UNIVERSITE DE LA MANOUBA

Institut Supérieur de Comptabilité et d'Administration des Entreprises
(I.S.C.A.E)

Commission d'Expertise Comptable

Mémoire en vue de l'obtention du diplôme d'expertise comptable

Sujet :

L'EVOLUTION DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION : IMPACT SUR L'AUDIT FINANCIER

Préparé par : Mohamed Lassâad

Encadré par : Ahmed BELAIFA

Année Universitaire 2000/2001

Sommaire :

Introduction Générale

Les technologies de l'information et de la communication 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 »[1].

Ces technologies touchent de plus en plus les entreprises en Tunisie. En effet, ces dernières sont devenues de plus en plus informatisées et beaucoup d'entre elles ont mis ou sont en cours de mettre en place des progiciels de gestion intégrée, dénommés aussi E.R.P (Enterprise Resource Planning) dont à titre d'exemple : SAP, JDEdwards, Oracle, etc.

Par ailleurs, la nouvelle technologie de l'Internet va certainement devenir, dans un proche avenir, l'une des préoccupations majeures de nos entreprises tunisiennes et ce, compte tenu des phénomènes de globalisation et de libéralisation ainsi que de l'émergence de la nouvelle économie.

Cette évolution de l'informatique, aussi bien au niveau du hardware que du software, et sa pénétration dans tous les domaines de l'entreprise est, sans doute, spectaculaire.

En effet, les systèmes informatiques actuels permettent de plus en plus :

- une mise à jour et un partage des données en temps réel,
- une intégration des systèmes d'information financiers et opérationnels (ERP : Entreprise Resource Planning),
- des échanges économiques intéractifs de l'entreprise, non seulement avec les clients, mais aussi avec les fournisseurs (E-commerce, E-business, etc.)

Toutefois, cette évolution a augmenté considérablement la dépendance des entreprises envers leurs systèmes informatiques et a affecté leurs systèmes comptables et de contrôle interne. Nous en citons, essentiellement, la dématérialisation tendant à devenir totale (zéro papier) de la transaction et par suite, de la preuve (Absence de documents d'entrée, absence de systèmes de références visibles, absence de documents de sortie visibles).

Parallèlement, ce développement de l'informatique augmente, dans des proportions importantes, la vulnérabilité du système d'information et engendre pour l'entreprise de nouveaux risques qu'elle est appelée à maîtriser. Ces risques touchent aussi bien la fonction informatique que les traitements automatisés.

Face à ce nouveau contexte, les auditeurs financiers ne peuvent plus ignorer le phénomène de l'informatisation des entreprises devenue de plus en plus complexe. S'ils ont estimé, au départ, qu'il fallait traiter l'informatique à part, ils sont convaincus, aujourd'hui, que l'informatique devrait être intégrée dans leur démarche professionnelle et dans chacune de leurs préoccupations.

Ainsi, l'approche d'audit, que nous avions l'habitude d'adopter dans nos entreprises tunisiennes, devrait répondre à ce nouveau contexte et aux risques nouveau-nés.

Cette mise à niveau de l'approche d'audit est une préoccupation majeure et d'actualité des organismes professionnels dans le monde et des cabinets internationaux. C'est ainsi que les organismes professionnels n'ont pas manqué d'apporter et de mettre à jour les lignes directrices et le minimum de diligences dans le cadre d'un audit dans un milieu informatisé et que les cabinets internationaux ont développé des méthodologies appropriées et ont fait de gros investissements pour adapter les approches d'audit à un environnement devenu de plus en plus complexe.

[1] Abderraouf YAICH, « La profession comptable et les nouvelles technologies de l'information et de la communication », La Revue Comptable et Financière RCF N°53, Troisième trimestre 2001, Page 17.

Parallèlement, la législation, la jurisprudence et la doctrine à l'échelle internationale se sont enrichies de règles nouvelles destinées à réglementer et à contrôler certains aspects des systèmes informatisés.

Par ailleurs, ce nouveau contexte implique, de la part de l'auditeur, un minimum de connaissances en matière informatique. Ceci n'écarte pas, bien sûr, la possibilité du recours à des spécialistes en cas de besoin.

Ainsi, la question qui se pose est de savoir comment ces nouveaux aspects informatiques sont pris en compte dans la démarche de l'audit financier ? Et quelles sont les évolutions nécessaires des pratiques en la matière en Tunisie ?

Pour répondre à cette problématique, ce mémoire sera structuré en deux parties :

- La première partie sera consacrée à l'étude de l'impact des nouvelles technologies de l'information et de la communication sur le système comptable et les contrôles internes de l'entreprise ainsi que sur l'audit financier. Elle traitera aussi les principales réactions des législations et des organismes professionnels en la matière.

  L'objectif de cette partie est de mettre en exergue les enjeux informatiques complexes et de montrer l'importance que revêt désormais l'audit informatique dans le processus de l'audit financier.

- La deuxième partie sera consacrée à la détermination du besoin de recours à l'audit informatique dans une mission d'audit financier, à l'étude des rôles qui lui sont dévolus et à une présentation de la démarche correspondante à suivre. Seront aussi traitées, les principales évolutions prévisibles des pratiques en la matière en Tunisie.

  L'objectif de cette partie est de présenter la manière avec laquelle s'intègre l'audit informatique dans les différentes étapes de l'audit financier et d'anticiper le développement futur de l'audit informatique en support à l'audit financier.

Aussi, faut il indiquer que le présent mémoire ne traite pas les aspects suivants :

- Description détaillée des impacts de chaque nouvelle technologie sur le système comptable et les contrôles internes : uniquement les domaines touchés sont traités. Des exemples ont été fournis à titre indicatif.
- Description détaillée des contrôles à mettre en place par l'entreprise pour couvrir les nouveaux risques engendrés par les nouvelles technologies de l'information et de la communication.
- Description détaillée des tests à entreprendre par l'auditeur pour la validation des contrôles clefs associés aux contrôles généraux informatiques et aux contrôles d'application.
- Conception des techniques d'audit assistées par ordinateur et description de la démarche de leur utilisation.
- Les problèmes comptables qui peuvent surgir de l'utilisation des nouvelles technologies de l'information et de la communication (exemples : l'impact de l'environnement informatique sur la continuité d'exploitation, la comptabilisation des revenus, l'estimation des provisions pour dépréciation clients pour les ventes via le Web, la comptabilisation du coût de développement des applications, la comptabilisation du coût des recherches et des développements touchant par exemple l'Internet, etc.).

Partie I : Nouvelles technologies de l'information et de la communication : Impact sur l'entreprise et sur l'audit financier

Introduction Partie I

Comme indiqué dans l'introduction générale, cette partie est consacrée à l'étude des principaux impacts des nouvelles technologies de l'information et de la communication sur le système comptable et les contrôles internes de l'entreprise ainsi que sur l'audit financier.

Ainsi, faut-il, tout d'abord, indiquer et décrire brièvement les principales nouvelles technologies de l'information et de la communication.

- **L'architecture Client / Serveur :**

  De nos jours, l'architecture Client / Serveur est, probablement, le changement le plus répandu dans le traitement des données. Elle répond à une nécessité de faire partager l'information entre les différents utilisateurs. Les applications informatiques et les bases de données sont localisées sur le serveur et sont partageables par les utilisateurs depuis leurs postes (client)[2].

  L'architecture client/serveur se caractérise par la division d'un traitement informatique exécuté sur des plates-formes interconnectées en réseau.

- **L'Echange de Données Informatisé (EDI) :**

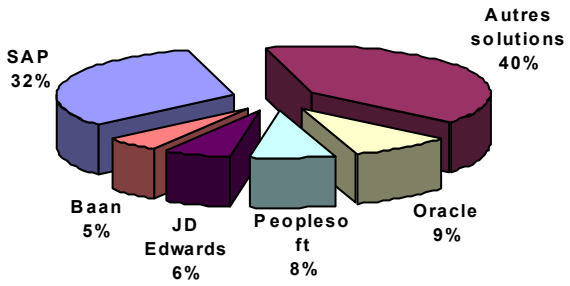
  L'E.D.I est un transfert de données, suivant des standards préétablis de messages (protocoles de communication), d'ordinateur à ordinateur par des moyens électroniques. Un système E.D.I. concerne généralement des partenaires juridiquement distincts. Il sert à supprimer les échanges sur support papier tout en conservant une même qualité sur le plan de la sécurité, et à éviter les ressaisies et l'accroissement des délais.

- **Les Progiciels de Gestion Intégrée (ERP) :**

  Après l'ère du développement spécifique et des premiers progiciels de gestion monodomaine (comptabilité, gestion de production...), les années 90 ont vu le développement des ERP ou progiciels de gestion intégrée.

  Il s'agit d'un ensemble de modules structurés autour d'une base de données unique et couvrant l'ensemble des domaines fonctionnels de l'entreprise, de la gestion de production à la gestion financière.

  Cinq grands fournisseurs de progiciels se partagent aujourd'hui 60% du marché des ERP dans le monde, avec SAP (32% de parts de marché en 1998) comme leader incontesté.



Source : The Gartner Group 1998

Le taux de pénétration des ERP dans les grandes entreprises mondiales est important. Plus de 40% des 500 entreprises les plus fortunées dans le monde ont choisi un outil ERP. Le secteur pétrolier vient en tête suivi du secteur de l'industrie chimique et pharmaceutique[3].

[2] Cette architecture a évolué vers une architecture 3-tiers : serveur de données (bases de données), serveur de traitement (applications) et utilisateurs.
[3] Etude réalisée par le cabinet PricewaterhouseCoopers sur les top 1000 entreprises, 1998.

Les ERP présentent les caractéristiques essentielles suivantes :

- Ils permettent une intégration totale des différents aspects de l'affaire
- Ils sont à fonctions multiples : devises, matières, services, produits, etc.
- Ils sont Flexibles : La totalité ou seulement certaines fonctionnalités peuvent être utilisées
- Ils permettent une large couverture du business : Planning, contrôle et traitement pour l'entité entière, couverture en cas de sites multiples
- Ils assurent une puissante gestion transactionnelle en temps réel

En outre, l'avantage des ERP est qu'ils cumulent l'expérience de quelques milliers d'entreprises et renferment ce que les spécialistes de la gestion appellent les « meilleures pratiques »[4].

Par ailleurs, il y a lieu d'indiquer que le marché des ERP est en pleine expansion. En 1998, le marché des ERP s'élève à 14,8 Milliards de dollars américains contre une prévision pour l'an 2002 s'élevant à 52 Milliards US$. Les principales raisons de cette forte progression sont :

- L'introduction de nouvelles fonctions intégrées (exemple : supply chain management, E-Business)
- L'extension vers de nouveaux secteurs : secteur public, santé, etc.
- Nouvelles cibles : (exemple : PME).

- **L'Internet : E-commerce, E-Business …**

  L'Internet a été développé en 1969 pour les scientifiques de la recherche militaire et les laboratoires de la défense comme réseaux informatiques décentralisés qui pourraient survivre à une attaque nucléaire. Peu après, les développeurs de l'Internet se sont rendus compte que son utilisation commerciale aurait un impact énorme sur notre économie mondiale.

  Il est certain qu'Internet a permis l'ouverture sur le monde à un prix réduit, et est en train de créer très rapidement un nouveau circuit de distribution, et plus encore, un nouveau modèle économique qui bouleverseront durablement la façon dont les entreprises produisent et entretiennent leurs relations avec leurs principaux partenaires économiques (clients, fournisseurs, etc.).

  Internet représente donc un véritable défi qu'aucune entreprise ne peut ignorer au risque d'être rapidement mise hors course dans une compétition désormais mondiale.

  Dans ce qui suit, nous allons décrire les deux concepts : E-commerce et E-Business.

  1. L'E- business :

  Selon une définition d'IBM, l'E-Business veut dire la transformation de processus clés à travers l'usage des technologies de l'Internet. Cette définition peut être étendue davantage pour inclure la connectivité entre l'Internet (par le Web) et la technologie de l'information d'une entité ainsi que ses différentes fonctions.

  Ainsi, l'E-Business consiste à connecter les chaînes de valeur entre les différentes entités, divisions et localités afin de vendre davantage, de se rapprocher des clients, de réduire les coûts et d'ouvrir de nouvelles voies.

  2. L'E-Commerce :

  L'E-Commerce est un sous-ensemble de l'E-Business. Plusieurs définitions ont été avancées par différentes organisations. A titre d'exemple, en 1997, l'AICPA[5] a défini l'E-commerce comme la conduite de transactions commerciales entre les individus et les organisations sur des réseaux publics ou privés. En l'an 2000, l'ISACA[6] a limité cette définition aux transactions conduites sur Internet.

[4] Traduction anglaise : « Best practices ».
[5] AICPA : « American Institute of Certified Public Accountants ».
[6] ISACA : « Information System Audit and Control Association ».

- **L'intégration Internet – ERP :**

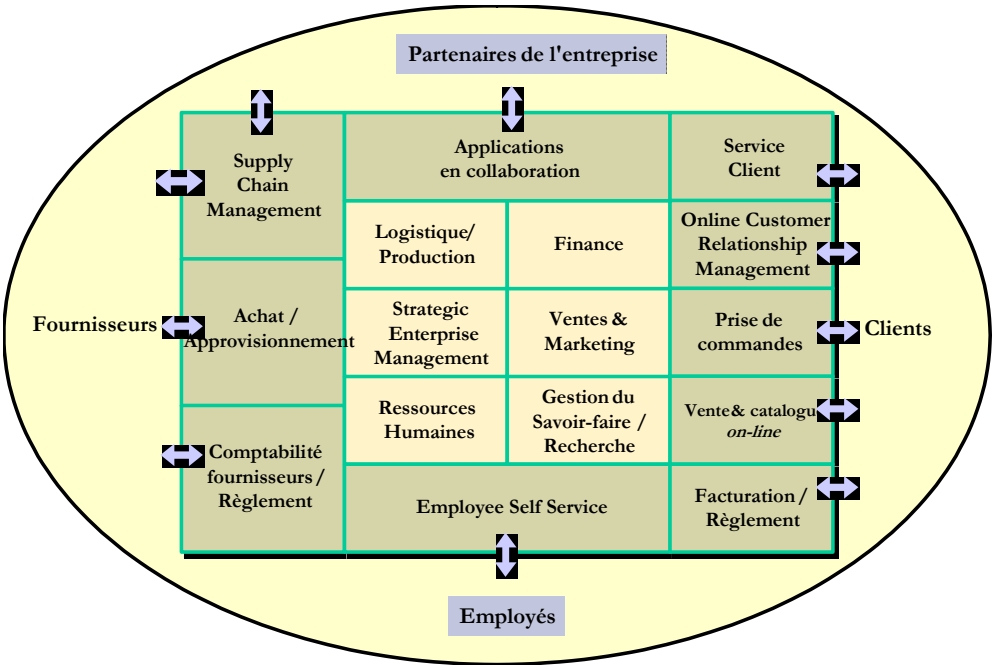
  Jusqu'à une date récente, l'ERP s'est concentré avant tout sur le système d'information interne à l'entreprise, bien qu'il ait développé des relations étroites avec l'extérieur grâce à la technologie EDI (en particulier dans le secteur de l'automobile, de la pharmacie, ...).

  Face aux enjeux et bénéfices potentiels de l'E-business, qui présupposent une intégration technique forte des systèmes d'information des partenaires (front office et back office), les ERP ont voulu sortir de leur simple image d'outil de back-office transactionnel et passer d'un système "égocentrique" à un système complètement ouvert sur l'extérieur.

  Nous citons à titre d'exemple :

  - Etendre l'accès à l'ERP à des personnes extérieures à l'entreprise et notamment les clients pour vérifier le statut de leur commande ou l'enregistrement d'un règlement sur leur compte.
  - Dans un souci d'optimisation du « supply chain »[7], les ERP ont développé des fonctionnalités de planification opérationnelle, tactique et stratégique de la chaîne logistique en combinant la puissance du système transactionnel de base, les fonctionnalités Internet et les produits et technologies novateurs.

Le schéma[8] suivant illustre l'intégration Internet – ERP :



[7] Le supply chain management (SCM) (traduction française : La gestion de la chaîne logistique) représente l'ensemble des outils et des méthodes permettant d'optimiser les flux des matières premières et des biens d'un bout à l'autre de la chaîne industrielle, c'est à dire du client le plus en aval au fournisseur le plus en amont. Il regroupe quatre domaines : La gestion des achats, la gestion de la production, la gestion de la demande et la gestion de la distribution.

[8] Schéma extrait du séminaire organisé par le cabinet PricewaterhouseCoopers (Bureau de Tunis) et la Société Tunisienne de l'Electricité et du Gaz (STEG) portant sur le thème « ERP et E-business », le 13 et 14 décembre 1999.

Chapitre 1 : Les Principaux Impacts des Nouvelles Technologies sur le Système Comptable et les Contrôles Internes de l'Entreprise

Introduction :

Le recours aux nouvelles technologies de l'information et de la communication est susceptible d'engendrer une incidence importante sur le système comptable et les contrôles internes de l'entreprise.

Il est aussi susceptible d'engendrer une incidence significative sur la gestion et la performance de l'entreprise, dont :

- l'optimisation du flux des matières premières et des biens au niveau interne de la société et en relation avec ses partenaires
- l'élargissement de son marché et l'établissement de liens directs, instantanés et intéractifs avec ses clients, ses fournisseurs, …

Toutefois, et étant donné que le présent mémoire est focalisé sur l'audit financier, nous allons nous limiter à l'étude des impacts se rattachant uniquement aux contrôles internes et au système comptable.

Parallèlement, nous examinerons les différentes catégories de risques et de pertes associés à la mise en place des nouvelles technologies et l'importance conséquente de la sécurité informatique.

Section 1 : Les caractéristiques du système comptable et des contrôles internes dans un milieu informatisé

Sous section 1 : Définitions

Avant de présenter l'impact des technologies de l'information et de la communication sur le système comptable et les contrôles internes de l'entreprise, nous avons jugé utile de rappeler la définition de ces deux derniers concepts et d'identifier quels sont les domaines susceptibles d'être affectés.

1. Le système comptable :

Selon la norme internationale d'audit ISA 400[9], « le système comptable est l'ensemble des procédures et des documents d'une entité permettant le traitement des transactions aux fins de leur enregistrement dans les comptes. Ce système identifie, rassemble, analyse, calcule, classe, enregistre, récapitule et fait la synthèse des transactions et autres événements ». Ainsi, il s'agit d'un système chargé de traduire les opérations liées à l'activité de l'entreprise en données financières.

