion de la sécurité physique	DRH	
FAR 3 : R8	Gestion de la sécurité physique	DRH et DSIE	3 mois
FAR 3 : R9	Gestion de la sécurité physique	DG et DSIE	

CESAG - BIBLIOTHEQUE

FAR 7 : R22	Gestion de la continuité des activités	DG et DSIE	Chaque 3 mois
FAR 4 : R12	Gestion de la sécurité physique	DG, DSIE, DFC	
FAR 1 : R3	Organisation et gestion des risques de la sécurité	DG	Prochain plan d'audit
FAR 2: R5	Organisation et gestion des risques de la sécurité	DG	Prochain CA

Source : Nous-mêmes

Conclusion du sixième chapitre

La sécurité des systèmes d'information est un ensemble qui concerne une chaîne d'éléments (infrastructures matérielles de traitement ou de communication, les logiciels (systèmes d'exploitation ou applicatifs), les données, le comportement des utilisateurs).

Dans ce chapitre, nous avons passé en revue les dispositifs et procédures de sécurité mis en place par la LONASE. Il nous a également permis de faire le point des forces et des faiblesses de ces contres- mesures. Ainsi, de ces analyses, a découlé notre projet de rapport qui a pris en compte les résultats des évaluations des dispositifs et des procédures de sécurité du SIC de la LONASE et des tests d'existence et de corroboration.

CESAG - BIBLIOTHEQUE

Conclusion de la deuxième partie

Le niveau global de sécurité étant défini par le niveau de sécurité du maillon le plus faible, les précautions et les contre-mesures doivent être envisagées en fonction des vulnérabilités propres au contexte auquel le système d'information est censé apporter services et appui.

A travers cette partie pratique de notre étude, nous avons pu découverts la LONASE ainsi que de son SIC. Nous avons mis en évidence, d'une part, les pratiques de sécurités actuelles à travers un ensemble de procédures légales, réglementaires, de dispositifs de sécurité physiques et logiques ; lesquelles ont fait l'objet, d'autre part, d'une évaluation. Nous avons également présenté les résultats qui sont par la suite analysés par thème à travers des Feuilles d'Analyse de Risques avec des recommandations en fonction des faiblesses et dont l'ensemble a constitué le projet de rapport de la mission.

CESAG - BIBLIOTHEQUE

CONCLUSION GENERALE

CESAG - BIBLIOTHEQUE

L'objectif de cette étude était de documenter le niveau de vulnérabilité du Système d'Information Comptable de la LONASE par rapport aux différentes menaces afin de proposer des pistes d'amélioration. Cela à travers l'évaluation de l'effectivité et de l'efficacité des mesures mises en place par la LONASE pour répondre aux critères de disponibilité, d'intégrité et de confidentialité de ce système.

En effet, deux parties nous ont permis de répondre aux différents questionnements attachés à cette étude.

La théorie sur le système d'information comptable et sur l'audit de sa sécurité a fait l'objet de la première partie. Nous avons parcouru les bonnes pratiques en la matière qui aident les organisations dans la définition de leur propre politique de sécurité des systèmes d'information et les aspects pratiques de l'audit de la SSI.

Dans la deuxième partie, nous avons passé en revue les pratiques liées à la sécurité du système d'information comptable de la LONASE.

Ainsi, après évaluation des dispositifs et des procédures de sécurité existants en ce qui concerne le SIC, il ressort que le risque est consubstantiel à l'activité de la LONASE comme pour toute organisation d'ailleurs. Ce qui rend fondamentale la définition, par la LONASE, d'un cadre approprié de gestion de risques. En effet, il est de plus en plus difficile, voire impossible, de connaître à l'avance toutes les menaces et de détecter toutes les vulnérabilités ; car il en apparaît de nouvelles chaque jour avec le développement des technologies de l'information.

Par ailleurs, nous avons pu noter que les dispositifs et procédures déployés par la LONASE pour assurer la sécurité de son SIC, certes, qu'ils présentent un niveau de sécurité appréciable, doivent être améliorés et surtout évalués périodiquement afin de s'assurer de leur efficacité. De même, il serait opportun que la LONASE intègre les questions de sécurité dans la gestion quotidienne de ses opérations et qu'un organe détienne la responsabilité de cette sécurité des SI tout en sollicitant le concours de tout le personnel. En reprenant le dit-on : « mieux vaut prévenir que guérir », nous pouvons rajouter qu'en ce qui concerne ce domaine, prévenir est plutôt impératif, parce que guérir est quasi impossible et de toute façon ne sert à rien.

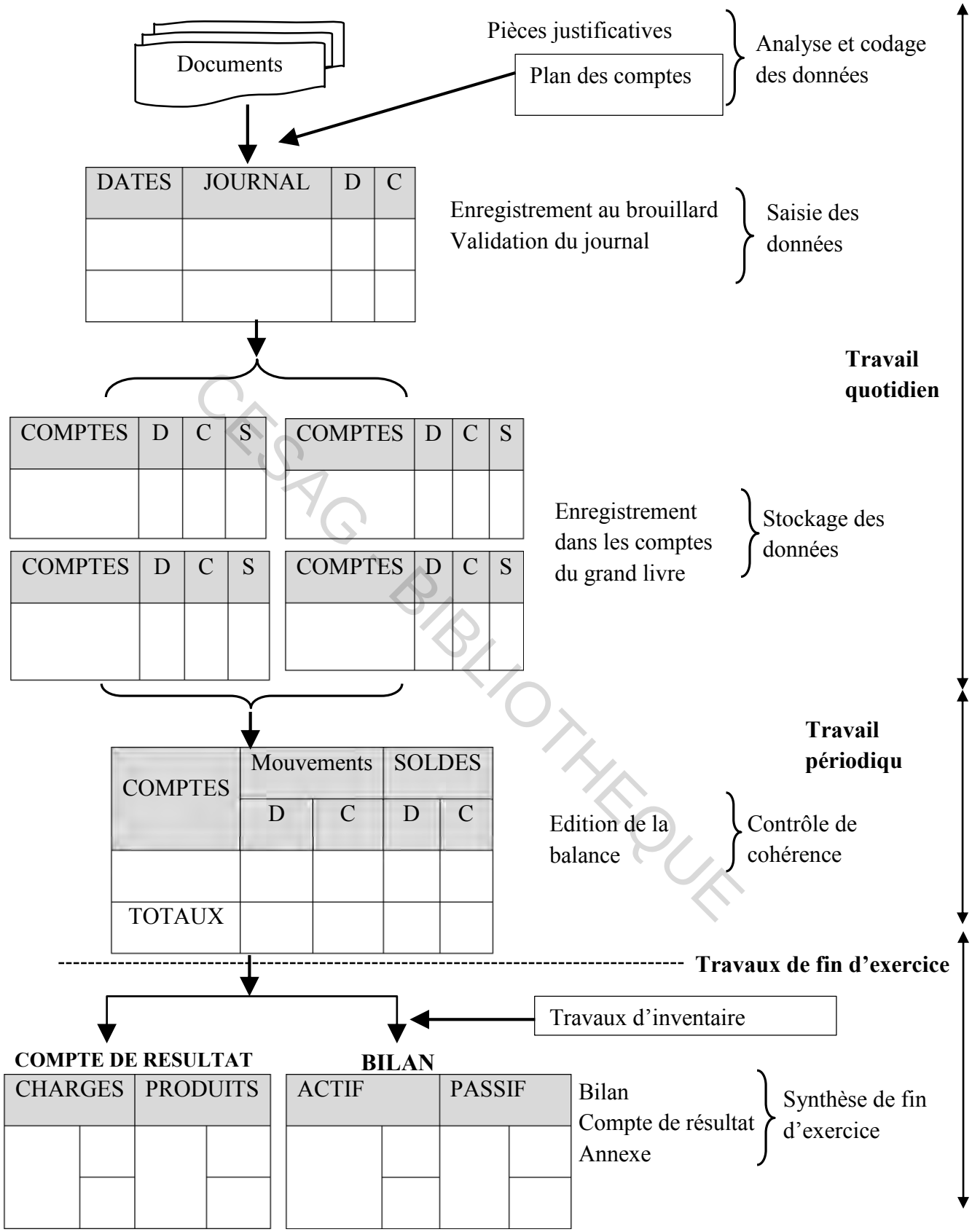
Notre étude étant limitée aux aspects procéduraux et organisationnels de la LONASE, des études techniques notamment les tests d'intrusion sur le réseau pourront révéler d'autres menaces, vulnérabilités qui susciteront des actions appropriées. Une évaluation de la sécurité des autres systèmes d'information serait également un atout considérable.

