UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU
FACULTE DES SCIENCES ECONOMIQUES, COMMERCIALES ET DES SCIENCES DE GESTION
DEPARTEMENT DES SCIENCES DE GESTION

MEMOIRE DE FIN D'ÉTUDES

EN VUE DE L'OBTENTION DU DIPLÔME DE MASTER ES SCIENCES DE GESTION

SPECIALITE : AUDIT ET CONTRÔLE DE GESTION

Thème

Audit interne et sécurité du système d'information de gestion
Cas pratique : L'Entreprise Nationale de Promotion Immobilière de Tizi-Ouzou.

Réalisé par :
M^elle^ BELGACEM Litissia
M^elle^ HATEM Soraya

Encadré par :
Mr. KHEFFACHE Kamal
Mr. AMIAR Habib

Soutenu devant le jury composé de:
DRIR, UMMTO, Président
Khaled GUEDECHE , UMMTO, Examinateur
Habib AMIAR, UMMTO, Rapporteur
Kamal KHEFFACHE, UMMTO, Rapporteur

3^ème^ Promotion

Année universitaire 2016/2017

REMERCIEMENTS

Nous remercions dieu le tout puissant de nous avoir donné force, courage et patience d'arriver au terme de ce travail.

Nous tenons à exprimer nos vifs remerciement à :

Nos encadreurs, Mrkheffachekamal MrAmiarhabib, pour avoir accepté de nous encadrer, diriger et orienter durant toute la durée de ce travail.

A tous nos enseignants du master qui nous ont formés et orientés durant notre cursus. Nous les remercions

Pour leurs sacrifices et la réussite de notre master.

Mr Semarde l'entreprise l'ENPI de Tizi-Ouzou, qui nous a aidés pour élaborer ce mémoire.

DÉDICACE

Je dédie ce modeste travail.

Ames chers parents:ma mère et mon père que j'aime et qui m'ont vraiment encouragé durant la réalisation de ce travail, je leur souhaite une longue vie.

Ama sœur :Sarah

Ameschèrefrères : Nassim, Said , Sofiane

Atoute la famille Belgacem et la famille Alem

Atous les gents qui m'ont aidé,de prés ou de loin,pour la réalisation de ce mémoire.

Ames amies et mes camarades.

B. Littissia

DÉDICACE

Je dédie ce travail à tous ceux qui me sont chères

Ma famille

Mes amis

Mes camarades

Tous ceux qui m'ont aidé dans mon cursus d'étude.

H.Soraya

SOMMAIRE

LISTES DES SIGLES ET ABREVIATIONS

AFAI : Association Française de l'Audit et du conseil Informatique

AMRAE : Association pour le Management des Risques et des Assurances en Entreprise

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

CIGREF : Club Informatique des Grandes Entreprises Françaises

CLUSIF : Club de Sécurité de l'Information Français

CobiT: Control Objectives for Information and related Technology

COSO: Committee of Sponsoring Organisations of the Treadway Commission

CRIPP : Cadre de Référence International des Pratiques Professionnelles

DG : Direction Générale

DSI : Direction des Systèmes d'Information

EBIOS : Expressions des Besoins et Identification des Objectifs de Sécurité

ENPI : Enterprise Nationale de Promotion Immobilier

EPE : Entreprise Publique Economique

IEC: International Electrotechnical Commission

IFACI : Institut Français des Auditeurs et contrôleurs Internes

IIA: Institute of Internal Auditors

ISACA: Information Systems Audit and Control Association

ISO : International Standards Organization

MEHARI : Méthode Harmonisée d'Analyse des Risques

MPA : Modalités Pratiques d'Application

OCTAVE: OperationallyCriticalTréatandVulnerability Evaluation

QCI : Questionnaire de Contrôle Interne

RM : Risk Manager

RSSI : Responsable de la Sécurité des Systèmes d'Information

SEI : Software Engineering Institute

SI : Système d'information

SMSI : Système de Management de la Sécurité de l'Information

SSI : Sécurité des Systèmes d'Information

SPA : Société Par Action

TI : Technologie de l'information

INTRODUCTION GENERALE

Parmi les structures de contrôle présentes dans l'entreprise pour aider le management dans la prise de décisions, on retrouve l'audit interne. C'est une fonction communément admisecomme étant un moyen à la disposition du management dans le cadre du processus de gestion des risques et d'évaluation du dispositif de contrôle interne en place. L'audit interne est défini comme une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Historiquement orientée vers la gestion financière et comptable, son champ d'action s'est étendu à tous les domaines de l'entreprise.

Les missions de contrôle et d'évaluation de la maîtrise des activités ainsi que de conseils ont suivi l'évolution économique et la croissance des organisations. L'audit interne, par son approche systématique et méthodique, accompagne les opérationnels dans l'identification et la maîtrise des risques, en vue d'atteindre les objectifs fixés par la Direction Générale. Dans le contexte actuel d'amélioration continue des technologies d'information et de communication, les risques liés aux systèmes d'information sont en général suivis de près dans les cartographies des risques des auditeurs. Dans le cadre de cette surveillance accrue, une attention particulière est accordée à la sécurité de l'information. En effet, l'information est essentielle, voire déterminante pour la pérennité de l'entreprise.

La finalité de beaucoup d'activités et d'opérations effectuées en entreprise est de produire des informations financières et opérationnelles fiables dont il faut assurer l'intégrité et la protection. Ainsi, des normes internationales telles que l'ISO 27000 définissent les exigences requises pour mettre en place un système de gestion de la sécurité de l'information. Elles sont conçues pour garantir la sélection de contrôles de sécurité adéquats et proportionnels au niveau du contrôle interne établit par la structure. Elles indiquent aux entreprises les règles de protection des données permettant de garantir la confiance des parties intéressées, notamment des clients. Les normes adoptent une approche basée sur les processus pour la création, la mise en œuvre, l'utilisation, la surveillance, l'analyse, le maintien et l'amélioration des systèmes de gestion de la sécurité de l'information.

Au regard de ce constat, nous nous interrogeons sur la contribution de l'audit interne à la sécurité de l'information.

La complexité des tâches de l'auditeur interne quant à la sécurité de l'information vient dans certains cas, d'un manque de connaissance ou d'une formation inadéquate sur les systèmes d'information électroniques modernes et d'autres domaines hautement sophistiqués. Plusieurs

autres raisons peuvent être évoquées : l'une pourrait être le fait que certains auditeurs ont quelque fois une tendance naturelle à ne pas changer leurs habitudes; une autre pourrait être la peur du changement. En dehors de celles précitées, nous avons d'autres difficultés rencontrées par les auditeurs internes telles que le manque de compréhension globale des processus d'activités et le suivi inadéquat des problèmes après leur détection. L'audit interne pourrait s'avérer inefficace si la direction n'assure pas toujours un suivi approprié des problèmes décelés. On pourrait parler dans ce cas-ci d'un manque d'accompagnement du management dans le processus de l'audit interne.

Les conséquences qui en résultent sont de plusieurs ordres :

- Non détection en temps réel des risques liés aux activités du système d'information ;
- Mauvaise utilisation des données nécessaires à l'évaluation des risques ;
- Fraude ;
- Mauvaise orientation;
- Perte de l'image ;
- Non atteinte des objectifs assignés par l'entreprise.

Pour pouvoir apprécier le rôle de l'audit interne dans la gestion de la sécurité de l'information, plusieurs solutions s'offrent à nous :

- Faire une enquête sur le service d'audit interne afin de comprendre son implication et sa responsabilité dans le maintien et l'amélioration de la sécurité de l'information ;
- Effectuer un examen critique du système de gestion de la sécurité de l'information ;
- Etablir des lignes directrices pour l'auditeur interne, lui permettant d'évaluer et de suivre promptement le maintien et l'amélioration du système de sécurité de l'information.

Problématique de recherche

Pour avoir une assurance suffisante, que le service d'audit interne fonctionne correctement afin de comprendre son implication et sa responsabilité dans le maintien et l'amélioration de la sécurité del'information,il serait impossible d'apprécier la contribution de l'audit interne dans la sécurité de l'information sans faire un examen de la sécurité de l'information et sans établir de lignes directrices que pourront suivre les auditeurs internes pour être toujours plus opérationnels.

Notre étudedoit nous permettre de répondre à cette problématique « **Comment l'audit interne contribue-t-il au maintien et à l'amélioration continue de la sécurité de l'information de gestion au sein de l'entreprise L'ENPI de Tizi-Ouzou ? »**

Pour élucider cette problématique, plusieurs questions doivent êtres éclaircies, qui sont comme suit:

- **Qu'est-ce que l'information ?**
- **Qu'est-ce que la sécurité de l'information ? de quoi s'agit-il en milieu de l'entreprise?**
- **Quels sont les risques inhérents à l'insécurité de l'information et comment y remédier ?**
- **Par quelle approche, l'auditeur interne s'assurera-t-il de la maitrise ou non des risques liés à la sécurité del'information?**
- **Sur quels référentiels, normes ou bonnes pratiques doit-il se baser ?**
- **De quelles compétences et connaissances l'auditeur interne a-t-il besoin ?**

C'est à l'ensemble de ces questions auxquelles nous attèlerons à répondre dans le corpus de notre présent travail de recherche. Pour une application pratique nous avons choisi l'entreprise nationale de promotion immobilière (l'ENPI), où nous allons effectuer une étude relative à l'application de l'objet de notre thème.

Les hypothèses :

Pour aborder cette problématique nous avons émis les hypothèses suivantes :

1ère Hypothèse : Les auditeurs internes jouent un rôle important et contribuentà l'améliorationcontinue de la sécurité des systèmes d'information de gestion au sein des entreprises.

2ème Hypothèse: Un système d'information de gestion sécurisé impacte positivement sur les décisions et le management d'une entreprise.

Intérêt du sujet

L'objectif principal de cette étude, est de connaitre etd'apprécier le rôle et la contribution de l'audit interne dans le maintien et l'amélioration continue de la sécurité de système d'information de gestion.

De cet objectif, dérivent les objectifs spécifiques suivants :

- Identifier les bonnes pratiques en matière de sécurité de l'information ;
- Mettre en exergue le type d'organisation que l'entreprise devra mettre en place pour assurer un bon fonctionnement de son système de sécurité de l'information ;
- Connaître les risques relatifs à un manque de sécurité de l'information ;
- Apprécier les caractéristiques de l'audit interne qui pourraient aider l'entrepriseà atteindre ses objectifs.

Pour le développement de notre étude, nous nous limiterons qu'aux onze (11) thèmes du cadre de gestion de la sécurité de l'information selon la norme ISO 27002 et aux normes internationales pour la pratique professionnelle de l'audit interne.

L'intérêt que revêt notre étude, surtout dans cet ère de la numérisation et ou l'intelligence est liée directement à l'information qui est source d'avantages, peut être situé à un double niveau:

- **Pour l'entreprise** : elle disposera des meilleures pratiques en termes de maintenanceet amélioration continue du système de sécurité de l'information. Aussi, elle aura ce dont elle a besoin en matière d'outils, de techniques et de moyens, tant humains que matériels, pour une bonne gestion de la sécurité de ses informations et une maîtrise totale du système d'information. Cette étude éclaircira d'avantage le rôle que l'audit interne devra jouer afin d'aider le management dans la prise de décisions et dans l'atteinte efficace et effective des objectifs en matière de sécurité de l'information.
- **Pour nous** : cette étude sera une occasion pour nous de confronter nos connaissances théoriques et pratiques acquises pendant notre formation académique. Il s'agira, pour nous, d'avoir une connaissance plus élaborée sur la gestion de la sécurité du système d'informationd'entreprise et aussi sur la contribution de l'audit interne à son maintien et à son amélioration.

Pour atteindre les objectifs que nous avons fixés, notre étude se fera en suivant une méthodologie.

Méthodologie

Afin de réaliser notre travail de recherche, nous avons adopté, d'une part, une méthode descriptive en donnant un aperçu sur l'audit interne etlasécurité du système d'information, clés

de voute de notre mémoire. Pour cela, nous avons fait un appel à une recherche documentaire à travers des ouvrages, des articles, des communications, des thèses et des sites internet.

D'autre part; nous avons adopté une approche analytique,afin d'analyser la contribution de l'audit interne et la sécurité du système d'information de gestion et cella avec l'exemple de l'ENPI de Tizi-Ouzou.

Structure du mémoire

Dans ce cadre notre plan sera articulé autour de trois chapitres :

D'abord à travers la partie théorique, de présenter les avis de différents auteurs qui seront contenus dans une revue de littérature

- Le premier chapitre portera sur : Cadre conceptuel de l'audit interne et de la sécurité du système d'information de gestion
- Le second chapitre se consacrerau : Normes, Référentiels et Méthodologie afférents à l'audit interne et à la sécurité de l'information.

Ensuite nous aborderons la partie pratiquedans,

- Le dernier chapitre présentera l'unité d'accueil,avec L'ENPI de Tizi-Ouzou comme exemple d'illustration dans le but de confronter la pratique de l'audit interne dans la gestion de la sécurité de l'information dans une entreprise avec la théorie.

Chapitre I

Cadre conceptuel de l'audit interne

et sécurité du système d'information de gestion

Introduction du chapitre

La sécurité des systèmes d'information est un domaine très vaste, puisqu'elle fait appel à toutes les entités de l'entreprise et à des connaissances techniques et technologiques de pointe. L'une des forces et en même temps une problématique du monde des affaires actuel est l'évolution constante des technologies de l'information. Il est vrai que plus les technologies évoluent, plus elles offrent une plus grande mobilité aux utilisateurs et révolutionnent les habitudes et les façons de travailler. Cependant elles sont empreintes de risques de plus en plus forts. Il faudrait donc trouver des solutions de sécurité de l'information pour mieux préserver la sécurité des systèmes d'information et aussi les intérêts de l'entreprise.

Dans les bonnes pratiques de sécurité, l'entreprise dispose d'agents régulateurs et garant des dispositifs de contrôle interne tel que l'audit interne. A cet effet, des auteurs divers ont développé plusieurs théories et avis mettant en exergue le rôle de l'audit interne dans la sécurité informationnelle. Nous nous sommes par conséquent atteler à présenter ces différentes opinions dans notre cadre théorique afin de mieux apprécier le concept de l'audit interne dans la sécurité des systèmes d'information de l'entreprise

Dans ce présent chapitre, il sera question d'aborder les notions d'audit interne et sécurité du système d'information, en présentant l'historique et le cadre de référence de l'audit interne a travers ses missions, objectifs et champ d'application.Nous aborderons les notions d'information et de sécurité du système d'information;ensuite nous établirons une relation entre ces deux concepts afin de faire ressortir la contribution de l'audit interne, de par ses missions et objectifs, au maintien de la sécurité de l'information au sein même d'une Entreprise.

Section 1 : Historique et cadre de référence de l'audit interne

Dans cette section, nous présenterons un bref historique qui ne retrace pas l'histoire de l'audit interne dans ses moindres détails mais il en reprend les grandes lignes.

1 Notion d'audit interne

Selon les normes ISO 9000:2015,l'audit(3.13.1)[1]est défini comme processus méthodique, indépendant et documenté, permettant d'obtenir des preuves objectives et de les évaluer de manière objective pour déterminer dans quelle mesure les critères de l'audit sont

[1]Extrait de la norme ISO 9000:2015 Systèmes de management de la qualité,https://www.iso.org/obp/ui/fr/#!iso:std:42180:fr, Ed2015.

satisfaits. Additivement à cela, plusieurs comités et organismes ont tenté de donner une définition à l'audit interne.

Cependant ils s'accordent tous sur cette définition de l'IFACI, approuvée par l'IIA le 29 juin 1999[2] :

« L'Audit Interne est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée , Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité»[3].

De cette définition, il ressort que la pratique de l'audit interne requiert une certaine indépendance de l'auditeur interne, vis-à-vis des autres membres de l'entreprise. Il améliore le fonctionnement de l'organisation et aide l'entreprise à atteindre ses objectifs.

2 Missions, Objectifs et Champ d'application de l'audit interne

Dans ce paragraphe, nous identifierons dans un premier temps les missions et objectifs de l'Audit Interne et, dans un second temps son champ d'application.

2.1 Les missions

Suivant la définition de l'IFACI, l'audit interne présente 3 missions :

- Contribuer à la création de valeur ajoutée : selon l'IFACI (CRIPP), l'audit interne apporte de la valeur ajoutée à l'organisation lorsqu'il fournit une assurance objective et pertinente et qu'il contribue à l'efficience et à l'efficacité des processus de gouvernement d'entreprise, de management des risques et de contrôle ;
- Améliorer le fonctionnement de l'organisation : par la réalisation de missions d'audit et d'apport de conseils ;
- Aider l'entreprise à atteindre ses objectifs : par l'évaluation des processus de management des risques, de contrôles et de gouvernement d'entreprise, à l'aide d'une approche systématique et méthodique.

[2]IIA, Cadre de références internationales des pratiquesprofessionnelles, http://www.ifaci.com/publications/audit-interne/cripp/, Ed. 2017,p15. Consulté le 12/09/2017.
[3]BERTIN, (E), *Audit interne*, Ed. Eyrolles, Paris, 2007, p.20.

Ainsi, l'audit interne étant une entité à part entière, doit être capable de rassurer l'entreprise sur la continuité d'exploitation, sur la maitrise des opérations (gestion des risques) et donner une garantie pas absolue mais raisonnable du succès des activités et de l'atteinte effective des objectifs.

Dans le cadre de **missions d'assurance,** l'auditeur interne procède à une évaluation objective en vue de formuler des opinions ou des conclusions sur une entité, une opération, une fonction, un processus, un système ou d'autres domaines. L'auditeur interne détermine la nature et le périmètre d'intervention de la mission d'assurance. Généralement trois catégories d'acteurs participent aux missions d'assurance [1]:

- La personne ou le groupe directement impliqué dans l'entité, l'opération, la fonction, le processus, le système ou le domaine examiné – autrement dit le propriétaire du processus ;
- La personne ou l'équipe réalisant l'évaluation – l'auditeur interne ;
- La personne ou le groupe qui utilise les résultats de l'évaluation – l'utilisateur.

Les missions de conseil sont le plus souvent entreprises à la demande d'un client. Leur nature et leur périmètre d'intervention font l'objet d'un accord avec ce dernier. Elles comportent habituellement deux intervenants:

- La personne ou l'équipe qui fournit les conseils, en l'occurrence l'auditeur interne ;
- La personne ou le groupe donneur d'ordre auquel ils sont destinés, le client. Lors de la réalisation de missions de conseil, l'auditeur interne devrait faire preuve d'objectivité et n'assumer aucune responsabilité managériale dans l'activitéconcernée.

2.2 Les objectifs

D'après la norme 2120.A1de l'audit interne contenu dans le CRIPP « l'audit interne doit évaluer les risques afférents au gouvernement d'entreprise, aux opérations et aux systèmes d'information de l'organisation au regard de :

- L'atteinte des objectifs stratégiques de l'organisation ;
- La fiabilité et l'intégrité des informations financières et opérationnelles ;
- L'efficacité et l'efficience des opérations et des programmes ;
- La protection des actifs;

[1]IIA, Cadre de références internationales des pratiques professionnelles, http://www.ifaci.com/publications/audit-interne/cripp/ , Ed. 2017, p.02 consulté le 12/09/2017.

- Le respect des lois, règlements, règles, procédures et contrats ».

Cette norme présente la responsabilité de l'auditeur interne dans l'évaluation des risques des systèmes d'information de l'entreprise. L'audit interne est devenu un acteur capital dans le dispositif de maîtrise des risques, du contrôle interne et de la gouvernance d'entreprise.

L'interprétation[1] de la norme 2120 donnée par L'IFACI (CRIPP 2013), soutenue par Renard.J,souligne que pour atteindre les objectifs en matière de management des risques, les auditeurs internes doivent s'assurer que :

- Les objectifs de l'organisation sont cohérents avec sa mission et y contribuent ;
- Les risques significatifs sont identifiés et évalués ;
- Leurs modalités de traitement des risques sont appropriées et en adéquation avec l'appétence pour le risque de l'organisation ;
- Les informations relatives sont recensées et communiquées en temps opportun au sein de l'organisation pour permettre aux collaborateurs, à leur hiérarchie et au conseil d'exercer leur responsabilité

2.3 Le champ d'application

Le champ d'actionde l'audit interne s'est rigoureusement élargi depuis son adoption par les francophones, en l'occurrence la France dans les années 1960.

Il apporte sa contribution à l'ensemble des activités de l'organisation. Car, dans chaque domaine (financier, commercial, administratif, informatique,...), diriger c'est synonyme de planifier les tâches, organiser leur exécution par la responsabilisation, conduire les opérations et en contrôler la marche et le résultat.Par son assistance au manager, l'auditeur interne combine le rôle d'auditeur et de consultant.

Le champ d'application d'une mission d'audit varie de façon significative en fonction de deux éléments[2] :

[1]Pour plus de lecture, prière de consulter RENARD, (J) : *Théorie et Pratique de l'Audit Interne,* Ed. D'Organisation, Paris, 2010, P144.

[2]Les éléments cités dans notre texte sont extrait du livre de JOANNY, (M) : *Théorie et pratique de l'audit interne*, Ed. D'organisations, Paris, 2000, P. 199.

- **L'objet**

L'objet permet de distinguer les missions spécifiques des missions générales. Les premières portent sur un point précis en un lieu déterminé. Par contre, les secondes ne connaissent aucune limite géographique de l'entreprise.

- **La fonction**

Se rapportant à la fonction, on parle d'une mission d'audit interne unifonctionnelle (qui ne concerne qu'une seule fonction) et mission d'audit interne plurifonctionnelle (concerne plusieurs fonctions au cours d'une même mission).

L'audit interne doit donc couvrir tous les domaines de gestion et l'auditeur doit avoir accès sans limitation, aux documents et données relatives à la gestion.

E. EBONDO, note que, si originellement, « le contrôle interne avait pour terre d'élection la régularité et la sincérité des opérations comptables, il s'impose désormais à toutes les activités, à tous les processus, bref à toutes les organisations qu'elles soient des entreprises publiques ou privées, des associations. Il semble aussi que le phénomène de la mondialisation avec ses exigences en termes de qualité et de standardisation ait fortement contribué à la mise en place ou au déploiement des processus des contrôles internes dans les entreprises »[1].

Etant concerné dorénavant par toutes les fonctions de l'entreprise, l'audit interne revêt plusieurs formes selon les objectifs à atteindre lors de la réalisation d'une mission.La typologie[2] d'audit interne est comme suit :

- L'audit de conformité : Vérifier la bonne application des règles procédures, descriptions de poste, organigrammes, systèmes d'information, etc.il va comparer la règle et la réalité, ce qui devrait être et ce qui est. Autrement dit, il va travailler par rapport à un référentiel et c'est en cela que son travail est relativement simple ;
- L'audit d'efficacité : Progressivement on est allé plus loin dans les objectifs assignés à l'auditeur interne. Étant devenu un spécialiste du diagnostic, de l'appréciation des méthodes, procédures, analyses de postes, organisation du travail, l'auditeur apris l'habitude d'émettre une opinion, non plus seulement sur la bonne application des règles, mais également sur leur qualité ;

[1] EBONDO WA MANDZALA E, *La gouvernance de l'entreprise : une approche par le contrôle interne et l'audit*, Ed. Harmattan, Paris, 2006, p.93.
[2] RENARD,(J) *: op cit*, p.48-55

- L'audit de management : L'audit de management consiste á observer les choix et les décisions, les comparer, les mesurer dans leursconséquences et attirer l'attention sur les risques ou les incohérences relèvebien de l'audit interne ;
- L'audit de stratégie : Conçu comme une confrontation de l'ensemble des politiques et stratégies de l'entreprise avec le milieu dans lequel elles se situent pour en vérifier la cohérence globale ;
- Le conseil:La mission de conseil ne se confond pas avec les recommandations des missionsd'audit, lesquelles s'appuient sur des constats de dysfonctionnement. Cesont des missions spécifiques, nommées comme telles et devant être si possibledéfinies dans un accord écrit.

3 Compétences et responsabilités des auditeurs

Pour réaliser l'ensemble de ses missions, l'auditeur interne se doit d'avoir une vision globale de l'entreprise et de ses métiers. Ainsi, les entreprises recherchent des profils aux expériences professionnelles variés pour qu'ils aient une meilleure appréhension des différentes activités de l'entreprise.L'audit interne doit disposer d'une gamme de compétences toujours plus étendue.

Le respect des normes internationales pour la pratique professionnelle de l'audit interne est essentiel pour que les auditeurs internes puissent s'acquitter de leurs responsabilités. Les normes relatives aux responsabilités des auditeurs internes sont appelées des normes de qualification[9] « normes 1000 - CRIPP 2013 ». Ces normes doivent être définies dans une charte formelle d'audit interne. De ces normes, découlent les caractéristiques de l'auditeur interne :

- **Indépendance :** capacité à assumer de manière impartiale, les responsabilités. L'audit interne doit être positionné à un niveau suffisamment élevé de la hiérarchie pour pouvoir être totalement indépendant et objective. Pour cela, selon la norme 1100, l'audit interne doit être doublement rattachée à la direction générale et au conseil d'administration (au comité d'audit plus précisément) ;
- **Objectivité** : avoir un jugement impartial et sans aucune forme de subordination à celui d'autres personnes (normes 1100 et 1120);

[9]IIA, Cadre de références internationales des pratiques professionnelles, www.ifaci.com/uploads/_ifaci/ani_fichiers/CRIPP-2013-3, Ed.2013 pp. 29-30 consulté 22/09/2017.

➢ **Compétence et conscience professionnelle** : le savoir-faire, la diligence dans le travail, des connaissances et autres compétences relatives à l'exercice de leur fonction. Aussi, faire preuved'une formation professionnelle continue (norme 1200).