Avec les nouvelles technologies de l'information et de la communication, et l'intégration des fonctions traitant les opérations et les informations depuis leur source jusqu'à leur enregistrement dans les états financiers, il n'est pas toujours facile de faire la distinction entre le système comptable et les systèmes qui traitent d'autres informations. Ainsi, un système de traitement des achats et comptes fournisseurs traite aussi bien des informations comptables que des informations portant sur d'autres aspects des activités (exemple : les quantités optimales à commander).

[9] ISA 400 : « Evaluation du risque et contrôle interne » (Risk Assessment and Internal Control) ; IFAC.

2. Le système de contrôle interne :

Le contrôle interne dans le sens traditionnel a eu un intérêt direct sur les contrôles internes se rattachant à la fonction financière et comptable. Les questions d'ordre financier étaient la principale inquiétude aussi bien des financiers de l'entreprise que de leur auditeur externe. Les activités opérationnelles clefs étaient omises par la plupart des acteurs de l'entreprise.

Pour faire face à cette situation, une étude a été lancée par le « Committee of Sponsoring Organizations », comité connu sous le nom « COSO » et englobant plusieurs organisations dont l'AICPA, IIA[10] et AAA[11].

Ce comité a redéfini le contrôle interne 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 suivants :

- Réalisation et optimisation des opérations
- Protection des actifs
- Fiabilité des informations financières
- Conformité aux lois, réglementation et directives de l'organisation ».

Il convient d'indiquer que cette définition a été adoptée par le Nouveau Système Comptable Tunisien. Elle implique que le système comptable fait partie intégrante du système de contrôle interne.

Les composants du système de contrôle interne comprennent :

- l'environnement de contrôle : Ceci englobe 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 : C'est développer et communiquer l'information à temps et dans une forme permettant aux différents intervenants de comprendre et d'assurer leurs responsabilités
- la direction (monitoring) : C'est une activité continue afin d'assurer que les procédures fonctionnent comme convenu.

Ces composants opèrent à travers l'ensemble des aspects de l'organisation. En outre, étant donné qu'ils 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 de l'organisation.

Par ailleurs, dans le cadre d'un audit financier, il est évident que les objectifs et les composants du contrôle interne précités ne sont pas tous pertinents. Ainsi, dans ce qui suit, nous allons focaliser uniquement sur les aspects importants pour l'audit financier et susceptibles d'être significativement affectés par les nouvelles technologies de l'information et de la communication.

Sous section 2 : La structure organisationnelle

L'informatisation croissante des entreprises a des impacts plus ou moins significatifs sur la structure organisationnelle de la société. Les principaux se résument dans ce qui suit :

1. L'organisation générale de la société :

La mise en place des nouvelles technologies de l'information et de la communication engendre des changements importants rattachés au flux des informations et à l'accès aux données. On assiste, désormais, à des centres de décision moins centralisés, à des utilisateurs finaux plus concernés par les nouvelles évolutions, à une implication et à une appropriation des systèmes par le "senior management" et à une augmentation du nombre de personnes accédant à l'information. Par ailleurs, l'informatisation peut engendrer une redéfinition des responsabilités des employés.

[10] IIA : Institute of Internal Auditors
[11] AAA : American Accounting Association

Toutefois, il y a lieu de préciser que vu la complexité de plus en plus importante des nouvelles technologies de l'information et de la communication, la maîtrise convenable de l'outil informatique dans son sens large, c'est à dire l'interdépendance entre la source des données, leur mode de traitement, leur sortie et leur utilisation, est limitée à un nombre de personnel très réduit. Ces personnes connaissent normalement un nombre suffisant de faiblesses de contrôle interne pour modifier les programmes, les données, leur traitement et leur conservation.

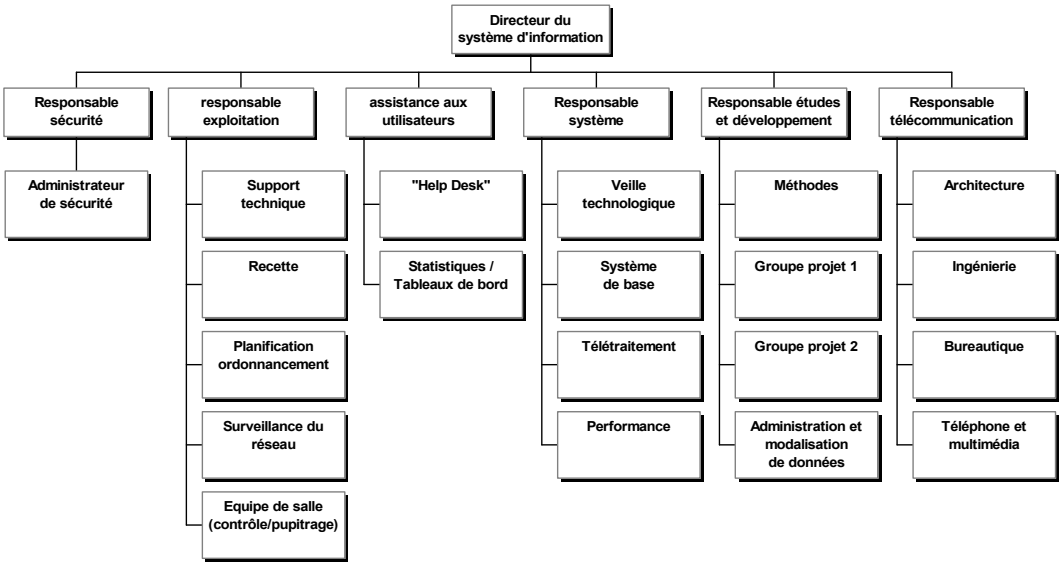
2. L'organisation du service informatique :

La structure organisationnelle du service informatique couvre deux aspects : (a) la place de la fonction dans la structure globale de l'entreprise et (b) la structure interne du service informatique.

Ces deux volets dépendent de l'importance des traitements informatiques, du nombre de personnes employées dans le service et des techniques de contrôle utilisées.

Ci-après, un organigramme d'une direction informatique importante :

3. L'externalisation du système d'information :



Certaines entreprises externalisent leur système d'information en le confiant à un tiers chargé d'assurer sa gestion et son exploitation. Il existe une multitude de formules possibles.

D'après les chiffres parus dans le journal « les Echos »[12], l'externalisation des technologies de l'information représentait sur le plan mondial un marché de 100 milliards de dollars en 1998, et passerait à 120 milliards de dollars en 2002 et 150 milliards de dollars en 2004.

Par ailleurs, et toujours selon la même référence, une étude récente montre que le quart des entreprises qui externalisent leurs technologies de l'information et de la communication rencontrent des difficultés sérieuses. Les coûts cachés et la crédibilité du prestataire restent les principaux risques de l'externalisation.

Parmi les principaux avantages et inconvénients de l'externalisation, nous citons :

Avantages :

- L'amélioration de la performance
- La réduction de la gestion du système d'information
- La mise en œuvre plus rapide de systèmes
- La limitation des dépenses
- Un meilleur contrôle sur l'activité principale
- Une plus grande expertise en système d'information

[12] Leslie Willcocks et Chris Sauer, « Externaliser les technologies de l'information », Les Echos, jeudi 2 Novembre 2000.

Inconvénients :

- Des coûts dépassant les attentes
- La perte de l'expertise interne en système d'information
- La perte de contrôle sur le Système d'Information
- La faillite du prestataire
- L'accès limité au produit
- La difficulté de renverser ou de changer les dispositions externalisées.

4. La séparation des tâches incompatibles :

La séparation des tâches incompatibles est parfois plus difficile dans un milieu informatisé en raison, essentiellement, des facteurs suivants :

- Réduction du nombre de personnes intervenantes, auparavant, dans le traitement manuel des opérations contre une augmentation du staff informatique centralisant, généralement, de nombreux aspects des systèmes.
- Les informations comptables et de gestion et les programmes d'application de l'entreprise sont stockés sur des mémoires électroniques et accessibles à beaucoup de personnes au 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 visibles.
- Quand le service informatique est important, il est en général plus facile de séparer les tâches incompatibles. Toutefois, dans les entreprises de taille moyenne, la formalisation des tâches à l'intérieur des différentes fonctions est beaucoup moins développée que dans un service d'une taille plus importante.

Ainsi, il convient de préciser que la séparation classique des tâches dans un environnement non informatisé, n'est pas totalement efficace dans un système informatisé, mais peut être renforcée par différents types de logiciels destinés à limiter l'accès aux applications et aux fichiers. Il est donc nécessaire d'apprécier les contrôles portant sur l'accès aux informations afin de savoir si la ségrégation des tâches incompatibles a été correctement renforcée.

Pour les petites entreprises, il est difficile de mettre en place une séparation convenable des tâches. Toutefois, l'implication plus importante de la direction peut compenser cette déficience.

Signalons qu'au regard du système informatique, il existe trois types d'utilisateurs :

1. Les utilisateurs non autorisés : Il s'agit des intrus externes comme par exemple : les pirates des systèmes (hackers) et les anciens employés. Des contrôles préventifs, particulièrement des contrôles d'authentification des utilisateurs, répondent à ce type de risque. Des contrôles détectifs complémentaires permettent de révéler les éventuels accès réussis.
2. Les utilisateurs enregistrés : L'accès de ces utilisateurs devrait être limité aux applications et aux données rattachées à leurs fonctions. Des contrôles préventifs pour ce type d'utilisateurs se présentent sous forme de contrôle d'authentification des utilisateurs et d'allocations de droits limités aux applications nécessaires à l'exécution de leurs tâches.
3. Les utilisateurs privilégiés : Il s'agit de l'administrateur système, les développeurs, les responsables de l'exploitation. Ces utilisateurs nécessitent des privilèges de système ou de sécurité pour la réalisation de leurs travaux.

Bien que les organisations aient besoin de confier les clefs de leur royaume à quelqu'un, c'est tout de même important de rappeler que le privilège et le contrôle ne doivent pas être mutuellement exclusifs. Les privilèges doivent être assignés avec la mise en place de contrôles afin de s'assurer que ces privilèges ne sont pas abusés. Les contrôles détectifs, tels que l'examen des événements de la sécurité et des changements de statut, sont nécessaires pour répondre aux abus potentiels de privilèges spéciaux.

Par ailleurs, à l'intérieur du département informatique, si les fonctions incompatibles ne sont pas correctement séparées, des erreurs ou irrégularités peuvent se produire et ne pas être découvertes

dans le cours normal de l'activité. Des changements non autorisés dans des programmes d'application ou dans des fichiers peuvent être difficiles à détecter dans un environnement informatique. C'est pourquoi, des mesures préventives touchant en particulier le respect de la séparation des fonctions principales de programmation et d'exploitation deviennent indispensables pour assurer la fiabilité de l'information financière. A titre indicatif, les dispositions suivantes devraient être respectées :

- Interdiction aux analystes fonctionnels et programmeurs de mettre en marche le système et de l'exploiter
- Interdiction aux programmeurs d'accéder aux environnements de production
- Interdiction aux opérateurs d'effectuer des modifications de programmes ou de données

Dans les départements informatiques plus petits, là où la séparation des tâches n'est pas possible, la capacité à éviter toute opération non autorisée à l'intérieur du département informatique est diminuée. Dans ce cas, les contrôles de compensation deviennent particulièrement importants. Ces contrôles compensatoires peuvent être des contrôles puissants lors de la saisie des données, un traitement correct et complet exercé par les départements utilisateurs et une forte supervision de l'exploitation en cours.

Sous section 3 : La nature des traitements

Les nouvelles technologies de l'information et de la communication influencent sur la manière avec laquelle les transactions sont traitées. Le traitement inclut des fonctions telles que la validation, le calcul, la mesure, l'évaluation, la synthétisation et la réconciliation.

Il est clair que l'ordinateur applique le même traitement à toutes les opérations similaires en utilisant les mêmes instructions. Ainsi, les systèmes informatisés exécutent leurs fonctions exactement selon le programme et sont, en théorie, plus fiables que les systèmes manuels.

1. Les types de traitement :

Il existe plusieurs types de traitements. Les plus communément utilisés sont :

- Traitement en temps réel (real time processing) : Les différentes transactions sont saisies sur les terminaux, puis validées et utilisées pour mettre à jour immédiatement les fichiers informatiques. Ainsi, les résultats du traitement sont immédiatement disponibles pour toute interrogation ou génération d'état.
- Traitement par lot (batch processing): Les transactions sont saisies sur un terminal puis soumises à certains contrôles de validation et ajoutées à un fichier transactions contenant les autres transactions de la période. Selon une périodicité définie, le fichier des transactions mettra à jour le fichier maître correspondant.
- Mise à jour mémorisée (memo update) : C'est une association du traitement en temps réel et du traitement par lot. En effet, les transactions mettent immédiatement à jour un fichier mémo qui contient les informations extraites de la dernière version du fichier maître. Ultérieurement, le fichier maître sera mis à jour par un traitement par lot.
- Traitement par extraction ou par chargement de données (downloading / uploading processing) : Ceci consiste à transférer les données du fichier maître à un terminal intelligent pour traitement ultérieur par l'utilisateur. Le résultat du traitement sera ensuite rechargé sur l'ordinateur central du siège.

De nos jours, la majorité des systèmes opérationnels sont des systèmes à temps réel. Les transactions sont traitées une fois produites, les informations sont mises à jour immédiatement et les données figurant sur les fichiers sont changées avec les données de la nouvelle transaction.

Toutefois, il convient de noter que certains systèmes continuent à utiliser le système de traitement par lot. Dans ce système, les saisies s'opèrent quotidiennement, tandis que la mise à jour des fichiers se fait la nuit ou à une date spécifiée (lors de l'absence de transactions).

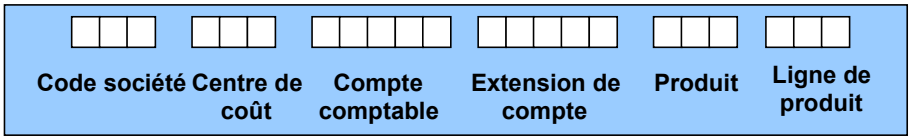
2. La clé comptable :

Dans la plupart des progiciels intégrés (ERP), c'est la clé comptable qui représente l'identifiant portant l'ensemble des imputations utiles à la bonne analyse de l'activité de l'entreprise. Elle doit permettre l'enregistrement de toutes les informations significatives pour la comptabilité de l'entreprise.

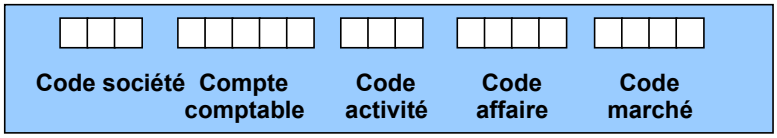
Pour cela, elle contient autant d'axes d'analyse que nécessaire : analyse par nature, par destination, par rubrique budgétaire, par produit, par projet, par zone géographique, etc.

Par ailleurs, la clé comptable est composée d'une succession de segments indépendants. Selon les progiciels, elle peut être unique et imposée pour tous les mouvements (tous les segments déclarés doivent être renseignés) ou flexible (le nombre de segments étant variable et la signification du segment pouvant être différente selon l'événement géré).

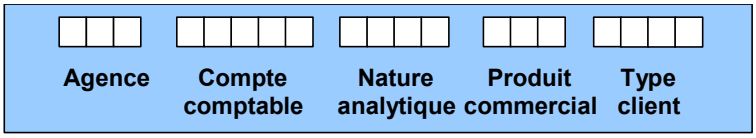
Exemple de clé comptable d'une entreprise industrielle :



Exemple de clé comptable d'une entreprise de service :



Exemple de clé comptable d'une banque :



3. La génération automatique des écritures comptables :

La génération automatique des écritures comptables représente l'une des importantes évolutions. En effet, les nouvelles technologies offrent la possibilité de paramétrer des règles de traduction automatique des opérations en écritures comptables.

Exemple 1 : Suite à l'édition d'une facture de vente, le système débite automatiquement le compte client correspondant et crédite les comptes appropriés de vente et de TVA.

Exemple 2 : Des intérêts peuvent être calculés et débités automatiquement sur les comptes clients sur la base des conditions préalablement définies dans le programme informatique.

Sous section 4 : Les aspects de conception et des procédures

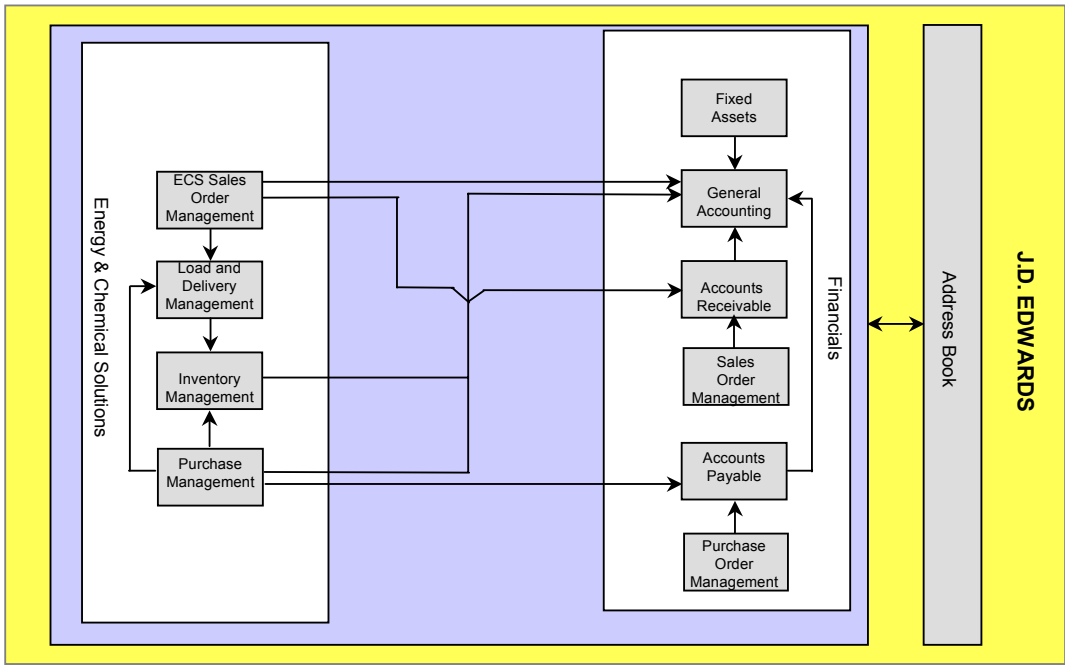
1. L'intégration des systèmes :

Les systèmes opérationnels englobent, de plus en plus, une variété d'applications en interface qui étaient auparavant séparées et qui engendraient des ressaisis des données d'une application à l'autre. Avec les nouvelles technologies de l'information et de la communication, l'intégration des systèmes opérationnels et des systèmes financiers et comptables est devenue une réalité.