CESAG - BIBLIOTHEQUE

ANNEXES

CESAG - BIBLIOTHEQUE

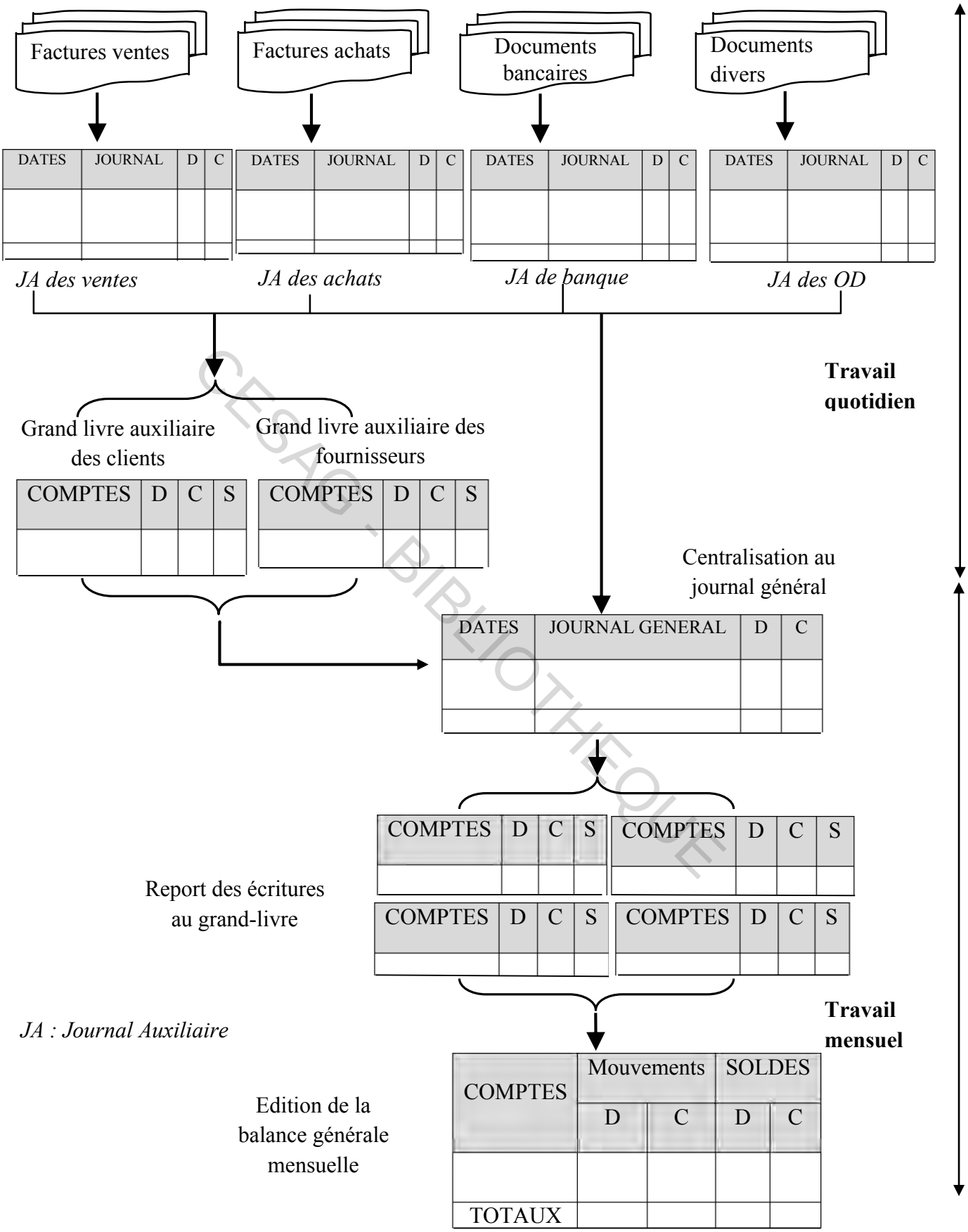
Annexe 1: Schéma de traitement des données comptables en système classique



Source : DORIATH & al. (2008 : 2)

CESAG BIBLIOTHEQUE

Annexe 2: Schéma de traitement des données comptables en système centralisateur

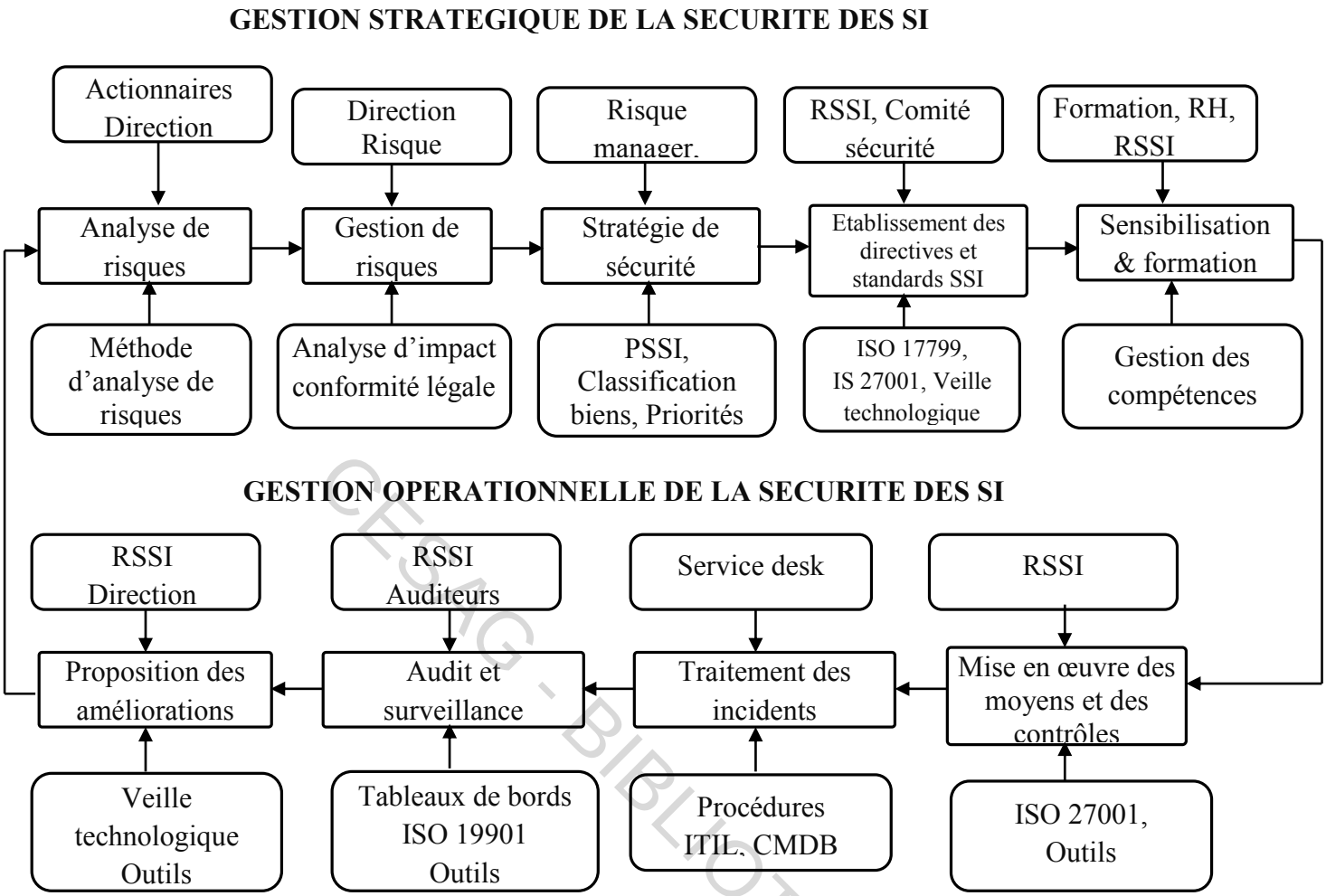


JA : Journal Auxiliaire

Source : DORIATH & al. (2008 : 3)