Concernant le système d'information et la sécurité de l'information, la MPA 1210.A3 (IFACI, 2013 : 36)précise que«les auditeurs internes doivent posséder une connaissance suffisante des principaux risques et contrôles relatifs aux technologies de l'information, et des techniques d'audit informatisées susceptibles d'être mises en œuvre dans le cadre des travaux qui leur sont confiés»[10]. La MPA 1220.A2 (IFACI, 2013 : 37) ajoute que « pour remplir ses fonctions avec conscience professionnelle, l'auditeur interne doit envisager l'utilisation de techniques informatiques d'audit et d'analyse des données»[11].Ces normes démontrent l'importance mise sur l'éventail de connaissance et compétence que doit avoir l'auditeur interne pour mener à bien ses missions d'audit de sécurité de l'information.

Toutes ces caractéristiques citées plus haut sont celles dont l'auditeur doit se revêtir pour ainsi assurer et contribuer au maintien et à l'amélioration du système d'information, notamment de la sécurité de l'information dans l'entreprise ; sécurité sans laquelle l'entreprise serait incapable de poursuivre correctement ses opérations et ainsi s'exposer à des pertes financières énormes.

Section 2 : La sécurité du système d'information

1 Notion d'information

Avec la mondialisation, l'évolution des technologies de l'information, l'ouverture des systèmes d'information au monde extérieur et la dépendance accrue des organisations vis-à-vis des données et ressources informatiques, la sécurité est aujourd'hui indispensable à la bonne marche de la plupart d'entre elles. Aucune entreprise ne pourrait survivre aux conséquences, notamment, en termes de coûts et de la perte d'intégrité de l'ensemble des données de son système.

Avant d'aborder la sécurité de l'information, nous définirons d'abord ce que l'on entend par information et quelle est son importance au sein de l'entreprise

[10]IIA, Cadre de références internationales des pratiques professionnelles www.ifaci.com /uploads/_ifaci/ani_fichiers/CRIPP-2013-3.pdf, Ed.2013 p. 36 consulté 22/09/2017.
[11]IIA, Cadre de références internationales des pratiques professionnelleswww.ifaci.com /uploads/_ifaci/ani_fichiers/CRIPP-2013-3.pdf,Ed.2013 p. 37 consulté 22/09/2017.

1.1 Définition de l'information :

Il existe plusieurs définitions pour ce concept :

- « l'information est une collection de donnéesorganisées pour donner à un message une forme visible, imagée, écrite ou orale»[12].
- « le terme information recouvre des données qui sont présentées sous une forme utile et utilisable par les personnes»[13].
- l'information est : « l'ensemble des données utiles pour prendre une décision .l'information est transmise par un système de communication qui transforme les faits en des informations directement compréhensibles par l'utilisateur»[14].
- L'information est : « un renseignement qui accroit la connaissance concernant la personne, un objet ou un évènement déterminé. Elle peut être :
  - Objective, quand elle reflète un ensemble de données porteur de sens ;
  - Subjective, quand elle résulte de l'interprétation d'un ensemble de données »[15].

Il y a une distinction entre les trois termes : données, informations et connaissance.

- Information : « est le processus (et son résultat) de rencontre d'une donnée et d'une question préalable ou potentielle que se pose le récepteur de la donnée.»[16] ;
- Donnée : «représentation conventionnelle, après codage d'une information sous une forme permettant d'en faire le traitement électronique»[17] ;
- Connaissance : Action, fait de comprendre, de connaitre la caractéristique, spécifique de quelque chose.

Nous constatons que les données sont des observations qui vont êtreanalysées et traitées pour l'obtentiond'informations.Le cumul de ces dernières conduit à la connaissance de l'entreprise et constitue un instrument de la communication interne et externe de l'organisation avec son environnement. Elle est considérée comme un élément essentiel pour l'aide à la prise de décision et la réduction de l'incertitude.

[12]BERDUGO (A) , MAHL(R) et GERARD(J) :*Guide du management des systèmes d'information (thèmes et termes essentiels)* **,** Ed, Lavoisier**,** Paris , 2002, p.345.
[13]LAUDON, (K) et LAUDON (L) :*Management des systèmes d'information*. Ed. Pearson, 2010, p.14.
[14]AURIAC, (J-M) *: Economie d'entreprise*, Tome 1,Paris : Casteilla, 1995, p.87.
[15]SORNET (J), HENGOAT (O) et LE GALLO (N) **:** *systèmes d'informations de gestion : tout –en-un*, Ed. DUNOD, Paris, 2010, p.2.
[16] LESCA, (H) *: L'information stratégique du dirigeant. Revue française de gestion*, novembre-décembre 1983, n043, p.16
[17]CACALY,(S) et alii *: Dictionnaire de l'information,*Ed. Armand colin , Paris, 2006, p.70.

1.2 Les caractéristiques de l'information

L'information présente sept critères précis significatifs pour chacune des entités de l'entreprise á savoir[18]:

- **Efficacité** : la mesure par laquelle l'information contribue au résultatdes processus métier par rapport aux objectifs fixés ;
- **Efficience** : la mesure par laquelle l'information contribue au résultatdes processus métier au meilleur coût ;
- **Confidentialité** : la mesure par laquelle l'information est protégée desaccès non autorisés ;
- **Intégrité** : la mesure par laquelle l'information correspond à la réalitéde la situation ;
- **Disponibilité** : la mesure par laquelle l'information est disponible pourles destinataires en temps voulu ;
- **Conformité** : la mesure par laquelle les processus sont en conformitéavec les lois, les règlements et les contrats ;
- **Fiabilité** : la mesure par laquelle l'information de pilotage est pertinente.

1.3 L'importance de l'information

L'information est une ressource fondamentale pour l'entreprise. Elle est un actif intangible, une ressource immatérielle qu'il faudrait traiter, décrypté, sélectionné en fonction des besoins. Pour cela, l'entreprise développe la veille informationnelle stratégique qui consiste à organiser la collecte des informations nécessaires aux prises de décisions.

Parmi quatre fonctions essentielles :

- Réduire l'incertitude sur un évènement donné ;
- Modéliser la complexité de l'entreprise et de son environnement par la mise en place de procédures et processus ;
- Prendre des décisions pour la réalisation des opérations et des objectifs de l'entreprise ;
- Diriger : la direction de l'entreprise se sert de l'information pour piloter, mener des actions et contrôler les accomplissements.

[18]MOISAND, (D) et GARNIER DE LABAREYRE (F) : *CobiT, pour une meilleure gouvernance des systèmes d'information*,Ed.Eyrolles, Paris,2009, p.31.

Il est important de savoir que l'information est la matière première qui alimente le fonctionnement de l'entreprise. Par conséquent, un manque d'information ou une mauvaise communication entraine tout simplement la mort du système et très souvent, des pertes financières importantes et même le dépôt définitif de bilan. C'est la raison pour laquelle elle a besoin d'être contrôlée et sécurisée.

2 La sécurité du système d''information

Cette partie servira à donner une définition et une explication du concept qu'est la sécurité de l'information pour l'entreprise.

2.1 Notion de sécurité du système d'information

La sécurité est une situation tranquille qui résulte de l'absence réelle de danger. C'est aussi un processus dont le but est de réduire les risques ou la probabilité de subir des dommages.

Plusieurs définitions ont été données au système d'information :

«Un SI se définit comme un ensemble de composantes interreliées qui recueillent (ou récupèrent) de l'information, la traitent, la stockent et la diffusent afin d'aider à la prise de décision, à la coordination et au contrôle au sein d'une organisation »[19].

Autrement définit, le système d'information est l'élément d'unification de toutes les dimensions de l'organisation ou bien le système d'information est l'ensemble d'élément (ressource : matériels, immatériels, logiciels...) permettant de communiquer, transmettre des informations selon un cycle bien défini.

Aucunedécision et aucune action ne peut être construite sans l'appui d'un SI, et ce qu'il soit simple ou complexe, à dominante technologique ou reposant sur des procédures manuelle.

De ces définitions, nous pouvons en déduire que la sécurité du système d'information, c'est un processus permettant à une entreprise donnée de réduire les risques ou la probabilité de subir des dommages quant à la perte d'informations.

Aujourd'hui, la sécurité est un enjeu majeur pour les entreprises ainsi que pour l'ensemble des acteurs qui l'entourent. Elle n'est plus confinée uniquement au rôle de

[19]LAUDON (J),LAUDON (K) :*Management des systèmes d'information,* Ed. Pearson, Paris, 2011, P18.

l'informaticien. Sa finalité sur le long terme est de maintenir la confiance des utilisateurs et des clients. La finalité sur le moyen terme est la cohérence de l'ensemble du système d'information. Sur le court terme, l'objectif est que chacun ait accès aux informations dont il a besoin.

Autrement dit, la sécurité de l'information désigne,donc, les mesures préventives qu'il faudrait mettre en place pour préserver les informations et les moyens.

2.2 Principes fondamentaux de la sécurité du système d'information

La sécurité de l'information se caractérise par les cinq piliers suivantsde l'information :

- **L'intégrité** : qui assure que la donnée reçue est la même que celle qui a été émise, c'est à dire qu'elle n'a pas été corrompue. L'altération des données (le manque d'intégrité) peut conduire à la prise de mauvaises décisions ;

- **La confidentialité** : qui assure que la donnée reste privée durant la transmission pour que seules les personnes concernées aient la possibilité de la traiter. Il faudrait pour cela un message crypté ou une clé d'accès détenue uniquement par le(s) destinataire(s) concerné(s). La divulgation d'informations privées (perte de la confidentialité) ou le transfert d'informations privées à un destinataire autre que celui concerné, peut affecter la crédibilité de l'entreprise et surtout favoriser la concurrence ;

- **La disponibilité** : qui assure que la donnée est présente et accessible à tout moment. L'indisponibilité des informations en temps réel pourrait entrainer un retard considérable dans les tâches à accomplir et occasionner par la suite la perte de clients et donc des pertes financières ;

- **La non-répudiation** : qui permet de s'assurer de l'identité réciproque à la fois de l'émetteur et du destinataire. Aussi qui permet de garantir qu'une transaction ne peut être niée par aucun des correspondants. Déroger au principe de non répudiation entraine une non-traçabilité des conversations ou messages entre l'émetteur et le destinataire et donc un non suivi quant au respect de la confidentialité des informations (divulgation frauduleuse d'informations) ;

- **L'authentification** : qui permet de s'assurer de la véracité de l'identité de l'utilisateur qui souhaite accéder à des données à accès restreint.

2.3 Missions et Objectifs de la sécurité du système d''information

Selon le siteeduscol,« la SSI c'est donc la sécurité du système informatique »[20].
« Le système informatique est le support technique du SI et sa partie croissante. Il comprend : les technologies de l'information, les ordinateurs, les applications, les réseaux et les autres systèmes qui permettent à tous d'accéder à l'information, de l'analyser, de la créer, de l'échanger et de l'utiliser »[21].

Le besoin de maintenir l'intégrité de l'information et de protéger les actifs informatiques exige un processus de gestion de la sécurité. Ce processus comporte la mise en place (et la maintenance) de rôles et de responsabilités, de politiques, de plans et procédures informatiques.

La gestion de la sécurité implique aussi une surveillance de la sécurité, des tests et des actions correctives lors d'incidents ou de découverte de failles dans la sécurité. Une gestion efficace de la sécurité protège tous les actifs informatiques pour réduire le plus possible les conséquences de vulnérabilités et d'incidents de sécurité.

Le CIGREF[22] définit la protection de l'information de la façon suivante « La protection de l'information est une démarche consciente visant à protéger, au sein de l'entreprise étendue, ce qui vaut la peine d'être protégé, tant au niveau des données que des supports d'information. Cette démarche implique un système de gestion, une identification des informations sensibles, une analyse de risques, des acteurs, avec des rôles et responsabilités et un programme de réduction des risques ».

Ainsi mettre en place la sécurité de l'information dans le système d'information, permet à l'entreprise de prévenir et éviter des incidents majeurs de même que la propagation de leur impact néfaste sur l'ensemble de son environnement.

[20] http//:eduscol.education.fr/ecogest/si/SSI/risk_conf.Lesapproches de sécurité de système d'information, Consulté le 25/09/2017.
[21] DEYRIEUX, (A) *: le système d'information : nouvel outils de stratégie, direction d'entreprise et direction du système d'information*, Ed. Maxima, Paris, 2003, P.11.
[22] Club Informatique des Grandes Entreprises Françaises,http://cigref.typepad.fr/cigref_publications/RapportsContainer/Parus2008/protection_onformation/Protection_information_2008.pdf Publications CIGREF,Ed 2007-2008 p.5 consulté le 02/10/2017.

Selon Ghernaouti-Hélie[23],L'objectif de la sécurité des systèmes d'information est de garantir qu'aucun préjudice ne puisse mettre en péril la pérennité de l'entreprise. Cela consiste à diminuer la probabilité de voir des menaces se concrétiser, à en limiter les atteintes ou dysfonctionnements induits, et autoriser le retour à un fonctionnement normal à des coûts et des délais acceptables en cas de sinistre. La sécurité ne permet pas directement de gagner de l'argent mais évite d'en perdre. Ce n'est rien d'autre qu'une stratégie préventive qui s'inscrit dans une approche d'intelligence économique.

La sécurité du SI fait appel à des solutions techniques, mais également à la mise en place rigoureuse d'une organisation adaptée aux objectifs recherchés. Cela passe par des mesures de sensibilisation, de formation des utilisateurs, ainsi que par l'expression de règles clairement définies.

De plus, les systèmes d'information sont ouverts au monde extérieur (clients, fournisseurs d'accès internet, partenaires etc.), la probabilité qu'il y ait perte ou divulgation non autorisée d'informations est relativement élevée ; sachant que la perte de l'un des cinq piliers de l'information cités plus haut peut être dommageable pour l'entreprise. Les conséquences qu'elle pourrait encourir sont de plusieurs ordres dont les plus importants sont l'impact financier, l'impact sur l'image, l'impact juridique et dans le cas extrême l'interruption partielle ou définitive de l'activité.

L'étape que nous aborderons maintenant est celle qui nous aidera à comprendre comment se fait la mise en œuvre de la sécurité de l'information et quels en sont les constituants, en d'autre termes savoir en quoi consiste la mise en place d'un cadre de gestion de la sécurité de l'information.

Section 3 : Mise en œuvre du cadre de gestion de la sécurité du système d'information

L'étape que nous aborderons maintenant est celle qui nous aidera à comprendre comment se fait la mise en œuvre de la sécurité de l'information et quels en sont les constituants, en d'autre termes savoir en quoi consiste la mise en place d'un cadre de gestion de la sécurité de l'information.

1 Engagement de la Haute Direction

En matière de systèmes d'information, la direction générale est responsable de l'évaluation des risques, de l'établissement de la politique de sécurité et de la mise en œuvre

[23] GHERNAOUTI-HELIE,(S) :*Sécurité Internet, Stratégies et Technologies* ,Ed. Dunod,2000, p.20.

d'une structure organisationnelle. Son rôle lui est délégué par le conseil d'administration, détenteur légal et suprême des actifs informationnels.

Selon l'IFACI : l'engagement de la haute direction consiste à :

- **Effectuer une évaluation des risques** liée à la confidentialité, l'intégrité et la disponibilité des données et des ressources ;
- **Etablir une politique de sécurité** à l'échelle de l'organisation dans le but de canaliser le développement efficace des procédures et des pratiques de sécurité, de protéger les infrastructures et actifs critiques de l'entrepriseet de responsabiliser l'ensemble du personnel .une politique de sécurité de l'information est un ensemble de documents indiquant les directives, procédures, lignes de conduite, règles organisationnelles et techniques à suivre relativement à la sécurité de l'information et à sa gestion. C'est une prise de position et un engagement clair et ferme de protéger l'intégrité, la confidentialité et la disponibilité de l'actif informationnel de l'entreprise ;

- **Mettre en place une structure organisationnelle adéquate :** afin de contrôler régulièrement la conformité des opérations avec la politique de sécurité.

La direction générale doit s'atteler à mettre en place, par le biais d'un service dédié à la sécurité de l'information du système d'information, des dispositifs sécuritaires adéquats à l'entreprise toute entière. Notons que les politiques, objectifs et activités de sécurité doivent être en phase avec les objectifs et buts globaux de l'entreprise et s'inscrire dans une approche conforme à sa culture. Il lui faut pour cela un plan de sécurité adapté à ses activités.

La sécurité est un processus dont le but est de réduire les risques ou la probabilité de subir desdommages.Donald L. Pepkin[24] , propose« les cinq phases »suivantes pour élaborer un plan de sécurité,à savoir :

- **Inspection**: Identifier les fonctionnalités qui sont à la base des activités de l'entreprise.Évaluer les besoins en sécurité de l'organisation ;
- **Protection** : Mettre en place des moyens pour une réduction dynamique des risques ;
- **Détection** : Mettre en place des moyens pour une réduction réactive des risques ;
- **Réaction** : Mettre en place un plan de secours d'urgence ;

[24]Stéphane Gill, sgill.profweb.ca/spip/IMG pdf/01_*Securite Information*.pdf p.6 consulté le 18/10/2017 á 10h00.

- **Réflexion**: Une fois l'incident terminé et tout remis en place, procéder à l'étude del'événement.

2 La constitution de la structure de mise en œuvre de la sécurité de l'information

Pour que le système d'information soit efficace, il faut mettre en place un cadre de gestion adéquat de la sécurité de l'information. Le cadre de gestion sert de fondement pour la mise en place de processus formels de gestion intégrée et continue de la SI, ainsi que des risques afférents. Il doit tenir compte des changements divers (technologique, juridique, social etc.) qui peuvent avoir une influence sur le système d'information. Le cadre de gestion vise principalement à établir une structure de gouvernance et de coordination et à énoncer formellement un ensemble de rôles et de responsabilités en SI.

Afin d'encadrer la démarche de mise en œuvre du cadre de gestion de la sécurité de l'information, notre étude se réfèrera à la norme ISO/IEC 17799 :2000, aujourd'hui appelé Norme ISO 27002[25],est une norme internationale concernant la sécurité de l'information, publiée en 2005 par l'ISO, dont le titre en français est « Code de bonnes pratiques pour la gestion de la sécurité de l'information ».ISO/IEC 27002 considère que beaucoup de systèmes d'information n'ont pas été conçus pour être sécurisés. Ainsi la mise en œuvre de moyens techniques de protection a un impact limité et doit être soutenue par une organisation appropriée et par des procédures. Ladite norme propose 133 règles regroupées en 11 thèmes décrivant les meilleures pratiques en matière de sécurité de l'information.Linlaud[26] par un tableau d'analyse des thèmes de la norme ISO/IEC 27002 et Hollopar son diagramme de répartition des catégories ISO 27002, ont défini chacun des éléments du cadre de gestion de la sécurité de l'information. Ainsi, le cadre de gestion de la sécurité de l'information prend donc en compte les 11 étapes suivantes[27] :

- **La gestion de la politique de sécurité** : elle traduit l'engagement de la direction à fournir une orientation stratégique et un support en ce qui concerne la gestion de la sécurité de l'information par l'établissement d'une politique de sécurité approuvée, publiée et communiquée par elle à tous les employés. Cette politique doit faire l'objet d'une révision constante et doit être en phase avec les objectifs de l'entreprise.
- **L'organisation de la sécurité :** il s'agit de l'organisation interne et externe liées à la sécurité de l'information de l'entreprise. L'organisation interne doit prendre en compte

[25]MOISAND, (D) et GARNIER DE LABAREYRE (F) :*opcit*,p.15
[26]Les éléments cités dans notre texte sont extrait du livre LINLAUD,(D) :*la sécurité de l'information*, Ed. afnor, Paris,2003,pp.55-80.
[27]https://fr.wikipedia.org/wiki/ISO/CEI_27002ISO/CEI 27002 — Wikipédia, contenu de la norme consulté le 06/10/2017.

un cadre adéquat de gestion de la sécurité par la présence d'un comité de gestion de la sécurité de l'information émanant de la direction, la répartition claire des responsabilités en matière de sécurité de l'information, les procédures de sécurité mises en place et les dispositifs de contrôle. Pour l'organisation externe en particulier pour la sécurité d'accès des tiers et les contrats d'externalisation, la politique de sécurité doit tenir compte des risques associés à l'accès des tiers au système d'information de l'entreprise ainsi que des contrôles adaptés qui doivent être mis en œuvre. Elle doit également prendre en compte le fait que les contrats d'externalisation fassent l'objet d'engagements contractuels très précis ;

- **La classification et le contrôle des actifs :** Deux points importants :
  - **la responsabilité liée aux actifs** : l'entreprise doit réaliser un inventaire régulier de tous ses actifs liés à son SI. En délégant des responsables de gestion de ces actifs, elle peut mieux contrôler et s'assurer qu'une mise à jour récurrente de l'inventaire est effectuée ;
  - **la classification de l'information :** elle doit être accompagnée de procédures formelles et être exécutée en tenant compte des besoins liés à l'exploitation, de la sensibilité des informations, des restrictions éventuelles et du degré d'impact des évènements nuisibles à leur exploitation.
- **Les éléments de sécuritéliés aux ressources humaines :** il s'agit ici d'intégrer la sécurité de l'information dans la description des tâches ; de sélectionner le personnel permanent, contractuel ou intérimaire en fonction des critères liés à la sécurité de l'information conformément à la politique de sécurité ; de faire signer au personnel des accords de confidentialité ; de sensibiliser et de former tous les employés de l'organisme et les tiers utilisateurs si nécessaire à l'application et au respect des procédures et politique de sécurité de l'information ; d'inciter les employés à réagir face aux incidents et aux défauts de sécurité en signalant toute forme de défaillance ou dysfonctionnement ;
- **La sécurité physique et la sécurité de l'environnement :** consiste en la mise en place de périmètres de sécurité dans le but de protéger les secteurs physiques qui abritent les équipements de traitement des informations de même que les équipements eux-mêmes. Il s'agira de protéger ces secteurs ainsi que leurs accès afin de garantir que l'entrée n'est accordée qu'aux personnes autorisées. Les équipements et les secteurs physiques doivent être protégés contre tout sinistre (coupure de courant intempestive,

tentative d'interception causée par une défaillance du câblage électrique, crise, guerre etc.) ;

- **La gestion des communications et des opérations :** inclut plusieurs objectifs. L'organisme doit mettre en place des procédures et documents formels d'exploitation afin de définir les responsabilités et de séparer au mieux les tâches qui s'avèrent incompatibles. Ces procédures devront prendre en compte la gestion des incidents, la gestion des réseaux, l'utilisation de services extérieurs, la protection contre les logiciels malveillants, la sauvegarde de l'information, l'accès du système aux parties externes (prestataires, clients, public...), la sécurisation du courrier électronique et des systèmes bureautiques. Ces procédures doivent s'encadrer de dispositifs de contrôles adaptés aux technologies de l'entreprise ;
- **Le contrôle des accès logiques :** il s'agira ici de contrôler les accès à l'information. Les exigences concernant ce contrôle doivent être documentées et contenues dans la politique de sécurité de l'information. Ce contrôle inclut que chaque utilisateur soit clairement identifié par une authentification et un mot de passe forts et uniques (pour le respect du principe de traçabilité) ; que les attributions et utilisations des privilèges sont limitées et contrôlées ; que les procédures d'enregistrement, de modification ou de suppression des droits d'utilisateurs existent et sont respectées et utilisées au moment opportun ; que les accès aux réseaux et aux applications sont restreints ; que les accès aux matériels, systèmes, applications, réseaux, ont été délivrés aux personnes indiquées ;
- **Le développement et la maintenance des systèmes** : il s'agit de mettre en place des sécurités dans les applications et les systèmes de fichiers (système de validation des données entrantes et sortantes, contrôle du traitement interne), et aussi des mesures de cryptographie (code, signature numérique etc.) dans le but d'assurer la confidentialité des informations. Il faut également que les processus de maintenance des systèmes soient adaptés et mis régulièrement à jour et en œuvre. Les logiciels et progiciels doivent être protégés contre toute attaque virale et les systèmes doivent être révisés lorsque une modification se produit. Les évènements des systèmes doivent être générés et conservés (journalisation des évènements) ;
- **La gestion des incidents de sécurité :** consiste d'abord en la journalisation ou l'élaboration d'un rapport des évènements exceptionnels et significatifs ayant attrait à la sécurité de l'information. Cela permet de surveiller les opérations et d'apporter en temps réel les corrections qui s'y rapportent. Ensuite il faudrait gérer à proprement dit les

incidents en définissant les responsabilités et en développant un processus d'amélioration continue qui prend en compte l'arsenal technologique de l'entreprise de même que les objectifs globaux ;

- **La gestion de la continuité de l'activité :** l'entreprise doit mettre en place un processus pour gérer les interruptions des activités d'exploitation causées par des défaillances majeures ou des sinistres. Ensuite elle doit développer non seulement un plan stratégique basé sur l'évaluation des risques afin de déterminer l'approche complète de la continuité d'activités, mais en plus elle doit définir des plans de continuité pour maintenir ou rétablir le fonctionnement de l'exploitation. Ces plans doivent être de façon récurrente contrôlés, testés et réévalués ;
- **La gestion de la conformité :** la politique de sécurité et les procédures doivent respecter les exigences légales, règlementaires et contractuelles applicables à la structure. Ces procédures doivent être mis à jour, protégés et correctement suivis par tous les employés de l'entreprise ; le département de l'audit interne ou de la conformité doit s'en assurer. Les dispositifs de sécurité des SI doivent être régulièrement vérifiés pour assurer leur conformité technique. Les exigences d'audit des systèmes opérationnels doivent être soigneusement planifiées et approuvées afin de minimiser au maximum le risque.

La mise en œuvre du cadre de gestion ainsi développé, doit permettre d'assurer une gestion efficace de la sécurité de l'information

3 Communication et responsabilité des différents acteurs

En plus de la Direction Générale qui définit les grandes lignes de la sécurité informationnelle, chaque acteur de l'entreprise a la responsabilité de l'application des clauses de sécurité prescrites pour une bonne marche de la structure. Les employés doivent être sensibilisés aux risques et aux comportements suivants :

- Utilisation des outils de l'entreprise à des fins personnels (internet, téléphone, courriel, etc.) ;
- Protection contre les virus ou autres logiciels malveillants ;
- Gestion de l'identité informatique et contrôle d'accès aux actifs informationnels ;
- Protection des droits d'auteur, des renseignements personnels et de la vie privée.