Certes, cette intégration a permis aux entreprises de tirer de nombreux bénéfices comme la cohérence des modes de fonctionnement, la réduction des délais (délais de clôture, délai de livraison….), l'unicité de l'information de référence (référentiels uniques et partagés entre les différentes fonctions) et la cohérence de l'information dans toute l'entreprise.

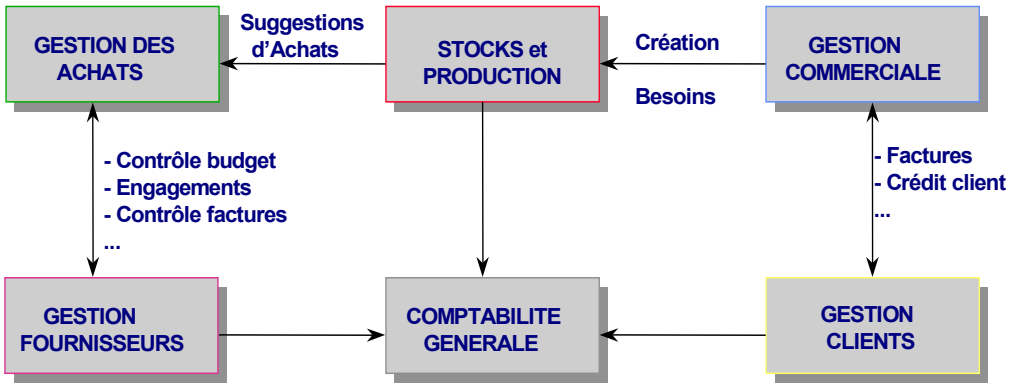
En outre, avec Internet, nous assistons à une intégration des chaînes de valeur des partenaires économiques. Internet permet, par exemple, au fournisseur d'accéder au plan de fabrication de son client et au client de transmettre aux fournisseurs ses prévisions commerciales facilitant ainsi la planification de la fabrication et des approvisionnements.

Le schéma, qui suit, montre l'intégration des modules de l'ERP « JDEdwards » installé dans une entreprise pétrolière en Tunisie.



Il convient de signaler que l'intégration suppose, généralement, l'existence de dictionnaire de données commun à toutes les entités de l'entreprise couvrant l'ensemble des domaines fonctionnels et partagé par les différents utilisateurs. A titre d'exemple, au niveau de JDEdwards, c'est l' « Address Book » qui centralise toutes les données se rapportant aux clients, fournisseurs, personnels, banques, etc.

L'intégration des modules peut être schématisée comme suit :



2. *La génération automatique des transactions :*

Il s'agit d'une programmation des systèmes pour générer des données ou initier une transaction. Cette génération peut se faire selon les façons suivantes :

1. Le traitement d'une transaction peut créer les conditions de génération d'une autre transaction : exemple : la constatation d'une vente peut réduire les stocks disponibles au-dessous du stock minimum. Ainsi, un bon de commande automatique peut être édité. Cela suppose l'existence d'un fichier permanent définissant les stocks minimums.
2. Un signal pour initier d'autres transactions peut être saisi : exemple : la saisie de l'avancement de la production d'un ordre de fabrication génère les charges dans le stock des travaux en cours.

3. Les types de données et de procédures :

A titre de rappel, dans un milieu informatisé, nous distinguons quatre éléments de traitement fondamentaux ayant des impacts plus ou moins importants sur la préparation d'une information financière fiable :

- Les données de transaction : Les données de transaction sont des données spécifiques à chaque transaction. Les erreurs se limitent à la seule transaction et ont, par conséquent, un impact limité.
- Les données permanentes ou semi-permanentes : Ces données sont utilisées lors du traitement des transactions mais ne sont pas spécifiques aux transactions individuelles. Ainsi, une erreur survenue dans ce type de données peut affecter plusieurs transactions se rattachant à cette donnée.
- Les procédures programmées (ou automatisées) : Il s'agit des procédures intégrées dans le software et/ou le hardware. Les erreurs de programmes affectent toutes les transactions et les données permanentes traitées.
- Les procédures manuelles : Ces procédures sont essentielles pour la préparation, le traitement et le suivi des résultats de traitement. Si le système crée des rapports d'exception, une personne devrait enquêter et corriger les conditions d'exception.

4. La dématérialisation des transactions et de la preuve :

La conception des systèmes fait que les procédures informatiques laissent moins de traces matérielles que les procédures manuelles. A titre d'exemple :

- Absence de justificatifs de certaines données saisies : Des données peuvent être introduites dans le système informatique sans documents justificatifs. De plus, les autorisations écrites de saisie des données sont remplacées par d'autres procédures intégrées aux programmes informatiques.
- Absence d'un système de références visibles : Les données sont de plus en plus gérées uniquement sur support informatique engendrant, ainsi, une difficulté de suivre une opération à travers les pièces justificatives correspondantes. En outre, les traces des transactions peuvent n'être que partiellement disponibles sur des supports lisibles par ordinateur et/ou peuvent avoir une durée de conservation limitée dans le temps.
- Absence de documents de sortie visibles : Dans certains systèmes, le résultat du traitement peut ne pas être imprimé ou l'être sous forme de résumé seulement (un état peut ne comporter que des totaux récapitulatifs, tandis que les détails des mouvements sont conservés en fichiers). De nos jours, la première situation reste rare, tandis que la seconde est assez fréquente.

  En raison de l'absence de documents de sortie visibles, il est parfois nécessaire de se reporter aux données conservées dans des fichiers exploitables seulement par ordinateur.

Sous section 5 : Les aspects des contrôles

Comme les organisations s'orientent de plus en plus vers un modèle de contrôle interne basé sur les risques, conforme à l'approche du COSO (Committee of Sponsoring Organizations), la mise en œuvre du contrôle interne dans les environnements informatisés continue à évoluer. Comme les systèmes informatiques deviennent de plus en plus complexes et intégrés, souvent par Internet, les difficultés de fournir des contrôles appropriés deviennent de plus en plus ressenties.

Les activités de contrôles englobent généralement une combinaison des procédures de contrôles programmés qui permettent la génération de rapports (exemple : les rapports d'exception) et des procédures manuelles de suivi et d'investigation des éléments figurants sur ces rapports. Ces deux opérations sont nécessaires pour aboutir aux objectifs de contrôle. En effet, s'il n'existe aucune personne qui fait le suivi des rapports prévus par le système, on peut dire qu'il n'y a pas de contrôle.

Le mix de ces contrôles dépend de la nature et de la complexité de la technologie utilisée. La croissance de la vitesse et de la capacité en mémoire a permis de mettre en place plus de procédures de contrôle intégrées dans le hardware et/ou dans le software que par le passé.

Outre les contrôles directs, les contrôles généraux informatiques sont nécessaires pour assurer l'intégrité des ressources d'information et pour garantir que les procédures de contrôles programmés (ainsi que les procédures comptables programmées) sont correctement mises en place et sont

opérationnelles et qu'uniquement les changements autorisés sont opérés sur les programmes et sur les données. Par exemple, à défaut de contrôles généraux informatiques appropriés, il n'y a aucune assurance que les rapports d'exception soient exacts et exhaustifs.

1. Les contrôles généraux informatiques :

Les contrôles généraux informatiques se rattachent à la fonction informatique et 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 contrôle interne sont atteints »[13].

Les qualités attendues d'un bon contrôle interne de la fonction informatique sont : la fiabilité des informations produites, la protection du patrimoine et la sécurité et la continuité des travaux.

Par ailleurs, les contrôles généraux informatiques portent sur plus d'une application et leur mise en œuvre est essentielle pour assurer l'efficacité des contrôles directs.

Ils touchent, essentiellement, les domaines suivants :

- L'organisation et la gestion
- La maintenance des programmes
- L'exploitation
- Le développement et la modification des programmes
- La sécurité (sauvegarde, plan de secours, etc.)

Ces contrôles peuvent être divisés en quatre catégories :

- La sécurité des systèmes : Il s'agit des procédures et des mécanismes en place destinés à s'assurer que l'accès à l'environnement informatique et aux programmes et données (physiques et logiques) est convenablement contrôlé.
- La sécurité de l'exploitation : Ce sont des contrôles permettant de s'assurer que les données sont traitées dans les bons fichiers, que les éléments rejetés sont convenablement identifiés et corrigés et que les programmes sont correctement mis en place et exécutés.
- La maintenance des applications informatiques : Ce sont les contrôles permettant de s'assurer que les changements dans les programmes informatiques sont autorisés, correctement conçus et effectivement mis en place.
- Le développement et la modification des applications : Ce sont les contrôles sur les nouvelles applications ou sur les modifications significatives des applications existantes permettant de s'assurer que les procédures programmées sont convenablement conçues et correctement mises en place.

2. Les contrôles directs :

Les contrôles directs sont des contrôles conçus pour prévenir ou détecter les erreurs et les irrégularités pouvant avoir un impact sur les états financiers.

On distingue trois catégories de contrôles directs :

1.1. Les contrôles d'application :

Les contrôles d'application sont des contrôles permettant de s'assurer que toutes les opérations sont autorisées, enregistrées, et traitées de façon exhaustive, correcte et dans les délais. Ces contrôles peuvent être défalqués en :

- Contrôles portant sur les données d'entrée : Ces contrôles visent à fournir une assurance raisonnable que toutes les transactions sont dûment autorisées avant d'être traitées et qu'elles ne sont pas perdues, ajoutées, dupliquées ou indûment modifiées. Ils visent aussi à assurer que les transactions incorrectes sont rejetées, corrigées et, si nécessaire, soumises en temps voulu à un nouveau traitement.
- Contrôles sur les traitements et les fichiers de données informatisés : Ces contrôles visent à fournir une assurance raisonnable que les transactions, y compris celles générées par le système, sont correctement traitées par l'ordinateur et qu'elles ne sont pas perdues, ajoutées, dupliquées ou indûment modifiées. Ils visent, aussi, à assurer que les erreurs de traitement sont détectées et corrigées en temps opportun.

[13] IAPS 1008 : « Evaluation du risque et contrôle interne : caractéristiques et considérations sur l'informatique », IFAC.

- Contrôles sur la production des résultats : Ces contrôles visent à fournir une assurance raisonnable que les résultats des traitements sont exacts, que l'accès aux informations produites est limité aux personnes autorisées et que ces informations sont communiquées aux personnes autorisées en temps voulu.

Avec les nouvelles technologies, beaucoup de contrôles, auparavant manuels assurés par le personnel informatique, par les utilisateurs du système ou par un groupe de contrôle indépendant, sont dés lors réalisés par ordinateur.

Exemple 1 : Les logiciels de l'E-Business incluent, généralement, des contrôles pour prévenir la répudiation ou la modification des enregistrements qui initient les transactions. Ces contrôles peuvent être une signature électronique et des certificats du serveur qui authentifient les parties de la transaction.

Exemple 2 : L'autorisation de l'entrée peut être assurée par des contrôles programmés d'autorisation (par exemple : approbation d'une commande qui ne dépasse pas le plafond de crédit consenti pour un client donné).

Une fonction de traitement informatisée peut constituer un contrôle clef si elle effectue un aspect essentiel du traitement des opérations de la société et des informations s'y rapportant.

Toutefois, il est à noter qu'il n'est pas toujours facile d'établir une distinction claire entre les contrôles et les fonctions intégrées. Certains traitements, comme l'édition, la validation ou la comparaison participent, en effet, au contrôle interne puisqu'ils servent à prévenir ou à détecter les erreurs ou irrégularités. D'autres comme l'enregistrement, le calcul et l'addition ne sont pas des contrôles à proprement parler, puisqu'ils n'ont pas pour but la prévention ni la détection des erreurs et irrégularités, mais sont des fonctions de base pour le système d'information pouvant affecter directement les états financiers.

Par ailleurs, dans un milieu informatisé, les contrôles se basent, de plus en plus, sur des rapports informatiques (intitulés : rapports d'exception ou logs d'audit) qui sont, généralement, suffisamment détaillés pour faire ressortir les opérations inhabituelles ou anormalement importantes ainsi que d'autres problèmes éventuels. Ils sont établis en temps voulu selon une présentation qui souligne les points importants et facilite leur compréhension.

Ces opérations, mises en valeur dans les rapports d'exception, peuvent être soient acceptées par le système, enregistrées dans un fichier d'attente ou rejetées par le système.

Mais pour l'efficacité de ce contrôle, encore faut-il que ces rapports soient convenablement conçus, paramètrés et contrôlés manuellement. Exemple : La chaîne fournisseurs peut éditer une liste des bons de réception manquants, que l'on examinera afin de savoir pourquoi ces bons n'existent pas. En outre, ce contrôle n'est efficace que si la liste sortie de l'ordinateur est exhaustive et fiable.

1.2. Les contrôles de direction :

Ces contrôles, qui portent sur des informations finales, sont réalisés à posteriori par des personnes indépendantes du processus de traitement. Leur but est de détecter des erreurs ou irrégularités susceptibles de s'être produites en amont.

Le système informatique peut offrir à la direction plusieurs informations utiles au pilotage de l'entité et une palette d'outils analytiques permettant d'examiner et de superviser ses activités.

Les contrôles de direction peuvent consister en la revue et le suivi des rapports d'exception sur les opérations et les soldes anormaux et des résumés des opérations traitées, en la vérification de la séquence des opérations traitées, etc.

1.3. Les contrôles visant à protéger les actifs :

Ces contrôles consistent en des mesures de contrôle et de sécurité assurant un accès limité aux personnes expressément autorisées et dans la limite de leurs responsabilités. Ils doivent aussi apporter la garantie que les actifs de la société sont à l'abri de toute création de documents qui en autoriseraient l'utilisation ou la cession.

Sous le terme « actifs », nous entendons aussi bien les actifs inscrits dans les comptes que les informations confidentielles ou non contenues dans les fichiers informatiques.

Il est évident que les contrôles visant à protéger les actifs sont encore plus nécessaires si ces actifs sont confidentiels, aisément transportables, convoités et/ou de valeur importante.

Section 2 : Les différentes catégories des risques et des pertes informatiques dans un milieu informatisé :

L'évolution des technologies de l'information et de la communication engendre pour l'entreprise une panoplie de risques informatiques qu'elle est appelée à maîtriser.

Hormis les simples vols, les documents financiers peuvent être modifiés et des transactions illicites peuvent être engagées au nom de l'entreprise sans son consentement. L'interception et l'abus d'utilisation des cartes de crédit ou des informations bancaires compromettent les intérêts du client de l'entreprise. Des documents confidentiels peuvent être divulgués au public ou aux concurrents de l'entreprise. Les droits d'auteurs, les marques et les brevets peuvent être violés. Mais aussi, bien d'autres dommages peuvent toucher la réputation et la notoriété de l'entreprise.

Ces risques peuvent engendrer des pertes que l'on mesure, soit quantitativement par le montant des pertes, soit de façon qualitative.

Sous section 1 : Les catégories des risques informatiques

Les risques informatiques sont de plusieurs ordres. Nous citons :

- Les risques stratégiques : Le sous emploi ou l'incapacité de suivre le rythme de mise en place des nouvelles technologies de l'information et de la communication peut faire qu'une entreprise s'exclue d'elle-même du groupe de partenaires que constitue son milieu professionnel concurrentiel.
- Les risques techniques : Ces risques englobent les risques associés à la fonction informatique ainsi que ceux rattachés aux applications.
- Les risques juridiques : Ces risques se rapportent au non respect de la réglementation en vigueur (juridique, comptable et fiscale), tel que le piratage des logiciels.

  En outre, il convient de préciser à ce niveau que la nouvelle technologie de l'Internet n'a pas encore ses propres lois ni de précédents juridiques à grande échelle. En fait, l'une des principales sources de risque est le trop grand nombre de lois régissant l'activité en ligne. Le danger pour tout site marchand est donc d'enfreindre par inadvertance la législation établie du pays où il vend ses produits ou services.

Pour l'audit financier, nous sommes intéressés, principalement, par les deux derniers risques à savoir les risques techniques et les risques juridiques. Nous traitons, dans ce qui suit, les risques techniques. Les risques juridiques feront l'objet d'une étude spécifique au niveau du chapitre 3 de la présente partie.

1. Les composants des risques techniques :

Les risques techniques se divisent en :

1.1. Risques associés à la fonction informatique :

Dans un milieu informatisé, les principaux risques associés à la fonction informatique sont :

a) L'organisation et les procédures d'exploitation du département informatique peuvent ne pas constituer un environnement de traitement favorable à la préparation d'informations financières fiables.

b) Les programmeurs peuvent modifier de façon erronée ou non autorisée les logiciels d'application, réduisant ainsi la fiabilité des informations financières traitées par le système.

c) Des personnes non autorisées (employés ou personnel extérieur) peuvent accéder directement aux fichiers ou programmes d'application utilisés pour le traitement des transactions et y apporter des modifications non autorisées.

En outre, avec les nouvelles technologies de l'information et de la communication, les systèmes informatiques constituent, de plus en plus, une fenêtre ouverte dans laquelle peuvent s'engouffrer des flux perturbateurs. L'entreprise qui ne maîtriserait pas ce nouveau contexte peut se rendre perméable aux intrusions et recevra, par conséquent, des flux indésirables dont le traitement correctif non anticipé reste manuel et coûteux.

En effet, au cours de la communication et la réalisation d'affaires sur Internet, les consommateurs et l'entreprise doivent envoyer et recevoir des informations réciproques. Les informations fournies sont susceptibles à des accès non autorisés lors de la transmission sur Internet et pendant qu'elles sont stockées sur le système informatique de la partie réceptionnaire.

Par ailleurs, les télétransmissions, sur lesquelles se basent les nouvelles technologies, présentent elles-mêmes des risques :

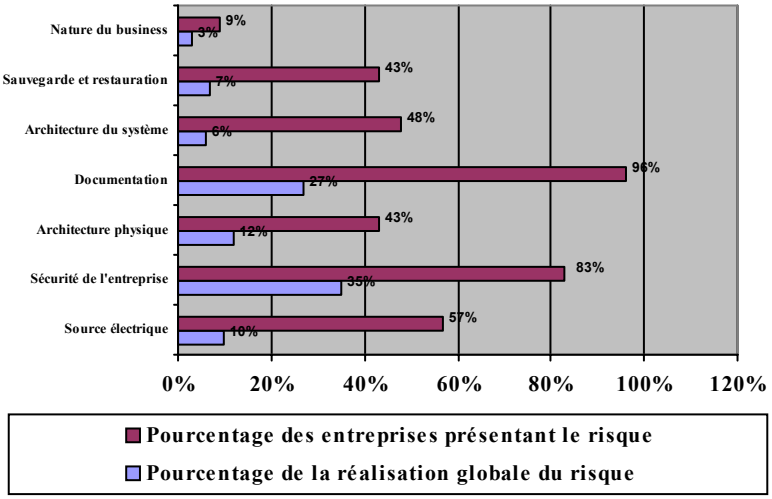
- le recours à des spécialistes hautement qualifiés sur lesquels un contrôle n'est pas aisé et qui ont parfois des autorisations d'accès étendues ;
- la complexité technique, une caractéristique des télécommunications, fragilise les systèmes qui en font un usage exclusif ;

Une étude portant sur les origines des risques les plus significatifs touchant la fonction informatique a été menée en se basant sur les résultats d'audit effectués auprès de 23 sociétés[14].

