MÂAREF ISSN 1112-7007 EISSN 6804-2600 | Volume: 15 / N°: 02 (Décembre 2020), pp143-163

Le contrôle interne en milieu informatique

Internal control in the IT environment

الرقابة الداخلية في بيئة تكنولوجيا المعلومات

Djekidel Yahia [(1)]* Messaoudi Abdelhadi[(2)] Boujlal Ahmed [(3)]

[(1)] Université Amar Thelidji Laghouat, Alger, y.djekidel@lagh-univ.dz
[(2)] Université Amar Thelidji Laghouat, Alger, a.messaoudi@lagh-univ.dz
[(3)] Université Amar Thelidji Laghouat, Alger, a.boudjelal@lagh-univ.dz

Date de réception: 15/02/2019; Date d'admission: 09/07/2020; Date de publication: 31/12/2020

Résumé :

Dans la plupart de grandes et moyennes entreprises, la mise en place de dispositif de contrôle interne s'appui principalement sur le contrôle de l'informatique. L'objectif de cette étude est d'appréhender le dispositif de contrôle interne ainsi que d'apprécier sa capacité à gérer les risques en milieu informatique. En effet, la quasi-globalité des procédures repose aujourd'hui sur des traitements informatiques. La mise en place de différents dispositifs de contrôle interne se fait et se fera de plus en plus à l'aide d'un système d'information conçus à cet effet. Toutes les applications informatiques existantes doivent en tenir compte et le cas échéant, doivent être revues pour prendre en compte des règles de contrôle interne et pour, éventuellement, corriger d'éventuelles fragilités des dispositions de contrôle interne en place.

Mots- Clés: contrôle interne, application informatique, milieu informatique, système d'information, NTIC.

Abstract:

In almost every large and medium-sized companies, the setup of internal control is mainly based on computer control. In fact, almost

* Auteur correspondant.

all procedures now rely on computer processing. The purpose of this study is to understand the devise of internal control system and to assess its ability to manage risks in the computer environment. The setting up of an internal control system is done or will be done with the help of information system designed for this purpose. This latter must be taken into account. Moreover, when appropriate, it must be reviewed with the full awareness of internal control rules, and to possibly strengthen any weaknesses in existing internal control arrangements.

Keywords :Internal control, computer application, computer environnement, information system, NTIC.

1. INTRODUCTION

Actuellement toutes les entreprises tiennent leurs comptabilités au moyen d'un système informatique. La pénétration de l'informatique dans tous les domaines de l'entreprise, est sans doute, spectaculaire. Cette informatisation peut aller de la simple utilisation d'un logiciel pour la tenue de la comptabilité à des procédures totalement informatisées ou l'intervention manuelle n'est qu'exceptionnelle. L'évolution de l'informatique a augmenté la dépendance des entreprises envers leurs systèmes informatiques et a affecté leur système comptable et celui du contrôle interne. Nous en citons la dématérialisation qui tend à devenir totale de la transaction et par suite, de la preuve. L'informatisation augmente et engendre pour l'entreprise de nouveaux risques qu'elle est appelée à maitriser. Ces risques touchent aussi bien la fonction informatique que les traitements automatisés. L'informatisation nécessite donc la mise en place de techniques d'évaluation du contrôle interne adaptées. Dans ce cas, il est évident que la qualité des procédures de contrôle interne découle, pour une part essentielle, des procédures de traitement de l'information, mais elle dépend également de sécurités mises en place pour que le non fonctionnement de l'informatique ne puisse pas perturber durablement l'entité et que l'accès à l'ordinateur soit correctement protégé. Les sécurités informatiques doivent transposer le principe de séparation des fonctions et donner des garanties de qualité équivalente aux procédures manuelles de contrôle interne. Donc, le recours aux nouvelles technologies de l'information (NTIC) peut engendrer des incidences sur le contrôle interne et le système

d'information de l'entreprise et peut engendrer aussi des incidences sur sa gestion. De ce fait, cet article pose la question suivante:

« Quelles sont les incidences du milieu informatique sur l'étude et l'évaluation du système d'information et le contrôle interne de l'entreprise ? ».

Devant cette situation, l'auditeur ne peut plus ignorer le phénomène de l'informatisation des entreprises devenues de plus en plus complexe.

L'évaluation du système de contrôle interne en milieu informatique nécessite de la part de l'auditeur une forte connaissance en informatique car des notions ainsi que des techniques sont à cerner pour comprendre et savoir gérer un processus d'informatisation. Pour cela, l'auditeur doit mettre en œuvre les procédures d'audit afin de s'assurer que l'entreprise dispose d'un système de contrôle interne effectif. Toutefois, on ne doit pas confondre l'audit des comptes en milieu informatique avec l'audit informatique du système d'information confié généralement à des experts spécialisés.