La sécurité du patrimoine informationnel repose également sur le repérage des rôles et responsabilités des différents acteurs de la SSI :

- **Le comité de sécurité :**

Selon la norme ISO27002 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 des fonctions explicites et d'une reconnaissance des responsabilitésliéesá la sécurité d'information.

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

- **La Direction Générale (DG)**

En matière de sécurité de système d'information, la DG n'est pas seulement impliquée mais elle en détient la responsabilitéultime.L'évaluation des risques,l'établissement de la politique de sécuritéet 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 êtreamenée á déléguer certaines responsabilités. Elle doit néanmoins disposer des moyens de contrôle et de pilotage de l'ensemble des actions de son équipe.

- **La Direction du Système d'Information (DSI)**

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

La nouvelle DSIest selon MANACO[28], « celle qui doit posséder les compétences technologiques, communicationnelles, organisationnelles et managériales. Elle doit s'assurer de l'adéquation du SI á la stratégie de l'entreprise ».

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

[28] MONACO, (L) : *les carrés DCG8-systèmes d'information de gestion*, éd. Gualino, Paris, 2014-2015,pp.21-24.

- **Le Responsable de la Sécurité du Système d'Information (RSSI)**

Le RSSI, « est le garant de la sécurité des SI de l'organisme. Il intervient dans des domaines multiples avec un seul objectif : assurer l'intégralité, la confidentialité et la disponibilité des données et des matériels qui les supportent »[29].

Sa mission est donc de concevoir et d'animer la démarche de SSI en veillant á 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.

- **Le Risk Manager (RM)**

Le RMou le gestionnaire de risque est le coordonnateur du processus de gestion globale des risques d'une organisation. Il est le responsable du recensement et du suivi des risquesde celle-ci en mettant en place notamment une cartographie des risquesquiestdéployée 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 desrisques des systèmes d'information aux pratiques existantes de gestion des risqueset en rendre compte périodiquement á la Direction Générale. Selon HASSID[30], le RM a pour mission de :

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

- **L'auditinterne**

L'audit interne par ca mission d'assurance, joue un rôle capital en matière de sécurité des SI. En effet, les auditeurs internes sont appelés á fournir à la direction, une assurance indépendante et raisonnable de la pertinence et de l'efficacité des objectifs de sécurité et des contrôles connexe á ces objectifs. Ils doivent se prononcer sur l'état de la sécurité de l'information et rapporter les anomalies significatives á la DG.

[29]LINLAUD, (D) *: op cit*, p.83.
[30]HASSID, (O) *: la gestion des risques*, Ed. Dunod, Paris, 2008, p.74.

Les auditeurs internes doivent également, selon JIMENEZ[31] s'assurer que les structures sont claires et bien adaptées, que les procédures comportent les sécurités suffisantes, que les opérations ne présentent pas d'irrégularitéset que les informations diffusées sont sincères. Ce qui permettra à la Direction Générale de connaitre le niveau de maitrise des risques.

Ainsi, ils doivent identifier les menaces et les vulnérabilités qui peuvent causer un préjudice á l'organisation ; évaluer les dispositifsde maitrise des risques et proposer des mesures d'améliorations tout en s'assurant de leur mise en œuvre.

- **Le personnel operational**

Dans le domaine de la sécurité des SI, « le succès de l'ensemble des mesures de sécuritédépend des actions du personnel opérationnel »[32].

Les opérationnels sont appelés á exécuter les instructions de sécurité de l'organisationdans l'exécution de leur tâches quotidiennes car ils sont dans la plupart des attaques les maillons faibles de la stratégie de prévention contre les risques liés aux SI.

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

Nous avons posé les bases de l'audit interne et celles de la sécurité de l'information. Ce chapitre s'applique à tout type d'entreprise. Cela nous permet donc par la suite de comprendre et d'apprécier le rôle que doit jouer l'audit interne dans la sécurisation de l'information au sein d'une entreprise.

Conclusion du chapitre

A travers ce premier chapitre, nous avons posé les bases de l'audit interne et celles de la sécurité du système d'information. Ce chapitre s'applique à tout type d'entreprise. Cela nous permet donc par la suite de comprendre et d'apprécier le rôle que doit jouer l'audit interne dans la sécurisation de l'information au sein d'uneentreprise. Dans le prochain chapitre, nous verrons quels sont les normes et référentiels applicables à l'entreprise et à l'audit interne et quel est l'apport de l'audit interne à la sécurité de l'information en entreprise.

[31]Pour plus d'information veuillez consulte le livre JIMENEZ,(C), MERLIER (P) et CHELLY (D) :,*risques opérationnel :de la mise en place du dispositif á son audit*, EdRevue Banque, Paris,2008, p.100.

[32]MENTHONNEX, (J) : *sécurité et qualité informatique : nouvelles orientations*, Ed presses polytechniques et universitaires romandes, Lausanne, 1995, p.174.

Chapitre II

Normes,

Référentiels et Méthodologie,

afférents à l'audit interne

et à la sécurité de l'information

Introduction du chapitre

Les compétences requises pour accomplir des audits exigent des normes et des référentiels qui s'appliquent à l'audit des SI. Il existe des normes professionnelles internationales et nationales, et des référentiels relatifs à l'audit des entités informatisées. Ils sont élaborés par des organisations internationales qui ont le plus souvent des correspondants nationaux.

L'objectif des normes est d'informer les auditeurs du niveau minimal acceptable pour répondre aux responsabilités professionnelles et les autres parties des attentes de la profession d'audit.

Nous présenterons dans ce chapitre, en premier lieu les normes et référentiels qui traitent de l'audit interne et de la sécurité de l'information. En second lieu, nous décrirons la méthodologie en matière de sécurité de l'information. En donnant un aperçu des méthodologies de gestion des risques du SI ainsi que ses principaux acteurs.

Section 1 : Les Normes et Référentiels afférents à l'audit interne et à la sécurité de l'information

Nous présenterons par la même occasion les référentiels applicables au système de sécurité de l'information de gestion afin de comprendre les dispositions prises pour la réglementation de l'audit interne et la sécurité de l'information de gestion au sein de l'entreprise.

1 Les normes et référentiels applicables à l'audit interne

Au niveau international, ce sont les normes internationales pour la pratique professionnelle de l'audit interne de l'IIAqui constituent le référentiel de la mission d'audit interne.Elles sont complétées par un code de déontologie fournissant aux auditeurs internes les principes et valeurs régissant leurpratique professionnelle.

Selon l'IFACI, les normes[33] ont pour objet :

- De définir les principes fondamentaux de la pratique de l'audit interne ;
- De fournir un cadre de référence pour la réalisation et la promotion d'un large champ d'intervention d'audit interne à valeur ajoutée;
- D'établir les critères d'appréciation du fonctionnement de l'audit interne;

[33]IIA, Cadre de références internationales des pratiquesprofessionnelles, http://www.ifaci.com/publications/audit-interne/cripp/, Ed. 2017, p. 1. consulté le 12/09/2017.

- De favoriser l'amélioration des processus organisationnels et des opérations.

On distingue trois types de normes, dans le Cadre de références internationales des pratiques professionnelles, de l'audit interne (CRIPP):

- **Des normes de qualification** qui précisent les caractéristiques que doivent présenter les organisations et les personnesaccomplissant des missions d'audit interne;
- **Des normes de fonctionnement** qui décrivent la nature des missions d'audit interne et définissent des critères de qualitépermettant de mesurer la performance des services fournis ;
- **Des normes de mise en œuvre** qui précisent les deux types des normes précédentes en indiquant les exigences applicables dansles activités d'assurance (évaluation objective en vue de formuler en toute indépendance une opinion ou des conclusions sur uneentité, une opération, une fonction, un processus, un système ou tout autre sujet) ou de conseil.

La norme de qualification 1210.A3, stipule notamment « Les auditeurs internes doivent posséder des connaissances suffisantesdes principaux risques et contrôles relatifs aux technologies de l'information, et des techniquesd'audit informatisées susceptibles d'être mises en œuvre dans le cadre destravaux qui leur sont confiés »[34].

Les Normes s'appliquent aux auditeurs internes et à la fonction d'audit interne. Tous les auditeurs internes ont la responsabilité de se conformer aux Normes relatives à l'objectivité, aux compétences et à la conscience professionnelle individuelles. De plus, ils doivent se conformer aux Normes relatives aux responsabilités associées à leur poste. Les responsables de l'audit interne ont la responsabilité supplémentaire d'assurer la conformité globale de l'audit interne avec les Normes et d'en rendre compte.

2 Les normes et référentiels applicables à la sécurité de l'information de gestion

Plusieurs normes, méthodes et référentiels de bonnes pratiques en matièrede sécurité des systèmes d'information sont disponibles. Ils sont constitués de guides méthodologiques ainsi que de moyens de garantir une démarche desécurité cohérente[35].La sécurité de l'information évolue dans un cadre défini par les normes ISO 2700x et le CobiT.

[34]IIA, Cadre de références internationales des pratiques professionnelles, www.ifaci.com/uploads/_ifaci/ani_fichiers/CRIPP-2013-3, Ed.2013 , p. 36 consulté 9/10/2017.
[35]MOISAND,(D) et GARNIER DE LABAREYRE (F) *: op cit,* p14.

2.1 La norme ISO 27002

L'ISO a entrepris un vaste effort de rationalisation des travaux existants, donnant naissance à la série de normes ISO/IEC 27000. Ce nombre correspondà la réservation d'une série de normes relatives à la sécurité. À cejour, seules les normes 27000, 27001, 27002 et 27006 sont publiées. Certainessont obligatoires pour obtenir une certification, les autres ne sontque de simples guides[36] :

- La norme ISO/IEC 27000 présente le vocabulaire et les définitions dudomaine de la sécurité, applicables à chacun des standards ;
- La norme ISO/IEC 27001 décrit la politique du management de la sécuritédes systèmes d'information au sein d'une entreprise qui sert de référence à la certification ;
- La norme ISO/IEC 27002 constitue le guide de bonnes pratiques de lasécurité des SI ;
- La norme ISO/IEC 27003 a pour vocation d'être un guide d'implémentation;
- La norme ISO/IEC 27004 sera un nouveau standard pour le pilotage desindicateurs et des mesures dans le domaine de la sécurité des SI ;
- La norme ISO/IEC 27005 sera un nouveau standard sur le managementdes risques pour la sécurité des SI ;
- La norme ISO/IEC 27006 résume les exigences applicables aux auditeursexternes dans leur mission de certification sur l'iso 27001.

Pour rappel,La norme ISO/IEC 17799 de 2005, renommée ISO/IEC 27002, spécifie une politique de la sécurité des systèmes d'information qui se présente commeun guide de bonnes pratiques en terme d'implémentation d'un cadre de gestion adéquat et fiable pour une meilleure organisation de l'entreprise et une atteinte effective des objectifs de sécurité de l'information.

De façon schématique, la démarche de sécurisation du système d'information selon la norme ISO 27002 passe par quatre étapes, á savoir :

- Périmètre à protéger (liste des biens sensibles) ;
- Identification de la Nature des menaces ;
- L'évaluation de leur impact sur le système d'information ;
- Détection des mesures de protection à mettre en place pour réduire les impacts

[36]MOISAND, (D) et GARNIER DE LABAREYRE (F) : *op cit*, pp.14-15.

La norme ISO/IEC 27002 est orientée processus et son application dépasse de ce fait les simples aspects de technique informatique. Elle s'intéresse à l'organisation du personnel ainsi qu'aux problèmes de sécurité physique (accès, locaux, Etc).

2.2 Le référentiel

Plusieurs référentiels existent et gouvernent les systèmes d'information.De façon générale, « un référentiel est une collection de bonnes pratiques sur un sujet donné. Lorsque celui-ci fait l'objet d'une large diffusion et qu'il est reconnu sur le marché on parle alors de standard »[37] .

Dans le domaine du SI, un référentiel est un ensemble cohérent et outillé de données du système d'information de l'entreprise, partagé par une communauté d'acteurs et qui possède « les cinq caractéristiques »[38]:

- **Centralité** : il doit être reconnu comme la référence sur le sujet qu'il traite ;
- **Stabilité** : ses données ne changent pas beaucoup avec le temps ;
- **Qualité** : les processus associés à un référentiel assurent une certaine maîtrise de la fiabilité des données ;
- **Unité de sens** : le sens sémantique de ses données ont une certaine homogénéité ;
- **Interopérabilité** : il est techniquement coordonné avec le système d'information et lui procure un certain nombre de services.

Le référentiel joue un rôle centralisateur et octroie à celui qui s'y conforme, une validité reconnue. Il est généralement élaboré par une organisation regroupant un ensemble d'experts. Dans le cadre de notre travail, nous ne présenterons que ceux qui ont une importance particulière dans le processus de gestion/maîtrise des risques informatiques.

- **COSO (Committee of Sponsoring Organizations of the Treadway Commission)**

Le COSO publie en 1992 une définition standard du contrôle interne et crée un cadre pour évaluer et améliorer le dispositif de contrôle interne.

[37] Club Informatique des Grandes Entreprises françaises http://www.cigref.fr/cigref_publications/RapportsContainer/Parus2009/Referentiels_de_la_DSI_CIGREF, Ed.2009.pdf. p.9.consulte le 02/10/2017.

[38] BIZINGRE(J), PAUMIER (J)et RIVIERE (P) : (*Référentiel du système d'information*, Ed. Dunod, Paris ,2013, p.13.

Pour atteindre ses objectifs, le COSO « présenté cinq composantes sur lesquelles une organisation peut s'appuyer »[39]Il s'agit :

- De l'environnement de contrôle ;
- D'évaluation des risques ;
- D'activités de contrôle ;
- D'information et communication ;
- Du pilotage .

- **CobiT (Control Objectives for Information and related Technology)**

Publié en 1996, le CobiT est une méthodologie d'évaluation des services informatiques au sein de l'organisation. Il propose un ensemble de bonnes pratiques de gouvernance IT.

Le CobiT propose au management un cadre de référence des pratiques de contrôle et de maîtrise de l'informatique, applicable pour évaluer un environnement informatique existant ou en phase d'implémentation. Ses processus concernent les domaines fonctionnels que sont : planification et organisation (domaine1), acquisition et mise en place (domaine 2), distribution et support (domaine 3), et surveillance et évaluation (domaine 5). Dans son guide de mise en œuvre, le CobiT propose également des outils d'analyse et d'évaluation de risques des environnements informatisés[40]. Les trente-quatre « 34 processus du CobiT » permettent de couvrir trois cent dix-huit « 318 objectifs »[41] .

L'utilisation du CobiT permet aux systèmes d'information de l'entreprise :

- De s'aligner sur le métier de l'entreprise ;
- D'apporter un plus aux métiers ;
- De gérer au mieux ses ressources ;
- De gérer les risques de façon efficace.

Le CobiTest l'élément de base pour une bonne gouvernance d'activité et institutionnelle de l'entreprise. La mise en œuvre de ses bonnes pratiques crée de la valeur ajoutée.

[39]Price Waterhouse Coopers et IFACI : *Référentiel intégré de contrôle interne*, Ed. Eyrolles, Paris, 2014, p.38.

[40] DESROCHES (A), LEROY (A) et VALLEE (F) : *La gestion des risques*, Editions Lavoisier, 2007, p.219-220.

[41] PILLOU (J.F) et CAILLEREZ (P) : *Tout sur les systèmes d'information : Grandes, moyennes et petites entreprises*, Editions Dunod, Paris, 2011, p.79.

CobiT aborde la gouvernance de la sécurité de l'information en s'intéressantà[42] :

- La prise en compte de la sécurité de l'information dans l'alignementstratégique ;
- La prise de mesures appropriées pour limiter les risques et leurs conséquencespotentielles à un niveau acceptable ;
- La connaissance et la protection des actifs ;
- La gestion des ressources;
- La mesure pour s'assurer que les objectifs de sécurité sont bien atteints ;
- L'apport de valeur par l'optimisation des investissements en matière desécurité de l'information ;
- Les bénéficesretirés ;
- L'intégration de la sécurité de l'information dans les processus.

Globalement, CobiT aborde la sécurité de l'information dans plus devingt(20) processus sur trente quatre(34). Mais les processus suivants font apparaître unedimension sécurité importante dans les objectifs de contrôle :

- PO6 − Faire connaître les buts et orientations du management ;
- PO9 − Évaluer et gérer les risques ;
- DS4 − Assurer un service continu;
- DS5 − Assurer la sécurité des systèmes.

Dans la mise en œuvre de CobiT, il est conseillé de mener des actions deconduite du changement qui regrouperont les acteurs concernés par unmême processus, à l'intérieur comme à l'extérieur de la DSI. Cettedémarche a pour effet de préciser à la fois les activités critiques et les responsabilités associées. Àpartir du standardCobiT, l'entreprise peut bâtir son référentiel pour mettresur pied un modèle de gouvernance des systèmes d'information.

3 La gestion des risques pour les systèmes d'information

Au sein des entreprises, la sécurité des systèmes d'information est de plus en plus abordée à l'aide d'approches basées sur les risques. L'expérience montre que de telles études prospectives réduisent de manière considérable les pertes liées aux faiblesses de sécurité des systèmes d'information.

[42]MOISAND, (D) et GARNIER DE LABAREYRE (F): *op cit,* p214.

3.1 Les fondements

Pour bien appréhender la gestion des risques, ses objectifs et ses limites, il est nécessaire de comprendre en premier lieu les concepts sous-jacents.

Définition du risqué

Le risque est défini comme « l'effet de l'incertitude sur l'atteinte des objectifs »[43]. Cet effet correspond soit à un écart négatif, soit à un écart positif par rapport à l'objectif initialement fixé. En général, l'écart positif correspond à une opportunité.

Par contre, pour l'IFACI, un risque est défini comme « 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 de maîtrise »[44].

Le risque informatique devrait donc être considéré comme le risque dû à l'utilisation, la possession, l'exploitation, l'influence et l'adoption de l'informatique dans une organisation.

D'après la norme ISO/CEI 27002 : 2005, la menace est définie comme « la cause potentielle d'un incident indésirable pouvant entraîner des dommages au sein d'un système ou d'un organisme ». La vulnérabilité (encore faille ou brèche) quant à elle est définie comme « la faiblesse d'un bien ou d'un groupe de biens pouvant faire l'objet d'une menace »[45]. En effet, le bien dont il est question ici est en fait un actif informationnel.

Gestion des risquesinformatiques

La gestion des risques est définie comme un ensemble de moyens, de comportements, de procédures et d'actions adaptées aux caractéristiques de chaque société qui permet aux dirigeants de maintenir les risques à un niveau acceptable pour la société. Cette gestion poursuit principalement quatre objectifs :

- **Créer et préserver la valeur, les actifs et la réputation de la société** :La gestion des risques permet d'identifier et d'analyser les principales Elle vise à anticiper les risques au lieu de les subir, et ainsi à préserver la valeur, les actifs et la réputation de la société ;

[43]CLAUDE, (P) :*10 clés pour la sécurité de l'information : ISO/CEI 27001*, Editions AFNOR, Paris, 2012, p.39.
[44]RENARD, (J) *: op cit*, p.155.
[45]CLAUDE,(P) :*op cit*, pp.41-42.

- **Sécuriser la prise de décision et les processus de la société pour favoriserl'atteinte des objectifs** : La gestion des risques vise à identifier les principaux événements et situations susceptibles d'affecter de manièresignificative la réalisation des objectifs de la société. La maîtrise de ces risques permet ainsi de favoriser l'atteintedes dits objectifs.

La gestion des risques est intégrée aux processus décisionnels et opérationnels de la société. Elle est un desoutils de pilotage et d'aide à la décision.La gestion des risques permet de donner aux dirigeants une vision objective et globale des menaces etopportunités potentielles de la société, de prendre des risques mesurés et réfléchis et d'appuyer ainsi leursdécisions quant à l'attribution des ressources humaines et financières. ;

- **Favoriser la cohérence des actions avec les valeurs de la société :**De nombreux risques sont le reflet d'un manque de cohérence entre les valeurs de la société et les décisions etactions quotidiennes. Ces risques affectent principalement la crédibilité de la société ;
- **Mobiliser les collaborateurs de la société autour d'une vision commune des principaux risques** et les sensibiliser aux risques inhérents à leur activité.

Toutefois, l'efficacité de tout dispositif nécessite au préalable la définition d'une bonne politique de gestion des risques car c'est elle qui donne l'impulsion à cette activité et définit les responsabilités des principaux acteurs.

3.2 La politique de gestion des risques informatiques

La politique de gestion des risques informatiques est généralement incluse dans la politique de sécurité informatique. Il s'agit d'un document qui présente les buts et les orientations du management.

Une politique de sécurité informatique contient quatre (04) thématiques clés[46] que sont :

- La gestion des risques fondée sur l'évaluation et la réduction des risques ;
- La qualification de l'information fondée sur une classification de l'information destinée à adapter le niveau de protection de celle-ci ;
- La conformité des systèmes avec les politiques et standards de sécurité en vigueur ;

[46]Club Informatique des Grandes Entreprises Françaises : www.cigref.fr/cigref_actualites/.../Controle_interne_du_SI_Assises_Securite, Ed. 2009, consulté le 02/11/2017 à 14h00.

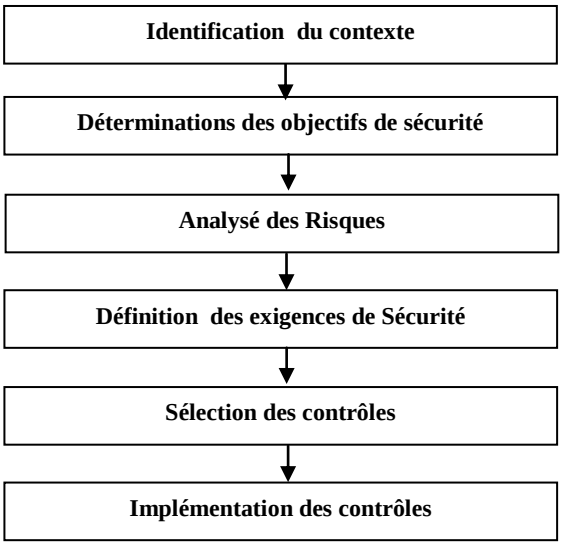
- La sensibilisation à la politique de SSI fondée sur une communication adéquate auprès de chaque employé (en modes « push et pull »).

« La politique de gestion des risques informatiques formule les objectifs du dispositif de gestion des risques en cohérence avec la culture de l'entreprise, le langage commun utilisé, la démarche d'identification, d'analyse et de traitement des risques et de cas échéant, le seuil de tolérance »[47].

3.3 Le processus de gestion des risques

Après avoir mis en évidence les concepts intervenant dans la gestion des risques, on peut identifier un processus de haut niveau couvrant ses activités. Ce processus est presque toujours appliqué dans les méthodes pratiques de gestion des risques, comme nous le verrons par la suite[48].

Figure 1: Le processus de gestion des risques



Source: Eric Papet, 2008.rmll.info/IMG/pdf/MEHARI_RMLL_2008_2-2.pdf, Ed 2008

- **L'identification du contexte** : Dans cette partie, il est question de prendre connaissance de l'organisation, son environnement, ses ressources, son SI et de déterminer précisément les limites du système sur lequel va porter l'étude de gestion des risques.

[47] HERVE (F), MADERS (H. P) et MASSELIN (J.L) : *Les métiers d'auditeur interne et de contrôleur permanent*, Ed.Eyrolles, Paris, 2014, p.6.

[48] Pour plus d'information consulté, Eric Papet,:2008.rmll.info/IMG/pdf/MEHARI_RMLL_2008_2-2.pdf, Ed 2008,Consulté le 15/10/2017.

- **La détermination des objectifs de sécurité**: vise à spécifier les besoins en termes de confidentialité, intégrité et disponibilité.

- **L'analyse des risques :** constitue le cœur de la démarche de gestion des risques. Elle a pour finalité l'identification et l'estimation de chaque composante du risque (menace/vulnérabilité/impact), afin d'évaluer le risque et d'apprécier son niveau, dans le but de prendre des mesures adéquates. Il y a deux grandes écoles pour l'identification desrisques : soit en réalisant un audit du système et de ses différents acteurs, soit à partir de bases de connaissances prédéfinies ;
- **Détermination des exigences :** réduction des risques identifiés ;
- **Sélection des contrôles :** Définitions des choix technique (gestion desFlux)
- **Implémentation des contrôles:**Une fois les contrôles sélectionnés, il reste alors à les implémenter dans le SI et à éventuellement les tester et les évaluer.

3.4 Aperçu des méthodologies de gestion des risques liés au système d'information et les principaux acteurs

Plus de 200 méthodes de gestion/analyse des risques sont déclinées actuellement à travers le monde. Le CIGREF a récemment rappelé, en regard du domaine de la sécurité des SI, que « l'abondance de normes et de méthodes est souvent source de confusion».

- **Les méthodes de gestion des risques**

Pour réduire le champ du choix au cœur des méthodes formelles, certaines sont actuellement très populaires, faisant référence dans leur domaine.A ce titre, nous avons choisi de détailler « EBIOS, MEHARI et OCTAVE »[49],qui remplissent efficacement leur rôle dans la conduite d'une démarche de gestion des risques.