Il y avait 256 constats générés de cet audit. Ces constats ont être groupés en sept catégories de risque, à savoir :

- Source électrique : Non fiabilité de la source électrique et absence de solutions en cas de sa rupture ou de son insuffisance ;
- Sécurité de l'entreprise : Sécurité physique et logique insuffisantes et absence de protection contre toute forme d'intervention humaine intentionnelle ou inattentive ;
- Architecture physique : Architecture inadéquate et non pratique du bâtiment abritant le matériel informatique : difficulté d'accès, absence de moyens de détection des incendies, etc. ;
- Documentation : Absence d'une documentation convenable et à jour et absence d'une procédure de mise à jour adéquate ;
- Architecture du système : Ceci englobe les insuffisances dues à l'âge, au type et à la configuration des ressources informatiques ;
- Sauvegarde et restauration des données : Ceci englobe toutes les insuffisances rattachées aux procédures de gestion de la sauvegarde et de la restauration des données ;
- Nature du business : Il s'agit des risques associés à la nature de l'activité de l'entreprise auditée qui se répercutent sur la fonction informatique ;

Les résultats de cette étude se présentent comme suit :



Ainsi, il ressort de cette étude que le principal pourcentage de risque se situe au niveau de la sécurité de l'entreprise (35%). Un pourcentage important des entreprises présente ce risque (83%).

[14] Extrait de l'ouvrage : « Handbook of Information Technology Auditing », D 6-08 ; Coopers & Lybrand 1997.

L'absence d'une documentation convenable et à jour et l'absence d'une procédure de mise à jour adéquate constituent aussi un risque important (27%). La quasi-totalité des entreprises présentent ce risque (96%).

1.2. Risques liés aux applications :

Les principaux risques liés aux applications peuvent se résumer comme suit :

a) Des personnes non autorisées peuvent avoir accès aux fonctions de traitement des programmes d'application et peuvent, ainsi, effectuer des opérations de lecture, d'altération, d'ajout ou de suppression d'informations des fichiers de données, ou de saisies de transactions non autorisées. Ceci peut conduire à des erreurs ou irrégularités pouvant fort bien demeurer cachées.

   Ce risque est similaire à celui provenant d'une mauvaise séparation des tâches ou à l'exercice de tâches incompatibles. Il concerne la possibilité d'accès non autorisé aux fonctions de traitement des programmes d'application par des procédures normales de déclenchement d'autorisation et d'enregistrement de transactions et ce, contrairement au risque que des personnes non autorisées accèdent directement à des informations mémorisées ou à des programmes d'application utilisés au travers de logiciels système, par des moyens de télécommunication, programmes utilitaires ou autres sources informatisées. Ce dernier risque est évoqué dans le paragraphe « risques associés à la fonction informatique ».

b) Les transactions et données permanentes introduites pour traitement peuvent être inexactes, incomplètes ou saisies plusieurs fois.

c) Les données rejetées ou en suspens peuvent ne pas être identifiées, analysées et rectifiées.

d) Des transactions valides saisies pour traitement ou générées par le système peuvent se perdre, être incorrectement ou incomplètement traitées ou imputées, ou bien encore traitées ou imputées à une mauvaise période comptable.

   Exemple, les transactions traitées par le commerce électronique sont susceptibles d'être perdues, traitées doublement ou d'une façon erronée. Ainsi, si une commande est envoyée par Internet d'une entreprise à une autre sans l'existence de contrôles d'intégrité appropriés, l'acheteur peut ne pas recevoir les marchandises commandées ou recevoir une quantité supérieure.

Ces risques sont d'autant plus importants avec l'intégration des systèmes où une seule donnée introduite dans le système peut mettre à jour automatiquement tous les renseignements correspondants. Ainsi, une erreur introduite peut engendrer une erreur dans différents fichiers et/ou bases de données.

2. Les types de risques :

Les risques peuvent être divisés en trois types : les accidents, les erreurs, et la malveillance[15].

2.1. Les accidents :

- Accidents sur les locaux : Incendie, explosion, dégâts des eaux, bris de machine, etc.
- Accidents sur les matériels : pannes, destruction, etc.
- Accidents du fait des services : électricité, télécommunication, etc.

2.2. Les erreurs :

- Erreurs de saisie, de transmission des données, et d'utilisation des informations (erreurs d'identification des documents informatiques, erreurs d'interprétation du contenu d'un document informatique, document insuffisamment contrôlé, etc.)
- Erreurs d'exploitation : exemple : destruction accidentelle d'un fichier
- Erreurs de conception et de réalisation de logiciels et procédures d'application.

2.3. La malveillance :

- Vol de matériels principaux ou accessoires
- Fraude : Utilisation non autorisée des ressources du système d'information :

[15] Selon l'ouvrage du CLUSIF (Club de la sécurité informatique français), « Evaluation des conséquences économiques des incidents et sinistres relatifs aux systèmes informatiques : France 1996 » ; Février 1997.

→ détournement de fonds,

→ détournement de biens ou services matériels ou immatériels,

→ les attaques ciblées vers une entreprise pour récupérer des informations ou modifier des dispositifs en vue d'opérer ultérieurement une autre opération malveillante

- Sabotage : Attentat, vandalisme et toute action malveillante conduisant à un sinistre matériel
- Attaque logique : Utilisation non autorisée des ressources du système d'information se traduisant, essentiellement, par une perte d'intégrité et/ou de disponibilité. Ces attaques sont de deux catégories :

  → les attaques non ciblées (les virus, etc.) qui représentent l'immense majorité des attaques en nombre, mais avec un impact modéré,

  → les attaques ciblées vers une entreprise (bombe logique, manipulation de données ou de programmes, etc.) dans le but de la paralyser au moins momentanément. Ces attaques sont très peu nombreuses, mais peuvent avoir un impact très nuisible.
- Divulgation : Utilisation non autorisée des ressources du système d'information, entraînant la divulgation à des tiers d'informations confidentielles.
- Autres : Grèves, départs individuels ou collectifs de personnels informatiques (aggravés par l'absence ou l'insuffisance de la documentation et par l'absence de rotation du personnel informatique. Ceci implique, souvent, que certaines applications ne peuvent être maintenues que par un seul informaticien), etc.

Sous section 2 : Les catégories des pertes informatiques

Les catégories des pertes informatiques sont les suivantes :

- Les dommages matériels et annexes : Ces pertes représentent les coûts de réfection ou d'acquisition de biens endommagés ou volés. Les biens concernés sont le matériel informatique, le matériel d'environnement (climatisation, onduleur, etc.), les supports magnétiques et les fournitures. Des frais annexes, pour la réfection des bâtiments et les honoraires de toutes sortes (expertise, bureau d'étude) s'ajoutent à ces coûts directs.
- Les frais supplémentaires et les pertes d'exploitation : Ces pertes sont les plus importantes et sont engendrées par tous les types de risques.

  1. Les frais supplémentaires : Ces frais correspondent aux moyens supplémentaires à mettre en œuvre suite à un sinistre informatique. Ils sont destinés à maintenir pour le système des fonctionnalités et des performances aussi proches que possible de celles qui étaient avant le sinistre. Nous citons, notamment :
     - des locaux informatiques de secours
     - des matériels informatiques de secours
     - un réseau de télétransmission de secours
     - du personnel de secours
     - des frais financiers

  2. Les pertes d'exploitation : Ce sont des pertes résultant d'une baisse temporaire ou durable de la marge brute de l'entreprise. Ces pertes correspondent, notamment, à :
     - Des pertes de chiffre d'affaires
     - Des pertes de créances ou augmentation des dettes fournisseurs
     - Des pertes de clientèle
     - Des pertes d'image de marque
- Les pertes de fonds et de biens : Ce type de perte a essentiellement pour origine la fraude et le sabotage immatériel. Les pertes de fonds correspondent à une diminution du patrimoine financier de l'entreprise soit par une diminution des comptes d'actif soit par une augmentation des comptes

de passif. Les pertes de biens consistent en des détournements de biens physiques (immobilisations et stocks). Nous citons :

- pertes de fonds ou de biens physiques,
- pertes d'informations confidentielles, de savoir-faire, etc.,
- pertes d'éléments non reconstituables du système (essentiellement données ou programmes) évalués en valeur patrimoniale.

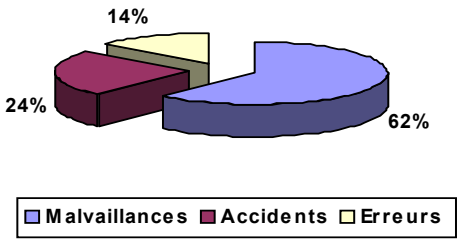
- Les autres pertes (réglementaires, déontologique, etc.) : Parmi les autres pertes, nous citons : les honoraires et les frais de justice liés à la mise en cause de la responsabilité de l'entreprise du fait des préjudices causés à autrui volontairement ou pas, la copie illicite des logiciels, etc.

Selon une étude réalisée par le CLUSIF[16], les pertes dues à des sinistres impliquant l'informatique, hors secteur gouvernemental et administration, sont évaluées, pour la France et pour l'année 1996, à 12,7 milliards de francs (environ 2,5 milliards de Dinars Tunisiens), dont :

→ 62% sont imputables à la malveillance

→ 24% sont imputables à des accidents

→ 14% sont dues à des erreurs

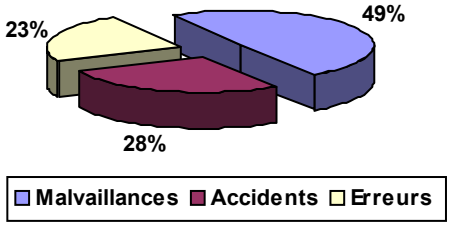


A titre de comparaison, cette étude précise que les pertes correspondantes de 1987 sont évaluées à 7,9 milliards de francs (Franc courant), soit environ 1,5 milliards de Dinars Tunisiens, dont :

→ 49% sont imputables à la malveillance

→ 28% sont imputables à des accidents

→ 23% sont dues à des erreurs



Par ailleurs et toujours selon la même étude réalisée par le CLUSIF, les pertes enregistrées en France pour l'année 1996 se détaillent comme suit :

[16] CLUSIF (Club de la sécurité informatique français), « Evaluation des conséquences économiques des incidents et sinistres relatifs aux systèmes informatiques : France 1996 », Février 1997.

Catégories	Pertes en millions de FRF	%
Dommages matériels et annexes	1.535	12,1
Frais supplémentaires et pertes d'exploitation	4.530	35,6
Pertes de fonds et de biens	2.760	21,7
Autres pertes	* 3.895	30,6
Total	**12.720**	**100**

(*) Dont 1.700 millions de Franc Français correspondent aux copies illicites.

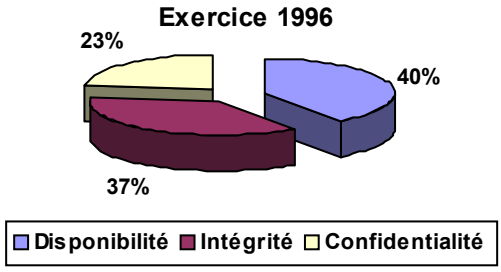
Il apparaît clairement que les frais supplémentaires et les pertes d'exploitation sont les pertes les plus importantes avec un pourcentage s'élevant à 35,6% de la totalité des pertes.

Quant aux conséquences de ces pertes, elles peuvent être regroupées en trois catégories :

- Disponibilité : c'est l'aptitude des systèmes à remplir une fonction dans des conditions prédéfinies d'horaires, de délais et de performances
- Intégrité : Propriété qui assure qu'une information n'est modifiée que par les utilisateurs habilités dans les conditions d'accès normalement prévues.
- Confidentialité : Propriété qui assure que seuls les utilisateurs habilités dans les conditions normalement prévues ont accès aux informations.

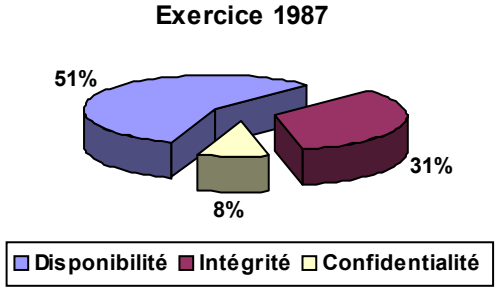
Pour l'exercice 1996, les conséquences des pertes détaillées ci-haut ont été regroupées comme suit :

- Disponibilité : 40 %
- Intégrité : 37 %
- Confidentialité : 23 %



Contre des pourcentages correspondants en 1987 de :

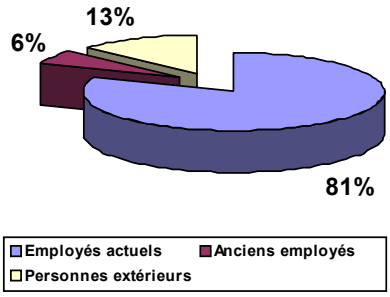
- Disponibilité : 51 %
- Intégrité : 31 %
- Confidentialité : 8 %



Il convient de préciser qu'il faut évaluer avec prudence l'évolution entre 1987 et 1996 du fait que certaines définitions ont changé depuis 1987, de l'imprécision des chiffres, de l'évolution des mentalités (diminution de la propension de non déclaration selon les catégories) et de la modification du contexte informationnel, juridique etc.

Enfin, la répartition des auteurs des sinistres, pour l'exercice 1999, se présente comme suit[17] :

- Employés actuels : 81 %
- Anciens employés : 6 %
- Personnes extérieures : 13%



Tous ces chiffres témoignent de l'importance des risques et des pertes informatiques dans un milieu informatisé. Le chef d'entreprise doit être conscient de l'importance, sans cesse croissante, de l'enjeu informatique.

Section 3 : La sécurité des informations et des communications dans un milieu informatisé

Les nouvelles technologies de l'information et de la communication constituent un facteur essentiel d'accroissement de la compétitivité et sont porteuses de bénéfices. Néanmoins, les conséquences peuvent être catastrophiques si l'entreprise ne s'y conduit pas correctement en matière de sécurité.

Cette dernière est devenue un sujet particulièrement médiatisé. On relaye largement les incidents et actes illicites touchant la sécurité des systèmes d'information, dont à titre d'exemple : le virus "I Love You" en mars 2000, les fraudes à la carte bancaire sur Internet, etc.

Parallèlement, la sécurité des informations et des communications est devenue de plus en plus complexe.

A titre d'exemple, pour sécuriser un environnement « Client / Serveur », il faut identifier tous les points d'accès (serveur, postes « clients », etc.) aussi bien au niveau individuel qu'au niveau de leur interaction d'ensemble afin de s'assurer qu'aucun risque ne demeure non vérifié.

En outre et concernant les ERP, selon les résultats de l'enquête annuelle 1998 d'Ernst & Young[18] sur la sécurité des systèmes d'information, il ressort que près d'une entreprise sur cinq n'a pas confiance en la sécurité de son progiciel intégré et par conséquent sur la fiabilité des processus informatisés. Ces inquiétudes ont été expliquées, en partie, par le fait que les progiciels intégrés nécessitent une prise en compte particulière des besoins de fiabilité et de sécurité. En effet, même si chaque module est bien maîtrisé en matière de contrôle informatique, il subsiste souvent des failles potentielles de contrôle interne entre les différents modules.

Quant à la sécurité sur Internet, les attaques cybernétiques peuvent compromettre l'entreprise et détruire tout son patrimoine. En effet, Internet fournit l'accès à des millions de clients potentiels mais aussi à des milliers de fraudeurs et d'escrocs éventuels.

[17] Informations extraites du séminaire « Global Risk Management Solutions : Joiners Course » (Initiation à la gestion du risque management), Marburg – Allemagne, PricewaterhouseCoopers, 2000.
[18] Philippe TROUCHAUD, « Appréciation du contrôle interne informatique des grandes entreprises et impact sur le contrôle des comptes », Revue Française de Comptabilité N° 316, Novembre 1999, page 21.

Nous allons étudier dans ce qui suit :

- les objectifs de la sécurité en milieu informatisé,
- les différents types de sécurité informatique au sein de l'entreprise,
- et, les méthodes d'évaluation de la sécurité informatique.

Sous section 1 : Les objectifs de la sécurité en milieu informatisé

L'objectif de la politique de sécurité du système d'information est de garantir la disponibilité, l'intégrité, la confidentialité et la possibilité de contrôle et de preuve.

1. La disponibilité :

C'est l'aptitude des systèmes à remplir une fonction dans des conditions prédéfinies d'horaires, de délais et de performances. Il s'agit de garantir la continuité du service, assurer les objectifs de performance (temps de réponse) et respecter les dates et heures limites des traitements.

Assurer la disponibilité de l'information nécessite des procédures appropriées de couverture contre les accidents ainsi que des contrôles de sécurité afin de se protéger contre les suppressions inattentives ou intentionnelles des fichiers.

Appliquée aux flux d'information, la disponibilité est destinée à garantir la continuité des échanges d'information, c'est à dire de pouvoir disposer, chaque fois que le besoin existe, des possibilités de réception ou de transfert.

En outre, appliquée aux traitements, elle est destinée à garantir la continuité de service des traitements, c'est à dire de pouvoir disposer des ressources en matériels et logiciels nécessaires à l'ensemble des services, des agences et à la clientèle extérieure.

Enfin, appliquée aux données, elle est destinée à garantir la disponibilité prévue pour l'accès aux données (délais et horaires), c'est à dire de pouvoir disposer, de l'accès aux données, chaque fois que le besoin existe, dans des conditions de performance prédéfinies.

2. L'intégrité :

C'est la propriété qui assure que les informations sont identiques en deux points, dans le temps comme dans l'espace.

Selon l'ISO 13-335-1, l'intégrité c'est la propriété de non-altération ou de non-destruction de tout ou partie du système d'information et/ou des données de façon non autorisée. Il s'agit de garantir l'exhaustivité, l'exactitude et la validité des informations ainsi que d'éviter la modification, par erreur, de l'information.

Assurer l'intégrité des données consiste à établir des contrôles aussi bien sur les entrées que sur les traitements des transactions et à sécuriser les fichiers des données cumulées de toute modification non autorisée.

A titre d'exemple, pour les entreprises utilisant le commerce électronique sans des contrôles d'intégrité adéquats, les opérations et les documents électroniques peuvent être aisément modifiés, perdus ou reproduits et faire l'objet d'erreurs de traitement. L'intégrité des opérations et des documents électroniques risque alors d'être mise en cause, ce qui pourrait provoquer à l'entreprise des litiges avec ses clients au sujet des conditions de transaction et de paiement.