2 – Le contrôle interne et ses composants en milieu informatique

Aux Etats-Unis, la loi Sarbanes-Oxley (SOX 2002) et en France la loi sur la sécurité financière (LSF 2003) ont rendu obligatoire l'installation et le renforcement de dispositifs de contrôle interne. En Algérie, Le règlement de la banque d'Algérie a introduit le contrôle interne dans la législation Algérienne(1). Le contrôle interne est défini comme étant un processus mis en œuvre par la direction générale, la hiérarchie, le personnel d'une entreprise et destiné à fournir une assurance raisonnable quant à la réalisation des objectifs suivant(2) :

- Réalisation et optimisation des opérations.
- Protection des actifs.

(1)- Règlement n°11-08 du 28/11/2011 **relatif au contrôle interne des banques et établissements financiers**.
(2)- Mémentopratique Francis Lefebvre, « **Audit et commissariat aux comptes**», Edition Francis Lefebvre. Pais 2010, P.530.

- Fiabilité des informations financières.
- Conformité aux lois, réglementation et directives de l'organisation.

Le contrôle interne a donc pour objectif de favoriser l'efficacité et l'efficience et contribue à la réduction des risques et de la perte des biens. Il contribue également à l'exactitude des états financiers et le respect des lois et des règlements.

Il convient de souligner que cette définition a été adoptée par le système comptable financier Algérien. Le Système Comptable Financier (SCF) utilise la notion du contrôle interne en définissant la comptabilité comme étant un système d'organisation qui nécessite de la part des organes de gestion de l'entreprise l'existence d'un ensemble de procédures permettant une répartition des taches ainsi qu'une organisation pratique de la comptabilité. Il précise uniquement que la comptabilité doit être organisée de telle sorte qu'elle permette(3):

- La saisie complète, l'enregistrement de toutes les opérations ;
- La conservation des données de base,
- La disponibilité des informations élémentaires,
- La restitution de l'information en temps opportuns sous forme d'état dont la production est prévue ou requise,
- Le contrôle de l'exactitude des données et des procédures de traitement.

D'après le paragraphe 57 de la norme 315 : « la plupart des entités utilisent des systèmes à technologie informatique (TI) pour les enregistrements comptables et pour des buts opérationnels. Cependant, même lorsque la technologie informatique (TI) est intensivement employée, il y a des éléments manuels dans les systèmes. L'équilibre entre les éléments manuels et informatisés varie. Dans certains cas, particulièrement dans les entités plus petites moins complexes, les systèmes peuvent être principalement manuels. Dans d'autres cas, l'étendue de l'informatisation peut varier, allant de

(3)- TEZDAIL Ali, « **Maitrise du systèmecomptable financier** », Edition ACG 2009, P.25.

systèmes très fortement informatisés comportant peu d'éléments manuels à d'autres principalement manuels, et ce, même dans la même entité. En conséquence le système de contrôle interne d'une entité est susceptible de contenir des éléments manuels et des éléments informatisés dont les caractéristiques sont à prendre en compte par l'auditeur ». Donc, le système d'information, manuel ou informatisé, y compris les processus connexes d'entreprise concernant les états financiers dans leur ensemble et leur communication, constitue l'une des composantes du contrôle interne. Il comprend les procédures et les données établies pour gérer, enregistrer, traiter et communiquer les opérations de l'entreprise pour rendre compte des actifs, des passifs et des capitaux propres connexes(4).Les composants du système de contrôle interne comprennent:

- L'environnement du contrôle : Ceci comprend l'intégrité, l'éthique et la compétence des différents intervenants de l'entreprise.

- L'évaluation des risques : Ceci englobe l'identification et l'analyse des risques aussi bien internes qu'externes rattachés à la réalisation des objectifs de l'entreprise.

- Les activités de contrôle : c'est la mise en place des actions nécessaires pour faire face aux risques pouvant affecter la réalisation des objectifs de l'entreprise.

- L'information et la communication : Ceci désigne le développement et la communication de l'information à temps et dans une forme permettant aux différents intervenants d'assumer leurs responsabilités. Les technologies de l'information et de la communication (NTIC) peuvent être définies comme « étant l'ensemble des technologies informatiques et de télécommunication permettant le traitement et l'échange d'informations et la communication construite autour de l'ordinateur et du téléphone(5) ».

- La direction : Il s'agit d'une activité continue dont son objectif est de garantir que les procédures fonctionnent comme convenu.

(4)- Paragraphe 9 de l'annexe 2 de la norme ISA 315.
(5)- Abderaouf YAICH, « **La profession comptable et les nouvelles technologies de l'information et de la communication** », RCF n°53, troisièmetrimestre 2001.

Etant donné que les composants qui opèrent à travers l'ensemble des aspects de l'organisation forment un système intégré, les forces dans un domaine peuvent compenser des faiblesses soulevées dans d'autres domaines et permettent d'avoir un niveau approprié de contrôle contre les risques. Pour formuler son opinion, l'auditeur cherche l'assurance que les comptes, pris dans leur ensemble, ne comportent pas d'anomalies significatives. Compte tenu de la masse des opérations, l'auditeur ne vérifie pas toutes les opérations comptabilisées par l'entreprise car il s'appuie sur la qualité du système de contrôle interne, notamment le système d'information concourant à l'élaboration et au traitement de l'information comptable et financière qui constitue un système significatif pour l'audit. Les informations à recenser sur ce système concernent la politique informatique, structure de la fonction, matériel utilisé et sécurité. Cette démarche est fondée sur une approche par les risques. Ainsi, l'objectif de l'auditeur est d'apprécier comment l'organisation, le processus, et le dispositif de contrôle interne mis en pace assurent un niveau de maitrise satisfaisant de ces risques et permettent donc de réduire le risque de survenance d'anomalies significatives dans les comptes.