- **EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)**

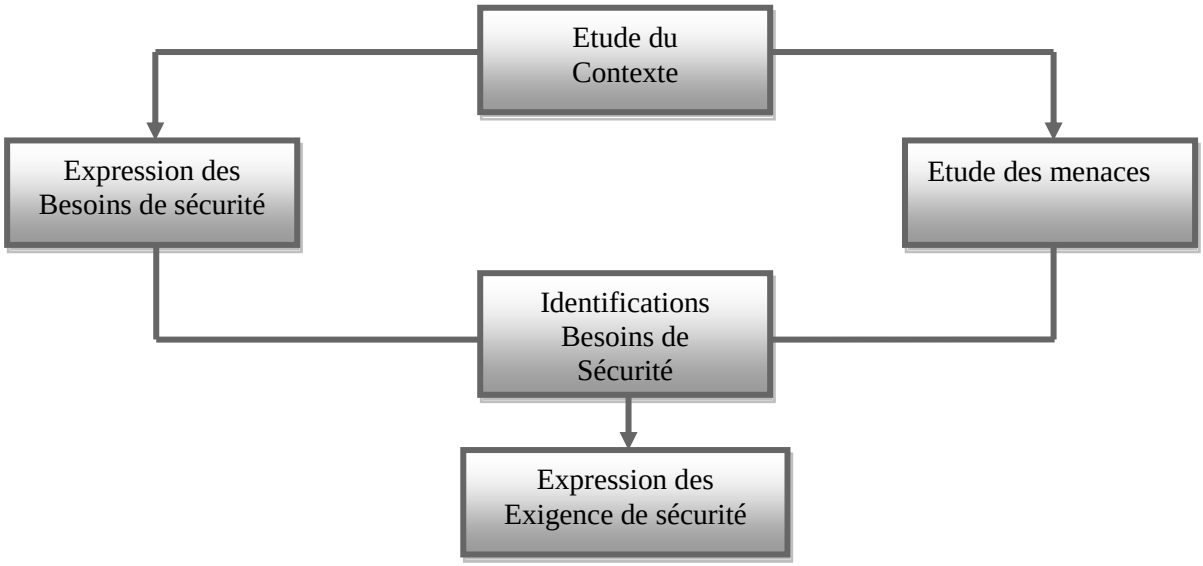
La méthode EBIOS est également une méthode de gestion des risques de la sécurité du SI développée par l'ANSSI et conforme aux normes ISO 27001, 27005 et 31000. Elle permet d'apprécier, de traiter les risques relatifs à la sécurité des SI et de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires, constituant ainsi un outil complet de gestion des risques. C'est une approche plus simple, plus claire. Elle contient des exemples et des conseils offrant la possibilité

[49]Hugo Etiévant,http://cyberzoide.devloppez.com/Sécurite/Méthode, Ed.2006publié le 18 aôut 2006 Consulté le 22/09/2017.

d'élaborer et d'assurer le suivi d'un plan d'actions relevant de la sécurité des systèmes d'information.

La démarche générale d'EBIOS comprend cinq (05) étapes résumées à travers le schéma[50] ci-dessous :

Figure 2 : Démarche globale d'EBIOS



Source : ANSSI(2010).

✓ **L'étude du contexte :** permet d'identifier quel système d'information est la cible de l'étude. Cette étape délimite le périmètre de l'étude : présentation de l'entreprise, architecture du système d'information, contraintes techniques et réglementaires, enjeux commerciaux. Mais elle étudié aussi le détail des équipements, des logiciels et de l'organisation humaine de l'entreprise.

✓ **L'expression des besoins de sécurité :** permet d'estimer les risques et de définir les critères de risque. Les utilisateurs du SI expriment durant cette étape leurs besoins de sécurité en fonction des impacts qu'ils jugent inacceptables.

✓ **L'étude des menaces :** permet d'identifier les risques en fonction non plus des besoins des utilisateurs mais en fonction de l'architecture technique du système d'information. Ainsi la liste des vulnérabilités et des types d'attaques est dressée en fonction des matériels, de l'architecture réseau et des logiciels employés. Et ce, quelles

[50] ANSSI, http://ww.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite , Ed.2010 Consulté le 18/10/2017 à 17h00.

que soient leur origine (humaine, matérielle, environnementale) et leur cause (accidentelle, délibérée).

✓ **L'identification des objectifs de sécurité :**confronte les besoins de sécurité exprimés et les menaces identifiées afin de mettre en évidence les risques contre lesquels le SI doit être protégé. Ces objectifs vont former un cahier des charges de sécurité qui traduira le choix fait sur le niveau de résistance aux menaces en fonction des exigences de sécurité.

✓ **La détermination des exigences de sécurité :** permet de déterminer jusqu'où on devra aller dans les exigences de sécurité. Il est évident qu'une entreprise ne peut faire face à tout type de risques, certains doivent être acceptés afin que le coût de la protection ne soit pas exorbitant. C'est notamment la stratégie de gestion du risque tel qu'il est défini dans un plan de risque qui sera déterminé ici : accepter, réduire ou refuser un risque. Cette stratégie est décidée en fonction du coût des conséquences du risque et de sa probabilité de survenue. La justification argumentée de ces exigences donne l'assurance d'une juste évaluation.

EBIOS fournit donc la méthode permettant de construire une politique de sécurité en fonction d'une analyse des risques qui repose sur le contexte de l'entreprise et des vulnérabilités liées à son SI**.**

- **OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation**

Cette méthode d'évaluation du risque est publiée par le Software Engineering Institute (SEI) de la Carnegie Mellon University (Etats-Unis) en 1999, reconnue dans le domaine de la sécurité des SI. Les fondements mêmes de cette méthode reposent sur la possibilité de réaliser une analyse des risques de l'intérieur de l'organisation, exclusivement avec des ressources internes.

OCTAVE est une méthode d'évaluation des vulnérabilités et des menaces sur les actifs opérationnels. Une fois ces derniers identifiés, la méthode permet de mesurer les menaces et les vulnérabilités pesant sur eux.

Les trois phases suivantes déclinées au cœur d'OCTAVE, respectent l'analyse progressive des trois blocs des concepts de gestion des risques présentés en amont[51] :

[51] Voir : Hugo Etiévant, http://cyberzoide.developpez.com/sécurité/méthodes-analyse-Ed.2006publié le /18/08/2006 Consulté le 16/10/2017.

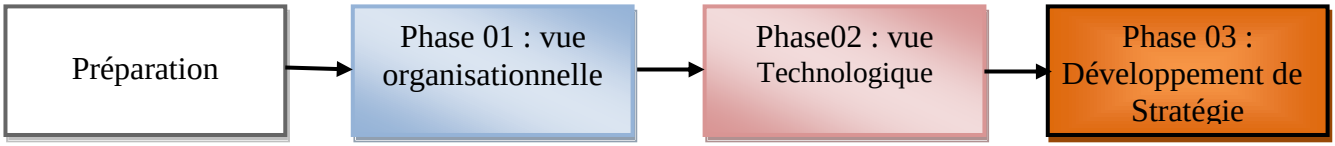
✓ **La phase 1** (vue organisationnelle) permet d'identifier les ressources informatiques importantes, les menaces associées et les exigences de sécurité qui leur sont associées.

✓ **La phase 2** (vue technique) permet d'identifier les vulnérabilités de l'infrastructure (ces dernières, une fois couplées aux menaces, créant le risque).

✓ **La phase 3** de la méthode décline le développement de la stratégie de sécurité et sa planification (protection et plan de réduction des risques).

Cette methode se resume a traver le schéma sous- dessous[52] :

Figure3 : Les phases principales d'OCTAVE



Source: Hugo Etiévant ,http://cyberzoide.developpez.com/sécurité/méthodes-analyse-Ed.2006

- **MEHARI (Méthode Harmonisée d'Analyse de Risques)**

LaMEHARI[53] demeure une des méthodes d'analyse des risques les plus utilisées actuellement. Elle est dérivée de deux autres méthodes d'analyse des risques (MARION et MELISA). La MEHARI est maintenue en France par le CLUSIF (Club de la Sécurité des Systèmes d'Information Français), via notamment le Groupe de Travail dédié à cette méthode.

LaMEHARI se présente comme une véritable boîte à outils de la sécurité des SI,est une méthode complète d'évaluation et de management des risques liés à l'information, MEHARI consiste à :

✓ Identifier et évaluer les risques dans le cadre d'une politique de sécurité (Planification) ;

✓ Faire des revues des points de contrôle des vulnérabilités (Contrôle) ;

✓ Fournir des indications précises sur les plans à bâtir à partir des revues effectuées (Déploiement) ;

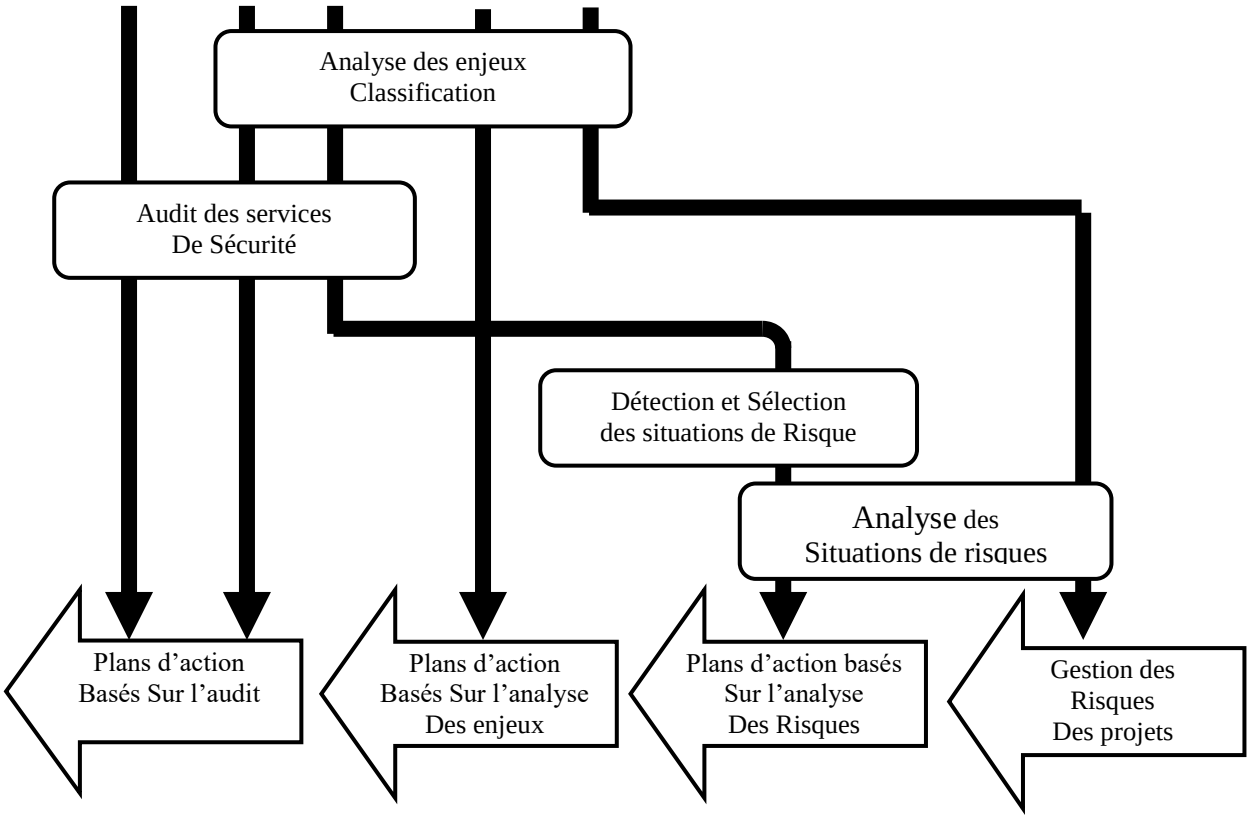
[52]ANSSI,cyberzoide.developpez.com/securite/methodes-analyse-risques/ publié le18/9/2006 Consulté le : 21/10/2017.

[53]Mag-securs,l'actualite de la securite informatique, https://www.mag-securs.com/news/id/17633/la-methode-mehari-methode-harmonisee,Ed.2006publié dans magsecurs N°12 –juin2006 consulté le 12/10/2017.

✓ Piloter ces plans d'action dans une approche cyclique (Amélioration) (CLUSIF, 2010).

LaMEHARI apporte une aide efficace pour manager et sécuriser l'information dans toutes sortes d'organisations. Cette méthode se résume à travers la figure ci-dessous[54].

Figure 4: Démarche MEHARI globale



Source :CLUSIF,www.nmayer.eu/publis/NMA-JPH_MISC24.pd ,Ed2010

La MEHARI présente une grande diversité dans l'utilisation de ses modules. Trois approches se détachent plus particulièrement[55] :

✓ En se basant sur une analyse détaillée des risques, il est possible de mettre en oeuvre des plans de sécurité. Cette démarche se décline au niveau stratégique, mais aussi opérationnel. Le premier niveau permet la cohérence des besoins et du contexte de l'ensemble de l'organisation. Le second niveau définit les unités business autonomes au cœur de l'organisation et en charge des décisions nécessaires en matière de sécurité.

[54]CLUSIF, www.nmayer.eu/publis/NMA-JPH_MISC24.pd ,Ed2010

[55] Extrait de : Mag-securs, l'actualite de la securite informatique,https://www.mag-securs.com/news/id/17633/la-methode-mehari-methode-harmonisee.,Ed.2006 publié dans mag-securs N°12 –juin 2006 consulté le 12/10/2017.

✓ En se basant sur l'audit de sécurité, ou plus précisément après un diagnostic de l'état de sécurité, la réalisation de plans d'actions est facilitée. En effet, des faiblesses relevées découlent alors directement des actions à entreprendre.

✓ Dans le cadre de la gestion d'un projet particulier, tenir compte de la sécurité, en se basant, de nouveau, sur l'analyse des risques, et ainsi faciliter l'élaboration de plans d'action. Les besoins de sécurité sont alors directement intégrés aux spécifications du projet, et à intégrer dans le plan de sécurité global de l'entité concernée.

Cette méthode s'aligne avec les deux premières en termes de couverture du processus de gestion des risques.

➢ **Les acteurs de la gestion des risques informatiques**

Les principaux acteurs de la gestion des risques informatiques sont : la Direction Générale, le Risk Manager, le Responsable de la Sécurité des Systèmes d'informationet l'Audit interne.

- **La Direction Générale**

« Il est de la responsabilité de l'équipe dirigeante, et de la Direction Exécutive de définir les orientations stratégiques et de les suivre en ce qui concerne la gestion des risques au sein de l'entreprise »[56].

La Direction Générale fait partager à toute l'entreprise la vision d'une gestion rigoureuse et efficace du risque, donne l'impulsion de celle-ci et crée les conditions de mise en œuvre du processus de management des risques. Il est également de sa responsabilité d'instaurer une bonne culture de gestion des risques au sein de l'entreprise sur le giron de la gouvernance des risques avec pour objectif principal, la maîtrise des risques.

➢ **Le Risk Manager (RM)**

« le RM est chargé de concevoir les méthodes et les outils de gestion des risques (cartographie des risques, etc.), d'élaborer et de mettre en œuvre la politique et le plan d'assurance de l'entreprise, de conseiller les métiers sur les mesures de prévention, de protection, de détection et de réaction face au risque »[57].

[56]GREUNING (H.V) et BRATANOVIC (S.B) :*Analyse et gestion du risque bancaire*, Ed. ESKA, Paris,2004, p.33.

[57]CLUSIF,https://clusif.fr/.../rm-rssi-deux-metiers-sunissent-pour-la-gestion-des-risques-du-si, Ed.2006 publié le 01/06/2006 Consulté le 16/10/2017.

- **LeResponsable de la Sécurité des Systèmes d'Information(RSSI)**

Le RSSI est chargé de prévenir les risques dès leur phase de développement, de proposer des plans d'action de réduction et de contrôle des risques, de suivre la mise en place des actions décidées, de rendre compte à la Direction Générale et de communiquer sur la sécurité du SI avec le ou les Directeurs en charge des SI.

- **L'audit interne**

« Les auditeurs internes ont une contribution très importante à apporter en ce qui concerne le processus de gestion des risques liés au système d'information »[58].

D'après la norme 2120.A1 de l'IIA « l'audit interne doit évaluer les risques afférents au gouvernement d'entreprise, aux opérations et aux systèmes d'information de l'organisation au regard de :

- ✓ L'atteinte des objectifs stratégiques de l'organisation ;
- ✓ La fiabilité et l'intégrité des informations financières et opérationnelles ;
- ✓ L'efficacité et l'efficience des opérations et des programmes ;
- ✓ La protection des actifs ;
- ✓ Le respect des lois, règlements, règles, procédures et contrats »[59].

Par ailleurs, une fois le processus de gestion des risques installé au sein de l'entreprise, la fonction d'audit interne est considéré comme un prolongement de la gestion des risques.Ce prolongement du processus de gestion des risques étant la maîtrise des risques, c'est dire donc que l'audit interne joue un rôle dans la maîtrise des risques du système d'information.

Face aux référentiels et aux bonnes pratiques précités, l'audit interne se doit d'établir et de structurer une méthodologie de travail adéquate afin de mener ses activités dans le cadre de la règlementation sécuritaire en vigueur.

Section 2 : Méthodologie de l'audit interne dans le cadre de la sécurité du système

L'audit de sécurité d'un système d'information se présente comme un moyen d'évaluation de la conformité d'une situation liée à la sécurité par rapport à une politique de sécurité ou par rapport à un ensemble de règles de sécurité, de procédures ou techniques de référence.

[58] GREUNING (H.V) et BRATANOVIC (S.B) *:opcit*, p.53.

[59] IIA, Cadre de références internationales des pratiques professionnelles, www.ifaci.com/uploads/_ifaci/ani_fichiers/CRIPP-2013-3.pdf, p.51 Consulté le 22/09/2017.

La démarche de l'audit devra suivre un plan de travail bien structuré, la mission de l'audit interne se déroule toujours de la même façon.

1La Démarche de réalisation d'un audit sécurité de système d'information

L'ensemble des étapes du processus d'audit est comme suite :

1.1 Définition de la charte d'audit

Avant de précéder à une mission audit, une charte d'audit doit être réalisée, elle a pour objet de définir la fonction de l'audit, les limites et modalités de son interventions, ses responsabilités ainsi que les principes régissant les relations entre les auditeurs et les audités. Elle fixe également les qualités professionnelles et morales requises des auditeurs.

De plus, « une charte d'audit interne doit garantir les conditions d'indépendance des auditeurs vis-à-vis des autres membres de l'entreprise mais aussi protéger les audités contre tout abus de la part des auditeurs internes. Cette charte doit préciser les missions, les objectifs, les responsabilités et les procédures de travail »[60].

1.2 Préparation de l'audit

Elle constitue une phase importante pour la réalisation de l'audit sur terrain. En effet, c'est au cours de cette Phase que se dessinent les grands axes qui devront être suivis lors de l'audit sur terrain. Elle se manifeste par des rencontres entre auditeurs et responsables de l'organisme à auditer. Au cours de ces entretiens, les espérances des responsables vis-à-vis de l'audit devront être exprimées. Aussi, le planning de réalisation de la mission de l'audit doit être fixé.

Les personnes qui seront amenées à répondre au questionnaire concernant l'audit organisationnel doivent être également identifiées. L'auditeur(ou les auditeurs) pourrait également solliciter les résultats des précédents audits. Cette Phase sera suivie par l'audit organisationnel et physique.

1.3 Audit organisationnel et physique

- **Objectifs**

Dans cette étape, il s'agit de s'intéressons à l'aspect physique et organisationnel de l'organisme cible, à auditer. Nous nous intéressons donc aux

[60]SCHICK, (P) *:Mémentod'audit interne,* Ed. Dunod, Paris, 2007,P.28.

aspects de gestion et d'organisation de la sécurité, sur les plans organisationnels, humains et physique.

L'objectif visé par cette étape est donc d'avoir une vue globale de l'état de sécurité du système d'information et d'identifier les risques potentiels sur le plan organisationnel.

- **Déroulement**

Afin de réaliser cette étape de l'audit ce volet doit suivre une approche méthodologique qui s'appuie sur « une batterie de questions ».Ce questionnaire préétabli devra tenir compte et s'adapter aux réalités de l'organisme à auditer. A l'issu de ce questionnaire, et suivant une métrique, l'auditeur est en mesure d'évaluer les failles et d'apprécier le niveau de maturité en termes de sécurité de l'organisme, ainsi que la conformité de cet organisme par rapport à la norme référentielle de l'audit.

1.4 Audit technique

- **Objectifs**

Cette étape de l'audit sur terrain vient en seconde position après celle de l'audit organisationnel. L'audit technique est réalisé suivant une approche méthodique allant de la découverte et la reconnaissance du réseau audité jusqu'au sondage des services réseaux actifs et vulnérables.

Cette analyse devra faire apparaitre les failles et les risque, les conséquences d'intrusions ou de manipulations illicites de données. Au cours de cette phase, L'auditeur pourra également apprécier l'écart avec les réponses obtenues lors des entretiens. Il testera aussi la robustesse de la sécurité du système d'information et sa capacité à préserver les aspects de confidentialité, d'intégrité, de disponibilité et d'autorisation.

Cependant, l'auditeur doit veiller à ce que les tests réalisés ne mettent pas en cause la continuité de service du système audité.

- **Déroulement**

Vu les objectifs escomptés lors de cette étape, leurs aboutissements ne sont possibles que par l'utilisation de différents outils. Chaque outil commercial qui devra être utilisé, doit bénéficier d'une licence d'utilisation en bonne et due forme.

Egalement les outils disponibles dans le monde logiciel libre sont admis. L'ensemble des outils utilisés doit couvrir entièrement ou partiellement la liste non exhaustive des catégories ci-après :

- Outils de sondage et de reconnaissance du réseau.
- Outils de test automatique de vulnérabilité du réseau.
- Outils spécialisés dans l'audit des systèmes d'exploitation.
- Outils d'analyse et d'interception de flux réseaux.
- Outils de test de la solidité des objets d'authentification (fichiers de mots clés)
- Outils de test de la solidité des outils de sécurité réseau (firewalls,IDS,outils d'authentification).
- Outils de scanne d'existence de connexions dial-up dangereusse (wardialing).
- Outils spécialisés dans l'audit des SGBD existants.

Chacun des outils à utiliser devra faire l'objet d'une présentation de leurs caractéristiques et fonctionnalités aux responsables de l'organisme audité pour les assurer de l'utilisation de ces outils.

1.5 Test d'intrusions (Audit instrusif)

- **Objectifs**

Cet audit permet d'apprécier le comportement du réseau face à des attaques. Également, il permet de sensibiliser les acteurs (management, équipe, informatique sur site, les utilisateurs) par des rapports illustrant les failles décelées, les tests qui ont été effectués (scénarios et outils) ainsi que les recommandations pour pallier aux insuffisances identifiées.

- **Déroulement**

La Phase de déroulement de cet audit doit être réalisée par une équipe de personnes ignorante du système d'audit avec une définition précise dans limites et horaires des tests. Etant donné l'aspect risque (pour la continuité de services du système d'information)que porte ce type d'audit, l'auditeur doit :

- Bénéficier de grandes competences;
- Adhérer à une charte déontologique ;

- S'engager (la charte d'audit) à un non débordement : implication à ne pas provoquer de perturbation du fonctionnement du système, ni de provocation de dommages.

1.6 Rapport d'audit

Afin des précédentes phases d'audit sur terrain, l'auditeur est invité à rédiger un rapport de synthèse sur sa mission d'audit.

Cette synthèse doit être révélatrice des défaillances enregistrées. Autant est –il important de déceler un mal, autant il est également important d'y proposer des solutions. Ainsi, l'auditeur est également invité à donner ses recommandations, pour pallier aux défauts qu'il aura constatés.

Ces recommandations doivent tenir compte de l'audit organisationnel et physique, ainsi que du technique et intrusif.

2 Les outils et tests de contrôle

Pour qu'une mission d'audit de la sécurité de l'information soit effective, l'auditeur interne doit premièrement avoir des compétences dans le domaine à auditer. Selon la norme 1210« Les auditeurs internes doivent posséder les connaissances, les savoir-faire et les autrescompétences nécessaires à l'exercice de leurs responsabilités individuelles. L'équipe d'auditinterne doit collectivement posséder ou acquérir les connaissances, les savoir-faire et lesautres compétences nécessaires à l'exercice de ses responsabilités »[61].

En matière de sécurité de l'information, comme le stipule la MPA 1210.A3, il n'est pas demandé à l'auditeur interne d'être un informaticien ou un auditeur informaticien mais plutôt d'avoir des compétences et connaissances dans les technologies de l'information et dans la gestion de la sécurité. Ceci pour pouvoir effectuer des évaluations professionnelles et apporter des recommandations créatrices de valeur ajoutée. L'entreprise attend de l'auditeur interne des compétences telles que :

- La réflexion analytique / œil critique ;
- La communication ;
- Le management des risques ;
- L'extraction et l'analyse des données ;

[61]IIA, Cadre de références internationales des pratiques professionnelles, http://www.ifaci.com/publications/audit-interne/cripp/ , Ed. 2017, p.9 Consulté le 12/09/2017.

- Les contrôles généraux des SI ;
- Le sens des affaires.

Comme outilset tests de contrôle en matière de système d'information,l'auditeur interne peut utiliser les techniques d'entretien (questionnaire de contrôle interne, enquête, interview), l'examen de la documentation (les procédures, politique de sécurité, documents relatifs aux ressources humaines etc.), l'observation, l'utilisation de logiciels d'audits spécialisés, les tests de corroboration, les tests de conformité, les tests de cheminement. Il peut également procéder à des tests d'intrusion afin d'éprouver la vulnérabilité du système informatique de gestion.

L'auditeur interne effectuera ces tests de contrôles afin de s'assurer de l'efficience du dispositif de contrôle mis en place pour assurer et maintenir la sécurité de l'information. A travers son esprit d'analyse et ses outils, il contribue d'une manière ou d'une autre à la gestion de la sécurité de l'information et ainsi crée de la valeur ajoutée.

3 Contribution de l'audit interne à la création de la valeur ajoutée

Pour assurer la création de la valeur ajoutée, l'auditeur interne doit analyser la gouvernance d'activité de l'entreprise relative au processus de maîtrise des risques informatiques. Pour ce faire, il peut se fonder sur les bonnes pratiques du CobiT pour effectuer un certain nombre de vérifications par rapport à ce qui est mis en place dans l'entreprise et formuler des recommandations. « Une bonne gouvernance d'activité conduit automatiquement à laperformance de l'entreprise et donc à une création de la valeur ajoutée »[62].