Appliquée aux flux d'information, l'intégrité est destinée à garantir la fiabilité et l'exhaustivité des échanges d'information. C'est à dire de faire en sorte que les données soient reçues comme elles ont été émises et d'avoir les moyens de le vérifier.

En outre, appliquée aux traitements, elle est destinée à assurer la conformité de l'algorithme des traitements automatisés ou non par rapport aux spécifications. C'est à dire de pouvoir obtenir des résultats complets et fiables.

Enfin, appliquée aux données, elle est destinée à garantir l'exactitude et l'exhaustivité des données vis à vis d'erreurs de manipulation ou d'usages non autorisés. C'est à dire de pouvoir disposer de données dont l'exactitude, la fraîcheur et l'exhaustivité sont reconnues et attestées.

3. La confidentialité :

C'est la propriété qui assure la tenue secrète des informations avec accès aux seules entités autorisées. La protection de la confidentialité des informations contre toute intrusion non autorisée est d'une exigence importante qui nécessite un niveau minimum de sécurité. Il s'agit de :

- réserver l'accès aux données d'un système aux seuls utilisateurs habilités (authentification) en fonction de la classification des données et du niveau d'habilitation de chacun d'eux ;
- garantir le secret des données échangées par deux correspondants sous forme de message ou de fichiers.

Ce dernier volet constitue l'aspect le plus vulnérable dans les échanges électroniques et intéresse aussi bien l'entreprise que les consommateurs. En effet, ces derniers se soucient pour la protection de leurs données personnelles et financières par peur que ces informations soient divulguées ou utilisées de façon à nuire à leurs intérêts. Il est donc normal que les personnes qui envisagent d'avoir recours au commerce électronique cherchent à obtenir l'assurance que l'entreprise a mis en place des contrôles efficaces sur la protection de l'information et qu'elle veille à la confidentialité des renseignements personnels de ses clients.

Appliquée aux flux d'information, la confidentialité est destinée à garantir la protection des échanges dont la divulgation ou l'accès par des tiers non autorisés porterait préjudice.

En outre, appliquée aux traitements, elle est destinée à assurer la protection des algorithmes décrivant les règles de gestion et les résultats dont la divulgation à des tiers non autorisés serait nuisible.

Enfin, appliquée aux données, elle est destinée à protéger les données dont l'accès ou l'usage par des tiers non autorisés porterait préjudice. C'est à dire de donner l'accès aux seules personnes habilitées par des procédures organisationnelles et informatiques.

4. La possibilité de contrôle et de preuve :

Ceci englobe la faculté de vérifier le bon déroulement d'une fonction et l'impossibilité pour une entité de nier avoir reçu ou émis un message (La non répudiation).

Elle garantit la possibilité de reconstituer un traitement à tous les niveaux (logique de programmation, déroulement du traitement, forme des résultats) à des fins de contrôle ou de preuve.

Appliquée aux flux d'information, la possibilité de contrôle et de preuve est destinée à garantir le fait de ne pouvoir nier avoir reçu ou émis un flux (logs, authentifiants, accusés de réception, ...) et de pouvoir reconstituer ce flux.

En outre, appliquée aux traitements, elle est destinée à garantir la possibilité de reconstituer à tout moment le déroulement d'un traitement et l'impossibilité de nier la réception des résultats.

Enfin, appliquée aux données, elle est destinée à garantir la possibilité de reconstituer à tout moment une donnée et l'impossibilité de nier l'accès à une donnée. C'est à dire assurer la possibilité de reconstituer une donnée et de retrouver trace de son utilisation.

Sous section 2 : Les différents types de sécurité informatique au sein de l'entreprise

Nous distinguons les types de sécurité informatique suivants :

1. La sécurité physique
2. La sécurité des matériels et logiciels de base
3. La sécurité des données
4. La sécurité de la production

5. La sécurité des études et des réalisations
6. La sécurité des télécommunications
7. La protection assurances

La mise en place de moyens de sécurité appropriés ne peut se concrétiser efficacement qu'à la condition de correspondre à une politique décidée par la Direction et précisée dans un plan (schéma directeur) impliquant l'entreprise toute entière. En outre, un contexte et un environnement socio-économique positifs influencent favorablement l'attitude du personnel et constituent un facteur de sécurité important.

1. La sécurité physique :

La sécurité physique englobe les éléments suivants :

1. L'environnement : C'est un paramètre à la fois externe (milieu naturel et artificiel) et interne (exemple : la structure du bâtiment et la situation des locaux administratifs) à l'entreprise.
2. La pollution : Certains éléments sont susceptibles d'influencer la qualité de l'environnement dans lequel fonctionnent les matériels et opère le personnel. Exemple : les vibrations, le magnétisme, la température, les particules en suspension dans l'air, etc.
3. La sécurité incendie : Elle nécessite des démarches dans les domaines de :
   - la protection passive, visant à diminuer la probabilité de survenance du sinistre (exemple : consignes de sécurité)
   - la détection, destinée à éviter qu'un incident mineur ne dégénère en un sinistre réel (exemple : capteurs de fumée)
   - la propagation, afin de limiter l'ampleur d'un sinistre (exemple : porte coupe-feu)
   - l'extinction, en vue de réduire les conséquences d'un accident (exemple : équipe de première intervention)
4. La sécurité dégâts des eaux : Cet élément est trop souvent négligé alors qu'il peut être à l'origine de l'indisponibilité totale ou partielle d'un centre informatique. Ce type de sécurité doit tenir compte de l'environnement du bâtiment ainsi que des diverses installations (canalisation d'extinction de feu, dispositifs de climatisation, etc.)
5. Le contrôle des accès : Ceci vise à protéger les cellules Etudes et Exploitation des entrées intempestives et de la présence inutile de personnes extérieures au service. Elle vise aussi à protéger les biens informatiques contre le vol et l'outil informatique contre le sabotage et l'attentat.
6. La fiabilité technique et énergétique : Ceci englobe la mise en place de dispositifs en vue de réduire la fréquence des incidents matériels et d'en limiter la durée (alimentation électrique, conditionnement d'air, etc.)

2. La sécurité des matériels et logiciels de base :

Ceci englobe :

1. L'acquisition et la maintenance des matériels : C'est l'ensemble des dispositifs nécessaires pour garantir un fonctionnement du matériel sans incident.
2. L'acquisition et la maintenance des logiciels de base : Ceci consiste en l'ensemble des sécurités limitant et identifiant les altérations non autorisées du fonctionnement du logiciel de base. En effet, toute altération du fonctionnement du logiciel de base est un facteur d'immobilisation quasi-totale de toutes les applications.
3. Le système de secours : C'est l'ensemble de moyens matériels (exemple : la salle redondante, le centre de backup) et organisationnels (exemple : traitement manuel) destinés à pallier la défaillance prolongée de l'outil informatique.

Signalons, à ce niveau, l'importance de la mise en place d'un plan de continuité des systèmes d'information. Chaque plan de continuité a des caractéristiques propres conditionnées par l'activité de l'entreprise et sa dépendance vis-à-vis du système d'information.

Un plan de continuité comprend :

→ Un plan de continuité utilisateur : dont l'objectif est de fournir un service minimum aux clients de l'entreprise en cas de sinistre

→ Un plan de secours qui prévoit une solution de secours en cas d'interruption du système ainsi que les procédures associées

→ Un plan de gestion et de communication de crise dont les objectifs sont de déclencher les mesures d'urgence au plus tôt et de façon opportune et de diffuser une information sur la crise la plus judicieuse pour l'entreprise

→ Un plan de test et de gestion du plan qui garantissent la pérennité du plan de continuité et son efficacité.

3. La sécurité des données :

Ceci englobe :

1. L'administration des données : C'est l'ensemble des dispositifs destinés à préserver la sécurité et la confidentialité des données et à veiller à la cohérence du système d'information.
2. La conservation des données : Ceci englobe l'archivage, le désarchivage et la sauvegarde. Par « données », on entend les fichiers, les programmes et la documentation.

4. La sécurité de la production :

La sécurité de la production couvre les domaines suivants :

1. La planification : Ceci englobe l'ensemble des mesures pour que le déroulement des travaux se fasse dans l'ordre et ce, afin d'assurer toutes les chances d'une production réussie.
2. Le contrôle des entrées / sorties : Il s'agit de contrôler l'ensemble des données entrées et sorties de l'entreprise et des traitements informatiques quels que soit leur origine, leur forme, leur support et leur destination.
3. Le traitement des applications : Il s'agit de l'ensemble des sécurités destinées à se prémunir, essentiellement, contre les modifications erronées et non conformes des programmes utilisés ainsi que contre les actions frauduleuses introduites dans le déroulement des travaux.
4. La sous-traitance : C'est l'ensemble des sécurités assurant que les travaux réalisés chez le sous-traitant sont convenablement sécurisés.

5. La sécurité des études et des réalisations :

Ceci consiste en l'ensemble des moyens assurant la sécurité de la maintenance (autorisation, validation, recettage, etc.). Elle consiste aussi à assurer une communication appropriée entre les informaticiens et les utilisateurs et à définir d'une façon précise la responsabilité de chacun.

6. La sécurité des télécommunications :

Ceci englobe :

1. La sécurité physique : C'est l'ensemble des sécurités touchant l'infrastructure de télécommunication et les constituants du réseau appartenant à l'entreprise.
2. La sécurité logique : Outre les protections qui s'appliquent aux logiciels de base et des contrôles mis au niveau des applications, des précautions supplémentaires sont nécessaires dans le cas du télétraitement. Les scénarios et les positions d'attaque peuvent être très différents.

A ce niveau, il convient d'indiquer que le grand défi de la sécurité des données, pour les entreprises utilisant la technologie Internet, inclut des procédés d'authentification électronique et de cryptage.

L'authentification électronique ou encore la signature électronique est un processus permettant de s'assurer de la fiabilité des données numériques et celles des différentes parties d'une transaction. Plusieurs pays ont proclamé des lois pour réglementer la signature électronique et la valider pour la conclusion des contrats.

Quant au cryptage, il se présente comme une solution efficace permettant à l'information d'être envoyée à travers les réseaux de communication publics sans perdre son caractère confidentiel

ou son intégrité et permettant aussi de vérifier la source des données. Signalons que la cryptographie a fait aussi l'objet, dans plusieurs pays, de régulation contrôlant l'import, l'export et l'usage national des logiciels et méthodes de cryptage. Les échanges de logiciels de cryptage sont suivis sévèrement vu les risques pouvant découler des abus d'utilisation des clés de cryptage.

7. La protection assurances :

La protection assurances se distingue des autres types de sécurité car elle correspond à une indemnisation financière du préjudice subi. Cette indemnisation intervient, généralement, avec un décalage dans le temps qui peut être important.

En dehors des couvertures spéciales, les compagnies d'assurances couvrent les pertes engendrées par deux grands types de dommages liés à l'informatique :

1. Les dommages matériels dus à des événements accidentels à l'exclusion des pannes et des erreurs quelles qu'elles soient,
2. Les dommages immatériels : détournements, fraudes, escroqueries, sabotages immatériels.

Sous section 3 : Les méthodes d'évaluation de la sécurité informatique

Nous allons dans ce qui suit présenter, d'une façon très brève, certaines méthodes d'évaluation de la sécurité informatique. Nous citons : la méthode statistique empirique, la méthode CHURCHMAN-ACKOFF et la méthode « Marion »[19].

Il est utile de préciser que dans le cadre de l'audit financier, nous ne sommes pas concernés par une évaluation numérique du risque mais nous avons plutôt besoin d'exprimer un jugement professionnel sur l'adaptation de la sécurité aux risques identifiés.

1. La méthode statistique empirique :

Elle consiste à estimer les pertes potentielles de l'entreprise sur la base des pertes subies dans le passé. Il s'agit de déterminer la distribution de la fréquence absolue des incidents (nombre d'incidents annuels possibles avec la probabilité de réalisation de chacun), et des pertes unitaires (montants possibles pour un incident et probabilité de chacun).

Cette méthode présente de nombreux inconvénients. Elle suppose, en effet, l'existence d'une base de données statistiques complète et fiable. En outre, elle est basée sur l'hypothèse que le nombre des incidents et leur montant unitaire sont linéaires et répétitifs dans le temps et que le passé est statistiquement représentatif de tous les risques possibles.

2. La méthode CHURCHMAN-ACKOFF :

Elle est basée sur une approche qualitative : l'importance de chaque risque identifié est pondérée par un coefficient de priorité. Les rangs de priorité sont attribués par comparaison des risques deux à deux. Une cotation de la gravité relative de l'un par rapport à l'autre est définie. Le tout est ensuite regroupé pour établir une hiérarchie des risques.

Ces deux méthodes sont essentiellement basées sur des schémas mathématiques. Or, la sécurité est avant tout basée sur une politique de sécurité qui ne peut être prise en compte par des modèles purement mathématiques. C'est la raison pour laquelle elles ont été plus ou moins abandonnées au profit d'autres méthodes telles que la méthode «MARION».

3. La méthode «MARION» (Méthode d'analyse des risques informatiques et optimisation par niveau) :

Cette méthode a été élaborée par l'APSAD[20]. Le CLUSIF en assure l'actualisation. Elle est fondée sur l'analyse des risques (elle tient compte de leur probabilité d'occurrence) et du coût de leurs conséquences comparé au coût de la prévention.

---

[19] Yves BEGON, mémoire : « Les professionnels des comptes et l'informatique : risques et principes de sécurité », session Mai 1997.
[20] APSAD : Assemblée Plénière des Sociétés d'Assurances Dommages

Elle permet de dresser un inventaire des risques importants et de rechercher les moyens de sécurité susceptibles de les réduire.

En outre, elle permet d'aboutir à la rédaction d'un schéma directeur de la sécurité et à la mise en œuvre de moyens de protection et de prévention cohérents et adéquats.

Schématiquement, elle comporte six phases :

a) l'analyse des risques (inventaire des risques encourus et évaluation de leur coût),

b) la définition du risque maximum tolérable,

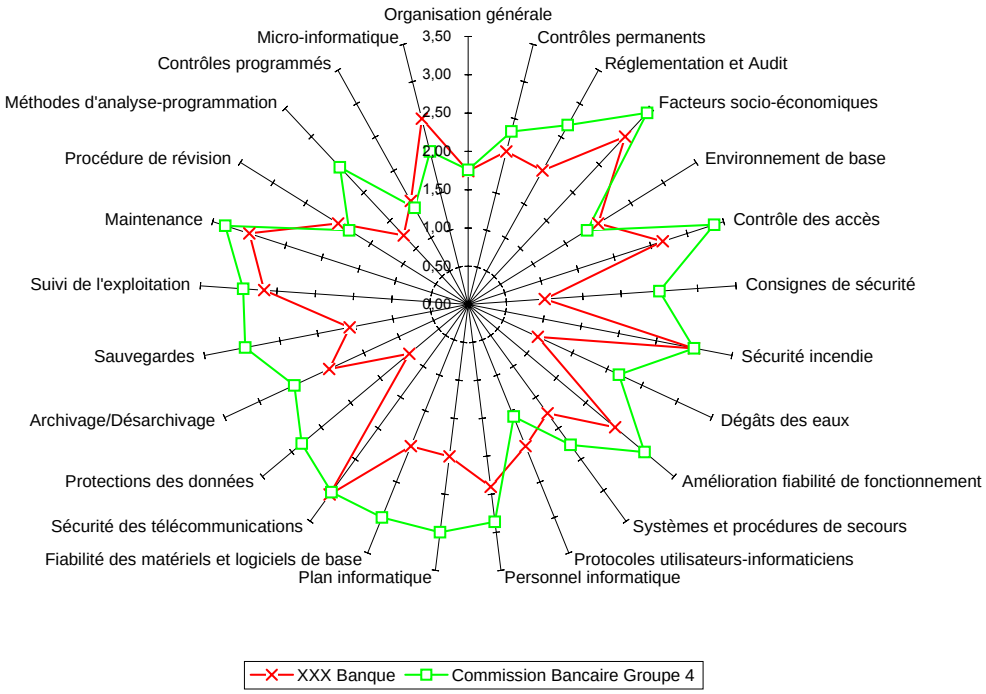
c) le questionnaire d'évaluation qui permet l'analyse de la sécurité existante. Les résultats sont reportés sur une grille / questionnaire qui donne lieu à une notation allant de 0 (niveau de risque maximum) à 4 (sécurité maximale). Les résultats sont ensuite présentés dans une rosace.

d) la prise en compte des contraintes techniques et humaines dans l'analyse des risques,

e) la définition des moyens à mettre en œuvre afin d'améliorer la sécurité,

f) la rédaction d'un plan de sécurité indiquant les modalités pratiques de mise en œuvre de la sécurité.

Exemple : Le diagramme qui suit présente l'évaluation de la sécurité d'une banque comparée à la sécurité requise dans le secteur bancaire.



Conclusion :

Les systèmes d'information ont une importance véritablement stratégique (décider du bon système à mettre en place, des nouvelles technologies à implanter, etc.). En outre, la gestion efficace de l'information et des technologies associées est d'une importance critique pour le succès et la survie d'une organisation. Cette importance a, essentiellement, pour origine :

- la dépendance croissante de l'information et des systèmes qui la délivrent
- le potentiel qu'ont les technologies à changer radicalement les organisations et les pratiques des affaires, à créer de nouvelles opportunités et à réduire les coûts
- une vulnérabilité croissante et un large spectre de menaces.

Par ailleurs, il a été démontré au cours de ce chapitre comment le milieu informatisé et plus particulièrement les nouvelles technologies de l'information et de la communication, peuvent affecter l'organisation et les procédures utilisées par l'entité pour satisfaire à la mise en place d'un contrôle interne fiable.

La mission de l'audit financier, qui repose généralement sur le contrôle interne en place, sera affectée en conséquence. L'approche d'audit doit tenir compte du nouvel environnement d'intervention qui est, généralement, plus difficile que l'environnement traditionnel et ce, en raison notamment de :

- la fréquence des modifications
- la complexité et l'intégration des traitements
- l'augmentation constante des volumes d'information
- la concentration et/ou de la dispersion croissantes des données.

Les principaux impacts des nouvelles technologies sur l'audit financier font l'objet d'une étude détaillée dans le chapitre suivant.

Chapitre 2 : Les Principaux Impacts des Nouvelles Technologies sur l'Audit Financier

Introduction :

Selon la norme internationale d'audit N°401[21] de l'IFAC, l'existence d'un environnement informatique ne modifie pas l'objectif et l'étendue de la mission d'audit financier.