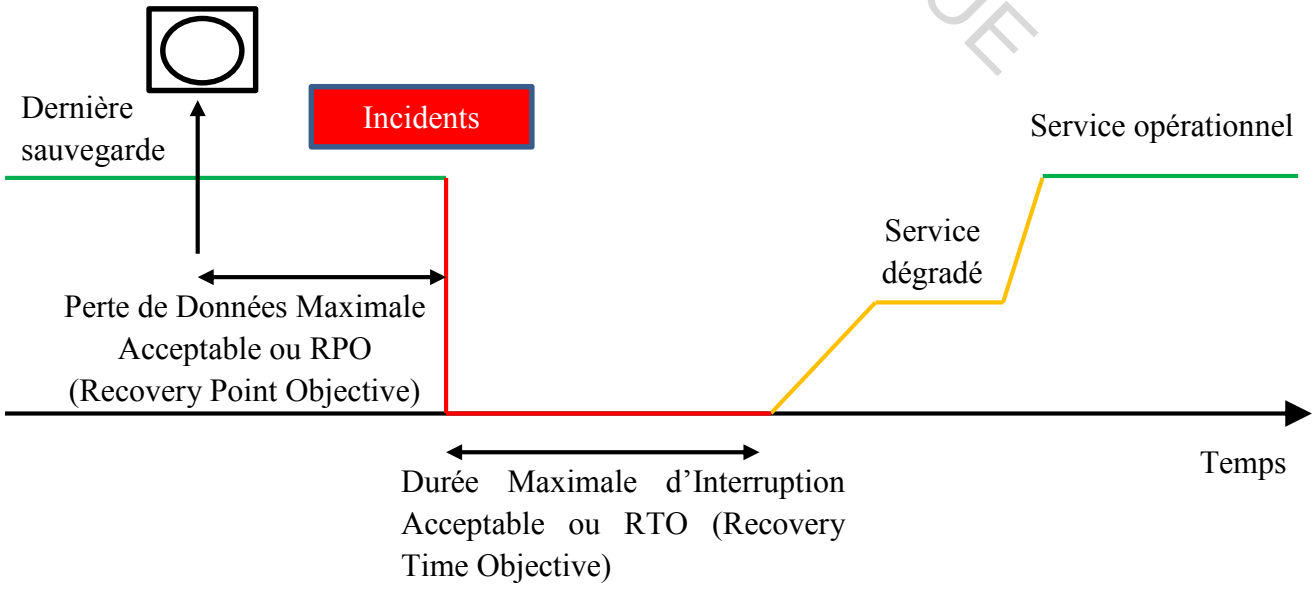
CESAG - BIBLIOTHEQUE

Annexe 3: Processus de la gestion de la sécurité des systèmes d'information



Source : CLUSIS (2007 : 2)

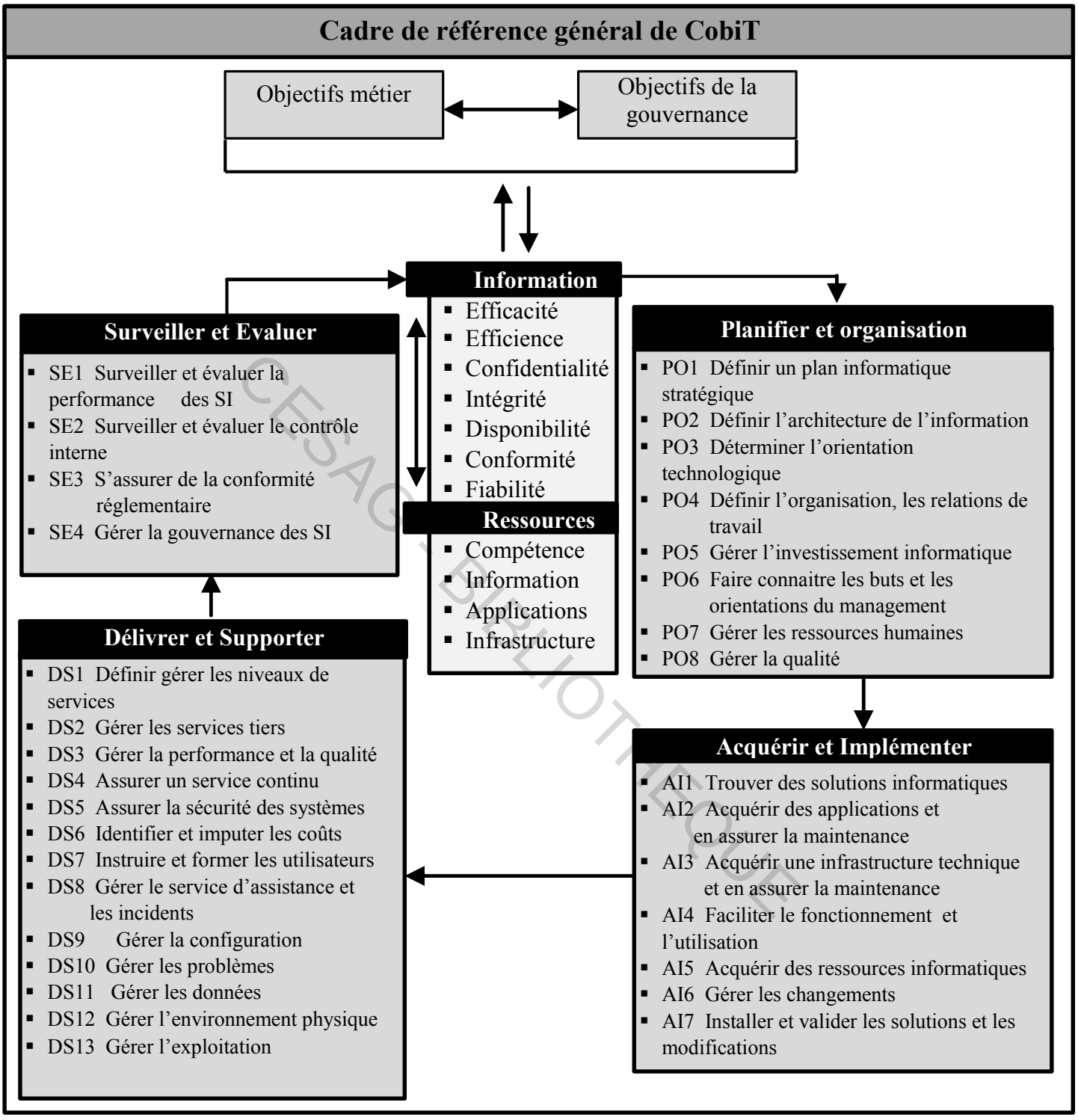
Annexe 4: Définition d'un plan de reprise en fonction du RPO et du RTO



Source : Nous-mêmes à partir de KEREBEL (2009 : 64).

CESAG - BIBLIOTHEQUE

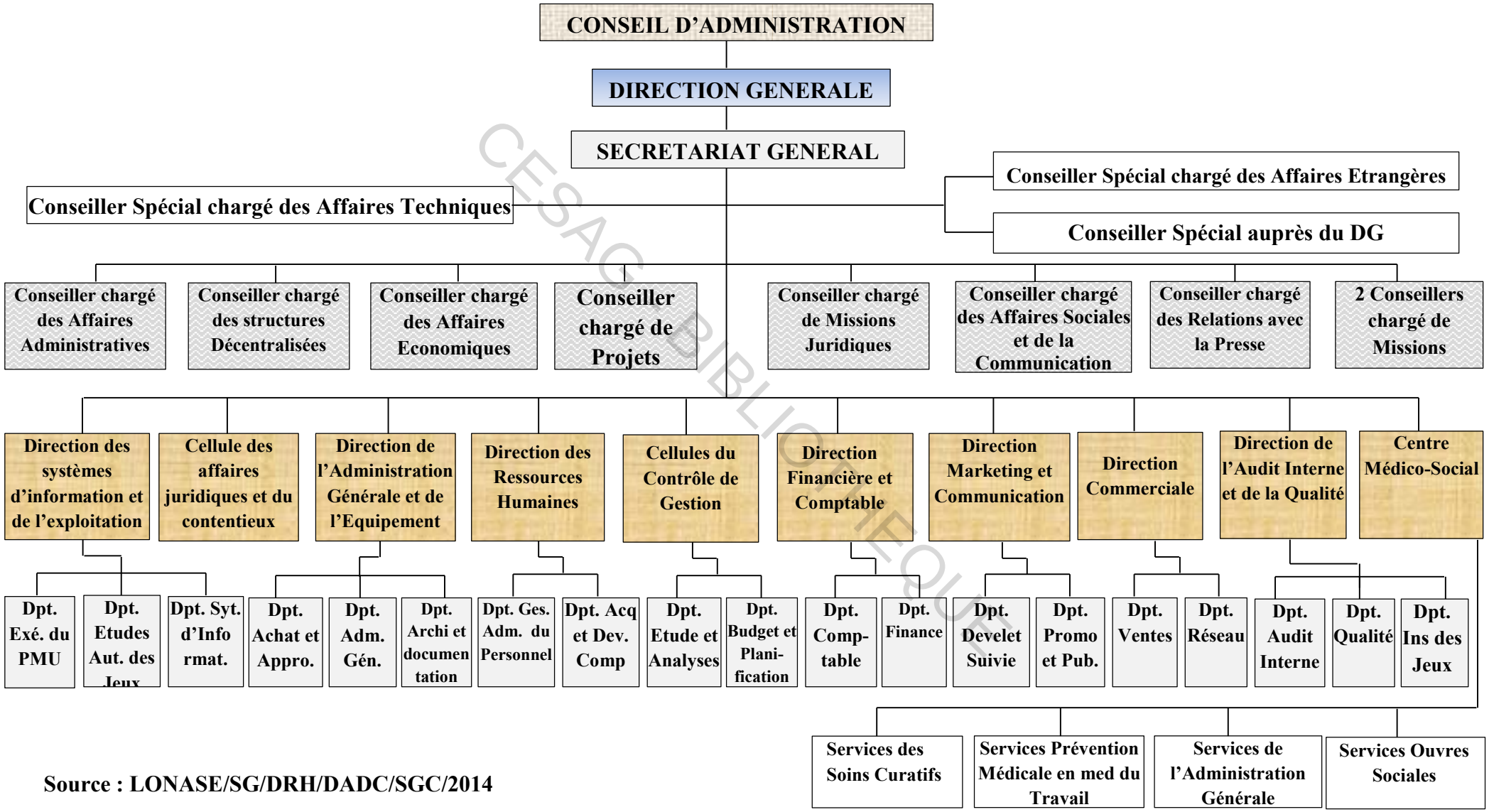
Annexe 5: Organisation du référentiel CobiT