La gouvernance d'activité concerne le « comment » des choses. L'auditeur devra vérifier:

- Comment sont identifiés les risques informatiques ?
- Comment sont appliquées les méthodologies d'analyse et de gestion des risques informatiques (EBIOS, MEHARI, etc.) ?
- Comment sont fixés les objectifs du processus de maîtrise des risques informatiques ?

Ainsi, en fonction des réponses obtenues, l'auditeur interne devra faire des recommandations au regard des bonnes pratiques du COBIT en vue de leurs optimisations.

[62]AFAI et CIGREF,http://www.itgi-france.com,Ed. 2005, p.4 consulte le 18/11/2017 á 16h00.

- **Au niveau de la gestion de la sécurité de l'information** :

L'entreprise aura une approche cohérente de la définition des processus TI.Elle comprendra mieux son environnement de contrôle informatique et l'importance des politiques de sécurité informationnelle. Elle saura sur quels points mettre l'accent afin d'aligner sa stratégie informatique avec sa stratégie globale.

L'entreprise pourraaisémentmettre à jour ses procédures et politiques en matière de sécurité de l'information et les suivre en fonction de son changement d'environnement ou de stratégie. Elle aura connaissance des risques liés à la sécurité de l'information susceptibles d'avoir un impact négatif sur ses activités et pourra mieux les classer par priorité. Par la compréhension des risques de sécurité, l'entreprise sera amène de prendre des décisionsqui s'alignent aisément à ses objectifs.

Chaque corps métier saura ce qu'il faut faire pour maintenir et améliorer la sécurité de l'information dans son domaine. L'entreprise saura de quelles compétences elle a besoin pour son fonctionnement et pourra ainsi attribuer convenablement les rôles et responsabilités. De même, cela favorisera une bonne protection et une bonne utilisation des actifs liés aux TI.

- **Au niveau des opérations et de la technologie de sécurité de l'information**

L'évaluation de ce facteur permettra à l'entreprise de mieux identifier les risques liés aux technologies de l'information.Elle saura quels sont les moyens et méthodes techniques modernes à adopter pour sauvegarder et protéger ses informations, comment les utiliser et comment les faire respecter. Les technologies seront utilisées de manière efficiente et efficace pour permettre la réalisation des objectifs au moment opportuns. Les rôles seront également clairement définis et les attributions et privilèges, nettement repartis.

Cette section nous a permis de cernerla démarche d'audit,à travers les outils et tests de contrôle.Par ailleurs, nous avons présenté l'apport de l'audit interne ainsi que sa participation à la création de la valeur ajoutée. La section suivante consistera à présenter les outils utilisés pour collecter les données ainsi que le modèle d'analyse de données.

Section 3 : Méthodologie de la recherche

Dans le souci de présenter l'apport de l'audit interne à la sécurité du système d'information de gestion, après avoir fait la revue du dispositif théoriqueconcernant la sécurité de l'information et sa gestion ainsi que le cadre référentiel , il s'agira pour nous dans la partie

pratique que nous réaliserons au seins de L'ENPI, de constater, d'observer, de diagnostiquer le Système de gestion de sécurité de l'information quant aux normes et aux bonnes pratiques et de présenter les résultats d'analyse.

Nous avons découpé cette section en deux points à savoir le modèle d'analyse d'une part et, d'autre part, la collecte et l'analyse de données.

1 Le modèle d'analyse

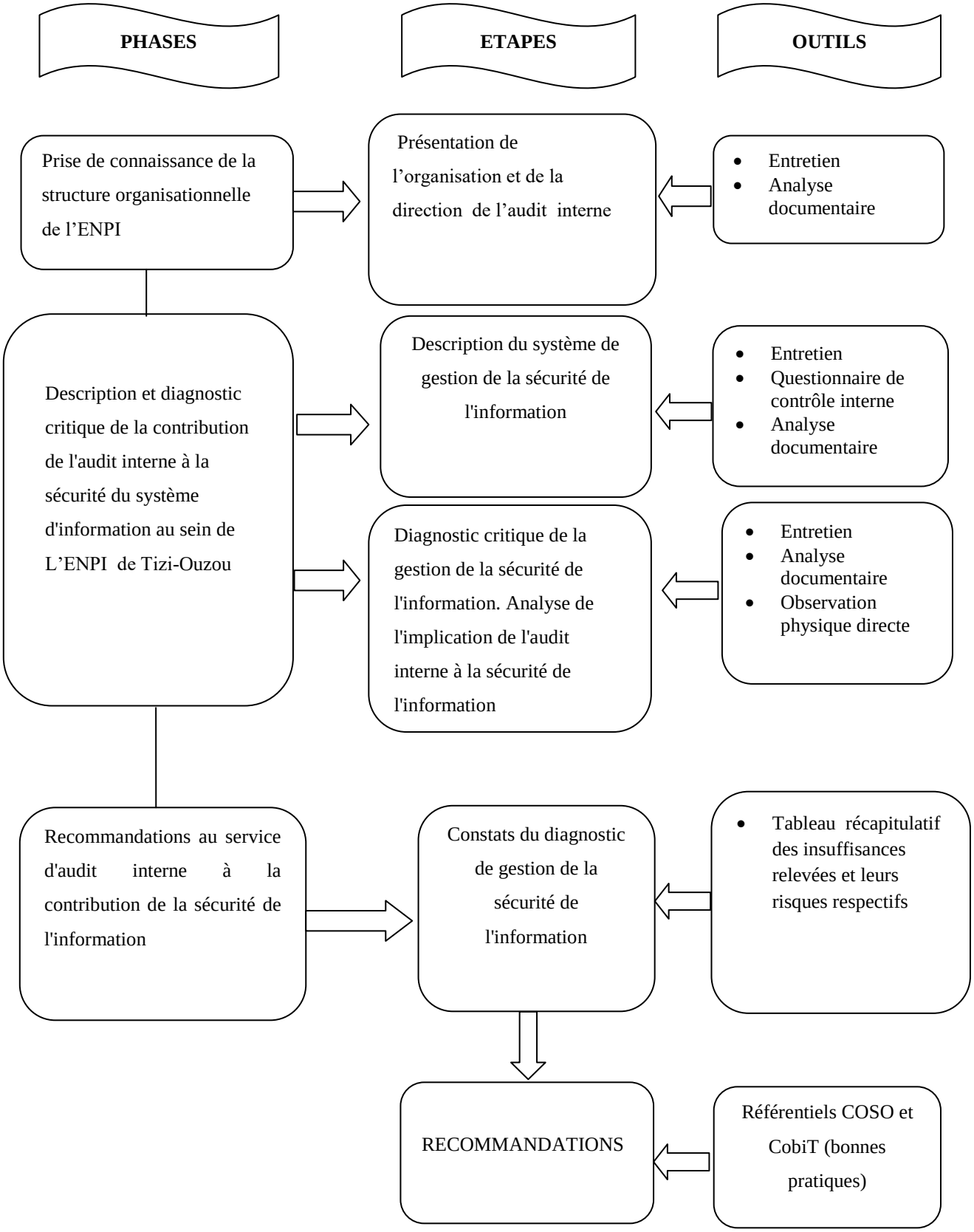
Le modèle d'analyse représente pour nous, la démarche que nous envisageons utiliser pour réaliser notre étude.

Présenté sous forme schématique, notre modèle est construit autour de trois phases qui sont :

- Une phase de prise de connaissance de la structure organisationnelle de l'ENPI de Tizi-Ouzou;
- Une phase de présentation du dispositif de sécurité du système d'information et la maîtrise des risques informatiques et l'apport de l'audit interne dans celui-ci ;
- Une phase d'analyse de l'apport de l'audit interne à la sécurité du système d'information de gestion.

Chacune de ces phases contient uneou deux étapes auxquelles nous avons associés des outils permettant de collecter et d'analyser les données.

Figure 5: Modèle d'analyse



Source : Nous- Même

2 Les outils de collecte et d'analyse de données

Les principaux outils retenus pour la réalisation de ce travail seront présentés en fonction des différentes étapes**.**

2.1 Etape 1 : Présentation de l'organisation et de la direction de l'audit interne

Dans cette étape, nous utiliserons principalement l'entretien et l'analyse documentaire.

- **Entretien**

L'entretien est une source importante d'information. En effet, il s'agit d'un échange interactif avec un interlocuteur ciblé et s'effectuant généralement en face à face (rarement par téléphone). Au cours de cette étape, l'entretien consistera à échanger principalement avec le Directeur des Ressources Humaines (DRH) de l'ENPI de Tizi-Ouzou afin que celui-ci nous présente les principales directions de LENPI de Tizi-Ouzou, leurs fonctionnements et leurs objectifs. Ce sera aussi l'occasion pour nous d'obtenir l'organigramme de l'ENPI.

- **Analyse documentaire**

L'analyse documentaire consistera à consulter les documents internes mais aussi externes à l'entreprise en vue de recueillir les données utiles pour notre étude. Ainsi, dans le cadre de ce travail, nous consulterons la fiche de présentation de l'ENPI de Tizi-Ouzou, et son l'organigramme. L'analyse documentaire nous permettra d'acquérir une bonne connaissance de l'ENPI de Tizi-Ouzou.

2.2 Etape 2 : Description du système de gestion de la sécurité de l'information

Comme outils, nous utiliserons, l'entretien, le questionnaire de contrôle interne et l'analyse documentaire.

- **Entretien**

A l'aide d'un guide d'entretien construit à l'avance (voir annexe 01),notre entretien sera semi directif avec l'Ingénieur en informatique du service informatique et nous permettra d'avoir une meilleure description du processus de sécurité du système informatiques. Ceci nous permettra ensuite de pouvoir confirmer ou d'infirmer certaines hypothèses formulées au début de notre travail.

- **Questionnaire de contrôle interne (QCI)**

Notre QCI ne sera composé que de questions fermées c'est-à-dire des questions qui ne nécessiteront qu'un OUI ou NON comme réponse (voir annexe 2).Le but de ce questionnaire est de s'assurer de l'existence d'un dispositif de sécurité du système informatique et la maîtrise de la gestion risques à l'ENPI de Tizi-Ouzou, de ressortir les principaux éléments constituants ce dispositif de maîtrise des risques s'il existe et enfin d'identifier les éventuelles faiblesses de ce dispositif.

- **Analyse documentaire**

A ce niveau, les politiques et documents relatifs à la sécurité du système d'information de gestionqui doit être normalement consulte, notamment la politique de gestion des risques informatiques, la charte informatique, la politique informatique, la cartographie des risques informatiques, la politique informatique. A l'issu de cette étape, on pourra faire un premier diagnostic de notre thème d'étude.

2.3 Etape 3 : Diagnostic critique de la gestion de la sécurité de l'information. Analyse de l'implication de l'audit interne à la sécurité de l'information

Nous aurons recours à l'entretien, à l'analyse documentaire et à l'observation physique directe.

- **Entretien**

A l'aide d'un guide d'entretien conçu à l'avance (voir annexe 3), notre entretien se fera face à face avec le Directeur d'Audit Interne de l'ENPI de Tizi-Ouzou,afin de ressortir la contribution des auditeurs internes à la sécurité du système d'information de gestion.

- **Analyse documentaire**

Dans le cadre de ce travail, nous consulterons principalement,lacharte d'audit interne de l'ENPI de Tizi-Ouzouainsi les rapports de missions réalisées au niveau du service informatique dans le cadre de sécurité du système d'information de gestion.

- **Observation physique directe**

L'observation est une technique de collecte d'informations qui se fonde sur l'étude du comportement ou de l'attitude d'un individu en train de réaliser ses activités.

Contrairement à l'entretien, cette méthode prend beaucoup plus de temps à réaliser**.** Au cours de celle-ci, l'attitude observée peut parfois être biaisée à cause de la présence de l'expérimentateur alors notre observation sera menée avec une grande discrétion.

Le but principal de cette observation dans le cadre de ce travail est de faire une comparaison entre ce qui est prescrit dans la charte d'audit interne et la pratique en ce qui concerne le processus de maîtrise des risques informatiques et la sécurité du système d'information de gestion à l'entreprise.

2.4 Etape 4 : Constats du diagnostic de gestion de la sécurité de l'information

Nous utiliserons principalement le tableau récapitulatif des insuffisances relevées et leurs risques respectifs lors de l'examen. Il nous permettra de ressortir les insuffisances et les risques décelées au niveau de la contribution de l'audit interneà la sécurité du système d'information de gestion

2.5 Etape 5 : Recommandations

Comme présenté au niveau du modèle d'analyse, en fonction des insuffisances relevées, nous formulerons des recommandations au regard des bonnes pratiques**.**

Parvenu au terme de cette section ayant porté sur la méthodologie de recherche, élément primordial pour juger de la pertinence des informations que nous présenterons au niveau de la partie pratique, nous avons jugé bon de retenir comme outils de collecte et d'analyse de données, l'entretien, l'observation physique directe, l'analyse documentaire, le QCI, et le tableau récapitulatif des insuffisances relevées et leurs risques respectifs.

L'usage de chaque outil dépendra de l'étape à laquelle nous nous situons et des types d'information que nous souhaiterions recueillir.

Conclusion du chapitre

Ce chapitre nous a permis de comprendre le cadre normatif et référentiel et les méthodologies de gestion des risques telles que MEHARI, EBIOS, etc. Nous avons également fait référence à l'apport de l'audit interne dans la gestion de la sécurité de l'information. De façon générale, son rôle est de veiller à l'atteinte des objectifs assignés par la Direction Générale dans ses procédures de sécurisation des actifs informationnels de la structure.

Chapitre III

Audit interne et sécurité du système d'information de gestion au sein de l'ENPI de Tizi-Ouzou

Introduction du chapitre

Le secteur de l'immobilier est d'une importance avérée dans la mesure où il contribue de manière conséquente à la satisfaction des besoins de la société en matière d'infrastructures et d'une manière sensible sur l'économie d'un pays.

La gestion commerciale des logements et des locaux est une action ou activité consistant à l'achat de terrains, la réalisation de projet et la vente des logements, locaux et équipements, etc.

Les sollicitations pour ce secteur notamment concernant le logement et avec l'évolution démographique aident particulièrement dans les pays en voie de développement à rendre les besoins toujours plus accentués.

Ce secteur de part son aspect stratégique et son importance vital constitue l'une des préoccupations majeures des dirigeants de la société et des acteurs économiques.

N'ayant pas reconduit sa certification ISO. l'ENPI, ne dispose d'aucun référentiel formel, ni d'aucune autre formalisation inhérente au système d'information de gestion. C'est ce que le préposé à la responsabilité en matière nous a déclaré.

Lors de nos déplacements au siège de l'entreprise, le responsable chargé de notre accueil, ne nous a remis aucuns document (même informel) ; il s'est contenté de nous faire une narration que nous avons essayé de rédiger pour lui conférer le caractère formalisé.

Une fois notre rédaction terminée, nous l'avons remise (pour lecture et confirmation) au responsables; grand fût notre étonnement, il nous a déclaré que tout ce qui est repris par nos soins ne se fait au sein de l'ENPI.

C'est pour quoi, ce chapitre est repris de ce que doit normalement ce faire au sein de l'ENPI.

Section 1 : Présentation générale de l'ENPI

La présentation de l'ENPI Direction de projet de Tizi-Ouzou va se faire à travers son historique, présentation de ses missions et objectifs, son organisation et ses différents produits immobiliers et enfin présentation de la direction de l'audit interne.

1 Historique l'ENPI

L'Entreprise Nationale de Promotion Immobilière « ENPI-SPA », Société par Actions a été créée le 06 Mai 2009 conformément à la résolution N° 05/92 du 22 janvier2009 du Conseil Participation de l'Etat(CPE), portant sur la réorganisation des Entreprises de Promotion du logement Familial « E.P.L.F » dont le siège social est situé à Alger, Route de Sidi Yahia, Bir Mourad Rais.

La mise en œuvre de la restructuration des Entreprises Publiques Economiques – EPLF, a donné naissance à l'entreprise ENPI, par voie de fusion-absorption.

La direction de projets de Tizi-Ouzou fait partie des 48 entités qui constituent l'Entreprise Nationale de Promotion Immobilière (ENPI).

2 Présentation, organisation et missions de l'ENPI

En premier lieu, nous ferons la présentation de L'ENPI direction de projets de Tizi-Ouzou, ainsi que sa création étant que direction de projets. Puis nous décrirons son organisation administrative et structurelle et enfin ses objectifs, missions et ses différents produits immobiliers.

2.1 Présentation de l'organisme d'accueil

L'Entreprise Nationale de Promotion Immobilière est une EPE, SPA crée en 2009 est considérée comme un promoteur immobilier public, par lequel l'Etat cherche à stabiliser le marché de l'immobilier et faire face à la spéculation sur un marché instable. Il ya lieu de signaler que celle –ci est régie par le code du commerce, ce qui sous-entend que sa survie dépend de son résultat.

- **La situation géographique**

  L'Entreprise Nationale de Promotion Immobilière par abréviation (ENPI), direction de projets de Tizi-Ouzou sis à : Rue MEGHNEM Med AKLI et fils LOUNES, Quartier A, bâtiment A3, cite 104 Nouvelle Ville, Tizi-Ouzou.

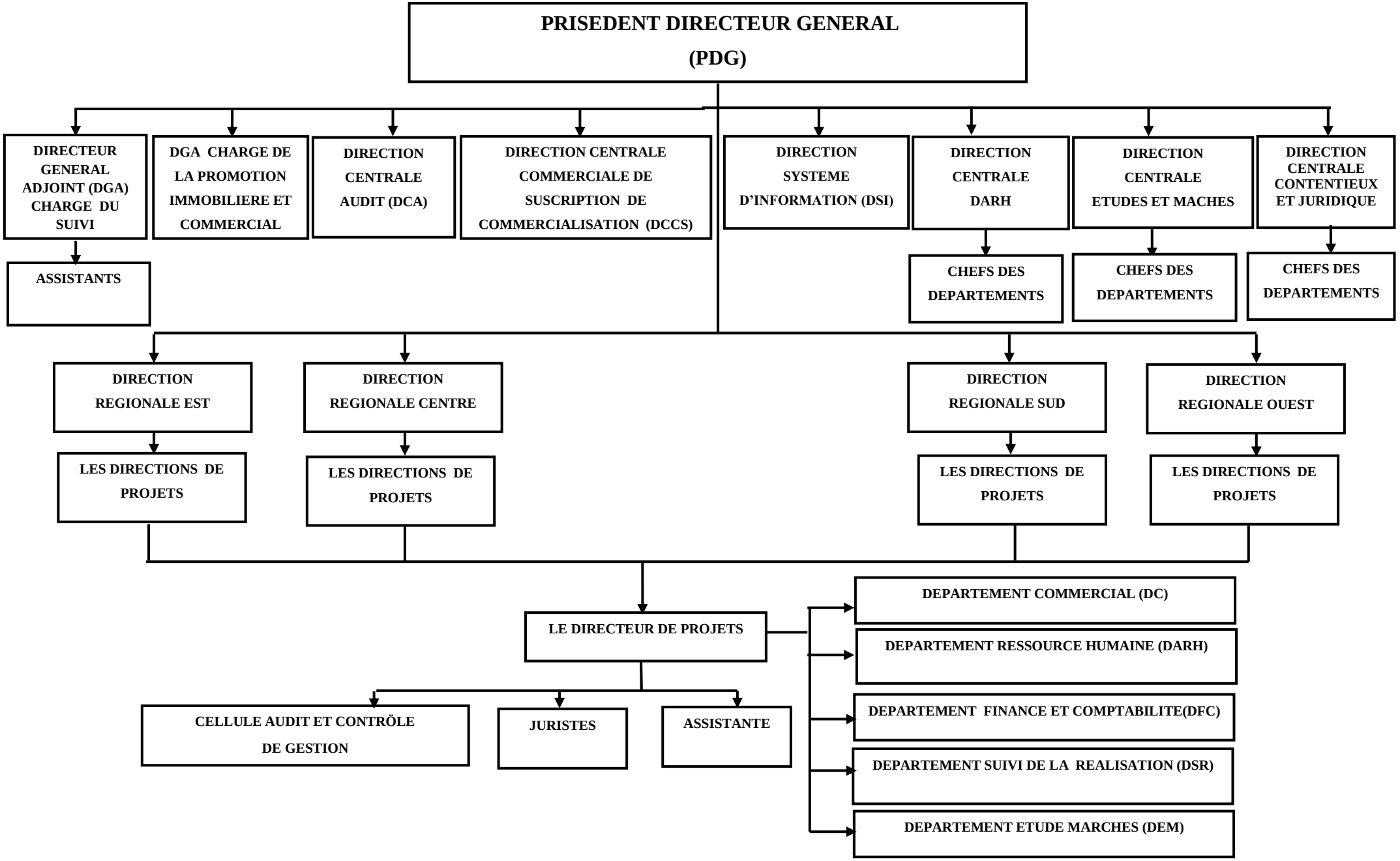
- **La création de la direction de projets de Tizi-Ouzou**

A la création de l'ENPI, l'ex EPLF de Tizi-Ouzou comme toutes les EPLF est passée à la direction de projets de l'ENPI ; elle a pris en charge les programmes lancés par l'ENPI au niveau des deux wilaya à savoir, Tizi-Ouzou et Bouira. Elle est rattachée actuellement à la direction régionale centre dont le siège est situé à AIN NAADJA. ALGER.

2.2 Organisations administratives et structurelles de l'ENPI de Tizi-Ouzou

- **Organigrammegénérale de l'entreprise**

L'organigramme de l'ENPI se schématise comme suit :


PRISEDENT DIRECTEUR GENERAL
(PDG)
DIRECTEUR GENERAL ADJOINT (DGA) CHARGE DU SUIVI
DGA CHARGE DE LA PROMOTION IMMOBILIERE ET COMMERCIAL
DIRECTION CENTRALE AUDIT (DCA)
DIRECTION CENTRALE COMMERCIALE DE SUSCRIPTION DE COMMERCIALISATION (DCCS)
DIRECTION SYSTEME D'INFORMATION (DSI)
DIRECTION CENTRALE DARH
DIRECTION CENTRALE ETUDES ET MACHES
DIRECTION CENTRALE CONTENTIEUX ET JURIDIQUE
ASSISTANTS
CHEFS DES DEPARTEMENTS
CHEFS DES DEPARTEMENTS
CHEFS DES DEPARTEMENTS
DIRECTION REGIONALE EST
DIRECTION REGIONALE CENTRE
DIRECTION REGIONALE SUD
DIRECTION REGIONALE OUEST
LES DIRECTIONS DE PROJETS
LES DIRECTIONS DE PROJETS
LES DIRECTIONS DE PROJETS
LES DIRECTIONS DE PROJETS
LE DIRECTEUR DE PROJETS
DEPARTEMENT COMMERCIAL (DC)
DEPARTEMENT RESSOURCE HUMAINE (DARH)
DEPARTEMENT FINANCE ET COMPTABILITE(DFC)
DEPARTEMENT SUIVI DE LA REALISATION (DSR)
DEPARTEMENT ETUDE MARCHES (DEM)
CELLULE AUDIT ET CONTRÖLE DE GESTION
JURISTES
ASSISTANTE

2.3Mission et objectif de l'ENPI de Tizi-Ouzou

- **Mission**

La mission principale de cette entreprise est la réalisation et la construction des logements, centres commerciaux et touristiques, équipements, restauration des immeubles en vue de leur revente.

Pour réaliser sa mission, L'entreprise Nationale de Promotion Immobilière « ENPI-SPA » est chargée de :

- L'acquisition de terrains d'assiettes en vue de lancer toutes les opérations concourantes à la conception, le financement de la réalisation d'ensembles immobilières ;
- L'acquisition de terrains d'assiettes, en vue de la réalisation de programmes de lotissements viabilisés dont les parcelles sont destinées à la vente ;
- L'acquisition d'immeuble bâtis, en vue de leur réhabilitation, rénovation ou restructuration et destinés à la vente ;
- La gestiond'ensemblesimmobiliers ;
- Le conseil et l'assistance en matière de gestion du patrimoine ;
- La réalisation du programme de logements Promotionnels « LPP » ; programme d'intervention sur tout le territoire national pour tous types de logements collectifs, semi-collectifs et individuels.

- **Objectif de l'entreprise :**

L'Entreprise National de Promotion Immobilière (ENPI) anciennement EPLF, a pour objectif la réalisation de projets immobiliers publics.

Comme toute entreprise économique L'ENPI doit générer des profits ; toutefois, elle a le double rôle à savoir, un outil de réalisation de l'Etat, qui concours à stabiliser le marché immobilier et la rentabilité pour sa survie.

- **Les différents types de produits immobiliers**

La segmentation du marché immobilier peut se faire comme suit :

- **Le logement social :** Sous toutes ses formes destine aux couches sociales qui ont un revenu mensuel inferieur ou égale à 24.000,00DA ;
- **Logement location-vente (LLV):**Programme confié à l'Agence d'Amélioration et Développent du Logement**, (AADL),** destiné aux ménages ayant un revenu mensuel se situant entre 24.000,00 DA et 108.000,00DA ;
- **Logement Promotionnel Public (LPP)** : Programme dont est chargée l'ENPI, il est destiné aux citoyens ayant un revenu mensuel supérieur à 108.000,00DA et inferieur à 201.600,00DA.
- **Logement Promotionnel Libre (LPL) :** Etant donné sa qualité d'entreprise public économique régie par le code du commerce, la survie de l'ENPI dépend exclusivement de sa rentabilité ; pour cette raison, elle consacre une bonne partie de son programme au segment du logement promotionnel libre.

3 Présentation de la direction de l'audit interne

L'audit interne a pour objectif de permettre á L'ENPI – SPA de mieux maitriser les risques auxquels elle est exposée, par une évaluation continue du dispositif de contrôle interne et par des recommandations d'améliorations.

La Direction Centrale d'audit interne est rattachée administrativement à la Direction Générale.