3 – Les spécificités du milieu informatique

Le milieu informatique est un milieu particulier qui a ses propres spécificités qui entrainent une démarche particulière pour l'évaluation du contrôle interne dans les entreprises ou l'on utilise des technologies informatiques et de télécommunication (TIC) permettant le traitement et l'échange d'information et la communication construite autour d'un ordinateur. L'existence d'un milieu informatique ne doit en aucun cas modifie l'objectif et l'étendue de la mission de l'auditeur. Néanmoins l'utilisation d'un ordinateur modifie :

- La saisie et le processus de traitement ;
- La conversation (échanges) des données entre modules ;
- La communication des informations comptables et financières.

L'existence de la fonction informatique peut avoir une influence sur toutes les étapes de la mission d'audit [(6)]:

(6)- Robert OBERT et Marie-Pierre MAIRESSE, « **Comptabilité et audit : Manuel et Applications** »,4°éditions, Dunod 2012, P.555.

- Lors de la prise de connaissance, l'auditeur doit comprendre les caractéristiques générales de l'informatique de l'entreprise afin d'apprécier son incidence sur son approche de la mission ;
- La fonction informatique, si elle est significative, doit faire l'objet d'une appréciation de contrôle interne spécifique qui portera sur l'organisation générale de la fonction elle-même et/ou sur certaines applications ;

Lors du contrôle des comptes, la fiabilité des systèmes informatiques influe sur la nature et l'étendue des contrôles à réaliser.

En effet, un milieu informatique pose des problèmes nouveaux tels que :

- La concentration des fonctions et des connaissances, qui provoque un risque de mauvaise séparation des fonctions ;
- La concentration des programmes et des données, qui augmentent le risque d'accès non autorisé ;
- L'absence éventuelle de matérialisation sur un support-papier des entrées, du traitement et des sorties ;
- La constance dans le traitement et éventuellement dans l'erreur.

Aujourd'hui, nous vivons une dématérialisation croissante de l'environnement de l'entreprise, l'audit traditionnel par contrôle sur pièces n'est pas toujours possible et adapté en termes de pertinence de résultats obtenus. Face à la complexité des systèmes informatiques, les grands cabinets internationaux ont développé des méthodologies propres et des équipes spécialisées dans l'audit informatique dans le cadre de l'audit financier. L'auditeur ne s'intéressera pas seulement aux comptes mais il examinera les modalités d'acquisition des données, leur gestion et leur traitement, étant précisé que certaines de ces données sont soumises au secret professionnel et à la qualité d'organisation du système informatique qui est une combinaison de ressources matérielles et des programmes informatiques qui permet[7] :

(7)-Décretexécutif n°09-110 du 07/04/2009, **fixant les modalités de tenue de la comptabilité au moyen de systèmesinformatiques.**

- L'acquisition d'informations, selon une forme conventionnelle ou réglementaire ;
- Le traitement de ces informations ;
- La restitution des données ou de résultats sous différentes formes.

Dès lors, la prise en compte de l'environnement du système d'information qui est défini comme « étant un ensemble des informations circulant dans l'entreprise des moyens mis en œuvre pour les gérer », et les applications qui le composent, deviennent une nécessité. La nature des risques dans un milieu informatique est liée aux spécificités suivantes :

- Le manque de trace matérielle justifiant les opérations qui entrainent un risque plus important de non détection des erreurs dans les logiciels d'exploitation et les programmes d'applications,
- L'uniformité du traitement des opérations qui permet d'éliminer quasiment toutes les erreurs humaines. En revanche, les erreurs de programmation peuvent entrainer un traitement incorrect de toutes les opérations,
- La séparation des taches intégrée dans le paramètre du système qui n'est plus physique mais également logique avec un risque accru,
- Le risque d'erreur ou d'irrégularités qui peut provenir :
  - D'erreurs humaines dans la conception, la maintenance et la mise en œuvre, plus importante que dans un système manuel,
  - D'utilisateurs non autorisés qui accèdent, modifient, suppriment des données sans trace visible.

Par ailleurs, la possibilité de détection de ces erreurs et irrégularités est affecté par le fait qu'elles sont souvent intégrées lors de la conception ou de la modification de programmes d'application ou de logiciels d'exploitation et sont aussi difficilement identifiables dans le temps. L'informatisation a modifié aussi le risque général de l'audit du fait :

- De la puissance et la fragilité qu'elle génère en facilitant la concentration des informations et leur circulation,

- De l'évolution technologique permanente des systèmes qui nécessitent une formation importante des « informaticiens » à proprement parler, mais aussi et surtout des « utilisateurs » dont elle bouscule souvent les habitudes,
- De l'automatisation du traitement de l'information qui augmente la sécurité par rapport à un système manuel ;
- De la capacité de certains systèmes à générer des informations sans intervention humaine, créant un risque de voir disparaitre ce qui est souvent appelé la « piste d'audit» ;
- De la prise de connaissance parfois insuffisante, dans les entreprises, des risques spécifiques liés à l'informatique.