Source : MOISAND & al. (2009 : 30)

CESAG - BIBLIOTHEQUE

Annexe 6: Organigramme de la LONASE



CESAG BIBLIOTHEQUE

Source : LONASE/SG/DRH/DADC/SGC/2014

Annexe 7: Questionnaire de Prise de Connaissance

Audit de la Sécurité du Système d'Information Comptable **QUESTIONNAIRE DE PRISE DE CONNAISSANCE**	**Entité : LONASE** **Référence : QCP/JD**
OBJECTIFS ❖ Comprendre l'environnement interne et externe de la LONASE ; ❖ S'imprégner du système d'information comptable de la LONASE et bien cerner les problématiques apparentes ; ❖ Prendre connaissance des risques liés au SIC.	
DOMAINES CONCERNES PAR LES QUESTIONS	**ACTIONS A MENER**
I. SECTEUR D'ACTIVITE	
1. DOMAINE ET PRODUITS DE LA LONASE ❖ nature du secteur d'activité ; ❖ historique du développement économique de la LONASE ; ❖ principaux produits ; ❖ risques particuliers du secteur d'activité ; ❖ positionnement de l'entité dans le secteur.	Examiner les documents qui peuvent nous informés sur le secteur d'activité et les réglementations en vigueur.
2. FACTEURS EXTERNES ❖ réglementation sur l'environnement de l'entreprise et celui du système d'information comptable ; ❖ facteurs de risques identifiés autres que sur le secteur et le SIC.	
II. ORGANISATION DE LA LONASE	
3. STRUCTURE INTERNE ❖ organigramme général de la LONASE et celui de la DFC ; ❖ fonctions et responsabilités ; ❖ identification des interlocuteurs importants pour notre mission ; ❖ existence de manuel de procédure comptable ; ❖ existence d'un comité de sécurité.	Prendre connaissance : ☐ de l'organigramme fonctionnel ☐ du manuel des procédures comptables

CESAG - BIBLIOTHEQUE

4. POLITIQUE DE LA DIRECTION ❖ perception du risque par la direction ; ❖ identification des systèmes mis en place.	Faire un entretien avec la Directrice Comptable et Financière.
III. DONNEES JURIDIQUES	
5. FORMES JURIDIQUES ❖ forme actuelle ; ❖ historique des formes sociales précédentes ; ❖ objet social.	
IV. SYSTEME D'INFORMATION COMPTABLE	Prendre connaissance du manuel de procédures comptables et financières et des documents spécifiques sur le système d'information comptable.
6. MODE DE GESTION COMPTABLE ❖ type de système comptable (manuel ou automatique) ; ❖ outil informatique ; ❖ liste des intervenants et fonctions respectives.	
7. ORGANISATION COMPTABLE ❖ plan comptable utilisé ; ❖ système d'organisation comptable (classique ou centralisateur) ; ❖ archivage des documents comptables.	
V. SUPPORT INFORMATIQUE	Prendre connaissance des documents informatiques qui nous seront accessibles
8. FONCTIONS INFORMATISEES ❖ liste des traitements comptables informatisés ; ❖ outils utilisés (logiciel intégré, application spécifique, outil bureautique) pour la gestion des opérations comptables ; ❖ opérateurs (compétence et formation) ; ❖ procédures de protection et de sauvegarde ; ❖ procédures de maintenance (intervenants et contrats).	
9. EXISTENCE DE PROCEDURES ET DOCUMENTATIONS ❖ politique informatique ; ❖ schéma directeur ; ❖ fonctions informatiques ; ❖ état de la documentation informatique (produit, source, utilisateur)	

Source : Nous-mêmes

CESAG - BIBLIOTHEQUE

Annexe 8: Questionnaire de Contrôle Interne

Audit de la Sécurité du Système d'Information Comptable **QUESTIONNAIRE DE CONTROLE INTERNE**	Entité : LONASE Référence : QCI/JD Date : 20 Août 2014

OBJECTIFS

- S'assurer que les risques liés à la Sécurité du Système d'Information Comptable sont maîtrisés ;
- Identifier les pratiques de sécurité et faire ressortir leurs forces et faiblesses ;
- S'assurer que le dispositif de contrôle interne favorise la disponibilité, l'intégrité et la confidentialité des informations comptables.

QUESTIONS	**REPONSES**			**COMMENTAIRES**
	Oui	**Non**	**N/A[7]**	
I. Organisation générale du système d'information comptable.				
1. Existe-t-il un organe chargé de l'organisation et de la gestion du système d'information comptable ?	X			Il s'agit de la Direction des SI
2. Certaines fonctions du système d'information comptable ont-elles été externalisées?		X		
3. Existe-t-il dans votre organisation un Responsable de la Sécurité du Système d'information ?		X		Le service réseaux, maintenance et sécurité en est la charge
4. Un document officiel ou charte de la sécurité du système d'information existe-t-il ?		X		En cours de validation
5. Cette charte ou document officiel sur la sécurité du système d'information a-t-elle été entérinée par l'ensemble des instances de l'organisation ?			X	
6. Quels sont les moyens de diffusion de cette charte?			X	

[7] N/A : Non applicable

CESAG BIBLIOTHEQUE

7. Cette charte prévoit-elle des mesures de sanctions à l'égard des personnes qui l'enfreignent ?			X	
II. Formation, Documentation technique et utilisateurs du SI comptable				
8. Des séances de formation et/ou de sensibilisation sont-elles organisées en ce qui concerne la charte de sécurité ?		X		
9. Les utilisateurs actuels des applications comptables ont-ils reçu une formation initiale spécifique ?	X			
10. La documentation utilisateur et/ou le manuel de procédures comptables sont-ils facilement accessibles et exploitables ?	X			Chaque service dispose de la partie du manuel qui lui est propre.
III. Sécurité du Système d'Information Comptable				
Analyse de la politique de gestion des risques				
11. Disposez-vous d'une cartographie des risques ; inclut les risques liés au système d'information comptable ?	X			En cours de validation par le Conseil d'Administration
12. Des actions spécifiques à la gestion des risques du système d'information comptables ont-elles été définies ?		X		En cours
13. Lesquelles des actions assurent: ❖ la protection du patrimoine et des actifs informationnels ? ❖ la conformité aux lois et règlements en vigueur ?				
Sécurité logique (identification et authentification des utilisateurs)				
Politique générale et identification des utilisateurs				
14. Existe-t-il une politique de sécurité logique documentée permettant la mise en œuvre de règles de sécurité communes et homogènes entre les différentes entités utilisatrices du Système d'information Comptable? NB : *Par logique, nous faisons référence aux contrôles d'accès par mots de passe (complexité, périodicité, etc.), aux actions de sensibilisation, formations, etc.*	X			La politique n'est pas documenter.