3.1 Organisation de l'audit interne au sein de L'ENPI

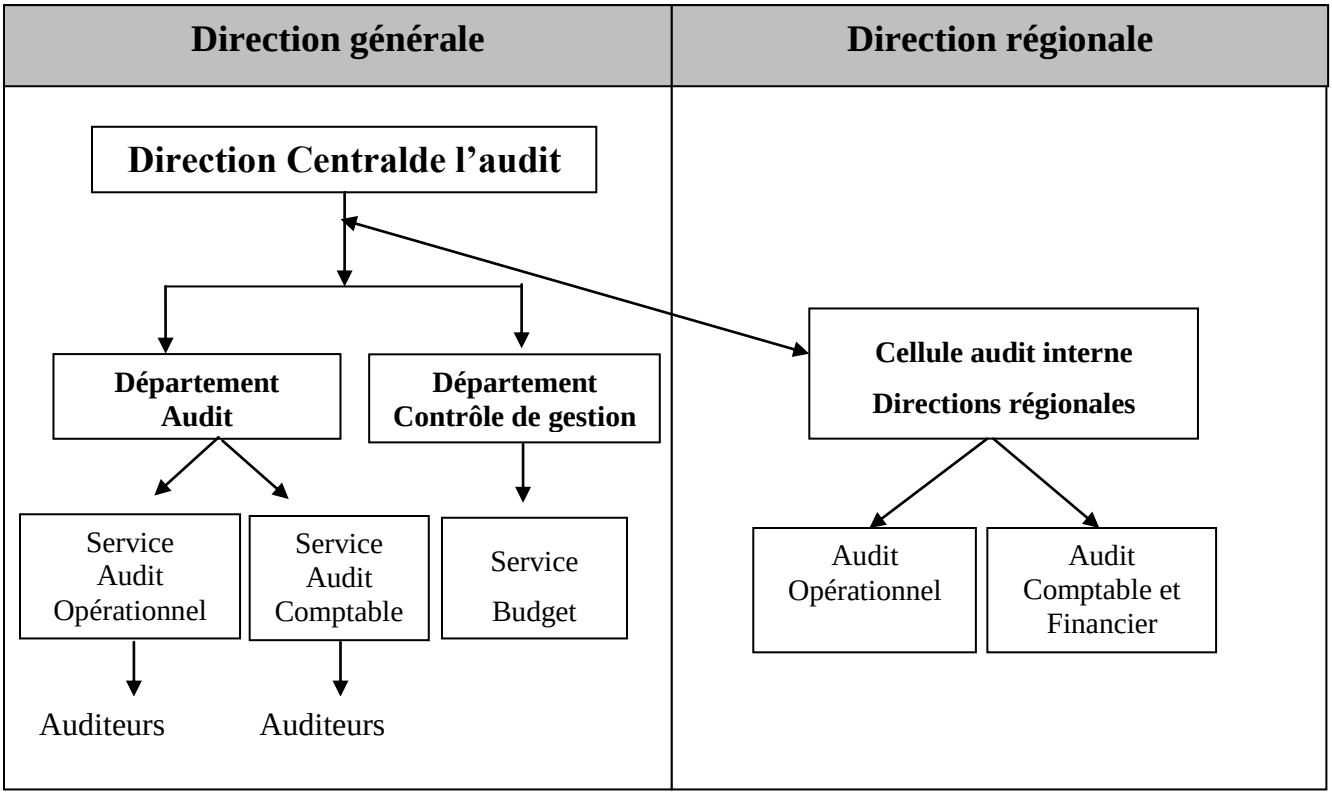
La fonction de l'audit interne au sein de L'ENPI est structurée comme suit :

- Une Direction Centrale au niveau de la Direction Générale de L'ENPI : Composée de sept (7) éléments.
- Une cellule d'Audit interne au niveau de chaque Direction Régionale: composée d'un responsable et de deux (2) auditeurs.
- Une cellule d'Audit au niveau de chaque filiale.

La Direction Centrale d'Audit Interne est rattachée hiérarchiquement au Président Directeur Général de l'ENPI.

Les cellules d'Audit des Directions Régionales sont rattachées hiérarchiquement aux Directeur Régionaux et fonctionnellement á la Direction Centrale d'Audit

Figure 6: **ORGANISATION DE L'AUDIT INTERNE**



Source : L'ENPI.

3.2 Champs d'application et d'intervention de l'audit interne

Le champ d'application de l'audit interne et d'intervention des missions sont étendue à l'ensemble des structures et des fonctions de L'ENPI.

- Les auditeurs de la direction centrale peuvent intervenir dans l'ensemble des entités de L'ENPI ;
- Les cellules d'audit interviennent au sein des directions régionales et des directions de projets ;
- Pour assurer une bonne exécution de leur mission, les auditeurs internes interviennent sur la base du plan d'audit approuvé par la direction générale ;
- Les auditeurs interviennent dans tous les domaines, ou processus administratifs, comptables et financiers, fonctionnels ou opérationnels.

3.3Les missions, objectifs de l'audit interne :

Les missions de l'audit interne de L'ENPI sont définies comme suit :

- S'assurer que les différentes structures de L'ENPI exercent efficacement leur fonction de direction et de contrôle ;
- S'assurer de l'adéquation du système de contrôle interne ;
- S'assurer de la fiabilité et l'intégrité de l'information financière ;
- La protection et la sauvegarde du patrimoine de l'entreprise ;
- Vérifier que les Directions Fonctionnelle de L'ENPI évaluent et contrôle les risques inhérents à leur activité ;
- S'assurer que les procédures internes sont définies, communiquées et mises en application ;
- L'efficacité et l'efficience du contrôle interne et la lutte contre la fraude ;
- S'assurer que les décisions stratégiques prises par le président Directeur Général, le Conseil d'Administration et l'Assemblée Générale sont mises en application ; les programmes, les plans et les objectifs sont réalisés.

Lors de leurs missions, les auditeurs doivent, respecter un certain nombre de règles déontologique et d'éthique. Les Auditeurs conduisent leurs missions sans préjugé, en toute objectivité, impartialité et honnêteté. Les auditeurs utilisent avec précaution les informations acquises au cours de leurs missions et respectent les règles de confidentialité (sûreté des informations). Ils réalisent leurs travaux conformément aux règles édictées par les Normes Internationales pour la Pratique Professionnelle de l'audit interne.

Les objectifs de l'audit interne sont les suivants :

- Améliorer les procédures et les méthodes d'audit afin de développer d'avantage l'efficacité et la précision des activités d'audit ;
- Développer et réaliser une stratégie permettant de s'assurer que les audits sont réalisés de manière efficace et efficiente ;
- Continuer à développer et engager du personnel afin de s'assurer que les équipes d'audit ont les ressources et les compétences requises pour réaliser leurs missions et atteindre leurs objectifs.

3.4 Rôles et responsabilités de la direction d'audit

Il faut dire que la compréhension du rôle de l'audit interne est visible au sein de L'ENPI. Dans le cadre de ses activités d'assurance et de conseil, la direction de l'audit est soumise directement au président directeur général de L'ENPI-SPA.

Dans ce cadre, il est de la responsabilité du directeur en charge de l'audit interne de maintenir et développer des compétences et expertises des auditeurs de manière á satisfaire les conditions de la charte d'audit et á l'effet de :

- Assurer l'indépendance de l'audit ;
- Elaborer, examiner et faire approuver le plan d'audit ;
- Faire régulièrement le point de son exécution ;
- Examiner les suites données aux recommandations.

Afin de réussir sa mission, le directeur de l'audit a la responsabilité d'établir lui-même des plans d'audit flexibles :

- Plan stratégique décline en plan opérationnel d'audit s'appuyant sur une méthodologie approprié basée sur les risques ;
- Ce plan d'audit sera soumis au président directeur général et conseil d'administration de L'ENPI-SPA, pour revue et approbation ;
- Le directeur d'audit et son équipe élaboreront des plans d'audit annuels incluant les missions spéciales ou projets réclames par le Président Directeur Général, ils optimiseront l'utilisation de l'ensemble de leurs ressources ;
- Le maintien d'une équipe d'audit professionnelle, avec des compétences, des connaissances et expérience suffisamment, du partage des meilleures pratiques d'audit et des ressources.

Les missions d'audit seront exécutées conformément au plan d'audit ; l'audit interne réalisera ses activités en respectant les standards de la profession. Il aura accès illimité á l'ensemble des informations de l'organisation sur toutes leurs formes, sous réserves des interdictions légales ou réglementaires, aux documents, informations et données qui ont un lien avec l'objet de leur mission.

Les auditeurs respectent le devoir de réserve á l'égard des informations confidentielles ainsi obtenues.

Le directeur de l'audit interne est autorisé à:

- Avoir un accès direct aux différentes structures de L'ENPI (les différentes structures de la direction générale, filiales, direction régionales et les directions de projets) ;
- Mobiliser les ressources, déterminer les périmètres des travaux, appliquer les techniques requises pour atteindre les objectifs d'audit.

En revanche, le directeur de l'audit interne et son équipe ne sont pas autorisés á

- Accomplir des tâches opérationnelles pour l'organisation de L'ENPI ;
- De diriger les travaux d'employés n'appartenant pas à la direction de l'audit ;
- Utilisations des données collectées durant les missions d'audit, la communication des conclusions a des employés non habilités à recevoir ce type d'informations.

Section 2 : Description et diagnostic critique de la contribution de l'audit interne à la sécurité du système d'information au sein de L'ENPI de Tizi-Ouzou

Dans cette section, nous décrirons le système de gestion de la sécurité de l'information au sein de l'ENPI direction de projets de Tizi -Ouzou, selon les six éléments clés de la norme ISO 27002 définis par ISACA. Ensuite nous procèderons à l'analyse et à l'interprétation de ces résultats et également à la présentation et à l'analyse des risques de sécurité dus aux insuffisances qui seront relevées

Les objectifs de l'ENPI en matière de sécurité de l'information sont : fiabilité, disponibilité et sécurité.

1 Description du système de gestion de la sécurité de l'information

Il est important avant toute évaluation de prendre connaissance de ce qu'il faut évaluer. Ceci nous permettra d'effectuer au mieux notre analyse et d'apprécier les risques inhérents à la sécurité de l'information et donc à l'activité. Cette description déroule les six étapes clés de la sécurité de l'information telles qu'elles sont comprises et effectuées par l'ENPI de Tizi-Ouzou.

1.1 Engagement et soutien de la haute direction

La haute direction de l'entreprise établie la stratégie concernant la sécurité de l'information et les grandes lignes pour son maintien et son respect. Les directions des filiales se chargent de décliner ces directives dans les procédures et processus de la filiale.

La haute direction s'implique dans la gestion de sécurité d'information et ceci se traduit par l'établissement d'une politique de sécurité et par la mise en place d'un groupe fonctionnel. Il définit les politiques et procédures applicables en matière de sécurité de l'information au niveau de l'entreprise, toujours sous l'approbation de haute direction. Le respect de ces procédures permet de garantir la fiabilité, l'exactitude et la sécurité de l'information. Ainsi parmi ces procédures, il y'a des procédures d'achat, de commercialisation des biens immobiliers et aussi la mise en place des procédures de contrôle qui veille sur le respect de circuit d'information mise en place.

Pour assure une gestion sécurisée de l'information, la direction de l'ENPI a défini à tous les niveaux les responsabilités. Elle a mis en place une traçabilité (qui a faite quoi ? Qui a ramené cette information ? Etc).

Par définition l'ENPI transmet le pouvoir de surveillance à l'audit interne parcequ'elle détient le pouvoir et les procédures.

1.2 Politique et procédures

Il existe au sein de l'ENPI de Tizi-Ouzou, une politique de sécurité ainsi que des procédures bien formalisées. La politique de sécurité est approuvée par la Direction générale qui est par ailleurs garante de son exécution. En pratique, la spécificité de ces directives l'oblige à déléguer son pouvoir aux directions des métiers telles quela Direction de l'Audit Interne.

Le groupe fonctionnel a défini des politiques qui régissent la sécurité de l'information concernant les points suivants: sécurité internet, contrôle d'accès, gestion d'actifs, communication, conformité, ressources humaines, gestion des incidents de manipulation, sécurité des échanges d'information, développement du système, l'organisation de l'information, l'environnement physique. Les processus et manuels de procédures découlent de ces politiques pour permettre à l'ENPI de fonctionner correctement. Des notes de service et des instructions sont établies et diffusées.

La mise à jour des procédures tient compte de l'évaluation annuelle des risques en chaque début d'année. La cartographie des risques comprend tous les risques y compris ceux relatifs aux technologies de l'information.

1.3 Organisation

Le garant de la sécurité de l'information est chargé du suivi de l'exécution des grandes lignes de sécurité définie par l'ENPI. Celui-ci émet aussi les objectifs de contrôle à atteindre en matière de sécurité de l'information. Cet organe a une forte implication et assure la promotion de la sécurité de l'information par la sensibilisation et la formation du personnel et aussi par l'acquisition de moyens de contrôle. Ces objectifs sont clairs et mesurables permettent de réduire le nombre de perte des données mensuelles ou annuelles, l'efficacité de l'information, la fiabilité, gain de temps et d'argent, la transmission de la bonne information aux destinataires…

Aussi l'audit interne est impliqué dans le bon fonctionnement du système de sécurité de l'information, elle s'assure de l'application des procédures établies pour le bon fonctionnement du SMSI. La mise en application de la politique de sécurité de l'information est auditée de façon indépendante dans le cadre des programmes d'audit établis régulièrement par la direction d'audit ; la sécurité du SI est passée en revue et auditée à l'effet d'évaluer ses points forts et ses faiblesses et par conséquent préconise des solutions aux problèmes ou faire des recommandations pour l'amélioration de la sécurité de SI.

Pour la gestion de la sécurité de l'information vis-à-vis de l'extérieur, l'ENPI met en place des moyens, des logiciels de protection, des codes comme désactiver les ports USB, des anti-virus internet pour éviter les attaques externes, etc.

1.4 Sensibilisation à la sécurité et éducation

Avant tout embauche ou stage, l'ENPI fait signer des contrats de travail comportant des clauses de confidentialité (si nécessaire). Ainsi tout travailleur doit tenir confidentiel toutes les informations se rapportant à l'entreprise, et à aucun cas ne doit divulguer les secrets professionnels. Ensuite, les différentes structures de l'ENPI sont sensibilisées sur l'importance de la sécurité de l'information, et assurer par l'organisation des réunions de sensibilisation périodique sur l'importance de la sécurisation et de la protection de l'information qui relève du domaine de tout un chacun. Ainsi, par la mise en évidence, le cas pratique pour initier les concernés aux exigences de la mission. Aussi, par des affiches, notes, instructions, réunions de coordination, petits séminaires, cycles de formation, etc. Même si ces formations ne sont pas régulièrement organisées (soit deux fois par an), à travers ces

dernières, le personnel prend connaissance des dispositifs de sécurité de l'information et des procédures et politiques.

Il faudrait noter que le personnel de l'ENPI de Tizi-Ouzou met en œuvre les différentes instructions concernant la sécurité de l'information malgré quelques petites erreurs que nous avons souvent eu à constater. Ces erreurs sont dues quelquefois à de mauvaises manipulations ou traitements des données et ont souvent eu des répercussions sur les missions d'évaluation.

Le personnel de l'ENPI participe également au maintien de la sécurité de l'information en signalant par une adresse de messagerie définie, tout cas qui pourrait laisser penser à des tentatives de violation du système de sécurité ou des tentatives non autorisées d'accès à l'information. Il participe, de plus, à la sécurité en se soumettant aux formations thématiques qui sont obligatoires et pilotées par la Direction des Ressources Humaines. Les cas de violation grave de la politique ou des procédures de sécurité de l'information sont traités comme des fautes professionnelles.

1.5 Contrôle et conformité

Pour ce qui est de la sécurité de réseaux et des outils informatiques, des mesures sont prises pour que les accès soient dûment authentifiés et que les medias amovibles fassent l'objet d'un contrôle particulier. Tous les ordinateurs connectés au système de l'ENPI sont contrôlables sous la responsabilité du Directeur de l'informatique qui assure son entretien et met en place les moyens nécessaires pour sa sécurisation et son bon fonctionnement, d'où il y a un suivi permanent de chaque action.

Il existe aussi à l'ENPI, des tests de restauration des données et des tests de cryptographie pour protéger et contrôler les informations. Ces informations pour être convenablement classées et conservées, sont dupliquées sur un site secondaire distant qui peut prendre le relais dès que le site primaire est non opérationnel.

Pour s'assurer de leur conformité avec la politique et les normes de sécurité, chaque entité de l'entreprise est sujette à des revues régulières par l'audit interne. Les directions, elles-mêmes, engagent des actions pour garantir que toutes les procédures de sécurité, dans le périmètre de leur responsabilité, sont correctement suivies.

1.6 Gestion et intervention face à l'incident

Il n'existe pas de procédures et des outils pour signaler les dysfonctionnements des programmes proprement dit. Le personnel est constamment sensibilisé sur les incidents et leur gestion. Ainsi, les incidents de sécurité sont signalés, en temps réel et dès leur survenance, au responsable hiérarchique qui évalue l'importance de l'incident, dans le même ordre, il procède á la transcription et description du disfonctionnement signalé à l'effet de le porter aux responsable informatique. Toujours est-il que lorsqu'un incident survient, qu'il soit majeur ou mineur, les plans d'intervention et de relance des activités se mettent en marche pour éviter un temps de latence trop long. Notons que ces plans sont régulièrement mis à jour. Les interventions pour la gestion des incidents dépendent de la nature de l'incident (les prestataires pour la gestion du serveur, la compagnie d'électricité pour les pannes de courant, e-Process pour la base de données).

Ainsi, voici décrit le cadre de gestion de la sécurité de l'information au sein de l'ENPI de Tizi-Ouzou. La prochaine étape sera de décrire la fonction de l'audit interne et son implication au maintien de la sécurité de l'information avant toute confrontation à la théorie.

2 Description de la fonction de l'audit interne et du dispositif de contrôle interne

Nous allons d'abord décrire la fonction d'audit et par la suite, nous prendrons connaissance du dispositif de contrôle interne mis en place par l'ENPI de Tizi-Ouzou pour la gestion de la sécurité informationnelle.

2.1 La fonction d'audit interne

Pour ce qui est de la pratique de l'audit interne concernant la sécurité de l'information, nous notons que les auditeurs internes ont une connaissance générale mais non suffisante de la norme ISO 27002 (selon les réponses au questionnaire de contrôle destiné à la direction de l'audit interne).

Concernant les missions d'audit interne à cet effet, il y a une seule mission d'audit interne sur la sécurité de l'information qui a eu lieu en 2014. La méthodologie adoptée pour la mission de 2014 a été de deux ordres:

- **L'audit organisationnel :** il s'intéresse aux aspects de gestion et d'organisation de la sécurité. Cette étape est donc d'avoir une vue globale de l'état de sécurité du système d'information et d'identifier les risques potentiels sur le plan organisationnel.

- **L'audit technique et physique :** il s'agit ici d'évaluer les mesures de sécurité physique des systèmes et réseaux et celles relative à la sécurité logique des données et ressources.

Les vérifications effectuées lors de la mission d'audit de sécurité de l'information étaient:

- L'organisation de la structure auditée;
- La mise en place et le bon fonctionnement des outils de sécurité adéquats;
- La formation des agents à l'utilisation et à l'entretien de ces outils;
- Le fonctionnement de la stratégie déployée sur les outils des agents;
- Les sauvegardes de données et test de restauration;
- Le test et la mise à jour du plan de continuité.

L'audit interne est chargé de l'évaluation du dispositif de contrôle internemis en place à tous les niveaux du traitement de l'information. Comme outils utilisés pour réaliser la mission, nous avons la revue documentaire, l'interview, les inspections physiques et la revue des logs[63].

Il faut aussi noter le soutien et l'accompagnement que la Direction Générale apporte à la direction de l'audit interne. Cela se démontre par les actions qu'elle engage pour assurer le suivi des procédures de sécurité et les recommandations d'audit. L'auditeur est également invité à donner ses recommandations, pour pallier aux défauts qu'il aura constatés. Il faut noter que les recommandations d'audit et les procédures de sécurité ne sont pas toujours suivies par les agents, mais ceci n'empêche pas l'audit interne de jouer pleinement son rôle au sein de l'ENPI.

2.2 Le dispositif de contrôle interne en matière de sécurité de l'information

Le SMSI[64] est encadré d'un dispositif de contrôle soumis à tout le personnel de l'ENPI et géré par la Direction du Contrôle interne. C'est cette Direction qui est chargé de veiller au jour le jour à l'applicationet au respect des mesures sécuritaires établies pour protéger et sauvegarder les informations. Les vérifications effectuées par la direction du contrôle interne couvrent trois principaux types de risques :

- Le risqué opérationnel ;

[63] Les logs sont des fichierscontenant des enregistrements d'évènements généralement datés et classés par ordre chronologique et générés par des déclencheurs ; ces derniers permettent d'analyser pas à pas l'activité interne du processus et ses interactions avec son environnement.
[64]L'expression *Système de Management de la Sécurité de l'Information* (SMSI) est désormais utilisée en français. Cette expression désigne un ensemble de politiques concernant la gestion de la sécurité de l'information.

- Le risque de crédit ;
- Le risque du marché.

Le dispositif de contrôle interne au sein de l'ENPI se compose de moyens pour la sécurité, l'ENPI dispose de pare-feu, d'antivirus, d'un système de codification des données, notamment pour les bons de versement, les décisions de vente.

La Direction du Contrôle Interne effectue un contrôle de toutes les opérations de l'entreprise pour réajuster les écarts et faire respecter les différentes procédures. Il s'assure que les tâches soient effectivement et convenablement exécutées et que les moyens physiques et techniques mis à disposition soient fonctionnels. L'audit interne se charge de faire un contrôle périodique pour attester du maintien de la sécurité de l'information et de l'efficacité du dispositif de contrôle interne.

Des formations obligatoires sont engagées pour le personnel et des conseils de sécurité sont transmis par courriel régulièrement. C'est également un moyen utilisé par l'ENPI de Tizi-Ouzou pour minimiser les risques inhérents à la sécurité de l'information.

Notre prochaine étape est l'essence même de notre étude à savoir le diagnostic critique de la gestion de la sécurité de l'information menée par l'ENPI de Tizi-Ouzou. Ce diagnostic nous permettra de confronter la théorie avec la pratique et déceler les manquements auxquelles il faudrait remédier.

3 Diagnostic critique de la gestion de la sécurité de l'information

L'analyse critique se fera suivant trois étapes, d'abord l'évaluation de la gestion de la sécurité de l'information, ensuite l'évaluation des activités et de la technologie relative à la sécurité de l'information et enfin la pratique de l'audit interne en matière de sécurité de l'information. L'analyse critique nous permet de comparer la pratique avec la théorie en vue de déceler les insuffisances et trouver des solutions adéquates pour le bon fonctionnement de l'ENPI de Tizi-Ouzou.

3.1 Evaluation de la gestion de la sécurité de l'information

Pour évaluer la gestion de la sécurité de l'information, nous procéderons par un examen plus ou moins détaillé de chaque point d'anomalie décelée dans la description du SMSI existant.

- **Absence d'un comité de pilotage de la sécurité de l'information**

La première remarque qui ressort de notre évaluation, c'est l'absence d'un comité de pilotage de la sécurité de l'information au niveau des filiales. Cette absence crée un problème dans le processus de gouvernance de la sécurité de l'information. Il est vrai qu'il existe un groupe fonctionnel au sein de la Direction Centrale qui se charge d'établir des politiques de sécurité et les pratiques et que des rapports sont transmis par les filiales pour un suivi. Cependant, les risques en l'absence d'un comité de pilotage de la sécurité de l'information au sein des filiales sont de plusieurs ordres. Premièrement, les objectifs fixés par la Direction Générale pour la gestion et le maintien de la sécurité ne sont pas correctement atteints au niveau de tous les corps métiers. On assiste par ricochet à une confusion au niveau des tâches à accomplir et des responsabilités. Ensuite les procédures ne sont pas correctement appliquées parce qu'elles ne sont pas comprises ou entièrement adaptées aux besoins du personnel.

Les risques qui en découlent sont la mauvaise gestion du système, la mauvaise gestion des actifs, le manque de coordination dans les tâches, un manque d'organisation, etc. L'absence du comité de pilotage peut entrainer une méconnaissance des réels risques inhérents aux corps métiers. L'ENPI ne pourra pas uniquement compter sur son Risk Manager ou son Responsable de sécurité de l'information ; il est, donc, d'une importance capitale pour la filiale d'avoir en son sein un comité de pilotage de la sécurité de l'information afin de mieux prendre en compte toutes les difficultés à l'ensemble de l'organisation.

- **Inexistence d'une politique d'appétence pour le risque de sécurité de l'information**

Nous constatons néanmoins l'absence d'une politique d'acceptation du risque de gestion. Les risques liés à la sécurité de l'information sont nombreux selon l'ampleur de l'activité de l'ENPI.

Les risques en matière de sécurité de l'information représentent une menace considérable pour les entreprises du fait des possibles pertes et préjudices financiers, perte de services essentiels de réseaux, ou encore perte de confiance des clients et autres atteintes à la réputation qu'ils entraînent. La gestion des risques est l'un des éléments clés de la prévention des fraudes en ligne, et autres incidents divers concernant la sécurité de l'information. L'absence de politique de l'acceptation du risque entraine donc des écarts dans les différentes

actions à mener étant entendu que les employés n'ont pas réellement connaissance de ce que l'ENPI attend d'eux en matière de gestion des risques de sécurité.

L'analyse de la gestion de la sécurité de l'information nous a permis de faire ressortir des insuffisances au niveau de l'organisation et de la gestion du risque de sécurité.

Notre prochaine étape concerne les activités et technologies de la sécurité de l'information car on ne peut évaluer la gestion organisationnelle de la sécurité de l'information sans évaluer les activités et technologies relatives à la sécurité de l'information.

3.2 Evaluation des activités et de la gestion des technologies relatives à la sécurité de l'information

Nous énoncerons point par point les différentes défaillances décelées dans la description du SMSI existant.