A la fois facteur de fiabilité et de fragilité, l'informatique implique une conscience claire et précise de ses risques spécifiques et une organisation rigoureuse assurant la fiabilité et la sécurité des données qu'elle gère et dont l'entreprise est de plus en plus dépendante.

- Prise de connaissance du milieu informatique

Le milieu informatique existe lorsqu'un ordinateur, quels que soient son type et ses capacités, est utilisé pour le traitement d'informations financières d'importance significative pour l'audit, que cet ordinateur soit exploité par l'entreprise ou par un tiers. Dans nos jours ci, les entreprises sont devenues dépendantes envers leurs systèmes informatiques à cause de l'évolution des technologies de l'information et de la communication (TIC) qui ont affectées leurs systèmes comptables et de contrôles interne. La prise de connaissance de l'entreprise et de son environnement est une des étapes indispensables de la démarche d'audit pour une planification efficace et efficiente. Elle doit permettre à l'auditeur de constituer un cadre de référence dans lequel il planifie son audit et exerce son jugement professionnel pour évaluer le risque d'anomalie significative dans les comptes et y répondre tout au long de son audit.

Pendant cette phase, l'auditeur doit prendre en compte l'environnement informatique et son incidence sur l'évaluation du système de contrôle interne, il s'agit des caractéristiques générales du milieu informatique de traitement des systèmes comptables informatisés. Les principales informations que l'auditeur doit obtenir concernent principalement :

- L'organigramme détaillé de la structure informatique et sa position au sein de l'entreprise, notamment par rapport à la direction générale ;

- La localisation de l'installation et du stockage d'éléments sensibles (copies de fichiers, programmes, documentation…), ainsi que les accès extérieurs (terminaux, moyens de communication) ;

- Le manuel des procédures mise en place, notamment pour les mesures générales de sécurité ;

- Le processus de traitement et de stockage des données ;

- Le matériel, aussi bien l'unité centrale que les périphériques (lecteur CD, CD, imprimante…);

- Les applications et logiciels utilisées, qu'elles aient été développés par l'entité, acquises à l'extérieur.

Les principales procédures de traitement automatisé de l'information comptable et financière doivent être organisées de manière à permettre de contrôler si les exigences de sécurité et de fiabilité requise en la matière ont bien été respectées, notamment les prescriptions spécifiques du système comptable financier. Les contrôles portent d'une part, sur l'environnement informatique, d'autre part, sur les applications et logiciels informatiques utilisées par l'entité. Donc, une prise de connaissance du système d'information de l'entité et la revue de l'environnement informatique et des contrôles généraux sont indispensables car elles permettent à l'auditeur de réaliser une étude plus approfondie du fonctionnement de service informatique, à travers l'analyse des contrôles généraux et ceci dans la vue d'identifier et d'évaluer les risques d'anomalies significatives probables. Si des risques existent, l'auditeur conçoit alors la nature, le calendrier et l'étendue des autres procédures d'audit. L'identification des risques liés aux systèmes informatiques et au contrôle dans un environnement informatiques concerne aussi bien les risques liés aux contrôles généraux de l'informatique que ceux liés aux applications. L'auditeur se focalise sur les risques ayant une incidence directe ou indirecte sur la fiabilité des états financiers. Une fois les risques recensés, l'auditeur devra évaluer les contrôlés mis en place par l'entreprise pour les gérer. Les tests des contrôles peuvent être effectués en utilisant aussi bien des techniques spécifiques aux environnements informatisés (contrôle assisté par ordinateur, revue

des codes, jeux de tests) que des techniques classiques (examen des pièces justificatives et document)[8].

5 – Contrôles généraux de l'informatique

Le contrôle interne propre aux systèmes d'information est appelés « contrôles généraux informatiques », en anglais : « Information Technology General Controls ou ITGC».

Les contrôle généraux de l'informatique se rattachent à la fonction informatique et comprennent tous les contrôles de l'environnement informatique nécessaire au fonctionnement des applications. Les contrôles généraux de l'informatique sont des contrôles et des procédures liés à plusieurs applications qui permettent le fonctionnement efficace des contrôles d'application en aidant à assurer le fonctionnement harmonieux et continu des systèmes d(information[9].