CESAG BIBLIOTHEQUE

15. Quels sont les critères d'attribution de droit d'accès (code d'utilisateur) à l'application comptable?	Identifiant à partir du nom et prénom de l'agent avec un mot de passe par défaut			
16. Qui fait la demande d'attribution de droit d'accès à l'application comptable? ❖ la DFC ou le chef comptable ; ❖ l'intéressé lui-même ; ❖ autres	La DFC ou le chef comptable			
17. Qui autorise l'attribution d'identification ? ❖ un agent du service informatique ; ❖ la directrice de la DFC le chef comptable ; ❖ autres.	L'administrateur des droits d'accès (service informatique)			
18. Existe-t-il un système d'identification de chaque utilisateur : ❖ pour l'accès au réseau local de l'établissement? ❖ pour l'accès au réseau Internet ? ❖ pour l'accès aux données et programmes stockés sur la poste de travail de l'utilisateur ? ❖ pour l'accès aux paramètres de l'application comptable?	X X X			
19. Les droits d'accès sont-ils en cohérence avec les fonctions exercées ?	X			
20. Les nouvelles autorisations d'accès au système d'information comptable donnent-elles systématiquement lieu à la signature par les agents d'une attestation de reconnaissance de responsabilité, par laquelle ils s'engagent à respecter les règles de sécurité définies par la LONASE ?		X		
21. Les demandes de désactivation des autorisations d'accès au système d'information comptable sont-elles systématiquement formalisées lors de la cessation de fonction :				

CESAG - BIBLIOTHEQUE

❖ d'un agent ? ❖ d'une personne exerçant des fonctions à titre temporaire ?		X	X	Elle n'a pas accès
22. Selon quelle périodicité la LONASE réalise-t-elle une revue des droits d'accès accordés à l'application comptable ?	Aucune périodicité définie			
Qui effectue cette tâche ?				DSI
23. Les documents justifiant l'ouverture des droits d'accès au SIC sont-ils archivés : ❖ par les services demandeurs ? ❖ la Direction Comptable et Financière? ❖ par le service informatique ?		X		
24. Existe-t-il dans l'application comptable un système d'authentification spécifique pour la validation d'opérations sensibles (exemple : code « validant » différent d'un code « saisissant») ?	X			
25. Les mots de passe apparaissent-ils en clair lors de leur saisie dans le système que vous utilisez ?		X		
26. Les mots de passe font-ils l'objet d'un renouvellement régulier ?		X		
Si oui, selon quelle périodicité ?	Selon la volonté du détenteur.			
27. Existe-t-il un enregistrement des tentatives d'accès non autorisés à l'application?		X		
28. Tout utilisateur du système d'information est-il systématiquement déconnecté après plusieurs tentatives d'accès infructueuses ?		X		
Si oui, la réactivation du compte désactivé nécessite-t-elle l'intervention d'une tierce personne (chef de département, agent du service informatique) ?			X	
29. Existe-t-il un mouchard dans l'application comptable accessible en lecture au seul administrateur d'application ?	X			Possibilité de retracer chaque opération à partir du code.

CESAG - BIBLIOTHEQUE

Sécurité physique du Système d'Information Comptable				
30. La Direction de la LONASE a-t-elle défini une politique de sécurité physique ? NB : *Par physique, nous entendons la protection contre le vol, l'incendie, les inondations, protection des accès physique, protection des supports de données (sauvegardes), etc.*	X			
31. Celle-ci a-t-elle été formalisée au travers d'un document diffusé à l'ensemble des agents comptables de la LONASE?		X		
32. L'accès aux locaux abritant les matériels informatiques (serveurs et autres) est-il limité aux seuls administrateurs du système informatique?	X			
33. Disposez-vous d'un processus permettant de journaliser et de surveiller les accès des locaux et d'enregistrement de tous les visiteurs ?		X		L'accès est surveillé par des vigiles mais pas d'enregistrement formel
34. Les personnes étrangères sont-elles accompagnées lors de leurs visites ?		X		
35. Est-ce qu'un règlement impose au personnel le port en permanence d'un signe d'identification visible ?		X		
IV. Exploitation du SI comptable et financier				
36. Existe-t-il une possibilité pour les utilisateurs de modifier les paramètres de l'application ?		X		
37. Une traçabilité de ces modifications existe-t-elle ?			X	
38. Est-ce que la maintenance est uniquement assurée par le personnel autorisé ?	X			
V. Sauvegarde et archivage des données comptables				
39. Est-ce qu'il existe une procédure de sauvegarde des données comptables clairement définie ?	X			
Si oui ; ces procédures de sauvegarde ont-elles été formalisées dans un document de référence mis à disposition des personnels concernés ?		X		

CESAG - BIBLIOTHEQUE

40. Les sauvegardes font-elles l'objet de tests de restauration périodique ?		X		Restauration à la demande
41. Disposez-vous d'un dispositif approprié pour la conservation des supports de sauvegarde ?	X			
VI. Plan de continuité de l'activité				
42. Une politique a-t-elle été définie par la LONASE en matière de procédure de secours en cas de sinistre majeur sur site (back-up) ? Est-elle formalisée ?	X	X		Nous avons un site de secours.
43. Ce document a-t-il été porté à la connaissance des personnes concernées par la procédure de reprise ?			X	
44. L'élaboration du plan de secours a-t-elle été basée sur une analyse préalable de l'impact des risques sur l'activité de la LONASE ?	X			
45. Des tests de simulation de reprise de l'exploitation de l'application comptable à partir du site de secours ont-ils été effectués ?		X		Des tests sont seulement faits avec l'exploitation des jeux.

Source : Nous-mêmes.

CESAG BIBLIOTHEQUE

<u>Annexe 9</u>: Guide d'entretien

AVEC LA DFC ET LE CHEF DE DEPARTEMENT COMPTABLE

1. Quelle application comptable vous utilisez ?
2. Quels sont les risques liés au système d'information que vous utilisez ?
3. Quelles sont les missions de l'organe qui est en charge du pilotage du système d'information comptable ?
4. Quel est le rôle de la Direction des Systèmes d'Information dans l'exploitation de l'application comptable?
5. Depuis quand les utilisateurs actuels travaillent-ils sur les différentes applications ?

6. Comment assurez-vous le maintien des compétences des utilisateurs du système d'information comptable ?
7. Quelles sont les règles de sauvegarde des données du SIC ?
8. Quelle est la fréquence des sauvegardes ?
9. a. Combien de temps au moins les données comptables sont-elles conservées ?

   b. Comment assurez-vous la conservation de ces données ?
10. a. Les sauvegardes font-elles l'objet de tests de restauration ?

    b. Si oui, selon quelle périodicité ?
11. Les résultats sont-ils documentés ?
12. Existe-t-il un suivi de ces tests ?

AVEC LE DSIE ET LE CHEF DU DEPARTEMENT DES SI

1. Quelles sont vos missions au regard du système d'information comptable ?
2. Quels sont vos dispositifs de sécurité physiques et logiques actuels ?
3. Comment vérifiez-vous leur efficacité ?
4. Quelle est la dernière date de la revue de ces dispositifs ?
5. Comment contrôlez-vous l'accès au poste de travail, à l'application comptable et aux données comptables par les utilisateurs ?
6. Faites-vous appel à un expert ou un organisme externe (cabinet spécialisé) pour les contrôles de sécurité physique logique du SI ?

   b. Si oui, quelle est la fréquence des contrôles extérieurs ?

   c. Quelle est la date du dernier contrôle ?

   d. Si non, un organe interne est-il désigné pour cette tâche ?
7. Comment assurez-vous la prévention contre l'incendie ?
8. Des anomalies ont-elles été identifiées dans l'application du système ?
9. Si oui, quelles sont les procédures qui ont été mises en œuvre pour les résoudre ?
10. Quels sont les dispositifs de reprise des activités en cas de sinistre sur le site ?
11. Comment assurez-vous de l'efficacité de ces dispositifs ?
12. Quels sont les protocoles d'accès à la salle des serveurs ?