Toutefois, il a été précisé dans le premier chapitre que la mise en place des nouvelles technologies de l'information et de la communication modifie la saisie et le processus de traitement, la conservation des données et la communication des informations financières et peut, par conséquent, avoir des incidences sur le système comptable et les contrôles internes de l'entité.

Aussi, ces nouvelles technologies redéfinissent un nouveau périmètre de risques de nature financière, opérationnelle et de conformité.

Ce nouveau cadre d'intervention :

- appelle un complément de normes de travail de l'auditeur aussi bien au niveau de la planification qu'au niveau de l'exécution ;
- exige, d'une façon continue, de nouvelles aptitudes et compétences pour faire face à la complexité, de plus en plus croissante, des environnements informatiques.

Ces deux volets font l'objet d'une étude détaillée dans les sections qui suivent.

Section 1 : Les effets des nouvelles technologies sur la réalisation de l'audit financier

L'audit financier repose, généralement, sur l'examen du système de contrôle interne en place. La démarche de l'auditeur consiste alors à recenser les procédures utilisées et ce, en procédant au découpage de l'entreprise en fonctions, indépendantes ou non, mais facilement isolables.

Cette approche n'a pas connu de révolutions particulières avec la mise en place des applications informatiques traditionnelles. En effet, ces dernières étaient associées aux différentes fonctions de l'entreprise : achats, ventes, stocks, etc.

Toutefois, la mise en place des nouvelles technologies entraîne d'importants changements sur le plan de l'organisation, des processus et de la technologie. Avec les ERP, par exemple, une commande client peut générer une commande fournisseur, un lancement en production, un bon de livraison, une facture, son règlement, et l'enregistrement en comptabilité de ces événements. L'intervention humaine est limitée à la validation ou non de certains processus.

C'est ainsi qu'on parle actuellement de la mutation de l'approche de l'auditeur, de systémique et verticale, pour devenir événementielle et transversale[22]. Par conséquent, il faudra suivre le chemin parcouru par un événement et étudier son impact sur l'ensemble du système d'information.

Ce nouvel environnement appelle de la part de l'auditeur un complément de normes de travail, dont essentiellement :

[21] I.S.A 401 : « Audit réalisé dans un environnement informatisé », (Auditing in a computer information system environment), IFAC.
[22] Daniel JOLY, « Les progiciels intégrés et les nouveaux outils informatiques vont ils changer l'approche d'audit ? »,, Revue Française de Comptabilité, Novembre 1999.

- L'examen des nouveaux domaines se rattachant aux nouvelles technologies afin d'obtenir une compréhension suffisante du système comptable et des contrôles internes de l'entreprise,
- L'analyse des nouveaux risques inhérents et des nouveaux risques de non contrôle nécessaire pour l'appréciation du risque d'audit et la planification des travaux,
- La conception, l'exécution et le timing des tests sur les contrôles et des tests substantifs afin de réunir des éléments probants suffisants et adéquats nécessaires pour fonder l'opinion d'audit.

Sous section 1 : Les effets sur la planification de la mission d'audit financier

L'auditeur doit considérer l'importance et la complexité des systèmes et de l'environnement informatique. Il doit, aussi, considérer les nouveaux risques inhérents et les risques de non contrôle associés aux traitements informatisés.

1. La prise de connaissance des systèmes et de l'environnement informatique :

Les changements dans la manière avec laquelle les entreprises réalisent leurs affaires dans un environnement d'ERP et/ou d'Internet devraient être considérés par l'auditeur lors de la planification de la mission. En effet, étant donné les caractéristiques uniques de ces entreprises, une bonne compréhension de ces caractéristiques lors de la planification de la mission est essentielle.

Cette prise de connaissance est limitée aux systèmes ayant une incidence sur les assertions sous-tendant l'établissement des états financiers.

Elle englobe la collecte d'un complément d'informations spécifiques concernant par exemple les éléments suivants :

- L'organisation de la fonction informatique et le degré de concentration et de décentralisation,
- Les contrôles de la direction sur la fonction informatique,
- Dans quelle mesure l'activité repose sur les systèmes informatiques et l'importance et la complexité des traitements informatisés (volume des opérations, calculs complexes, génération automatique des traitements et/ou des opérations, échanges de données, etc.),
- Les caractéristiques principales des systèmes et des environnements et les contrôles qui y sont rattachés (conception, configuration du matériel informatique, sécurité, disponibilité des données, contrôles liés à l'environnement informatique, contrôles liés aux ERP, etc.),
- Les changements significatifs en termes de systèmes et d'environnements informatiques,
- Les problèmes antérieurs identifiés au niveau des systèmes.

La phase de collecte de l'information est plus importante la première année ou l'année du changement avant de pouvoir décider de la stratégie. En revanche, les années suivantes, compte tenu des connaissances d'audit accumulées, le processus doit être plus rapide puisque focalisé uniquement sur les changements de l'exercice.

2. La prise en compte des nouveaux risques inhérents :

Le risque inhérent est « la possibilité que le solde d'un compte ou qu'une catégorie de transactions comporte des erreurs significatives isolées ou cumulées à des erreurs dans d'autres soldes ou catégories de transactions, du fait de l'insuffisance de contrôle interne »[23].

Les risques inhérents associés à l'utilisation des nouvelles technologies de l'information et de la communication sont généralement élevés et ce, en raison de leur extrême flexibilité et complexité, de la multiplicité des systèmes en intégration et de la multiplicité des utilisateurs.

A titre d'exemple, l'absence de sécurité du système d'exploitation peut résulter en des changements de données ou de programmes altérant, par conséquent, la fiabilité des états financiers. En effet, en l'absence de contrôles appropriés, il existe un risque accru que des personnes situées à l'intérieur ou

[23] Norme internationale d'audit (ISA) N°400 : « Evaluation du risque et contrôle interne », IFAC.

à l'extérieur (par l'utilisation d'équipements informatiques à distance) de l'entité aient indûment accès aux données et aux programmes et les modifient.

Par ailleurs, « le risque d'erreurs humaines dans la conception, la maintenance et la mise en œuvre d'un système informatique est supérieur à celui d'un système manuel à cause du niveau de détail inhérent à ces systèmes »[24].

En outre, en raison de la diminution de l'intervention humaine dans le traitement informatisé d'opérations, les erreurs ou irrégularités se produisant lors de la conception ou de la modification des programmes risquent de passer longtemps inaperçues et entraînent, en général, un traitement incorrect de toutes les opérations.

L'auditeur peut considérer, par exemple, les éléments suivants :

- L'intégrité, l'expérience et les connaissances de la direction informatique
- Les changements dans la direction
- Les pressions exercées sur la direction informatique qui pourraient l'inciter à présenter des informations inexactes
- La nature de l'organisation de l'affaire et des systèmes (Exemples : le commerce électronique, la complexité des systèmes, le manque de systèmes intégrés)
- Les facteurs qui affectent l'organisation dans son ensemble (Exemple : changements technologiques)

Le niveau d'influence d'une partie externe sur le contrôle des systèmes (Exemples : l'externalisation des traitements informatiques, l'accès direct par les clients)

- La susceptibilité de perte ou de détournement des actifs contrôlés par le système

3. La prise en compte des risques liés au contrôle :

Le risque lié au contrôle est défini comme étant « le risque qu'une erreur significative dans un solde de compte ou dans une catégorie de transactions, isolée ou cumulée à des erreurs dans d'autres soldes ou catégories de transactions, ne soit ni prévenue ou détectée, et corrigée en temps voulu par les systèmes comptable et de contrôle interne »[25].

Au niveau de la planification, l'auditeur procède à une évaluation préliminaire du risque lié au contrôle. Cette évaluation doit être fixée à un niveau élevé sauf si l'auditeur :

- Parvient à identifier des contrôles internes appliqués à une assertion particulière et susceptibles de prévenir ou détecter et corriger une anomalie significative
- Envisage de réaliser des tests de procédures pour étayer son évaluation.

Les risques liés au contrôle ont été traités au niveau du chapitre précédent. Ils se composent des risques liés aux contrôles directs et des risques liés aux contrôles généraux informatiques.

4. Considérations particulières en cas d'externalisation :

Certaines entreprises font appel à des services bureaux pour tout ce qui se rattache à leur système d'information. Ceci est d'autant plus noté avec l'E-Business où beaucoup d'entreprises utilisent un fournisseur de service Internet (ISP : Internet Service Provider) pour abriter leurs sites Web, y compris les bases de données utilisées pour l'initiation des ventes et des encaissements par cartes de crédit.

Afin de planifier l'audit et concevoir une approche d'audit efficace, l'auditeur doit déterminer l'étendue des prestations rendues par le service bureau et leur incidence sur l'audit.

Les éléments à prendre en considération[26] sont, à titre indicatif :

- La nature des prestations du service bureau
- Les conditions contractuelles et relations entre l'entreprise et le service bureau

[24] Norme internationale d'audit (ISA) N°401 : « Audit réalisé dans un environnement informatisé », IFAC.
[25] Norme internationale d'audit (ISA) N°400 : « Evaluation du risque et contrôle interne », IFAC.
[26] Norme internationale d'audit N° 402 : « Facteurs à considérer pour l'audit d'entités faisant appel aux services bureaux », IFAC.

- Les assertions significatives sous-tendant l'établissement des états financiers influencées par le recours au service bureau
- Les risques inhérents associés à ces assertions
- Les interactions entre les systèmes comptables et de contrôle interne de l'entreprise et ceux du service bureau
- Les contrôles internes de l'entreprise auxquels sont soumises les transactions traitées par le service bureau
- L'organisation interne et la surface financière du service bureau et l'incidence éventuelle d'une défaillance de ce dernier sur l'entreprise
- Les informations sur le service bureau telles que celles figurant dans les manuels utilisateurs et les manuels techniques
- Les informations disponibles sur les contrôles généraux et d'application de l'entreprise.

L'auditeur doit ensuite évaluer l'incidence des prestations du service bureau sur le système comptable et sur le système de contrôle interne de l'entreprise auditée.

Si l'auditeur conclut que l'incidence en question est significative, il doit rassembler des informations suffisantes pour comprendre les systèmes et évaluer le risque lié au contrôle.

5. La stratégie d'audit :

Les différentes étapes décrites ci-dessus, doivent permettre à l'auditeur de recueillir des indicateurs lui permettant de fixer la stratégie d'audit par cycle et ce afin d'atteindre les objectifs d'audit.

La stratégie d'audit vise à déterminer le mix des procédures à mettre en œuvre pour atteindre les objectifs d'audit, en conciliant au mieux l'efficacité, la gestion du risque et la rentabilité. Elle est définie par rapport au niveau de confiance accordé aux contrôles de direction, contrôles informatiques généraux et les contrôles d'applications.

Avec l'évolution des technologies de l'information et de la communication, l'approche basée sur les systèmes semble être, dans la plupart des cas, la plus adaptée et la plus efficace et ce, en raison notamment de :

- la conscience de plus en plus ressentie des dirigeants des entreprises de la nécessité de mettre en place les sécurités nécessaires comme condition indispensable de la pérennité,
- le volume de plus en plus important des transactions, leur complexité et leur étendue,
- la dématérialisation des informations.

Par ailleurs, cette approche permet aux auditeurs d'apporter de la valeur à l'entreprise à travers des conseils touchant aussi bien les processus que la sécurité des traitements.

Sous section 2 : Les effets sur les objectifs de contrôle

L'évaluation des contrôles par l'auditeur se fait par référence aux objectifs de contrôle. Ces derniers se détaillent comme suit :

1. La validité des transactions :

Il est essentiel que seulement les transactions valides et autorisées par la direction soient saisies dans le système. Les contrôles sur la validité et l'autorisation sont importants pour la prévention contre les fraudes qui peuvent survenir suite à la saisie et au traitement de transactions non autorisées.

Dans la plupart des cas, les procédures d'autorisation sont similaires à celles d'un système non informatisé. Toutefois, les procédures dans le cadre informatisé peuvent présenter les différences suivantes :

- L'autorisation des données se fait, souvent, lors de la saisie dans le système (ou aussi, dans certains cas, après avoir effectué les contrôles d'exhaustivité et d'exactitude des inputs et des mises à jour) et non lors de l'utilisation des outputs correspondants. Dans ce cas, il est important de s'assurer que l'autorisation demeure valable et que des changements ne peuvent pas être apportés durant les traitements subséquents.

- L'autorisation des données peut être gérée par exception. En effet, c'est l'ordinateur qui identifie et rapporte les éléments identifiés et nécessitant une autorisation manuelle. Dans ce cas, l'attention est focalisée sur les éléments importants susceptibles d'être incorrectes améliorant ainsi l'efficacité et l'efficience des contrôles manuels (exemple : nombre d'heures saisies pour un employé dépasse de 50% les heures normales de travail).
- Dans certains cas, la capacité du programme à tester la validité des éléments est si précise que le recours aux autorisations manuelles n'est plus requis. Exemple : une réception de marchandise peut être rejetée par le système si un bon de commande autorisé correspondant ne figure pas dans ledit système ou figure pour des quantités différentes.

2. L'exhaustivité des inputs :

Le contrôle de l'exhaustivité, qui est l'un des contrôles les plus fondamentaux, est nécessaire afin de s'assurer que chaque transaction a été introduite dans le système pour traitement.

En outre, les contrôles de l'exhaustivité consistent à s'assurer que :

- toutes les transactions rejetées sont rapportées et suivies
- chaque transaction est saisie une seule fois
- les transactions doublement saisies sont identifiées et rapportées.

Il existe plusieurs techniques disponibles pour contrôler l'exhaustivité des inputs. Nous citons, à titre indicatif, les contrôles suivants :

- Le contrôle automatisé du respect de la séquence numérique des différents documents : L'ordinateur rapporte les numéros manquants des pièces justificatives ou ceux existants doublement afin d'être suivis d'une façon manuelle. La réalisation effective de ce contrôle suppose l'existence de procédures adéquates dont par exemple les procédures de gestion des ruptures de la séquence, les procédures à suivre en cas d'utilisation concomitante de plusieurs séquences à la fois (cas d'une entreprise à plusieurs agences, exemple : banques). En outre, le fichier des numéros manquants ou doubles devrait être protégé contre toute modification non autorisée.
- Le rapprochement automatique avec des données déjà saisies et traitées : Exemple : rapprochement des factures avec les bons de livraison. Dans ce cas, l'ordinateur doit permettre la génération d'un rapport des éléments non rapprochés pour s'assurer que toutes les livraisons clients ont été facturées.

3. L'exactitude des inputs :

L'exactitude des inputs consiste à s'assurer que chaque transaction, y compris celle générée automatiquement par les systèmes, est enregistrée pour son montant correct, dans le compte approprié et à temps.

Le contrôle de l'exactitude se rattache aux données de la transaction traitée par contre le contrôle de l'exhaustivité se limite à savoir, uniquement, si la transaction a été traitée ou pas.

Le contrôle de l'exactitude devrait englober toutes les données importantes que ce soit des données financières (exemple : quantité, prix, taux de remise, etc.) ou des données de référence (exemple : numéro du compte, date de l'opération, les indicateurs du type de la transaction, etc.). L'appréciation des contrôles de l'exactitude se fait par référence aux éléments de données jugés importants.

Il existe plusieurs techniques qui peuvent être utilisées pour contrôler l'exactitude des inputs. Nous en citons, à titre d'exemple, les suivantes :

- Le rapprochement automatique avec les données déjà saisies et traitées : Il s'agit de la même technique détaillée ci-dessus. Toutefois, l'action devrait être focalisée sur les données composant la transaction et non uniquement sur l'existence de la transaction.
- Le contrôle de la vraisemblance : Il s'agit, par exemple, de tester si les données saisies figurent dans une limite prédéfinie. Les données n'obéissant pas à cette limite ne sont pas nécessairement des données erronées mais sont douteuses et nécessitent des investigations supplémentaires.

Ce type de contrôle est mis en place pour les éléments de données qu'il est souvent difficile ou non pratique de contrôler autrement. Exemple : dans une application de paie, contrôler si le nombre d'heures travaillées par semaine ne dépasse pas 60 heures.

4. L'intégrité des données :

Il s'agit des contrôles permettant d'assurer que les changements apportés aux données sont autorisés, exhaustifs et exacts.

Les contrôles d'intégrité sont requis aussi bien pour les données des transactions que pour les fichiers de données permanentes et semi-permanentes. Ils sont désignés pour assurer que :

- les données sont à jour et que les éléments inhabituels nécessitant une action sont identifiés
- les données conservées dans les fichiers ne peuvent être changées autrement que par les cycles de traitements normaux et contrôlés.

Les techniques les plus utilisées pour contrôler et maintenir l'intégrité des données sont les suivantes :

- La réconciliation des totaux des fichiers : Cette réconciliation peut se faire d'une façon manuelle ou par le système.
- Les rapports d'exception : Cette technique implique que le système informatique examine les données du fichier et rapporte sur les éléments qui semblent incorrects ou hors date. Exemple : cette technique peut être utilisée pour contrôler l'exactitude des fichiers des prix de valorisation des stocks en produisant périodiquement les rapports d'exception suivants :
  - Les prix n'ayant pas été modifiés pour une certaine période
  - Les prix ayant des relations anormales avec les prix de vente
  - Les prix ayant eu des fluctuations anormales.
- Vérification détaillée des données des fichiers : Cette vérification se fait par sondage. Sa fréquence dépend largement de l'importance des données et de l'existence et de la force des autres contrôles en place.

5. L'exhaustivité des mises à jour :

Le contrôle de l'exhaustivité des mises à jour est désigné pour s'assurer que toutes les données saisies et acceptées par l'ordinateur ont mis à jour les fichiers correspondants.

Les contrôles sur l'exhaustivité des inputs peuvent être applicables pour contrôler l'exhaustivité des mises à jour. Toutefois, d'autres techniques propres existent dont, notamment, la réconciliation manuelle ou automatisée du total des éléments acceptés.

6. L'exactitude des mises à jour :

Lorsque les fichiers informatiques sont mis à jour, des contrôles sont nécessaires afin de s'assurer que la nouvelle entrée est correctement traitée et a correctement mis à jour les bons fichiers.

Parmi les techniques utilisées pour s'assurer de l'exactitude des mises à jour, nous citons : Le rapprochement avec des données antérieures. Cette méthode est communément utilisée pour s'assurer de l'exactitude des modifications du fichier des données permanentes. Exemple : La modification du prix d'un article est saisie avec son ancienne valeur. L'ordinateur rapproche la référence et l'ancien prix saisi avec le fichier des données permanentes correspondant. La modification n'est acceptée que si le rapprochement aboutisse.

7. Limitation d'accès aux actifs et aux enregistrements :

Ces contrôles visent la protection des actifs et des enregistrements contre les pertes dues aux erreurs et aux fraudes. Nous distinguons : la limitation d'accès et la séparation des tâches.