Ces différents contrôles sont mis en œuvre pour vérifier l'exactitude, l'exhaustivité et l'autorisation des opérations. Ils ont pour objectif« d'établir un cadre de contrôle global sur les activités informatiques et de fournir un niveau d'assurance raisonnable que les objectifs de contrôles interne sont atteints »[10]. Il y' a lieu aussi de préciser que les contrôles généraux de l'informatique peuvent être regroupés en quatre familles qui couvrent le cycle de vie de la donnée[11]:

- **C**ontrôles portant sur l'organisation: Cet aspect désigne le contrôle de l'organisation du service informatique et des relations avec les utilisateurs. Cette concentration peut conduire au non-respect du traditionnel principe de séparation des fonctions. Ainsi, l'auditeur recherchera-t-il, si les fonctions, donc les responsabilités sont bien séparés, notamment entre :

(8)- Petit G., JOLY D.et Michel J., « **Audit et informatique : guide pour l'audit financier des entreprisesinformatisées,** volume 1, Editions Paris : CLET 1985.P.234.
(9)- Mohamed HAMZAOUI, « **Gestion des risquesd'entreprise et contrôle interne** », 2°édition Pearson 2008, P.159.
(10)- IAPS 1008 : « **Evaluation des risques et contrôle interne : caractéristiques et considérations sur l'informatique**», IFAC.
(11)- Société nationale de comptabilité, « **Revue technique SNC** », n°03 décembre 1990. P .36.

- Les services d'études, c'est-à-dire les organisateurs responsables de l'implantation des systèmes dans leur ensemble, les analystes chargés de la conception des applications et les programmeurs char gés de traduire ces analyses en langage informatique, qui ne doivent avoir accès qu'aux programmes en développement ;
- Les services d'exploitation, c'est-à-dire les opérateurs et pupitreurs, qui ne doivent pas avoir accès qu'aux programmes et aux supports de fichiers en exploitation ;
- Les utilisateurs, qui peuvent procéder à des interrogations des fichiers, à des saisies de données et à des éditions d'informations.

- **C**ontrôles relatifs à la sécurité, à la sauvegarde et à la reprise des travaux : le traitement Informatique de la donnée conduit à une concentration d'éléments du patrimoine dans un même lieu (matériel, logiciels, supports et informations stockées).

L'auditeur devra vérifier que la protection de ces éléments est suffisante et que la confidentialité est assurée.

La protection physique vise en particulier le contrôle efficace de l'accès physique aux locaux d'exploitation ainsi que les protections contre les dommages physiques, quelle que soit leur origine.

- **C**ontrôles portant sur le traitement ou la gestion de l'exploitation informatique ;
- **C**ontrôles du développement des applications, de leur documentation et de leur mise en application.

L'identification des risques liés aux systèmes informatiques et au contrôle dans un milieu informatique concerne aussi bien les risques liés aux contrôles généraux de l'informatique que ceux lié aux applications en se focalisant sur les risques ayant un impact direct ou indirect sur la régularité, la sincérité et l'image fidèle des comptes.

Les risques liés à l'informatique sont relatifs à l'organisation de la fonction informatique, à la gestion d'exploitation et à la gestion de la sécurité. Les risques liés aux contrôles généraux de l'informatique sont ceux qui peuvent résulter de déficiences dans plusieurs des activités informatiques telles que : développement et maintenance de programmes, support logiciel, opérations, sécurité physique des

équipements informatiques, contrôle d'accès à des utilisateurs privilégiés. Ces déficiences ont un effet diffus sur toutes les applications traitées par l'ordinateur.

5 – 1 Contrôles portant sur la séparation des fonctions

La séparation des fonctions est un des principes fondamentaux de contrôle interne et une mesure essentielle et fondamentale qui facilite la détection des erreurs commises en toute innocence. Il s'agit d'un contrôle critique visant à limiter les possibilités de fraude de la part d'une personne unique. L'environnement informatisé de l'information comptable et financière peut conduire au non respect du traditionnel principe de séparation des fonctions c'est-à-dire les taches autrefois dévolues aux différentes personnes sont aujourd'hui exécutées par le seul département informatique en raison :

- Réduction du nombre de personnes intervenantes, auparavant, dans le traitement manuel des opérations contre une augmentation de staff informatique centralisant, généralement, de nombreux aspect des systèmes.
- Les informations comptables et financières et les programmes d'application de l'entreprise sont stockés sur des mémoires électriques et accessibles à beaucoup de personnes à moyen de terminaux. En l'absence de contrôle d'accès appropriés, les personnes ayant accès à des traitements informatiques ou à des fichiers peuvent être en mesure de réaliser des fonctions qui devraient leur être interdites ou de prendre connaissance de données sans y être autorisées et sans laisser de traces lisibles.
- Quand le service informatique est important, il est en général plus facile de séparer les taches incompatibles. Toutefois dans les entreprises de taille moyenne est beaucoup moins important que dans une structure de taille importante. Dans ce cas l'auditeur doit s'assurer que les fonctions ou les responsabilités sont bien définies et séparées, notamment entre :
    - Les services d'étude, c'est-à-dire les organisateurs responsables de l'implantation des systèmes dans leur ensemble, les analystes chargés de la conception des applications et les programmeurs chargés de traduire ces analyses en langage informatique, qui ne doivent avoir accès qu'aux programmes en développement ;

- Les services d'exploitation, c'est-à-dire les opérateurs et les pupitreurs, qui ne doivent avoir accès qu'aux programmes et aux supports de fichiers en exploitation ;
- Les utilisateurs, qui peuvent procéder à des interrogations de fichiers, à des saisies de données et à des éditions d'informations.