CESAG - BIBLIOTHEQUE

Annexe 10: Tableau des risques

Tâches	Objectifs	Risques associés	Appréciation du niveau du risque	Dispositifs de contrôle existants ou souhaitables	Constats
Organisation et gestion de la sécurité du SIC	S'assurer que l'organisation et la gestion de la sécurité du SIC est efficace	Inadéquation des moyens de sécurité mise en œuvre par rapport aux objectifs de la LONASE	Moyen	Existence d'une politique de sécurité des systèmes d'information approuvée par la haute hiérarchie	Oui
				Description d'un schéma directeur informatique	Non
		Inefficacité dans l'organisation de la sécurité de l'information	Elevé	Mise en place d'un comité de gestion de la sécurité de l'information	Non
				Existence de fonction de gestion des risques SI (Risk Manager et RSSI)	Non
		Non alignement stratégique des objectifs de sécurité par rapport aux objectifs de LONASE	Moyen	Définition d'une politique générale de sécurité adaptée incluant la sécurité du SIC	Oui
				Communication de la politique de sécurité à tout le personnel	Non
				Revue périodique de la politique de sécurité	Non
		Insatisfaction des utilisateurs	Moyen	Enquête de satisfaction périodique	Non
				Existence de modalité d'échange entre les informaticiens et les utilisateurs	Non

CESAG - BIBLIOTHEQUE

Gestion des risques SI et protection des actifs informationnels	S'assurer de l'existence d'une procédure de gestion efficace des risques liés au SIC	Identification et/ou évaluation inadéquate des menaces, des vulnérabilités et des impacts des sinistres potentiels	Moyen	Utilisation d'une méthode formalisée d'analyse et de gestion des risques	Non
				Existence d'une cartographie des risques comprenant les risques liés au SIC	Oui
				Intégration des procédures de gestion des risques dans les activités quotidiennes	Oui
	S'assurer de la protection des actifs informationnels	Protection insuffisante des actifs informationnels	Elevé	Existence d'une procédure d'identification et de classification des ressources du SIC	Non
				Désignation d'un propriétaire pour chaque ressource	Non
		Destruction des matériels et/ou des données suite à un incendie	Elevé	Détecteur de fumée	Oui
				Existence des extincteurs	Oui
				Formation à l'usage des extincteurs	Non
		Coupure d'électricité	Moyen	Existence d'un groupe électrogène à démarrage automatique et des onduleurs	Oui
Gestion de la sécurité physique (accès et protection)	S'assurer que seules les personnes autorisées ont accès au SIC	Accès non autorisé aux locaux abritant les actifs sensibles	Elevé	Formalisation des procédures réglementant l'accès physique aux zones sécurisées	Non
				Dispositifs de contrôle physique des accès et traçabilité des accès aux zones sécurisées	Non
				Port obligatoire de signe visible d'identification par les personnes internes ou externe accédant aux locaux	Non

CESAG - BIBLIOTHEQUE

Gestion de la sécurité physique (accès et protection)	S'assurer que seules les personnes autorisées ont accès au SIC	Protection insuffisante des équipements contre les menaces physiques (pertes, des vols, des destructions, d'interruption de service, etc.)	Moyen	Confinement des actifs critiques dans des zones sécurisées	Oui
				Vidéosurveillance	Non
				Sécurité de l'alimentation électrique	Oui
				Service de gardiennage	Oui
				Existence des extincteurs	Oui
Gestion de la sécurité logique (gestion des habilitations)	S'assurer de la protection du SIC contre les accès logiques non autorisés	Mauvaise gestion des habilitations	Elevé	Définition de procédures formalisées de gestion des habilitations	Non
				Existence de procédures formalisées d'attribution, de désactivation et de mise à jour des droits d'accès	Non
				Journalisation des évènements (accès, tentatives d'accès)	Oui
		Usurpation des droits d'accès	Elevé	Sensibilisation à la tenue sécurisée des droits d'accès	Non
				Existence d'une liste des droits d'accès actifs ou non	Non
		Utilisation abusive du SIC pouvant entrainer le ralentissement des traitements	Moyen	Restriction d'accès à l'information en fonction des droits	Oui
				Limitation des téléchargements	Non
				Firewall, Logiciel antivirus	Oui
				Isolement des réseaux sensibles de l'Internet	Oui
				Contrôle des accès à l'Internet	Non
		Accès non discriminé aux applications	Moyen	Séparation des tâches incompatibles	Oui
				Politique de gestion des privilèges	Oui

CESAG - BIBLIOTHEQUE

Gestion des mots de passe	S'assurer de la bonne gestion des mots de passe	Mots de passe non sécurisés	Moyen	Définition d'une politique formalisée des critères de choix et de gestion des mots de passe	Non
				Renouvellement périodique obligatoire des mots de passe	Non
		Déni de service	Faible	Formation périodique sur l'ingénierie sociale	Non
Sauvegarde et stockage de données	Etre sûr que les données comptables sont sauvegardées de manière périodique sur différents supports à différents endroits	Absence de sauvegarde régulière	Faible	Procédures de sauvegarde automatisée des données	Non
		Sauvegarde et archivage non exhaustifs	Faible	Contrôle périodique des sauvegardes (restaurations périodiques)	Non
		Altération du support de sauvegarde	Faible	Diversification des supports de sauvegarde	Non
				Isolation des supports de sauvegarde des sites principaux	Oui
				Test périodique de la qualité des supports de sauvegarde	Non
		Accès non autorisés aux sauvegardes	Moyen	Tenue d'un registre des personnes accédant aux sauvegardes	Non
				Salle de confinement des sauvegardes avec des accès sécurisés et limités	Oui
Les processus de gestion opérationnelle de la sécurité de l'information	S'assurer de la prise en compte de la sécurité dans la gestion des activités quotidiennes	Accès non autorisés aux données	Faible	Politique de gestion des profils	Non
				Dispositif de déconnexion automatique en cas de tentatives d'accès erronées	Non
		Vol, altération des données	Faible	Dispositif de traçabilité des actions dans le SIC	Oui
		Non utilisation optimale du SIC	Moyen	Echange entre informaticiens et utilisateurs	Non

CESAG - BIBLIOTHEQUE

Documentation	Etre sûr qu'il existe une base de documentation du SIC et qu'elle est régulièrement mise à jour	Documents sur le SIC non exhaustifs	Moyen	Existence de documentation fournie et variée.	Oui
		Documents non mise à jour	Faible	Mise à jour périodique des documents du SIC.	Non
		Difficulté de formation des employés	Moyen	Mise à disposition des utilisateurs des documents en temps opportun.	Oui
				Création d'un archivage papier en parallèle de l'archivage numérique	Non
Sensibilisation et formation	S'assurer de la formation périodique des utilisateurs aux risques de sécurité	Non maîtrise des risques de sécurité par les utilisateurs	Elevé	Définition d'un plan de formation des utilisateurs aux risques de sécurité des SI	Non
		Panique en cas de sinistre	Moyen	Mise en place d'une politique de gestion des sinistres	Non
				Communication des procédures à suivre en cas de sinistres aux employés	Non
Gestion de la continuité des activités	S'assurer de la continuité des activités en cas de sinistre	Panne matérielle	Moyen	Serveur de secours	Oui
		Interruption du logiciel	Faible	Mise à jour périodique de l'application comptable	Oui
				Disposition d'une licence valide	Oui
		Reprise compromise de l'exploitation	Moyen	Définition d'un plan de continuité des activités en fonction des objectifs de sécurité	Non
				Plan de secours informatique	Oui
				Tests et évaluation périodiques du plan de continuité de l'activité	Non
				Formation du personnel aux procédures de secours et d'urgence	Non
		Perte d'informations stratégique	Faible	Duplication des données sur autres sites	Oui

Source : Nous-mêmes à partir de RENARD (2013 : 219) et SCHICK & al ; (2010 : 266-269)

CESAG - BIBLIOTHEQUE

Annexe 11: Programme de vérification

PROGRAMMME DE VERIFICATION				
MISSION : AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE		**CHAMP DE LA MISSION : DFC & DSIE de la LONASE** **PERIODE : 01 août au 30 septembre 2014**		**Page 1/6** **Réf : PV/JD**
PROCESSUS OU ACTIVITES	**OBJECTIFS GENERAUX**	**OBJECTIFS SPECIFIQUES**	**TACHES A EFFECTUER**	**Durée prévue**
Organisation et gestion de la sécurité du SIC	S'assurer d'une gestion efficace et efficiente de la sécurité du SIC	S'assurer de l'existence d'une structure apte à gérer au sein de la LONASE, le système de sécurité de l'information.	Entretenir avec la DFC, le DSIE	30 mn
		S'assurer que la politique de sécurité établie est en adéquation avec la mission de LONASE et qu'elle est conforme aux bonnes pratiques.	Analyser la politique de sécurité	10 mn
		Vérifier la communication de la politique de sécurité et de la connaissance du document par le personnel.	Entretenir avec le personnel de la DFC et de la DSIE	15 mn
		Vérifier l'existence d'une procédure pour la révision périodique de la politique de sécurité.	Entretenir avec la DFC et le DSIE	10 mn
Gestion des risques SI et protection des actifs informationnels	S'assurer de l'existence d'une procédure de gestion efficace des risques et de protection des actifs informationnels sensibles	S'assurer que la définition et la révision de la politique de sécurité de l'information sont fondées sur une analyse systématique et documentée des risques.	Faire un recoupement de la cartographie des risques avec la politique de sécurité des SI.	45 mn
		S'assurer de l'efficacité du dispositif de gestion des risques SI.	Analyser le dispositif de gestion des risques SI.	30 mn
		S'assurer que chaque ressource est placée sous la responsabilité d'un "propriétaire" régulièrement nommé.	Entretenir avec le DSIE, la DFC et le DAIQ.	45 mn