- **Gestion de la sauvegarde des données sur les ordinateurs et appareils mobiles**

Dans notre description du SMSI de l'ENPI de Tizi-Ouzou, nous avons pu noter que les plans de sauvegarde sont assez performants. Les serveurs conservent les informations des différents systèmes de l'ENPI et se relaient en cas de panne de l'un d'eux. Ainsi, les informations concernant les clients (particuliers ou entreprises) contenues dans les logiciels d'enregistrement et de gestion des bases de données sont sauvegardées. Ceci répond au plan de continuité des activités de la l'ENPI pour éviter toute rupture d'informations.

Néanmoins nous pouvons remarquer qu'aucune mesure n'a été prise pour la conservation des données sur les ordinateurs de bureau ou portables et autres appareils mobiles (tablette numérique, téléphone portable, clé USB,Etc.). Les antivirus ont uniquement pour rôle la protection des données mais pas leur conservation.

- **Périodicité des formations trop longue**

Nous savons que le maillon le plus faible au sein d'une entreprise est l'homme. Ainsi, il est important de notifier que l'ENPI de Tizi-Ouzou, dans le souci d'atteindre effectivement ses objectifs, met en place des formations et des tests en lignes obligatoires pour son personnel. Plus de 80% des employés ont déjà complétés leur formation et cela réduit considérablement le taux d'erreurs et permet aux employés de mieux comprendre l'ampleur de leur tâche et les éléments de sécurité qui s'y rattachent.

Si l'aspect humain n'est pas pris en compte, ceci peut entrainer des pertes financières, des pertes d'informations importantes et sensibles.

Ce que nous remarquons par contre au niveau des formations, c'est la périodicité ou la fréquence de celles-ci. En effet, les agents peuvent recevoir seulement une ou deux formations dans l'année. Ce qui est très peu vu l'évolution technologique rapide et l'environnement de mondialisation dans lequel évolue l'ENPI. Il y a par conséquent de nouveaux risques qui surviennent dont le personnel doit prendre connaissance et quels sont les mesures et moyens de sécurité à adopter pour réduire le risque

- **Méthodologie de classification des informations non optimale**

Nous avons remarqué que les informations sont classées seulement par catégorie et non par ordre de priorité particulier. Les informations physiques telles que les dossiers d'ouverture de compte, les dossiers de crédit et autres sont stockés à différents endroits selon la classification personnelle des gestionnaires de ces actifs. Les informations numériques personnelles quant à elles sont stockées sur les ordinateurs de bureaux, les ordinateurs portables et autres appareils mobiles sans balises de sécurité et méthodes de classification particulières.

Nous savons que la protection de l'information commence par la classification de celle-ci selon son degré de sensibilité et son niveau de partage. Une mauvaise classification peut occasionner une mauvaise prise de décisions de la part du management. Il sera difficile pour ce dernier d'apprécier quelles informations sont les plus importantes à prendre en compte. Ce fait peut aussi entrainer l'ENPI vers des horizons risqués qu'elle n'avait pas forcément prévu. La norme ISO 27002 exige que les informations soient classées par ordre de priorité afin de mieux orienter les outils de sécurité pour les données sensibles. Les informations doivent être classées du plus important au moins important et du plus sensible au moins sensible

- **Inefficience de la gestion de la sécurité de l'information**

De l'évaluation des opérations ou activités de sécurité de l'information, nous pouvons noter l'existence d'un service responsable de la sécurité de l'information avec à sa tête un responsable Security, encore appelé Responsable de la sécurité de l'information.

Le responsable Security est un staff sous la direction informatique ; ce qui n'est pas de nature à faciliter ses tâches. Il pose donc le problème d'indépendance de la fonction par rapport au système à évaluer, de temps de réponse aux préoccupations particulières de la filiale et de gestion efficace de la sécurité de l'information. Le responsable Security ne sera pas en mesure de couvrir correctement toutes les zones de sécurité sans l'aide permanente d'un comité de pilotage de la sécurité du système d'information. De plus, chacune des filiales évolue dans un pays différent et donc dans un environnement de travail différent. Par ricochet, les besoins de sécurité et les risques sont également différents.

Le système d'information automatisé se compose d'humains, de matériel informatique et de données diverses. Il est important d'avoir une bonne organisation, impliquer le personnel, appréhender son SI de manière globale. Mais il est aussi nécessaire d'avoir un système informatique sécurisé, car il y a toujours des portes d'entrée qui doivent être protégées.

4 Analyse de l'implication de l'audit interne à la sécurité de l'information

Dans cette analyse, nous énoncerons de façon détaillée chaque point qui nous semble être une faiblesse dans l'implication de l'audit interne à la sécurité de l'information.

4.1 Les missions d'évaluation de la sécurité de l'information

Comme nous l'avons dit plus haut, chaque filiale évolue dans un environnement de travail différent. De 2014 à cette année-ci, l'ENPI de Tizi-Ouzou a connu beaucoup d'évènements tels que l'acquisition de nouveaux biens, le changement du système de gestion informatisé des données, l'accroissement de la clientèle, la signature de nouveaux contrats avec des partenaires extérieurs etc. Cette situation a occasionné de nouveaux risques qui devraient faire l'objet de nouveaux audits. Fort heureusement, l'audit interne couvre périodique lors de ses missions les aspects qui touchent la sécurité de l'information. Néanmoins des revues dédiées à la sécurité de l'information devraient être instituées afin de couvrir le maximum des risques qui y sont inhérents.

4.2 La méthodologie d'audit du SMSI

Concernant la méthodologie d'audit du SMSI, les auditeurs internes ont opté pour une analyse en deux étapes: audit organisationnel et l'audit technique et physique. L'audit organisationnel pour vérifier l'organisation de la structure à auditer, la formation du personnel

et le fonctionnement de la stratégie déployée sur les outils ; ensuite l'audit technique et physique pour s'assurer de la mise en place et le bon fonctionnement des outils de sécurité, de la sauvegarde des données et de la mise à jour du plan de continuité. Nous notons que la méthodologie utilisée en elle-même est une méthode établie par l'IFACI. Mais ce qui nous importe ici c'est le contenu de la méthode pour évaluer la gestion de la sécurité de l'information.

Le constat que nous avons fait concernant la centralisation des systèmes sensibles de l'ENPI de Tizi-Ouzou, une grande partie des risques de sécurité ne sont plus du ressort de la filiale. C'est aussi la raison pour laquelle les missions d'évaluation de la sécurité de l'information sont partielles et sommaires. Elles ne sont effectuées que pour s'assurer de l'application des recommandations par les utilisateurs finaux. L'insuffisance de cette méthode est que l'audit ne se fait que pour un souci de respect de la conformité aux politiques et procédures et non pour une analyse spécifique des systèmes de pilotage ou de gouvernance de la sécurité de l'information en interne (c'est-à-dire, au sein de la filiale elle-même).

Les actions bien que conformes aux règles, peuvent ne pas répondre convenablement au besoin de sécurité de l'information et au besoin d'affaires de l'ENPI. L'IFACI explique que l'audit interne ne doit pas restreindre ses tâches aux procédures ou aux activités de contrôle, mais également prendre en compte l'organisation, le pilotage et la surveillance du processus qui se fondent sur une approche par les risques et une diffusion fiable de l'information**.**

Les normes ISO 27000 permettent d'établir un cadre adéquat pour la gestion des systèmes d'information de l'entreprise et aussi d'implémenter un SMSI qui répond aux besoins et d'obtenir des moyens de l'évaluer. Si nous partons du fait que les filiales dépendent de la maison mère, il faut aussi savoir que les environnements de travail et de contrôle sont différents. Ainsi, la direction de l'audit interne doit donner l'assurance que le SMSI correspond à son environnement de travail**.**

4.3 Les compétences et outils de travail

Concernant la compétence des auditeurs, à travers le questionnaire d'audit interne sur la sécurité de l'information, nous avons noté en moyenne, une méconnaissance des exigences de la norme ISO 27002 pour les systèmes d'information de l'ENPI. Il est vrai que le référentiel de l'audit interne, selon l'IIA, n'oblige pas les auditeurs à posséder l'expertise d'un auditeur informatique. Néanmoins, nous avons remarqué que, comme auditeurs internes, la sécurité de l'information ne fait pas souvent partie de leur programme annuel de mission.

Un autre point est le faible nombre des auditeurs n'offre pas à la Direction de l'audit interne et donc à l'ENPI de Tizi-Ouzou une pluralité de spécialités. Cette situation favorise que certaines agences ne soient évaluées que chaque deux ou trois ans. Ce qui occasionne l'accumulation de risques divers et des pertes financières.

A propos des outils de travail, nous constatons que la Direction de l'audit interne ne dispose pas de logiciels d'audit spécialisés utiles pour les tests d'intrusion ou les tests d'appréciation de la vulnérabilité du système de l'ENPI. Ce manque ne permet pas à l'auditeur interne d'inspecter et d'évaluer en intégralité les systèmes informatiques et les risques présents et ceux qui pourraient survenir.

Nous savons à travers la théorie que l'audit de la sécurité de l'information est rendu obligatoire. De plus, l'IFACI précise que le processus de contrôle de l'audit interne doit viser l'ensemble du dispositif de contrôle interne. En matière de système d'information, l'IFACI explique que les auditeurs doivent effectuer des contrôles des technologies de l'information. Ces contrôles viennent en appui de la gestion et de la gouvernance de l'organisation et comportent des contrôles généraux et des contrôles techniques sur les infrastructures des technologies de l'information dans lesquelles on retrouve les applications, les informations, les installations et les personnes. Pour cela ils doivent posséder une connaissance suffisante des principaux risques et contrôles relatifs aux technologies de l'information, et des techniques d'audit informatisées susceptibles d'être mises en œuvre dans le cadre des travaux qui leur sont confiés.

Un SI est dit fiable s'il procure des informations pertinentes et en temps réel à l'entreprise. Par ailleurs les flux d'information qui en découlent, doivent faire l'objet d'un excellent cadre de sécurité de l'information. La prochaine étape sera pour nous l'occasion d'apporter des suggestions aux difficultés qui ressortent de notre évaluation

Section3 : Recommandations au service d'audit interne à la contribution de la sécurité de l'information

Le but du processus d'audit interne est d'apporter des suggestions d'amélioration, créant ainsi de la valeur ajoutée pour l'entreprise qui en bénéficie. Notre étude portant sur la contribution de l'audit interne à la sécurité de l'information, a révélé que le rôle de l'audit interne dans la sécurité de l'information n'était pas totalement compris et mis en exergue. Notons que l'avenir de l'entreprise dans un environnement automatisé dépend de la force de son système de gestion de la sécurité de l'information. Nous allons premièrement rappeler le

diagnostic critique effectué et ensuite nous apporterons des recommandations qui pourront être des lignes directrices pour les prochaines missions d'audit de la sécurité de l'information.

1 Constats du diagnostic de gestion de la sécurité de l'information

L'évaluation de la gestion de la sécurité de l'information et du rôle de l'audit interne pour son maintien et son amélioration a révélé différentes insuffisantes.

Premièrement, l'ENPI de Tizi-Ouzou, bien qu'ayant en son sein un responsable de la sécurité de l'information, ne possède pas de comité de pilotage de la sécurité de l'information. De par cette absence, il s'est posé le problème de gouvernance et donc d'organisation de la sécurité de l'information au sein de la filiale. Les procédures étant très récentes, il n'est donc pas évident que les objectifs de sécurité définies par la maison mère soient réellement compris et atteints par les opérationnels de l'ENPI de Tizi-Ouzou.

Nous avons aussi pu déceler les problèmes dus à la sauvegarde sur les stations de travail et divers appareils mobiles. En cas de perte d'un appareil ou de sinistre, les informations contenues dans ces machines seront définitivement perdues ou utilisées à d'autres fins. Nous avons également fait ressortir l'approche réactive du comite de gestion des incidents (encore appelé comité d'urgence) qui fait abstraction de la prévention et qui peut entrainer un retard dans les réponses face aux incidents. Deux autres défaillances ont pu ressortir de notre analyse à savoir la fréquence de formations des agents et l'absence de méthodologie pour la classification des informations.

Ensuite nous avons apprécié l'implication de l'audit interne à la sécurité de l'information. Il en est ressorti que le nombre des missions pour l'évaluation de la sécurité de l'information reste insuffisant.

A travers le tableau récapitulatif, nous allons, avec les différentes étapes d'audit de la sécurité qui nous ont permis d'effectuer notre diagnostic, apprécier les risques dus aux insuffisances relevées. Chaque constat sera noté d'une mention (élevée, moyen, faible) afin de montrer son criticité au sein de l'ENPI. Le tableau récapitulatif se présente comme suit :

TABLEAU : Tableau récapitulatif des insuffisances relevées et leurs risques respectifs

ETAPES D'AUDIT	CONSTATS	RISQUES
Gestion de la sécurité de l'information	Absence d'un comité de pilotage	-inexistence d'une organisation claire de sécurité de l'information.
	Politiques et procédures très récentes	-adaptation lente ; - difficultés à gérer le changement et à impacter la culture de l'entreprise.
	Méconnaissance de la politique de risques par les opérationnels	-réalisation de tâches incompatibles ; - fraudes ; - mauvaise manipulation de données à répétition ; -incompréhension dans l'accomplissement des tâches ; - tolérance d'incidents qui peuvent s'avérer de haute importance pour l'ENPI ; - disparité des pratiques en matière de risques.
Evaluation des opérations de sécurité	Inefficience dans la gestion de la sécurité de l'information	-insuffisance dans la transmission des objectifs de la maison mère en matière de sécurité de l'information ; - évaluation erronée ou insuffisante des risques de sécurité - mauvaise attribution des responsabilités ; - méconnaissance des risques inhérents à la sécurité de l'information.
	Approche réactive du comité de gestion des incidents	- insuffisance dans la planification des réponses aux incidents ; - réponses médiates aux incidents ; - pertes financières.
	Périodicité des formations trop longue	- méconnaissance des risques actuels liés à la sécurité de l'information ; - méconnaissance des nouvelles technologies de l'information - pertes financières.
	Inexistence d'une méthodologie formelle de classification des informations	- retard dans les prises de décision ; -prises de décision erronée ; -pertes d'informations ; -transfert d'informations confidentielles ou sensibles aux personnes non autorisées ; -mauvaise utilisation des informations.
Evaluation des technologies de sécurité	Gestion de la sauvegarde des données sur les stations de travail et appareils mobiles	- pertes d'informations ; - fraudes ; - utilisation des informations à mauvais escient ; - atteinte à la réputation de l'ENPI.

Source : l'ENPI

2 Recommandations pour l'amélioration de la sécurité de l'information et l'audit interne au sein de l'ENPI de Tizi-Ouzou.

Nos recommandations se feront sur toutes les anomalies prises ensemble, que nous avons pu faire ressortir au cours de notre analyse à savoir : celles sur la gestion de la sécurité de l'information et celles relatives aux activités et technologies de la sécurité de l'information.

2.1 Création d'un comité de pilotage de la sécurité de l'information

La première recommandation que nous ferons, c'est la mise en place d'un cadre de gouvernance de la sécurité de l'information au sein de la filiale. Cela signifie établir un comité de pilotage de la sécurité de l'information dans lequel chaque métier clé de l'ENPI sera représenté par son directeur ou un représentant ayant une haute fonction hiérarchique au sein du corps métier. Ce comité aura pour mission première de représenter la maison mère quant aux objectifs de sécurité qu'elle s'est fixée. Le comité devra examiner la stratégie de sécurité et sa mise en place ou son adaptation au sein de la filiale et par rapport à son environnement de travail. Il devra aussi veiller à ce que chaque membre de l'entreprise soutienne l'intégration de ce cadre de sécurité de l'information. Le comité de pilotage aide à réaliser un consensus sur les priorités et les compromis. Il sert également de canal de communication efficace et fournit une base continue pour garantir l'alignement du programme de sécurité sur les objectifs opérationnels.

Une bonne gouvernance de la sécurité permet d'obtenir les résultats suivants :

- Un alignement de la sécurité de l'information sur la stratégie commerciale pour appuyer les objectifs de l'ENPI ;
- Une gestion des risques et une exécution de mesures appropriées pour diminuer les risques et réduire à un niveau acceptable les impacts possibles sur les ressources d'informations ;
- L'apport de valeur en optimisant les investissements dans la sécurité pour appuyer les objectifs opérationnels ;
- La mesure de la performance pour garantir le respect des objectifs ;
- La gestion des ressources utilisées avec efficacité et efficience ;
- L'intégration des processus pour garantir leur bon fonctionnement.

La mise en place d'un tel comité donne à l'ENPI de s'assurer de la participation et de l'implication de tous les intervenants touchés par les considérations de sécurité. Chaque directeur sera donc responsable et garant du processus de sécurité dans sa direction.

2.2 Gestion efficace de la sécurité de l'information

Le responsable Security de l'ENPI de Tizi-Ouzou ne pourra pas travailler tout seul sur les méthodes et mesures de gestion de la sécurité de l'information commandées par la maison mère pour les adapter au sein de l'ENPI. C'est aussi la raison pour laquelle il est important d'avoir un comité de pilotage de la sécurité de l'information. Le responsable Sécurité pourra s'appuyer sur ce comité pour être mis au courant des risques éventuels actuels liés à la sécurité de l'information pour chaque métier. Il sera également en mesure d'adapter correctement les politiques et procédures de sécurité à chaque direction concernée afin que chacun prenne part à l'implémentation et l'amélioration du SMSI de l'ENPI.

Ce que nous recommandons en plus, c'est une position hiérarchique élevée pour permettre au responsable Sécurité d'être plus proche des autres directeurs mais aussi de la direction générale. Cela concoure à renforcer la collaboration et permet une gestion efficace et efficiente de la sécurité de l'information.

2.3 Communication / formation régulière du personnel

Il est important de communiquer ses politiques et procédures afin de mettre au courant le personnel sur la conduite à tenir pour maintenir l'image de l'ENPI. Les politiques notamment celle du risque devront leur être communiquées par divers moyens afin que les opérationnels sachent l'importance de leurs actions et la finalité sur le système et les objectifs de l'entreprise.

Ne dit-on pas que le maillon faible de l'entreprise c'est l'homme. Ainsi plus le personnel prend conscience des objectifs de sécurité de l'entreprise, moins le taux d'erreurs est élevé. Par cette considération, l'ENPI rencontrera la motivation et l'implication des agents dans l'amélioration continue du SMSI.

Aussi, concernant la périodicité des formations trop longue, nous recommandons des formations régulières (au moins cinq(5) à six(6) fois dans l'année) pour les agents de l'ENPI de Tizi-Ouzou, soit en atelier, sous forme de conférence ou en ligne. Les formations permettent au personnel d'avoir une mise à jour sur les dernières technologies de

l'information, les risques liés à leurs activités, la gestion de la sécurité à tous les niveaux. Ces formations doivent être pratiques suivis de test d'aptitudes obligatoires. Des ateliers pourront être organisés dans les différentes directions pour faire participer le personnel à l'actualisation des procédures, à la bonne gouvernance des technologies de l'information et l'apport de solutions favorables au maintien et à l'amélioration de la gestion de la sécurité de l'information.

La direction du contrôle interne ou de l'audit interne pourra faire une enquête régulière d'évaluation des connaissances pour s'assurer que les agents ont bien assimilé les formations et en comprennent désormais les enjeux. Notons que, lorsque les employés sont actifs et participent à l'amélioration d'un système, ils se sentent plus impliqués et plus respectés au sein de la structure. Ainsi ils sont dévoués et s'attèlent à travailler dans l'intérêt de l'entreprise.

2.4 Mesures de sauvegarde des données sur les ordinateurs et appareils mobiles et gestion des privilèges

Nous savons que malgré tous les débats et les formations au sujet des pirates et des intrus, les violations de sécurité au sein de l'entreprise restent nombreuses. Les employés peu honorables et mécontents sont une menace constante. Aussi nous pouvons souligner que la négligence souvent est considérable, notamment chez les personnes fréquemment en déplacement qui transportent avec elles des ordinateurs portatifs et des disques amovibles. Les cadres dirigeants et les administrateurs qui bénéficient de droits d'accès pratiquement non contrôlés sont presque impossibles à arrêter. De même, le personnel de livraison, les employés temporaires et même les concierges sont trop souvent autorisés à circuler librement dans les services de l'entreprise.

Ainsi, s'il est impossible de garantir une protection totale, il existe tout de même quelques mesures que l'ENPI peut prendre pour réduire les risques. Premièrement, elle peut vérifier la distribution des systèmes et privilèges pour s'assurer que personne ne dispose d'un trop grand contrôle par le biais d'un service de sécurité de l'information. Ensuite, l'ENPI peut répertorier l'emplacement de stockage des sauvegardes, archives et copies des bases de données utilisées pour les tests et la résolution des logiciels. L'ENPI de Tizi-Ouzou peut aussi mettre en place un système de cryptage des enregistrements précis des personnes qui utilisent les appareils informatiques portatifs et veiller à ce que les employés sachent comment protéger leurs appareils et leurs données lorsqu'ils sont en déplacement.

Ce que nous recommandons également pour une meilleure gestion des privilèges, c'est que cette tache soit attribuée à une direction autre que la direction du contrôle interne. Cela permettra à cette dernière d'avoir un meilleur contrôle sur cette activité et de maintenir son objectivité. Selon que l'indique la norme ISO 27000, cette activité devrait revenir au responsable de la sécurité de l'information pour un meilleur suivi.

2.5 Classification des informations par valeur et niveau de sensibilité

Concernant la classification des données, la norme ISO 27002 explique que l'information devrait être classée et étiquetée selon un système généralement admis, assurant ainsi un niveau de protection approprié. Comme nous l'avons spécifiée dans le développement du troisième (3) thème de la norme ISO 27002, la classification des informations doit être accompagnée de procédures formelles et être exécutée en tenant compte des besoins liés à l'exploitation, de la sensibilité des informations, des restrictions éventuelles et du degré d'impact des évènements nuisibles à leur exploitation. De plus, les actifs technologiques liés à la sécurité de l'information, doivent avoir un propriétaire désigné qui se charge de leur gestion et de l'inventaire régulier.

Aucune méthode particulière de classification n'est définie étant donné la diversité des secteurs économiques et l'interprétation variante d'une information d'une entreprise à une autre. Cependant, notre recommandation, c'est que l'ENPI garde en mémoire que, quel que soit la méthode de classification adoptée, elle doit tenir compte du degré de sensibilité et de criticité et du niveau de partage de ses informations. Les informations doivent être classées et foncièrement protégées pour éviter que celles jugées sensibles et confidentielles soient diffusées en interne comme à l'extérieur aux personnes non autorisées accidentellement ou volontairement.

Pour protéger et classer une information, il faut la connaître et identifier son niveau de sensibilité et de criticité et sa valeur. Il faut pour cela :

- Lister les données et leur localisation dans les processus et activités ;
- Formaliser une échelle de classification et des règles d'utilisation (à travers une politique de classification et protection des informations) ;
- Qualifier la sensibilité des données au regard des impacts liés à un incident de sécurité ;

- Sensibiliser les utilisateurs à ces impacts et à la nécessité d'appliquer les règles de classification.

2.6 Intervention du comité de gestion des incidents de sécurité

La gestion des incidents est très importante dans le maintien de la sécurité de l'information et l'atténuation des impacts dus aux risques de sécurité survenus. Un incident aussi petit soit-il peut être préjudiciable pour l'ENPI. Il est donc de mise de recadrer le rôle du comite de gestion des incidents selon la norme ISO 27002 afin de prendre en compte tous les contours nécessaires à une gestion efficace des incidents de sécurité.

Ce que nous recommandons, c'est un comité de gestion des incidents en interne disponible et en activité qu'il y ait ou non un incident quelconque. Aucune des tâches de ce comité ne doit pas se faire sur une base réactive. Il serait intéressant qu'une planification anticipée des incidents soit faite.il est important qu'une classification claire des incidents de sécurité soit défini par ordre de priorité et d'importance et aussi des ébauches de réponses qui seront communiquées aux agents correspondants pour qu'ils sachent comment s'y prendre lorsque l'incident surviendra. Chacune des réponses devra être testée pour s'assurer qu'elle répond bien à l'objectif qui est de réparer ou de réduire l'impact de l'incident.

Toutes ces mesures et bonnes pratiques relevées dans les normes ISO 27000 permettent à l'ENPI de garantir une meilleure gestion de la sécurité de ses systèmes d'informations. Afin de donner l'assurance que les mesures de sécurité de l'information mises en place fonctionnent correctement, la Direction de l'audit interne doit avoir les compétences, les connaissances et les outils nécessaires pour les évaluations diverses. Notre prochaine étape nous donne l'occasion de faire des recommandations d'amélioration des prestations de l'audit interne en matière de sécurité de l'information.

3 Recommandations pour le perfectionnement de l'audit interne en matière de sécurité de l'information

L'audit interne, de par sa définition, aide l'entreprise à atteindre ses objectifs en évaluant ses processus de management des risques, de contrôle et de gouvernance. C'est un organe de contrôle, conseiller de la Haute Direction, qui aide au management et qui est créateur de valeur ajoutée. Il doit pour cela posséder les meilleures méthodes et outils de travail afin de mener à bien ses missions d'audit**.**

Pour la sécurité de l'information, les audits doivent se faire de façon régulière. Au moins une fois par an, les bonnes pratiques voudraient que l'audit interne évalue la gestion de la sécurité de l'information au niveau de l'ENPI toute entière de même que les opérations et les technologies de sécurité. Aussi une évaluation des risques de sécurité constante et régulière, en collaboration avec le RSI et le RM, est importante voire obligatoire pour mieux établir un plan d'audit pertinent.

Aucune agence ni entité de l'ENPI ne doit rester incontrôlée pendant plus d'un an au maximum. Nous recommandons pour cela l'augmentation du nombre des auditeurs internes et aussi l'augmentation des audits de sécurité de l'information. Il serait encore plus intéressant que la Direction de l'audit interne regorge de plusieurs spécialités. Pour cela une formation continue des auditeurs est recommandée de même qu'une auto-évaluation de leurs compétences et aptitudes. Les auditeurs qui ont plus de compétences en matière de sécurité de l'information pourraient formés ceux qui en ont moins (création d'un centre de partage et de réflexion) afin d'accroitre le potentiel de l'audit interne.