- La limitation d'accès : Ce contrôle est destiné à éviter que des personnes non autorisées puissent accéder aux fonctions de traitement ou aux enregistrements, leur permettant de lire, modifier, ajouter ou effacer des informations figurant dans les fichiers de données ou de saisir des transactions non autorisées pour traitement.

  Les contrôles d'accès visent, ainsi, à :

- Protéger contre les changements non autorisés de données
- Assurer la confidentialité des données.
- Protéger les actifs physiques tels que la trésorerie et les stocks.

- La séparation des tâches : Le principe de la séparation des fonctions incompatibles est le même quel que soit le moyen de traitement (manuel ou informatisé). Toutefois, dans un milieu informatisé, la séparation des tâches peut être renforcée par différents types de logiciels destinés à limiter l'accès aux applications et aux fichiers. Il est donc nécessaire d'apprécier les contrôles portant sur l'accès aux informations afin de savoir si la ségrégation des tâches incompatibles a été correctement renforcée.

Enfin, il convient de préciser que ces objectifs de contrôle peuvent être regroupés selon les objectifs de contrôle classiques d'exhaustivité, d'exactitude, de validité et d'accès limité comme précisé dans le tableau suivant :

	Exhaustivité	**Exactitude**	**Validité**	**Accès limité**
La validité des transactions			✔	
L'exhaustivité des inputs	✔			
L'exactitude des inputs		✔		
L'intégrité des données	✔	✔	✔	✔
L'exhaustivité des mises à jour	✔			
L'exactitude des mises à jour		✔		
Limitation d'accès aux actifs et aux enregistrements				✔

Sous section 3 : Les effets sur les éléments probants

L'auditeur doit obtenir, à travers la réalisation de procédures de conformité et de validité des éléments probants **suffisants**, **appropriés** et **fiables** lui permettant de tirer des conclusions raisonnables pour fonder son opinion sur l'information financière.

Le caractère « **suffisant** » s'établit par rapport au nombre des éléments probants collectés. Le caractère « **approprié** » d'un élément probant s'apprécie par rapport à sa couverture des objectifs d'audit. Enfin, le caractère « **fiable** » d'un élément probant s'apprécie par rapport à son objectivité et à l'indépendance et à la qualité de sa source.

Les principales caractéristiques des éléments probants dans un milieu de nouvelles technologies se présentent comme suit :

1. La dématérialisation des preuves d'audit :

Avec les nouvelles technologies de l'information et de la communication, plusieurs documents, qui constituent des preuves d'audit tels que les factures, les bons de commande, les bons de livraison, etc., sont devenus électroniques.

Par ailleurs, l'initiation ou l'exécution de certaines transactions peut être opérée d'une façon automatique. L'autorisation de ces opérations peut être assurée par des contrôles programmés.

Ces preuves électroniques nécessaires pour l'audit peuvent n'exister que pour une courte période. L'auditeur doit prendre en compte ce phénomène pour la détermination de la nature, l'étendue et le timing des procédures d'audit.

En outre, la preuve électronique est fondamentalement plus risquée que la preuve manuelle parce qu'elle est plus susceptible d'être manipulée et qu'il est plus difficile de comprendre et de vérifier sa source.

Face à ces nouvelles données, l'auditeur ne peut plus se limiter aux tests substantifs mais doit aussi se baser sur les tests sur les contrôles. Exemple : l'auditeur doit s'assurer qu'il n'y a pas de modifications non autorisées de l'application pour le volet traitant des conditions d'autorisation automatique des transactions.

2. Considérations pour l'appréciation des éléments probants se rapportant aux contrôles :

Plusieurs considérations devraient être prises en compte pour l'appréciation des éléments probants recueillis et se rapportant aux contrôles. En effet, la défaillance des contrôles peut avoir des effets différents selon la nature du contrôle. A titre d'exemple, les défaillances de contrôle touchant les données permanentes ont souvent une incidence plus importante que celles touchant les données variables.

Les éléments probants, se rattachant aux contrôles, peuvent être obtenus à travers l'examen :

- des contrôles généraux informatiques
- des contrôles manuels effectués par les utilisateurs
- des contrôles programmés et des suivis manuels.

2.1. Eléments probants liés aux contrôles généraux informatiques :

Il est nécessaire d'examiner la conception même des contrôles généraux informatiques et leur incidence sur les contrôles relatifs aux applications, qui revêtent un caractère significatif pour l'audit, car la mise en œuvre des contrôles généraux informatiques est souvent déterminante pour l'efficacité des contrôles d'application et par suite, de la fiabilité des éléments probants correspondants.

En outre, étant donné que la fiabilité des informations produites par le système dépend du paramétrage du progiciel, l'auditeur doit s'assurer que des contrôles généraux informatiques appropriés entourent ledit paramétrage.

L'appréciation des éléments probants liés aux contrôles généraux informatiques doit tenir compte des contrôles compensatoires. A titre d'exemple :

- Certaines faiblesses touchant la fonction informatique sont parfois compensées par des contrôles spécifiques d'application. Par exemple, en l'absence d'un logiciel de contrôle d'accès, l'auditeur ne peut conclure automatiquement que les risques d'accès sont élevés, étant donné que certains contrôles d'accès à l'intérieur du système d'application peuvent compenser ce risque.
- Pour les petites entreprises, il est difficile de mettre en place une séparation convenable des tâches. Toutefois, l'implication plus importante de la direction peut compenser cette déficience.
- Le risque de changements non autorisés des programmes peut être diminué si l'entreprise n'utilise que des progiciels achetés et qu'elle n'a pas accès au code source.

2.2. Eléments probants liés aux contrôles manuels effectués par les utilisateurs :

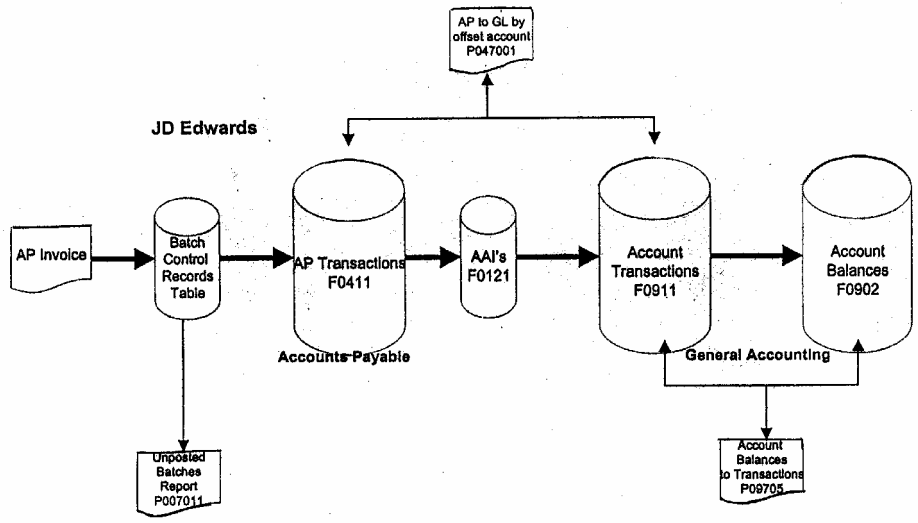
Les contrôles manuels effectués par les utilisateurs d'un logiciel se rapportent, généralement, à la vérification de l'exhaustivité et de l'exactitude des restitutions informatiques et ce, en les rapprochant avec les documents sources ou toute autre entrée (input).

Les tests sur les contrôles des utilisateurs peuvent être suffisants dans les systèmes informatiques où l'utilisateur vérifie toute la production du système (output) et aucune confiance n'est placée sur les procédures programmées ou sur les données tenues sur fichier informatique.

Dans un environnement de nouvelles technologies, ce type de contrôle est de plus en plus limité à cause de la difficulté de réaliser le rapprochement en raison de la dématérialisation de la preuve, de l'importance du volume des opérations et de la complexité des traitements. Par conséquent, le contrôle des utilisateurs ne peut être que très sommaire et vise à identifier les éléments ayant un caractère inhabituel ou douteux.

2.3. Eléments probants liés aux contrôles programmés et aux suivis manuels :

Le résultat des contrôles programmés fait, généralement, l'objet d'une production de rapports informatiques intitulés « rapports d'exception » ou « logs d'audit ». Exemple : Rapports d'exception indiquant les autorisations de dépassement du plafond des crédits clients.



Au niveau de l'ERP « JDEwards », le processus de génération des écritures comptables relatif au cycle achats, fournisseurs et comptes rattachés est schématisé[27] comme suit :

Les rapports d'exception correspondants se rapportent aux :

- lots de factures fournisseurs non traitées (P07011)
- factures non prises en charge au niveau du Grand Livre « GL » par l'instruction comptable automatique (P47001)
- Ecarts entre les soldes du GL et les soldes correspondants au niveau de la Balance Générale (P09705)

Exemple d'un rapport d'intégrité de JDEdwards (A/R to GL by offset accounts):

037001 J.D. Edwards & Company
A/R to G/L by Offset Account

Account	Detail (F0311) Amount Open	A/R Account Balance (F0902)	Difference
1.1210.	60,779.77	3,307,442.75	3,246,662.98-
40.1210.	1,244.23	28,765.90-	30,010.13
50.1210.	188,181.50		188,181.50
70.1210.	12,244.72	54,855.72	42,611.00-
Total	284,509.27	3,255,591.62	3,071,082.35-

L'efficacité de ce contrôle programmé est liée à la production informatique exacte des rapports d'exception. Encore faut-il que ces rapports soient contrôlés manuellement.

Exemple : La chaîne fournisseurs peut éditer une liste des bons de réception manquants, que l'on examinera afin de savoir pourquoi ces bons n'existent pas. En outre, ce contrôle n'est efficace que si la liste sortie de l'ordinateur est exhaustive et fiable.

Enfin, il convient d'indiquer que l'auditeur peut utiliser les fonctions de traitement informatisées (exemple : les règles de génération des événements et des écritures comptables) comme des contrôles à condition de s'assurer, avec un degré de certitude raisonnable, de leur validité et de leur fonctionnement effectif et régulier au cours de la période considérée. Cette condition est vérifiée si l'auditeur obtient des preuves de l'existence de contrôles sur les changements de programmes, ou s'il effectue, au cours de la période qui l'intéresse, des sondages périodiques sur les fonctions de traitement informatisées.

[27] Schéma extrait de la présentation « ERP & E-business : Les systèmes d'informatin et la gestion du changement », séminaire organisé par PricewaterhouseCoopers et STEG, le 13 et 14 décembre 1999.

Sous section 4 : Les effets sur la nature et le calendrier des procédures d'audit

Selon la norme internationale d'audit N°401 de l'IFAC, un environnement informatique, et plus particulièrement de nouvelles technologies, peut avoir une incidence sur la conception et l'exécution des tests sur les contrôles et des tests substantifs nécessaires pour atteindre l'objectif d'audit.

En effet, certains objectifs de l'évolution des technologies de l'information et de la communication sont antinomiques des besoins de l'auditeur, dont par exemple :

Objectifs		Impact sur les procédures d'audit
- Eviter le travail manuel par l'automatisation des tâches et des contrôles	➔	Exclut l'analyse des procédures par l'observation et l'entretien
- Dématérialiser l'information pour supprimer le papier	➔	Ceci rend difficiles les travaux de contrôle sur documents
- Unifier l'accès aux informations en favorisant le partage de données communes - La sécurité d'accès est gérée par le système	↘ ↗	Ceci rend plus complexe l'approche des procédures d'habilitation et d'autorisation

L'auditeur doit répondre, essentiellement, aux questions suivantes :

- Comment vérifier l'existence et le fonctionnement des contrôles qui deviennent informatiques ?
- Comment vérifier la génération des informations, qui s'appuie sur des mécanismes préprogrammés ?
- Comment remonter aux documents d'origine, s'ils n'existent plus ?
- Comment s'assurer de la réalité de la séparation des fonctions ?

Nous présentons, dans ce qui suit, les principaux effets sur la nature et le calendrier des procédures d'audit.

1. Les tests sur les contrôles :

Dans un milieu informatisé, les types de tests sur les contrôles sont les mêmes que dans un milieu non informatisé. Normalement, l'auditeur applique une ou plusieurs des procédures suivantes (classées selon l'ordre croissant du niveau d'assurance et du temps d'exécution) :

- La demande et l'affirmation : Les demandes consistent à chercher les informations et affirmations appropriées auprès du personnel de l'entreprise. Ils peuvent avoir pour but de connaître et mettre à jour la connaissance de l'activité de l'entreprise et d'obtenir des preuves concernant la fiabilité des systèmes de l'entreprise.

  En général, les preuves obtenues à partir des demandes et affirmations ne constituent pas en elles-mêmes des preuves d'audit suffisamment fiables et pertinentes. L'auditeur doit les confirmer par d'autres procédures d'audit.

- L'observation : En général, l'observation ne peut apporter des preuves très fiables du fonctionnement des contrôles qu'au moment de sa réalisation. De ce fait, l'auditeur doit réaliser d'autres procédures destinées à s'assurer que les contrôles ont été mis en œuvre de manière continue tout au long de la période auditée.

- L'examen d'une évidence tangible : La preuve que les procédures de contrôle interne ont été correctement appliquées peut être apportée par la recherche dans les documents de signes, tels que des initiales ou une signature, indiquant que le contrôle a été effectué.

  Des preuves concernant le contrôle interne peuvent aussi être fournies par l'examen de la documentation des systèmes, des manuels d'utilisation, des organigrammes ou des descriptions des postes. Ces documents décrivent les systèmes préconisés par la direction générale mais n'apportent pas la preuve que, dans la pratique, les contrôles sont effectués de manière régulière.

- La répétition : Il s'agit de refaire les contrôles effectués par l'entreprise ou les fonctions de traitement afin de s'assurer de leur exactitude. Refaire un contrôle peut fournir deux sortes de preuves :

- Des preuves de l'exactitude arithmétique et de la fiabilité du traitement des transactions comptables. Cette démarche est généralement essentielle pour obtenir l'assurance que les documents comptables sont complets et exacts.
- La découverte dans une transaction d'erreurs non détectées par les systèmes de contrôle est le signe du non-fonctionnement d'un contrôle ou d'une faiblesse dans les systèmes de contrôle.

En cas d'erreurs dans la transaction, la répétition d'un contrôle prouve soit son efficacité, si les erreurs ont été détectées et résolues de manière satisfaisante, soit son inefficacité. En l'absence d'erreurs dans la transaction, la répétition du contrôle ne permet pas de déterminer son manque de fiabilité ou les cas dans lesquels il n'a pas été réalisé avec efficacité.

Il y a lieu d'indiquer que la répétition n'est normalement considérée que si les autres procédures ne permettent pas l'obtention d'une assurance suffisante que le contrôle fonctionne d'une façon effective. En outre, un contrôle peut être si significatif (ayant des conséquences significatives sur la fiabilité des états financiers) que l'auditeur doit obtenir d'autres éléments probants assurant son fonctionnement effectif.

Exemple : Le contrôle désigné pour assurer l'exhaustivité, l'exactitude et l'autorisation de la mise à jour du fichier des données permanentes afférent aux taux d'intérêt dans une banque peut être si significatif pour l'exactitude des intérêts comptabilisés que l'auditeur cherchera d'autres éléments probants assurant le fonctionnement effectif du contrôle.

Signalons qu'en cas d'exceptions relevées, l'auditeur doit apprécier leurs implications possibles sur l'audit. Ceci est d'autant plus important en cas d'exceptions qui mettent en cause des systèmes informatiques. En effet, si les contrôles automatisés (et les contrôles manuels s'y rattachant) ou les fonctions de traitement informatisées sont inefficaces à un moment donné, il est probable qu'un certain nombre de transactions soient affectées. Par exemple :

- Une erreur décelée dans la logique de la fonction de traitement informatisée qui calcule les factures de vente affectera tous les calculs effectués de la même façon,
- Une erreur dans les prix de vente unitaires utilisés dans la préparation des factures aura pour conséquence de fausser toutes les facturations effectuées depuis l'apparition de l'erreur.

Une fois l'auditeur a déterminé que le contrôle automatisé fonctionne comme prévu, il doit considérer la réalisation des tests pour s'assurer que les contrôles ont fonctionné d'une façon permanente.

En raison de l'uniformité des traitements informatiques, un contrôle programmé est censé fonctionner d'une façon permanente sauf en cas de changement d'application. Par conséquent, la permanence des procédures de contrôles programmés n'est pas mise en cause lorsque les contrôles généraux informatiques sont effectivement opérationnels.

Il en découle que si l'auditeur a testé les contrôles généraux informatiques et a conclu qu'ils sont réellement fonctionnels, ceci constitue une évidence que les procédures de contrôles programmés ont été opérationnelles tout au long de la période auditée.

Ces tests peuvent englober la détermination que des modifications n'ont pas été apportées aux programmes sans respecter les contrôles appropriés des changements de programmes, que la version autorisée du programme est utilisée et que les contrôles généraux informatiques sont effectifs.

2. Les tests substantifs :

L'élaboration d'une approche d'audit adaptée aux risques identifiés suppose que l'on choisisse des procédures apportant un niveau approprié de conviction globale pour chaque assertion. Ainsi, les tests substantifs servent à valider les assertions d'audit non couvertes par les contrôles.

Les principaux types de tests substantifs sont les suivants :

- Procédures analytiques
- Demande d'informations et de confirmations
- Examen des documents et des enregistrements.

Dans un environnement de nouvelles technologies, les procédures analytiques sont, généralement, plus efficaces et plus efficientes que les tests de détail.

Par ailleurs, il y a lieu de noter que dans certaines circonstances où les éléments probants sont sous forme électronique, il peut ne pas être pratique ou possible de réduire le risque d'audit à un niveau acceptable en réalisant uniquement des tests substantifs. Le recours aux tests sur les contrôles est indispensable pour s'assurer de l'exactitude et de l'exhaustivité de ces éléments probants.

3. *Le recours aux techniques d'audit assistées par ordinateur (TAAO) :*

Dans un environnement de nouvelles technologies et en raison de la nature des systèmes informatiques, il est rarement possible de réaliser tous les tests requis d'une façon manuelle.

L'auditeur peut être conduit à appliquer des techniques qui utilisent l'ordinateur comme aide à l'audit. Ces techniques sont appelées Techniques d'Audit Assistées par Ordinateur[28] (TAAO).

Le recours aux TAAO peut être nécessaire dans les cas suivants :

- L'absence de documents d'entrée ou la production informatisée de transactions comptables par des programmes informatiques (par exemple, le calcul automatique des escomptes) peuvent empêcher l'examen des pièces justificatives par l'auditeur ;
- L'absence de visualisation du chemin d'audit ne permet pas à l'auditeur de suivre matériellement les opérations ;
- L'absence d'un document de sortie matérialisé peut exiger l'accès à des données conservées dans des fichiers lisibles uniquement par l'ordinateur.
- Le temps imparti à la réalisation de l'audit est limité.