CESAG - BIBLIOTHEQUE

PROGRAMMME DE VERIFICATION				
MISSION : AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE		**CHAMP DE LA MISSION : DFC & DSIE de la LONASE** **PERIODE : 01 août au 30 septembre 2014**		**Page 2/6** **Réf : PV/JD**
PROCESSUS OU ACTIVITES	**OBJECTIFS GENERAUX**	**OBJECTIFS SPECIFIQUES**	**TACHES A EFFECTUER**	**Durée prévue**
Gestion des risques SI et protection des actifs informationnels (suite)	S'assurer de l'existence d'une procédure de gestion efficace des risques et de protection des actifs informationnels sensibles	Vérifier l'existence d'une classification des ressources du SIC et s'assurer qu'elle est conforme aux exigences de la politique de sécurité	Entretenir avec le DSIE, la DFC et le DAIQ.	45 mn
		Vérifier l'existence d'un inventaire des ressources du SIC et de sa mise à jour régulière.	Entretenir avec la DFC.	15 mn
		S'assurer que les dispositions sont prises pour assurer une alimentation électrique en cas de coupures d'électricité	Documenter l'état des lieux des dispositifs de sécurité	30 mn
Gestion de la sécurité physique (accès et protection)	S'assurer que seules les personnes autorisées ont accès au SIC	S'assurer de la sécurisation suffisante des locaux abritant le personnel et les équipements traitant l'information comptable.	Observer les dispositifs de sécurité des locaux.	Tout au long de la mission
		S'assurer de l'existence de procédures définissant les règles et consignes de sécurité applicables et de leur respect.	Entretenir avec la DFC, la DSIE et le DAIQ.	30 mn
		S'assurer que les risques liés à l'accès des tiers aux ressources du SIC sont clairement identifiés et traités.	Analyser la cartographie des risques	30 mn

CESAG - BIBLIOTHEQUE

PROGRAMMME DE VERIFICATION				
MISSION : AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE		**CHAMP DE LA MISSION : DFC & DSIE de la LONASE** **PERIODE : 01 août au 30 septembre 2014**		**Page 3/6** **Réf : PV/JD**
PROCESSUS OU ACTIVITES	**OBJECTIFS GENERAUX**	**OBJECTIFS SPECIFIQUES**	**TACHES A EFFECTUER**	**Durée prévue**
Gestion des habilitations et des profils	S'assurer de la protection du SIC contre les accès logiques non autorisés	S'assurer que les exigences concernant les contrôles des accès logiques sont clairement définies et documentées pour les différentes ressources informationnelles.	Entretenir avec le chef du Département des SI et analyse documentaire	20 mn
		S'assurer de l'accès sécurisé aux systèmes et aux applications et de l'intégrité des informations comptables	Faire un test de validation concernant la sécurité des accès et des données	1 h
		Vérifier que la gestion des habilitations et les contrôles mis en œuvre, assurent une prévention efficace des accès non autorisés au système d'information	Entretenir avec les personnes (DFC, DSI) qui interviennent dans l'attribution d'un droit d'accès	30 mn
Gestion des habilitations et des profils (suite)	S'assurer de la protection du SIC contre les accès logiques non autorisés	S'assurer que la protection contre les logiciels malicieux s'appuie sur des pratiques et des outils reconnus et éprouvés	Entretenir avec le chef service chargé de la sécurité des SI.	15 mn
		S'assurer que les postes de travail ne sont pas laissés en session sans surveillance et sont verrouillés quand ils ne sont pas utilisés.	Observer les pratiques de sécurité concernant la gestion des postes de travail.	Tout long du contrôle

CESAG - BIBLIOTHEQUE

PROGRAMMME DE VERIFICATION				
MISSION : AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE		**CHAMP DE LA MISSION : DFC & DSIE de la LONASE** **PERIODE : 01 août au 30 septembre 2014**		**Page 4/6** **Réf : PV/JD**
PROCESSUS OU ACTIVITES	**OBJECTIFS GENERAUX**	**OBJECTIFS SPECIFIQUES**	**TACHES A EFFECTUER**	**Durée prévue**
Gestion des habilitations et des profils (suite)	S'assurer de la protection du SIC contre les accès logiques non autorisés	S'assurer de la traçabilité suffisante des événements, de la protection des fichiers de journalisation et de l'efficacité des contrôles à prévenir et à détecter les activités non autorisées.	Apprécier les pratiques de gestion des habilitations.	1h
		S'assurer d'une bonne séparation des tâches dans la gestion des autorisations d'accès	Analyser les fiches de poste.	45 mn
Gestion des mots de passe	S'assurer de la bonne gestion des mots de passe	S'assurer de la définition des critères de choix des mots de passe sécurisés	Entretenir avec le Directeur du DSI et avec la DFC.	30 mn
		S'assurer que les mots de passe font l'objet de renouvellement périodique	Entretenir avec les utilisateurs de l'application comptable.	1 h
Documentation du SIC	Vérifier qu'il existe une base de documentation du SIC et qu'elle est régulièrement mise à jour.	S'assurer de l'existence d'une documentation assez fournie sur le SIC et régulièrement mise à jour	Prendre connaissance de la gestion documentaire.	30 mn
		S'assurer de l'accès facile à la documentation	Entretenir avec les responsables des services de la DFC.	15 mn

CESAG - BIBLIOTHEQUE

PROGRAMMME DE VERIFICATION				
MISSION : AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE		**CHAMP DE LA MISSION : DFC & DSIE de la LONASE** **PERIODE : 01 août au 30 septembre 2014**		**Page 5/6** **Réf : PV/JD**
PROCESSUS OU ACTIVITES	**OBJECTIFS GENERAUX**	**OBJECTIFS SPECIFIQUES**	**TACHES A EFFECTUER**	**Durée prévue**
Sensibilisation et formation	S'assurer que le personnel est sensibilisé et former en matière des bonnes pratiques de sécurité.	S'assurer qu'il existe une bonne politique de sensibilisation à la sécurité	Entretenir avec le Chef de service « maintenance, sécurité et formation ».	15 mn
		Vérifier l'existence de procédures assurant une réaction rapide face aux incidents et aux défauts de sécurité	Documenter les procédures de gestion des incidents et entretien avec le DSIE.	20 mn
		Vérifier si le personnel est suffisamment formé et sensibilisé aux menaces pesant sur la sécurité du SIC	Entretenir avec les chefs de service de la Direction Comptable et financière.	1 h
Gestion des sauvegardes et de l'archivage des données comptables	S'assurer que les données comptables sont sauvegardées régulièrement sur différents supports à différents endroits.	Apprécier la politique de sauvegarde des données comptables.	Consulter la politique de sauvegarde des données comptables.	15 mn
		S'assurer que les sauvegardes sont effectuées régulièrement.	Consulter la liste des sauvegardes effectuées.	10 mn

CESAG - BIBLIOTHEQUE

PROGRAMMME DE VERIFICATION				
MISSION : AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION COMPTABLE		**CHAMP DE LA MISSION : DFC & DSIE de la LONASE** **PERIODE : 01 Août au 30 Septembre 2014**		**Page 6/6** **Réf : PV/JD**
PROCESSUS OU ACTIVITES	**OBJECTIFS GENERAUX**	**OBJECTIFS SPECIFIQUES**	**TACHES A EFFECTUER**	**Durée prévue**
Gestion des sauvegardes et de l'archivage des données comptables (suite)	S'assurer que les données comptables sont sauvegardées régulièrement sur différents supports à différents endroits.	Vérifier l'existence et l'efficacité des dispositifs de sécurité destinés à assurer la sauvegarde et la protection des données.	Entretenir avec la DFC et le DSIE et apprécier la qualité des supports de sauvegarde.	30 mn
		S'assurer que les supports de sauvegarde sont gardés dans des lieux sécurisés.	Entretenir avec le DSIE.	15 mn
Gestion de la continuité de l'activité	S'assurer de la continuité des activités en cas de sinistre	S'assurer de l'existence de procédures couvrant notamment, l'identification de la cause des incidents et les correctifs à apporter pour éviter la répétition de l'incident.	Documenter la procédure de mise à jour périodique du plan de continuité des activités.	20 mn
		S'assurer de l'existence de moyens pour reprendre l'exploitation en cas de sinistre.	Entretenir avec le DSIE.	15 mn
		S'assurer de l'existence d'une hotline pour signaler les problèmes de sécurité éventuels.	Entretenir avec les utilisateurs	45 mn
		Vérifier qu'il existe un système de reporting des bugs rencontrés	Entretenir avec le DSIE	15 mn