5 – 2 Contrôles portant sur la sécurité des installations

L'information est un actif précieux de l'organisation. A ce titre, il faut la protéger contre la perte, l'altération et la divulgation. Les systèmes qui la supportent doivent quant eux protégés contre l'indisponibilité et l'intrusion. La sécurité est une démarche globale de l'entreprise organisée autour d'une politique d'une politique de sécurité1[(12)].

Le traitement informatique des données conduit à une concentration d'éléments du patrimoine dans un même lieu (matériels, logiciels, supports et informations stockées). L'auditeur devra vérifier que la protection de ces éléments est suffisante et que la confidentialité est assurée. La protection physique vise en particulier le contrôle efficace de l'accès physique aux locaux d'exploitation ainsi que les protections contre les dommages physiques, quelle que soit son origine. La protection logique est principalement obtenue par l'utilisation de moyens de contrôle d'accès tels que badges ou mots de passe régulièrement modifiés et par l'enregistrement des tentatives d'accès non autorisé. L'auditeur doit aussi évaluer les mesures prises pour palier d'éventuelles pertes de capacités de traitement ponctuelles ou prolongées.

Il doit contrôler l'existence d'un équipement de secours et/ou de procédures de reprise (existence d'un plan de sauvegarde, des procédures d'arrêt,…).La politique de sécurité mise en place par l'entreprise doit être formalisée et détaille notamment les modalités et procédures mises en œuvre sur les points suivants :

- Anti-virus : le fichier de signature est mis à jour régulièrement et supervisé,

(12)- CHAI, « **Guide d'audit des systèmesd'information** », version 1.0-juin 2014, P.43.

- Des actions de sensibilisation aux pratiques relatives à l'utilisation de la messagerie et de l'internet sont réalisées,
- Des règles sont définies par l'utilisation des supports physiques par les utilisateurs du système d'information pour échanger les données (disques externes, clés USB, graveur).

Concernant l'accès aux programmes et aux données, la gestion des habilitations revêt une importance majeure. Elle a pour objectif de s'assurer de la définition de profils utilisateurs en adéquation avec les fonctions occupées. Ces points seront particulièrement importants à préparer, tout comme la gestion des mots de passe et l'authentification au système d'information de l'entité. Ces contrôles réalisés relatifs à la politique de sécurité de qualité pourront notamment permettre de mettre en évidence la séparation de fonctions insuffisante et de comprendre son incidence sur le système de contrôle interne et d'apporter les correctifs nécessaires.

5 – 3 Contrôles portant sur la gestion de l'exploitation informatique

La gestion de l'exploitation informatique couvre les fonctions nécessaires à la mise en œuvre et la sécurisation des composants du système d'information, qu'ils soient applicatifs, matériels ou autres. Elle recouvre classiquement les moyens et dispositifs mis en œuvre afin de garantir la fiabilité et la sécurité des traitements, des infrastructures dans ses objectifs et d'apporter aux utilisateurs du système d'information la qualité de l'information comptable et financière.

L'information financière produite par ce système est enregistrée sur un support numérique qui est composé de données. Les données peuvent être regroupées en deux grandes familles :

- Les données référentielles : clients, fournisseurs, plans comptables, etc.
- Les données transactionnelles : factures, bon de commande, devis, etc.

A l'échelle de l'entreprise, chaque type de données doit être identifié, enregistré et mis à jour de manière unique et adéquate au regard de l'activité.

Les données peuvent être stockées sur des serveurs possédés et/ou hébergés par l'entreprise, ou bien à l'extérieur. Dans ce cas, il convient de contrôler les dispositions de conformité et/ou les dispositions contractuelles. Lors du contrôle d'applications informatiques traitant d'informations à conséquences comptables et financière, l'auditeur étudie en détail les contrôles de traitement qui concernent principalement :

- La qualité des procédures d'exploitation, notamment des procédures de restriction d'accès aux bibliothèques de programme en exploitation ;

- Le degré de confiance que l'on peut avoir dans les contrôles et les procédures programmes des applications comptables informatiques, ainsi que dans les opérations générés par le système ;

- Le respect des principes d'autorisation, d'exactitudes et d'intégralité du traitement des données ;

- La sauvegarde qui doit être au minimum tous les jours, le bon fonctionnement des sauvegardes est suivie selon une procédure formelle ;

- Les changements apportés aux matériels, aux logiciels, aux systèmes d'exploitation.

5 – 4 développement et maintenance des applications: documentation et mise en exploitation

Tout projet majeur qui pourra conduire l'entreprise à faire l'acquisition d'une application ou, à réaliser un développement spécifique et plus largement de tout changement majeur pouvant avoir une incidence sur la production des états financiers doit faire l'objet d'une analyse et d'une évaluation. Il convient d'évaluer les opérations d'une migration qui pourront avoir une incidence sur la cible définie par l'entreprise. La migration représente le passage d'un état existant d'un système d'information ou d'une application vers une cible définie dans un projet ou un programme. La migration des données vise à modifier l'ensemble des données générées par un système informatique source (matériel et logiciel) pour pouvoir les utiliser sur une autre cible. Les différences entre les logiciels obligent à transformer les données pour qu'elles soient compatibles avec le nouveau système. Après changement dans le système cible, les données migrées doivent être vérifiées pour déterminer si elles sont

exactes, exhaustives et supportent correctement le processus du nouveau système.