L'IFACI recommande aux auditeurs internes d'avoir des connaissances et des compétences suffisantes pour conduire à bien leurs missions d'audit. Nous suggérons donc pour l'évaluation de la sécurité de l'information que chaque auditeur interne ait une connaissance des normes ISO 27000 actualisées, du référentiel CobiT et autres bonnes pratiques en matière de sécurité des systèmes d'information. Avec ces connaissances, la Direction de l'audit interne sera à mesure de fournir des recommandations pertinentes pour l'amélioration de la gestion de la sécurité de l'information.

Concernant la méthodologie d'audit, nous recommandons que, les différentes étapes de l'audit interne passent par trois phases : phase de planification, phase de réalisation et phase de conclusion matérialisée par un rapport final d'audit. La phase de planification doit déjà prendre en compte: évaluation de la gestion de la sécurité de l'information et l'évaluation des opérations et des technologies de sécurité de l'information. L'évaluation générale de la sécurité de l'information pourra être effectuée au moins une fois par an pour ne pas perdre un seul aspect de sécurité qui pourrait s'avérer préjudiciable pour l'ENPI. De plus, il faudrait aux auditeurs internes des outils ou logiciels d'audit spécialisés pour effectuer les tests de contrôle conformément aux recommandations de l'IFACI quant à l'évaluation des technologies de l'information.

Cette méthode permet d'évaluer les différents aspects de sécurité de l'information, au moins une fois dans l'année permet de s'assurer que les objectifs de sécurité définis par la maison mèresont atteints avec efficience et efficacité.

L'assurance sera également donnée quant au bon fonctionnement du SMSI et de sa conformité avec les règlementations et exigences établies par l'ENPI.

L'auditeur interne doit constamment se former avec d'acquérir des connaissances nouvelles sur les TI, les systèmes d'information, la gestion des SMSI et autres sujets susceptibles de l'aider dans l'accomplissement de ses tâches périodiques et dans l'apport pour la création de valeur.

Conclusion du chapitre

L'exemple de l'ENPI de Tizi-Ouzou nous a permis de constater et d'apporter un jugement sur la pratique de la sécurité de l'information au sein même de l'ENPI. De notre diagnostic, nous avons remarqué quelques anomalies susceptibles de compromettre le SMSI de l'ENPI et donc l'intégrité, la confidentialité et la disponibilité des informations. De la théorie, ont découlé des bonnes pratiques qui nous ont permis de faire des recommandations afin que l'ENPI de Tizi-Ouzou évite ou réduise considérablement tous les risques inhérents de sécurité qui pourraient survenir.

Nous avons également apprécié le rôle de la Direction de l'audit interne dans la sécurité de l'information à travers la méthodologie et le contenu du travail effectué. Nous avons pu noter que l'audit interne jouer son rôle pour rassurer au mieux l'efficacité et l'efficience de la sécurité de l'information. Nous avons fait des recommandations qui, nous l'espérons, aideront la Direction de l'audit interne à redéfinir sa méthodologie d'audit de la sécurité et à être un véritable contributeur à la sécurité de l'information.

CONCLUSION GENERALE

L’objectif de cette étude était d’abord de présenter la contribution de l’audit interne à la sécurité du système d’information de gestion. Pour ce faire, nous avons construit notre travail autour de deux parties dont l’une théorique et l’autre pratique.

La partie théorique a consisté à parcourir les notions d’audit interne et sécurité de système d’information et les normes, référentiels et méthodologie de l’audit interne.

Dans la deuxième partie, il a été question pour nous de passer en revue les pratiques en place à l’ENPI dans la sécurité du système d’information.

Au regard de la théorie et de la pratique la notion de sécurité de l'information a pris de l'ampleur dans ce monde actuel de nouvelles technologies. Compte tenu des risques énormes encourus par la vulnérabilité des systèmes, par la maladresse ou l'insouciance du personnel, par des dégâts physiques et autres, les entreprises ont jugé dorénavant primordial de se munir de moyens divers pour protéger leurs actifs informationnels. La sécurité des systèmes informatiques et plus globalement des SI a été considérée pendant très longtemps par les entreprises comme un aspect de second plan. Peu à peu, une prise de conscience amène la SSI devant la scène. La raison principale est liée à la multitude d'incidents et plus grave, aux sinistres qui provoquent de lourdes pertes pour l'entreprise

La trilogie confidentialité, intégrité, disponibilité, détermine la valeur d'une information. La SSI a pour but de garantir la valeur des informations qu'on utilise. Si cette garantie n'est plus assurée, on dira que le système d'information a été altéré. Ainsi la sécurité de l'information est aujourd'hui appliquée à différents secteurs d'activités économiques.

Et pour les aider dans l'amélioration de leur système de management de la sécurité de l'information, la fonction d’audit interne joue le rôle d'évaluateur et de conseiller de bonnes pratiques. Cependant lors de mondialisation sans cesse changeant et la complexité des systèmes ont rendu la tâche de l'audit interne relativement difficile. Cela nécessite plus de connaissance et un long cycle d'adaptation qui ne rencontrent pas la plupart du temps l'adhésion des auditeurs internes. Ce fait a occasionné que l'on se pose la question de savoir comment l'audit interne contribue au maintien et à l'amélioration continue du système d’information de gestion au sein de l’ENPI.

L'exemple de l’ENPI de Tizi-Ouzou nous a permis d'apprécier la gestion de la sécurité de l'information. Nous savons qu'aucun système quel, qu'il soit, n'est à 100%assurer de façon absolue contre les divers menaces ou risques qui sont de plus en plus multiples par les

technologies nouvelles de l'information. Ainsi nous avons décelé quelques insuffisances qui ont fait l'objet d'analyse critique. Ces insuffisances étaient, entre autres, contenues dans la gestion globale de la sécurité de l'information (aspect humain, organisationnel et technologique) et dans le rôle de l'audit interne relatif à l'amélioration continue de cette sécurité.

Nous proposons ainsi des recommandations pertinentes pour contribuer tant bien que mal à la gestion de la sécurité de l'information au sein de l'ENPI de Tizi-Ouzou. Nous avons aussi recommandé une reconsidération de la méthodologie d'audit de la sécurité de l'information pour les auditeurs internes.

La méthodologie d'audit permet d'apprécier plus en profondeur la gestion de la sécurité de l'information en passant par son organisation jusqu'à ses activités et sa technologie. L'audit de la sécurité de l'information doit être un processus. Il doit permettre de s'assurer que les SI maintiennent la confidentialité, l'intégrité et la disponibilité des données et des systèmes et que ces derniers fournissent des renseignements pertinents et fiables. L'audit de la sécurité de l'information doit donner l'assurance que les SI 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 rapidement.

Ainsi, la sécurité de l'information est importante pour toute entreprise qui souhaite pérenniser son activité et son image de marque dans le monde des affaires actuel. Elle doit être du ressort de chaque acteur de l'entreprise quel que soit son poste hiérarchique. Aussi les auditeurs internes doivent être vigilants et toujours en alerte afin d'orienter au mieux la gestion de la sécurité de l'information et de favoriser l'atteinte effective et efficace des objectifs de l'entreprise. Assurément, les systèmes d'informations ne pourront pas être totalement protégés compte tenu de l'évolution constante de l'informatique.

Ce qui est considérable à faire est de s'atteler à réduire au maximum les risques qui pourraient survenir et ainsi préserver les différents systèmes d'informations.

Bibliographie

Ouvrages

1. AURIAC,(J-M) : *Economie d'entreprise* ,Tome 1,Paris : Casteilla, 1995.

2. BERDUGO (A), MAHL(R) et GERARD(J) : *Guide du management des systèmes d'information (thèmes et termes essentiels)* , Edition, Lavoisier,Paris , 2002.

3. BERTIN, (E), *Audit interne*, Editions Groupe Eyrolles, Paris, 2007.

4. BIZINGRE (J), PAUMIER (J) et RIVIERE (P) *: Référentiel du système d'information*, Editions Dunod, Paris ,2013.

5. CACALY, (S) et alii : Dictionnaire de l'information, édition Armand colin, 2emeédition , Paris, 2006.

6. CLAUDE, (P) *: 10 clés pour la sécurité de l'information : ISO/CEI 27001*, Editions AFNOR, Paris, 2012.

7. DESROCHES (A), LEROY (A) et VALLEE (F) *: La gestion des risques*, Editions Lavoisier, 2ème édition, Paris, 2007.

8. DEYRIEUX, (A) : *le système d'information : nouvel outils de stratégie, direction d'entreprise et direction du système d'information*, éditions Maxima, Paris, 2003

9. EBONDO WA MANDZALA E, *La gouvernance de l'entreprise : une approche par le contrôle interne et l'audit,* édition Harmattan, Paris, 2006.

10. GHERNAOUTI-HELIE, (S) *: Sécurité Internet, Stratégies et Technologies*, éditions Dunod, 2000.

11. GREUNING (H.V) et BRATANOVIC (S.B) : *Analyse et gestion du risque bancaire*, Editions ESKA, Paris,2004.

12. HASSID, (O) : *la gestion des risques,* éd. Dunod, Paris, 2008.

13. HERVE (F), MADERS (H. P) et MASSELIN (J.L) : *Les métiers d'auditeur interne et de contrôleur permanent*, Editions Eyrolles, Paris, 2014.

14. JIMENEZ, (C), MERLIER (P) et CHELLY (D) : *risques opérationnel :de la mise en place du dispositif á son audit*, Ed. Revue Banque, Paris, 2008.

15. JOANNY, (M) : *Théorie et pratique de l'audit interne*, édition D'organisations, Paris, 2000.

16. LAUDON,(K) et LAUDON (L) *:Management des systèmes d'information*. Editions Pearson, 2010.

17. LESCA, (H) *: L'information stratégique du dirigeant. Revue française de gestion*, novembre-décembre 1983, n043

18. LINLAUD,(D) : *la sécurité de l'information,* éd. afnor, Paris,2003.

19. MENTHONNEX, (J) *: sécurité et qualité informatique : nouvelles orientation*s, Editions presses polytechniques et universitaires romandes, Lausanne, 1995.

20. MOISAND,(D) et GARNIER DE LABAREYRE(F) :CobiT pour une meilleure gouvernance des systèmes d'information, Editions Eyrolles, Paris,2009.

21. MONACO,(L) : *les carrés DCG8- systèmes d'information de gestion*, éd. Gualino, Paris, 2014-2015.

22. PILLOU (J.F) et CAILLEREZ (P) : *Tout sur les systèmes d'information Grandes, moyennes et petites entreprises*, Editions Dunod, 2ème édition, Paris,2011.

23. Price Waterhouse Coopers et IFACI *: Référentiel intégré de contrôle interne*, Editions Eyrolles, Paris, 2014.

24. RENARD,(Jacques) :*Théorie et Pratique de l'Audit Interne*, Editions d'Organisation, 7ème édition , Paris, 2010.

25. SCHICK, (P) :*Mémentod'audit interne*, Editions Dunod, Paris, 2007.

26. SORNET (J), HENGOAT (O) et LE GALLO (N) : *systèmes d'informations de gestion : tout –en-un*, édition DUNOD, Paris, 2010.

Webliographie[65]

27. Extrait de La norme ISO 9000 :2015 Systèmes de management de la qualité, https://www.iso.org/obp/ui/fr/#!iso:std:42180:fr, Ed.2015

28. IIA, Cadre de références internationales des pratiques professionnelles,http://www.ifaci.com/publications/audit-interne/cripp/, Ed. 2017.

29. IIA, Cadre de références internationales des pratiques professionnelles www.ifaci.com/uploads/_ifaci/ani_fichiers/CRIPP-2013-3 .pdf.

30. http//:eduscol.education.fr/ecogest/si/SSI/riskconf. Les approches de sécurité de système

31. Club Informatique des Grandes Entreprises Françaises, http://cigref.typepad.fr/cigref_publications/RapportsContainer/Parus2008/protection_onformation/Protection_information_2008.pdf Publications CIGREF 2007-2008

32. Stéphane Gill,sgill.profweb.ca/spip/IMG pdf/01_Securite Information.pdfStéphane Gill.

33. Club Informatique des Grandes Entreprises Françaises http://www.cigref.fr/cigref_publications/RapportsContainer/Parus2009/Referentiels_de_la_DSI_CIGREF,Ed.2009.

[65] Ou **sitographie** désigne une liste de contenus, d'ouvrages ou plus généralement de pages ou ressources du Web relatives à un sujet donné. Ce mot est récent mais déjà très utilisé. Il est construit sur le modèle du mot bibliographie

34. Club Informatique des Grandes Entreprises Françaises www.cigref.fr/cigref_actualites/.../Controle_interne_du_SI_Assises_Securite,Ed._2009

35. Eric Papet, 2008.rmll.info/IMG/pdf/MEHARI_RMLL_2008_2-2.pdf, Ed 2008.

36. HugoEtiévant, http://cyberzoide.devloppez.com/Sécurite/Méthode,Ed.2006

37. ANSSI,http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite,Ed.2010.

38. ANSSI, cyberzoide.developpez.com/securite/methodes-analyse-risques.

39. CLUSIF,www.nmayer.eu/publis/NMA-JPH_MISC24.pd, Ed2010

40. Mag-securs , l'actualité de la sécurité informatique, https://www.mag-securs.com/news/id/17633/la-methode-mehari-methode-harmonisee,Ed.2006.

41. CLUSIF,https://clusif.fr/.../rm-rssi-deux-metiers-sunissent-pour-la-gestion-des-risques-du-si, Ed.2006

42. AFAI et CIGREF, http://www.itgi-france.com ,Ed. 2005.

Liste des tableaux et figures

Annexes

Annexe 1: Guide d'entretien avec l'Ingénieur en informatique de l'ENPI de Tizi-Ouzou

Entité: l'Entreprise Nationale de Promotion Immobilière de Tizi-Ouzou	
Département /Service: Service Informatique	
Fonction: Ingénieur en informatique	
QUESTIONS	**RÉPONSES**
Quelle est l'organisation de votre service ?	
Pouvez-vous nous faire une description de l'activité de votre service ?	
Existe-t-il une coordination entre les travaux du service informatique et ceux de l'audit interne ?	
Considérez-vous que l'équipe informatique dispose d'une compétence suffisante en matière de gestion de sécurité informatique pour pouvoir s'acquitter de manière efficace de cette tâche ?	
Quels sont les objectifs du dispositif de la sécurité de système informatiques ?	
Qui est le gestionnaire des risques informatiques ?	
Pour quelles méthodes avez-vous optée dans le cadre de la gestion des risques informatiques? ➢ MEHARI ➢ EBIOS ➢ AUTRE ➢ AUCUNE	
Pouvez-vous nous faire une description synoptique du processus de sécurité de système d'information?	
Compte tenu du fait que l'ENPI de Tizi-Ouzou n'est qu'une direction de projet, la contribution de l'audit interne à la sécurité de système d'information est-elle de votre ressort ?	

Source :l'ENPI

Annexe 2: Test d'existence du dispositif de sécurité du système d'information de gestion

Entité: l'Entreprise Nationale de promotion immobilière **Processus**: sécurité de système d'information de gestion	**Question de contrôle interne**		**2016-2017**
			Folio :
Objectif du questionnaire : s'assurer de l'existence d'un référentiel de sécurité du système d'information de gestion			
Questions	**Oui**	**Non**	**Commentaires**
➢ Un référentiel de gestion de sécurité informatique existe-t-il ?			
➢ Existe-t-il une méthodologie de gestion de sécurité d'information ?			
➢ Comment la haute direction s'implique-t-elle dans la gestion de la sécurité de l'information ➢ Quelles sont les actions déjà menées ?			
➢ Etablit-elle un mandat pour des auditeurs SI spécialisés ou transmet-elle le pouvoir de surveillance à l'audit interne ?			
➢ Existe-t-il une politique de sécurité de l'information au sein de l'ENPI ? ➢ La politique de sécurité est-elle approuvée par la haute direction ? Est-elle régulièrement mise à jour ?			
➢ Existe-t-il des manuels de procédures régissant la sécurité de l'information ? ➢ Ces procédures sont-elles constamment mises à jour ? ➢ La politique et les procédures sont-elles mise en œuvre ? ➢ Qui est le garant de l'exécution de la politique et des procédures de sécurité de l'information ?			
➢ Le garant de la sécurité de l'information a-t-il des objectifs clairs et mesurables ?			

➢ Quelssontcesobjectifs?			
➢ L'audit interne est-il impliqué dans le bon fonctionnement du système de sécurité de l'information ? ➢ Est-ce que la mise en application de la politique de sécurité de l'information est auditée de façon indépendante ?			
➢ Comment est gérée la sécurité de l'information d'avec l'extérieur ?			
➢ Existe-t-il une procédure d'attribution des droits d'accès ? ➢ si oui est-elle régulièrement revue ?			
➢ Les différentes structures de l'ENPI sont-ils sensibilisés sur l'importance de la sécurité de l'information ? ➢ Par quels moyens le sont-ils ?			
➢ Connaissent-ils les dispositifs de sécurité et leur importance ?			
➢ En cas de violation de la politique de sécurité de la banque et de non-respect des procédures de sécurité de l'information, est-il prévu des sanctions disciplinaires ? ➢ Le personnel a-t-il connaissance des procédures et politique de sécurité de l'information ?			
➢ A-t-il connaissance des risques liés à la sécurité de l'information?			
➢ Le personnel met-il en œuvre les procédures ?			
➢ Quels sont les apports du personnel en matière de sécurité de l'information ?			
➢ Les contrats de travail ou de stage contiennent ils des clauses de confidentialité ?			
➢ Existe-t-il des contrôles permettant d'établir ou de maintenir la sécurité des réseaux ? ➢ Les medias informatiques amovibles tels que les clés USB, les disquettes, les CD, les bandes etc. font-ils l'objet d'un contrôle particulier ?			

➢ Est-ce que la gestion des privilèges fait l'objet de contrôles particuliers ? ➢ Est-ce que seuls les utilisateurs dument autorisés peuvent accéder aux services en réseaux ? ➢ Est-ce que les accès sont dument authentifiés ?			
➢ Combien de temps faut-il pour retirer ou supprimer l'accès d'un employé temporaire ou non après son mandat de travail ? ➢ Tous les ordinateurs de l'ENPI sont-ils connectés à un système commun de réseau facilement contrôlable par le responsable TI ?			
➢ Existe-t-il des tests pour protéger et contrôler les données ? ➢ Si oui, lesquels? ➢ Existe-t-il des techniques de cryptographie pour protéger l'information ?			
➢ Les informations sont-elles convenablement conservées et classées ? comment et par quels moyens ? ➢ Existe-t-il des procédures pour surveiller l'utilisation du système ?			
➢ Est-ce que toutes les exigences statutaires, règlementaires et contractuelles dont relèvent les systèmes d'information, sont explicitement définies et documentées ? ➢ Est-ce que le système de sécurité de l'information et les systèmes d'information sont contrôlés régulièrement pour vérifier leur conformité avec la politique et les normes de sécurité ? ➢ Est-ce que les directions engagent des actions pour s'assurer que toutes les procédures de sécurité, dans leur périmètre de responsabilité, sont correctement suivies ? ➢ Est-ce que toutes les entités de l'ENPI sont sujettes à des revues régulières par l'audit interne ?			

➢ Existe-t-il une collaboration efficace les principaux acteurs de la sécurité du système d'information de gestion ?			
Gestion et intervention face à l'incident ➢ Existe-t-il des procédures de gestion des incidents ? ➢ Est-ce que les incidents de sécurité sont signalés en temps réel et à travers de bons canaux dès leur survenance ?			
➢ Existe-t-il des plans de relance des activités après la survenance d'un incident majeur ? ➢ Ces plans sont-ils régulièrement mis à jour ?			
➢ Existe-t-il des procédures pour signaler les dysfonctionnements des programmes et sont-elles suivies ?			
➢ Le personnel est-il sensibilisé sur la gestion des incidents ?			

Source : l'ENPI

Annexe 3: Guide d'entretien avec le Directeur de l'Audit Interne

Entité : l'ENPI de Tizi-Ouzou	
Département/Service : Département Audit interne	
Fonction : Directeur de l'Audit Interne	
QUESTIONS	**RÉPONSES**
Quelle est l'organisation de votre département ?	
Quel est le rattachement hiérarchique de votre département ?	
Votre charte d'audit tient elle compte des évolutions normatives ?	
Pouvez-vous nous faire une description synoptique de votre activité ?	
L'équipe d'audit interne bénéficie-t-elle d'un programme de formation continue adéquat ?	
Existe-t-il une coordination efficace entre les travaux de l'audit interne et ceux du service informatique ? Connaissez-vous la norme ISO 17799 ? Si oui, de quoi parle-t-elle ? Pour vous, qu'est-ce qu'une information ? Qu'entendez-vous par « sécurité de l'information » ?	
Considérez-vous que l'équipe d'audit interne dispose d'une compétence suffisante en matière de gestion de sécurité de SI pour pouvoir s'acquitter de manière efficace de cette tache? ➢ Quelles sont les domaines à compléter ?	
Quelle responsabilité vous a été attribuée au sein de l'entreprise en ce qui concerne la sécurité du système informatiques ?	
Comment décrivez-vous votre contribution dans le processus de sécurité du système informatique au regard de vos activités ?	
Vous arrive-t-il de faire des tests sur ces dispositifs ?	
Quelle est votre approche pour l'élaboration de vos plans d'audit annuel ?	

Inscrivez-vous des missions d'audit des systèmes informatiques dans votre plan d'audit ? ➢ Si oui à quand date la dernière mission ?	
Etes-vous associé à la formation et la sensibilisation des agents sur la sécurité informatiques ?	
Quelle est la périodicité de vos revues des procédures des systèmes informatiques ?	
Participez-vous à la conception de la politique de sécurité informatique, de la charte informatique, de la politique informatique, de la procédure d'attribution des droits d'accès, de sauvegarde des données et lacartographie ? ➢ procédez-vous à leur revue ?	
Quelle est votre part de responsabilité dans la gestion de sécurité informatique ?	
Avez-vous déjà effectue des missions d'audit de la sécurité de l'information ?	
Avez-vous une méthodologie d'audit de la sécurité de l'information ?	
En quelques mots, que vérifiez-vous lors d'une mission d'audit de la sécurité de l'information ?	
Selon vous, quel est l'apport de l'audit interne au maintien et à l'amélioration continue de la sécurité de l'information ?	

Source : l'

Mot clé

Audit interne, Système d'information, Sécurité des Systèmes d'Information, Système de Management de la Sécurité de l'Information

Résumé

La sécurité des systèmes d'information est un domaine très vaste, puisqu'elle fait appel à toutes les entités de l'entreprise et à des connaissances techniques et technologiques de pointe. L'une des forces et en même temps une problématique du monde des affaires actuel est l'évolution constante des technologies de l'information. Il est vrai que plus les technologies évoluent, plus elles offrent une plus grande mobilité aux utilisateurs et révolutionnent les habitudes et les façons de travailler.

L'objectif des normes est d'informer les auditeurs du niveau minimal acceptable pour répondre aux responsabilités professionnelles et les autres parties des attentes de la profession d'audit.

L'exemple de l'ENPI de Tizi-Ouzou nous a permis de constater et d'apporter un jugement sur la pratique de la sécurité de l'information au sein même de l'ENPI. De notre diagnostic, nous avons remarqué quelques anomalies susceptibles de compromettre le SMSI de l'ENPI et donc l'intégrité, la confidentialité et la disponibilité des informations. De la théorie, ont découlé des bonnes pratiques qui nous ont permis de faire des recommandations afin que l'ENPI de Tizi-Ouzou évite ou réduise considérablement tous les risques inhérents de sécurité qui pourraient survenir.

Nous avons également apprécié le rôle de la Direction de l'audit interne dans la sécurité de l'information à travers la méthodologie et le contenu du travail effectué. Nous avons pu noter que l'audit interne jouer son rôle pour rassurer au mieux l'efficacité et l'efficience de la sécurité de l'information. Nous avons fait des recommandations qui, nous l'espérons, aideront la Direction de l'audit interne à redéfinir sa méthodologie d'audit de la sécurité et à être un véritable contributeur à la sécurité de l'information.

إن أمن نظم المعلومات مجال واسع، حيث أنه يناشد جميع كيانات الشركة والمعارف التقنية والتكنولوجية المتقدمة. واحدة من نقاط القوة، وفي الوقت نفسه مشكلة في عالم الأعمال اليوم هو التطور المستمر لتكنولوجيا المعلومات. صحيح أن المزيد من التكنولوجيات تتطور، وكلما توفر للمستخدمين المزيد من التنقل وثورة العادات وطرق العمل.

والغرض من هذه المعايير هو إطلاع مدققي الحسابات على الحد الأدنى المقبول للوفاء بالمسؤوليات المهنية والأجزاء الأخرى من توقعات مهنة التدقيق.

تشخيصنا، لاحظنا عدة ENPI. تيزي وزو لنا أن نرى وإصدار حكم على ممارسة أمن المعلومات ضمن ENPI وقد سمح مثال القمة وبالتالي النزاهة والسرية وتوافر المعلومات. من الناحية النظرية، قد أسفرت عن ENPI مفارقات شأنه أن ينتقص من تيزي وزو يتجنب كل أو الحد بشكل كبير من مخاطر الأمنية التي قد ENPI الممارسات الجيدة التي مكنتنا من تقديم توصيات إلى تحدث.

كما أعربنا عن تقديرنا لدور إدارة التدقيق الداخلي في أمن المعلومات من خلال منهجية ومحتوى العمل المنجز. وقد لاحظنا أن المراجعة الداخلية للحسابات تؤدي دورها في تحسين فعالية وكفاءة أمن المعلومات. لقد قدمنا توصيات نأمل أن تساعد فرع التدقيق الداخلي على إعادة تعريف منهجية التدقيق الأمني الخاصة به وأن يكون مساهما حقيقيا في أمن المعلومات