Source : Nous-mêmes

CESAG - BIBLIOTHEQUE

BIBLIOGRAPHIE

CESAG - BIBLIOTHEQUE

OUVRAGES

1. ANDRESS Jason (2014), *The basics of information security*, 2ème édition, Edition Elsevier Science, New York, 217 pages.
2. AUTISSIER David et DELAYE Valérie (2008), *Mesurer la performance du système d'information*, Editions d'Organisation, Paris, 214 pages.
3. BERRADA Moshin (2012), *L'audit interne tout simplement,* Editions Afrique Challenges, Casablanca, 139 pages.
4. BLOCH Laurent et WOLFHUGEL Christophe (2011), *Sécurité informatique : Principes et méthode*, 2ème édition, Editions Eyrolles, Paris, 273 pages.
5. BOHNKE Sabine (2010), *Moderniser son système d'information*, Editions Eyrolles, Paris, 303 pages.
6. BOUVIER Anne-Marie et DISLE Charlotte (2008), *Introduction à la comptabilité : Cas pratique*, Editions Dunod, Paris, 331 pages.
7. CARPENTIER Jean-François (2009), *La sécurité informatique dans la petite entreprise: état de l'art et bonnes pratiques*, Editions ENI, Paris, 277 pages.
8. CLUSIF (2014), Menaces informatiques et pratiques de sécurité en France, *Rapport de l'enquête sur les menaces et les pratiques de sécurité Edition 2014*, Paris, 118 pages.
9. CORDEL Frédéric (2013), *Gestion des risques et contrôle interne : de la conformité à l'analyse décisionnelle*, Edition Vuibert, Paris, 304 pages.
10. COSSU Claude et MILKOFF Richard (2005), *Contrôle de gestion - Des informations pour la maîtrise des décisions et du contrôle*, Edition Armand Colin, Paris, 158 pages.
11. DAYAN Armand (2008), *Manuel de gestion*, Vol. 1, 2ème édition, Edition Ellipses/AUF, Paris, 1088 pages.
12. DOBILL Marcel (2013), *Comptabilité OHADA Tome 2, systèmes comptables-travaux de fin d'exercice-opération spécifiques*, Editions KARTHALA, Douala, 218 pages.
13. DORIATH Brigitte, LOZATO Michel, MENDES Paula et NICOLLE Pascal (2008), *Comptabilité et gestion des organisations*, 6ème édition, Edition Dunod, Paris, 357 pages
14. GHERNAOUTI Solange (2013), *Sécurité informatique et réseaux*, 4ème édition, Edition Dunod, Paris, 349 pages.
15. GOUADAIN Daniel et WADE El Bachir (2002), *Comptabilité générale : système comptable de l'OHADA*, Editions ESTM, Paris, 365 pages.
16. GRENIER Claude et BONNEBOUCHE Jean (2004), *Système d'information comptable,* 2ème édition, Edition FOUCHER, Paris, 320 pages.

CESAG BIBLIOTHEQUE

17. HASSID Olivier (2008), *La gestion des risques,* 2ème édition, Edition Dunod, Paris, 150 pages.

18. IFACI (1993), *Audit et contrôle des systèmes d'information, module 8 : sécurité*, Paris, 130 pages.

19. IFACI (2013) , *Les outils de l'audit interne - 40 fiches pour conduire une mission d'audit*, Editions Eyrolles, 109 pages.

20. IFACI (2013), *Cadre de Référence International des Pratiques Professionnelles de l'Audit Interne*, Editions Ebzone, Paris, 238 pages.

21. ISACA (2013), *Manuel de préparation CISA 2013*, Rolling Meadows, USA.

22. JACQUOT Thierry et MILKOFF Richard (2011), *Comptabilité de gestion : analyse et maîtrise des coûts*, 2ème édition, Editions Pearson Education, Paris, 335 pages

23. JIMENEZ Christian, MERLIER Patrick et CHELLY Dan (2008), *Risques opérationnel : de la mise en place du dispositif à son audit*, Editions Revue Banque, Paris, 273 pages.

24. KEREBEL Pascal (2009), *Management des risques*, Editions d'Organisation, Paris, 184 pages.

25. LAFITTE Michel (2003), *Sécurité des systèmes d'information et maîtrise des risques*, Editions Revue Banque, Paris, 127 pages.

26. LAUDON, Kenneth et LAUDON Jane (2013), *Le management des systèmes d'information*, 13ème édition, Editions Pearson, Paris, 696 pages.

27. LEMANT Olivier (1995), *La conduite d'une mission d'audit interne*, 2ème édition, Editions Dunod, Paris, 279 pages.

28. LEMANT Olivier (2003), L'Audit Interne, Edition e-theque, Paris, 75 pages.

29. LINLAUD Daniel (2003), *La sécurité de l'information*, Edition AFNOR, Paris, 249 pages.

30. MENTHONNEX Jean (1995), *Sécurité et qualité informatiques: nouvelles orientations*, Editions Presses polytechniques et universitaires romandes, Lausanne, 422 pages.

31. MOISAND Dominique et GARNIER DE LABAREYRE Fabrice (2009), *CobiT : Pour une meilleure gouvernance des systèmes d'information*, Editions Eyrolles, Paris, 274 pages.

32. MONACO Laurence (2014), *Les Carrés DCG 8 - Systèmes d'information de gestion 2014-2015,* 3ème édition, Edition Gualino, Paris, 224 pages.

33. MORLEY Chantal, BIA-FIGUEIREDO Marie et GILLETTE Yves (2011), *Processus métiers et Système d'Information,* 3ème édition, Editions Dunod, Paris, 319 pages.

34. PILLOU Jean-François et CAILLEREZ Pascal (2011), *Tout sur les systèmes d'information,* 2ème édition, Edition Dunod, Paris, 189 pages.

CESAG - BIBLIOTHEQUE

35. PINET Claude (2012), *10 clés pour la sécurité de l'information,* Edition AFNOR, Paris, 116 pages.

36. PriceWaterhouseCoopers et IFACI (2014), *Coso-Référentiel intégré de contrôle interne: Principes de mise en oeuvre et de pilotage*, Editions Eyrolles, Paris, 264 pages.

37. REIX Robert, FALLERY Bernard, KALILA Michel et ROWE Frantz (2011), *Systèmes d'information et management des organisations*, 6ème édition, Editions Vuibert, Paris, 472 pages.

38. RENARD Jacques (2013), *Théorie et pratique de l'audit interne*, 8ème édition, Editions d'Organisation, Paris, 452 pages.

39. SCHICK Pierre, VERA Jacques et BOURROUILH-PAREGE Olivier (2010), *Audit interne et référentiels de risques*, Editions Dunod, Paris, 384 pages.

40. TENEAU Gilles et AHANDA Jean-Guy (2009), *Guide commenté des normes et référentiels*, Editions d'Organisation, Paris, 371 pages.

41. WHITMAN Michael et MATTORD Herbert (2011), *Principles of Information Security*, 4ème édition, Editions Cengage Learning, Boston, 658 pages.

ARTICLES

42. FEVRIER Rémy (2013), Les Collectivités Territoriales face aux menaces numériques *Revue de Gestion et management public,* Volume 1/n°3 : pages 24-39.

43. IFA (2010), Le suivi de l'efficacité des systèmes de contrôle interne et de gestion des risques, *Les travaux de l'IFA*, Paris, 24 pages.

SOURCES INTERNET

44. ANSSI (2014), *EBIOS*, http://www.ssi.gouv.fr/fr/confiance/ebios.html,

45. CLUSIF (2010) *MEHARI*, http://www.clusif.asso.fr/, site officiel du Club Informatique de la Sécurité de l'information Français. visité le 10 Novembre 2014 ;

46. FERNANDEZ Alain (2013), *Analyse de risques business plan*, http://www.piloter.org/livres-blancs-pdf/asoncompte/analyse-de-risques-business-plan.pdf

47. ISACA (2013), *Normes d'audit et d'assurance des SI,* http://www.isaca.org ;

48. MAURY Claude (2007), *Le role du RSSI*, http://www.clusis.ch/pdf/LeroleduRSSI.pdf

49. OHADA (2000), *Acte Uniforme portant Organisation et Harmonisation des Comptabilités des Entreprises*, http://www.ohada.com/actes-uniformes/693 ;

50. VERNHET Alexander (2008), *Comptabilité générale : l'organisation et la normalisation comptable*, http://vernhet.com/PDF/Compta_cours_13_intro.pdf.

CESAG - BIBLIOTHEQUE