Un nettoyage de données est communément effectué afin d'améliorer la qualité des données migrées et d'éliminer les données redondantes ou obsolètes. Ainsi, l'auditeur doit vérifier que les indicateurs suivants ont été pris en considération :

- Quelles sont les procédures de contrôle sur la migration des données relatives aux transactions des données permanentes et des nouvelles données qui n'existaient pas dans l'ancienne application ;
- Existe-il des procédures pour s'assurer que les données sont correctement vérifiées par les utilisateurs et les équipes informatiques.

Dans le cadre de développement ou acquisitions de nouveaux programmes, l'auditeur s'assure de l'existence d'une méthodologie de développement et de maintenance des applications en portant son attention plus particulièrement sur les points suivants :

- Autorisation et suivi des projets ;
- Documentation : contenu et mise à jour, notamment au regard des dispositions du système comptable financier (SCF) et de la législation fiscale ;
- Séparation des bibliothèques de développement et des bibliothèques d'exploitation ;
- Procédures de test avant la mise en exploitation et la réception;
- Procédures de maintenance des programmes.

D'une manière générale, l'audit d'une application opérationnelle est de donner aux dirigeants de l'entreprise une assurance raisonnable sur son fonctionnement, c'est par exemple de vérifier que le logiciel utilisé est sûr, efficace et adapté.

6– Contrôles d'application informatique

L'audit est devenu un défi pour les auditeurs de plus en plus grand ; d'un cotél évolution rapide de normes comptables internationales IAS/IFRS, de l'autre coté, l'automatisation croissante de la préparation des états financiers au moyen de systèmes

d'information toujours plus complexe. La qualité de l'information comptable et financière dépend, en premier lieu de la qualité des processus métiers et des flux de traitement des données s'y rapportant. Il est donc nécessaire que les travaux de l'auditeur seront concentrés sur les processus métiers et le contrôle des applications correspondantes dans son approche d'audit destinée à aider l'auditeur à développer une approche d'audit intégrée et à recentrer la procédure d'audit de manière plus efficace et plus ciblée sur les risques, en intégrant l'audit des processus métiers pertinents et des applications correspondantes(13). Les applications informatiques sont le support incontournable des processus métiers ou fonctionnels. Les contrôles d'application concernent le traitement des applications individuelles. Ils aident à s'assurer que les opérations se sont bien produites, ont été autorisées et sont enregistrées et traitées complètement et correctement. Les exemples de contrôles d'application incluent la vérification de l'exactitude arithmétique des enregistrements, la maintenance et le passage en revue des comptes et des balances intermédiaires, les contrôles automatisés (comme ceux qui éditent des contrôles de séquences numériques) et le suivi manuel des rapports d'exception. Cette approche commence donc avec l'analyse des états financiers de l'entreprise et se termine par l'appréciation de l'impact des résultats d'audit sur ces états financiers. L'analyse des états financiers vise à orienter les procédures d'audit des processus de l'entreprise et des applications correspondantes sur les tests des comptes significatifs et sur les risques s'y rapportant. Une fois les applications de base identifiées, l'auditeur s'intéresse au système de contrôle interne, il détermine d'abord si sa conception est adaptée à la situation des risques actuelle des processus de l'entreprise et enfin, si les contrôles prévus sont implémentés et efficaces. L'évaluation du système de contrôle interne permet à l'auditeur de savoir s'il peut s'appuyer sur les procédures de production des états financiers et le cas échéant, de définir l'étendue des procédures d'audit substantives supplémentaires qu'il doit effectuer.

Enfin, l'auditeur doit obtenir une assurance suffisante que toutes les transactions de l'entreprise qui doivent transiter par les applications sont autorisées, enregistrées et qu'elles sont traitées

(13)- ISACA et AFAI, « **Guide d'audit des applications informatiques : Une approcheinspirée des audits financiers** »,SwitZerlande Chapter, 2008, P.4.

intégralement et correctement dans les délais fixés. Il veille également à ce que les dispositions générales relatives à l'utilisation des traitements automatisés prescrits par le système comptable financier (SCF) soient respectées(14). Les risques liés aux contrôles d'application sont ceux qui peuvent accroitre le potentiel d'erreur, et de fraudes dans des applications spécifiques, des bases de données, des fichiers maitres ou des traitements spécifiques. Ainsi, les erreurs sont relativement fréquentes dans des systèmes exécutant des opérations logiques ou des calculs complexes, ou qui gèrent un nombre élevé d'exceptions. De même, les systèmes qui contrôlent les sorties de fonds ou d'autres liquides peuvent faire l'objet de fraudes de la part des utilisateurs ou du personnel informatique.

7 – Les effets de l'informatique sur l'évaluation du contrôle interne

Comme dans un cadre non informatisé, l'auditeur doit posséder une connaissance suffisante de l'environnement informatique (systèmes et processus informatiques) pour planifier, diriger, superviser et revoir le travail effectué et en déduire leur incidence sur les procédures d'élaboration des comptes(15). Il s'agit de la collecte d'information concernant :

- Les principales caractéristiques de la fonction informatique.
- Les contrôles généraux de l'informatique.

L'auditeur doit évaluer l'incidence de l'environnement informatique sur le système d'information et le dispositif du contrôle interne en procédant à une évaluation préliminaire des forces et des faiblesses des contrôles (contrôles généraux informatiques et contrôles d'application informatisées). Après avoir décrits les contrôles existants, l'auditeur doit procéder, comme en milieu non informatisé, à une vérification par sondage du fonctionnement des procédures en tenant compte de l'importance et de la complexité des systèmes

(14)-Décretexécutif n°09-110 du 07/04/2009 **fixant les conditions et modalités de tenue de la comptabilité au moyen de systèmesinformatiques**.
(15)- Compagnie nationale des commissaires aux comptes, « **Priseencompte de l'environnementinformatique et incidence sur la démarched'audit** », édition CNCC, avril 2003, P.11.

informatiques et de la disponibilité des données pouvant être utilisées pour l'audit, en particulier :

- De l'importance et de la complexité du traitement informatique pour chaque application comptable importante.
- De l'organisation des activités informatiques de l'entreprise et du degré de concentration ou de décentration du traitement informatique dans l'entreprise, notamment lorsqu'ils ont une influence sur la séparation des taches.
- De la disponibilité des donnés, certains fichiers et d'autres éléments probants nécessaires à l'auditeur existent parfois pour une courte durée seulement ou uniquement sur un support lisible par une machine.

En cas de faiblesses dans ces contrôles, il convient alors d'atteindre par d'autres procédures les objectifs que l'auditeur s'est fixé. L'auditeur peut améliorer l'utilité et l'efficacité des tests de conformité en ayant recours aux techniques de contrôle assisté par ordinateur, notamment programmes utilitaires, utilisation de langage d'interrogation, programmes spécifiques, progiciels d'aide à l'audit et jeux d'essai. Une telle utilisation devient indispensable lorsque l'auditeur se trouve en situation de perte du chemin d'audit et n'a pas la preuve de la réalité des contrôles effectués au cours du traitement. Il doit, en outre, s'assurer que ces contrôles ont effectivement fonctionné pendant toute la période d'audit. L'objectif du test de conformité et de l'évaluation finale est de donner la garantie et l'assurance à l'auditeur du bon fonctionnement des contrôles. L'objectif que poursuit l'auditeur en appréciant le contrôle interne est de déterminer dans quelle mesure il pourra s'appuyer sur le contrôle interne pour définir la nature, l'étendue et le calendrier de ses travaux ultérieurs. Il pourra aussi pour orienter sa mission, synthétise dans une note qui résume pour chaque significatif :

- Le ou les systèmes qui l'alimentent ;
- Le processus du jugement qui l'affecte ;
- Les contrôles internes sur lesquels il a décidé de s'appuyer et les conséquences sur l'étendue des contrôles si les résultats des tests sur ces contrôles sont satisfaisants ;
- La nature, l'étendue et le calendrier des autres vérifications à effectuer, lors qu'il n'y a pas de contrôles internes sur lesquels

il puisse s'appuyer, pour qu'il ait la possibilité de s'assurer qu'l n'y a pas d'erreurs significatives.

Il convient alors que l'auditeur ait recours à d'autres procédures pour atteindre ses objectifs. Les défaillances, insuffisances et imperfections décelées par l'auditeur au cours de l'examen dans ce domaine particulier doivent faire l'objet d'un rapport détaillé adressé aux dirigeants.

8 - Conclusion

L'efficacité d'un système de contrôle interne contribue à la création d'un environnement de contrôle sain et établit une bonne gestion de l'information et de la communication mais cela ne s'arrête pas là, le système de contrôle interne nécessite une évaluation régulière afin de savoir s'il est toujours efficient et d'actualité. Un système de contrôle interne même correctement installé avec le plus grand soin possible, peut devenir rapidement inefficace, s'il reste immobile et statique alors que l'environnement, notamment la technologique de l'information et de la communication (TIC) est, lui, en perpétuelle mouvance. La mise en place de dispositif de contrôle interne repose en grande partie sur le contrôle de l'informatique. Quelque soit le milieu audité, l'objectif de l'auditeur reste toujours la fiabilité de l'information produite et communiquée par l'entreprise à ses tiers. Le maintien efficace du système de contrôle interne représente un processus permanent et continu d'évaluation de chacune de ses composantes qui doit être effectué à la lumière des innombrables changements qui peuvent influencer la gestion de l'entité. Donc, lors de la phase d'évaluation du contrôle interne, il est indispensable pour l'auditeur de prendre en compte l'environnement ou le milieu informatique afin d'apprécier l'incidence de cet environnement sur la démarche d'audit au travers notamment l'identification des principales composantes du système d'information et son niveau de complexité. Pour élaborer son programme de travail d'audit du système d'information, il convient de s'assurer qu'on dispose de compétences internes au cabinet.

A défaut, se faire assister d'un confrère qui maitrise ce type de missions. Si l'auditeur souhaite développer cette compétence au sein de son cabinet un programme de formation approprié doit être envisagé.