Par ailleurs, l'utilisation des TAAO peut, dans certains cas, améliorer l'efficacité et l'efficience des procédures d'audit. En effet, l'utilisation des techniques informatisées offre l'accès à une quantité plus importante de données conservées dans le système informatique. En outre, dans le cas de systèmes informatiques complexes et intégrés, l'utilisation des TAAO ne répond pas uniquement à un objectif d'efficience de l'audit mais représente aussi à un élément nécessaire à son efficacité.

Les deux techniques d'audit assistées par ordinateur les plus fréquemment utilisées sont les logiciels d'audit et les jeux d'essai.

En outre, certains systèmes prévoient des commandes qui peuvent être utilisées par l'auditeur. Nous en citons à titre d'exemple la commande qui renseigne sur la gestion des mots de passe.

4. *Le cas particulier de l'externalisation :*

Les éléments probants, se rattachant aux contrôles, sont obtenus par :

- La réalisation des tests sur les contrôles auxquels l'entreprise soumet les activités du service bureau
- La réalisation des tests sur les contrôles directement sur le service bureau
- L'obtention d'un rapport de l'auditeur du service bureau sur l'efficacité du fonctionnement du système comptable et des contrôles internes du service bureau relatifs aux applications considérées dans l'audit.

Pour ce dernier cas, nous devons signaler que les rapports sont de deux types :

- Rapport sur l'adéquation de la conception
- Rapport sur l'adéquation de la conception et sur l'efficacité de fonctionnement

Dans tous les cas, l'auditeur doit envisager de vérifier les compétences professionnelles de l'auditeur du service bureau pour la mission spécifique qui lui a été confiée.

Toutefois, et vu la nouveauté des nouvelles technologies de l'information et de la communication, il est improbable que l'auditeur puisse obtenir ce genre de rapports. Dans ce cas, et en absence des autres possibilités mentionnées ci-dessus, l'auditeur peut être amené à considérer une limitation d'étendue au niveau de son opinion.

5. *Le calendrier des procédures d'audit :*

Le calendrier des procédures d'audit est devenu un point critique de l'audit. Dans un environnement de nouvelles technologies, le calendrier traditionnel peut être, dans certains cas, inadéquat.

5.1. Limitation de la conservation des évidences électroniques :

Le déroulement des procédures d'audit peut être influencé par le fait que des documents source, certains fichiers informatiques et d'autres éléments nécessaires à l'auditeur ne sont disponibles que pendant une courte période.

[28] Traduction française de « Computer Assisted Audit Techniques » (CAAT's).

En effet, les programmes informatiques peuvent résumer des transactions sur une base périodique et après purger, mettre à jour, changer, modifier, ou écrire sur les enregistrements originaux et détaillés des transactions. (Exemple : L'ERP Système 21 de JBA ne permet pas l'édition ou la consultation d'un état détaillé des stocks à une date antérieure donnée mais uniquement à la date de l'édition).

Par conséquent, l'auditeur devrait considérer, lors de l'élaboration de son calendrier d'intervention, la période au cours de laquelle l'information à tester existe ou est disponible.

5.2. Dispositions en cas de mise en place de nouvelles applications :

Lorsque le système est nouveau, l'auditeur peut décider de ne pas se fier aux contrôles de mise en place. Il pourra décider de tester les procédures de programmes au moment où le système devient opérationnel.

Toutefois, l'auditeur peut participer lors de la mise en place ou lors des modifications de tout système même s'il n'entend pas s'y fier et ce afin de fournir un service additionnel à la société en lui indiquant les déficiences au moment où l'on peut encore y remédier et afin de s'assurer que les modalités de contrôle nécessaires ont bien été prévues.

Cette possibilité correspond à une nécessité de la pratique dans la mesure où les demandes a posteriori de l'auditeur pour une amélioration des procédures programmées de contrôle sont souvent irréalistes pour l'entreprise en raison des coûts et des aspects techniques à résoudre. La mise en œuvre de cette possibilité suppose la compétence et le maintien de l'indépendance de l'auditeur[29].

Section 2 : Les effets des nouvelles technologies sur les aptitudes et les compétences nécessaires de l'auditeur financier

L'impact des nouvelles technologies sur les aptitudes et les compétences nécessaires de l'auditeur financier est certain. En effet, ce nouveau cadre d'intervention exige de sa part et d'une façon continue, de nouvelles aptitudes et compétences pour faire face à la complexité, de plus en plus croissante, des environnements informatiques. Ceci n'écarte pas la possibilité du recours à des spécialistes en cas de besoin.

Nous traitons au niveau de cette section :

- L'exigence d'un niveau de formation minimal de l'auditeur
- La composition de l'équipe intervenante dans une mission d'audit financier
- Les considérations en cas de recours à des spécialistes.

Sous section 1 : L'exigence d'un niveau de formation minimal de l'auditeur

L'auditeur doit avoir une connaissance suffisante des nouvelles technologies de l'information et de la communication et ce, afin de :

- déterminer l'effet de ces technologies sur l'évaluation du risque d'audit global et du risque au niveau du compte et au niveau de la transaction
- obtenir une compréhension de la structure du contrôle interne telle qu'affectée par ces technologies et son effet sur les transactions de l'entité
- déterminer et exécuter les tests sur les contrôles et les tests substantifs appropriés adaptés à la démarche particulière d'audit
- pouvoir mettre en œuvre les techniques d'audit assistées par ordinateur
- évaluer les résultats des procédures effectuées.

[29] Gérard PETIT, Daniel JOLY et Jocelyn MICHEL, « Guide pour l'audit financier des entreprises informatisées », Association technique d'harmonisation des cabinets d'audit et conseil ATH, édition CLET, 1985.

Par ailleurs, les nouvelles technologies de l'information et de la communication exigent de l'auditeur :

- une compétence et une expérience à la hauteur des difficultés rencontrées et de l'efficacité requise ; la formation permanente en séminaires et sur le terrain doit constituer un investissement important ;
- une recherche permanente des méthodes et techniques nouvelles et mieux adaptées.

Avec les développements constants dans tous les domaines, il est difficile que l'expert comptable soit spécialiste dans tous ces domaines. Il doit choisir soit de devenir un spécialiste dans le domaine des nouvelles technologies de l'information et de la communication, soit d'être spécialiste dans d'autres domaines. Dans ce dernier cas, l'auditeur doit, quand même, veiller à avoir un minimum de formation et de compétence en matière de nouvelles technologies de l'information et de la communication.

Ce niveau minimal doit lui permettre de :

- détecter la nécessité de faire appel à un spécialiste
- définir le domaine d'intervention du spécialiste
- diriger et superviser le déroulement des travaux du spécialiste
- intégrer les conclusions des travaux du spécialiste avec celles de l'audit.

En effet, il est utile de rappeler que l'auditeur ne peut en aucun cas déléguer la responsabilité de tirer les conclusions finales de l'audit ou celle d'exprimer son opinion sur l'information financière. En conséquence, lorsqu'il délègue certains travaux à des assistants ou qu'il a recours à des travaux effectués par d'autres auditeurs ou des experts qualifiés en nouvelles technologies de l'information et de la communication, l'auditeur doit posséder des connaissances suffisantes en la matière pour diriger, superviser et examiner les travaux des assistants qualifiés et/ou pour obtenir un degré raisonnable de certitude que les travaux effectués par d'autres auditeurs ou des experts qualifiés répondent bien à ses besoins.

Sous section 2 : La composition de l'équipe intervenante dans une mission d'audit financier

L'équipe d'audit est responsable de tous les aspects de la mission, même dans le cas où elle se heurte à des problèmes dépassant son champ de compétence. Qu'ils fassent appel à leurs propres compétences ou à des spécialistes externes travaillant sous leur direction, les membres de l'équipe doivent avoir une compréhension suffisante des problèmes affectant la mission d'audit pour pouvoir effectuer la planification et l'exécution.

Dans un système complexe, le recours à des auditeurs spécialisés dans le domaine informatique est l'une des conditions du succès de la mission d'audit.

Un système complexe est défini comme étant un système qui exige une connaissance profonde des environnements informatiques et qui présente, à titre d'exemple, les caractéristiques suivantes[30] :

- Une infrastructure et des contrôles informatiques complexes (décentralisation, intégration complexe, etc.)
- Le volume des opérations est tel qu'il est difficile aux utilisateurs d'identifier et de corriger des erreurs de saisie, de traitement, de restitution, de programmes, etc.,
- Le système génère automatiquement des opérations ou des écritures importantes intégrées directement dans une autre application
- Le système exécute des calculs complexes d'informations financières et/ou génère automatiquement des opérations ou des écritures importantes qui ne peuvent être validées indépendamment,
- L'existence d'opérations importantes faisant l'objet d'un échange électronique avec d'autres entités (EDI, E-commerce, E-business, etc.)
- La dématérialisation et la disponibilité limitée de la preuve d'audit.

[30] Norme internationale d'audit N°401 : « Audit réalisé dans un environnement informatisé », IFAC.

Un environnement de nouvelles technologies satisfait à la majorité de ces caractéristiques et est, par conséquent, jugé complexe.

Par ailleurs, la complexité d'un système est aussi appréciée par rapport au type de l'activité. A titre d'exemple : les activités financières sont supposées être complexes.

Sous section 3 : Considérations en cas de recours à des spécialistes

Le spécialiste peut être soit engagé par l'entité, ou engagé par l'auditeur, ou employé par l'entité, ou employé par l'auditeur.

Le recours aux spécialistes obéit à certaines règles détaillées ci-après[31].

1. La compétence du spécialiste :

Quand l'auditeur compte utiliser le travail d'un spécialiste, il doit s'assurer que celui-ci possède la compétence suffisante en vérifiant ses qualifications professionnelles, son autorisation d'exercer ou tout autre signe de reconnaissance de sa compétence.

Si le spécialiste fait partie d'un groupement professionnel édictant des normes que ses membres doivent respecter, l'auditeur peut se contenter de savoir que cette personne a bonne réputation au sein de ce groupement.

2. L'objectivité du spécialiste :

L'auditeur doit prendre en considération toutes les circonstances pouvant affecter l'objectivité de l'expert. Le risque de manque d'objectivité est plus élevé si le spécialiste est employé par l'entité auditée ou a avec elle une liaison directe ou indirecte.

En règle générale, il vaut mieux faire appel à un spécialiste indépendant de l'entité auditée et par conséquent plus objectif mais, si les circonstances l'exigent, on peut envisager d'utiliser le travail d'un membre du personnel de la société auditée, à condition que celui ci possède la compétence requise. Dans ce dernier cas, il est à notre avis plus judicieux de mettre en œuvre des procédures plus approfondies pour vérifier les hypothèses, les méthodes ou les conclusions du spécialiste employé par la société.

3. Définition des termes de l'intervention du spécialiste :

L'auditeur doit préciser clairement au spécialiste les conditions de son intervention et ce, en indiquant notamment l'objectif et l'étendue de ses travaux, les points spécifiques à traiter dans le rapport, l'utilisation que compte faire l'auditeur de ses travaux, les limites éventuelles d'accès aux documents et aux dossiers nécessaires, etc.

De son côté le spécialiste a la responsabilité de :

- comprendre la portée de son travail sur l'ensemble de l'audit
- porter rapidement à la connaissance du personnel d'audit approprié toutes les conclusions pouvant avoir une incidence significative sur l'audit ou devant être communiquées à la direction de l'entreprise
- contrôler la progression de son travail et d'avertir le personnel d'audit approprié de leurs difficultés éventuelles à respecter les délais ou les budgets.

4. L'évaluation des travaux du spécialiste :

Ceci englobe l'assurance que les travaux du spécialiste constituent des éléments probants appropriés au regard de l'information financière et ce, en examinant l'adéquation de la démarche suivie et la suffisance, la pertinence et la fiabilité des données utilisées pour aboutir aux conclusions formulées.

---

[31] Ces règles sont inspirés, essentiellement, de :

- la norme internationale d'audit N°620 : « Utilisation des travaux d'un expert », IFAC ;
- la directive d'audit des systèmes d'information : « Using the work of other auditors and experts », ISACA ;
- l'ouvrage : « Audit Guidance Series : Computer information system », Price Waterhouse ;
- mémoire de Mohamed Hichem RAIES : « Les aspects juridiques et techniques des recours aux spécialistes dans les missions d'audit », Avril 1987.

Bien que ce soit au spécialiste de garantir la pertinence et la vraisemblance de ses hypothèses et de ses méthodes, l'auditeur doit comprendre comment il les met en œuvre, afin de déterminer si elles sont raisonnables et identiques à celles qui ont été précédemment appliquées. L'auditeur se basera sur sa connaissance des activités de l'entreprise ainsi que du résultat des autres procédures d'audit.

5. La mention de l'intervention du spécialiste dans le rapport d'audit :

Lorsque l'auditeur émet une opinion sans réserve, il doit éviter de faire allusion dans son rapport de l'intervention du spécialiste car elle peut être interprétée comme une réserve ou comme un partage de responsabilité. Dans le cas contraire, si le rapport ou les conclusions du spécialiste amènent l'auditeur à émettre des réserves dans son rapport d'audit, il peut être utile d'en expliquer les raisons en faisant référence au travail du spécialiste et ce, avec l'accord de ce dernier et en citant son nom.

Si l'auditeur conclut que les travaux du spécialiste ne confirment pas l'information figurant dans les comptes annuels ou ne constituent pas des éléments probants suffisants et appropriés, il doit, selon le cas, émettre une opinion avec réserve ou émettre une opinion défavorable.

Conclusion :

Il est certain que les auditeurs financiers ne peuvent plus ignorer le phénomène de l'informatisation des entreprises devenue de plus en plus complexe avec les nouvelles technologies de l'information et de la communication.

L'environnement des nouvelles technologies devrait, par conséquent, être intégré dans la démarche de l'audit financier. En outre, il doit constituer, en permanence, l'une des préoccupations de l'auditeur afin de mettre à niveau ses aptitudes et ses compétences.

Cette mise à niveau de l'approche d'audit est une préoccupation majeure et d'actualité des divers organismes professionnels et de la majorité des cabinets internationaux d'audit.

Parallèlement, la législation, la jurisprudence et la doctrine à l'échelle internationale se sont enrichies de règles nouvelles destinées à réglementer et à contrôler certains aspects des systèmes informatisés.

Ces deux volets font l'objet d'une étude plus détaillée dans le chapitre suivant.

Chapitre 3 : Les Principales Réactions des Législations et des Organismes Professionnels Face aux Evolutions Informatiques

Introduction

Ce chapitre est destiné à présenter les principales réactions des législations et des organismes professionnels face aux évolutions informatiques.

Cette présentation n'est pas limitée aux seuls aspects des nouvelles technologies mais couvre aussi les différentes réactions se rattachant à l'informatique en général.

En outre, nous avons essayé, tout au long de ce chapitre, de comparer les réactions en Tunisie par rapport à celles d'autres pays (dont, essentiellement, la France) et par rapport à d'autres réflexions internationales.

Section 1 : La réglementation comptable, fiscale et juridique

Sous section 1 : La réglementation comptable

Les dispositions du Code de Commerce, non abrogées par la loi 2000-93 du 3 novembre 2000 portant promulgation du nouveau code des sociétés commerciales, se rapportant aux obligations en matière comptable sont les suivantes :

- Article 8 : « … Conserver, pendant dix ans tous les documents justificatifs des opérations inscrites sur les livres susvisés ».
- Article 9 : « Le livre journal et le livre d'inventaire prévus à l'article 8 sont cotés et paraphés, soit par le juge, soit par le Président de la Municipalité ou un adjoint, dans la forme ordinaire et sans frais ».
- Article 10 : « les livres sont tenus chronologiquement sans blanc ni altération d'aucune sorte. Ils seront conservés pendant 10 ans ».
- Article 11 : « Les livres, que les commerçants sont obligés de tenir et pour lesquels ils n'auront pas observé les formalités ci-dessus prescrites, ne pourront être représentés ni faire foi en justice au profit de ceux qui les auront tenus, sans préjudice de ce qui sera réglé au livre du concordat préventif et de la faillite. ».

Ainsi, le code de commerce tunisien n'a pas prévu de dispositions particulières en cas de comptabilité informatisée. En effet, il n'a pas précisé les conditions de forme pour les pièces justificatives des opérations ni les conditions et les moyens de conservation.

Au niveau du livre journal et du livre d'inventaire, ils doivent être tenus manuellement sur des registres cotés (attestant le nombre des pages) et paraphés (certifiant l'existence du livre obligatoire et lui conférant une date certaine).

En outre, il convient de signaler qu'aucune nouvelle disposition comptable n'a été prévue par le nouveau code des sociétés commerciales promulgué par la loi 2000-93 du 3 novembre 2000.

La loi N°96-112 du 30 décembre 1996 relative au système comptable des entreprises a apporté de nouvelles dispositions et a aussi confirmé les des articles 8, 9 et 10 du code de commerce.

Ces principales dispositions, qui se rapprochent de celles du Nouveau Plan Comptable Général Français de 1999, se résument comme suit :

1. Les livres comptables :

Les livres comptables comportent le journal général, le grand-livre et le livre d'inventaire. Le journal général et le livre d'inventaire sont cotés et paraphés. En outre, les livres sont établis sans blanc ni altération d'aucune sorte.

Selon l'article 14 de la loi 96-112, « les documents écrits issus de l'informatique peuvent tenir lieu de livres et journaux auxiliaires. Dans ce cas, ces documents doivent être identifiés, numérotés et datés dès leur élaboration par des moyens offrant toute garantie en matière de preuve..... Les écritures portées sur les livres et journaux auxiliaires ainsi que les totaux des opérations et des soldes doivent être centralisés dans le journal général et le grand livre au moins une fois par mois. »

Ainsi, nous devons formuler les remarques suivantes :

- Les documents informatiques ne peuvent tenir lieu de livre journal et de livre d'inventaire comme c'est le cas en France[32]. Cette possibilité n'a été accordée que pour les livres et journaux auxiliaires.
- Que faut-il entendre par « des moyens offrant toute garantie en matière de preuve » ?

  Signalons d'abord que cette disposition est identique à celle prévue en France[33]. Plusieurs solutions critiquables ont été avancées. Selon le Mémento Comptable dans son paragraphe 311-2, bien que la réglementation française a considéré que les documents informatiques peuvent tenir lieu de journal général et de livre d'inventaire, « la manière la plus pratique de respecter actuellement l'obligation de la tenue du livre journal sans aucun risque, reste et demeure, pour l'instant, la transcription manuelle des totalisations des écritures mensuelles sur un livre coté et paraphé ».

2. La documentation des procédures et de l'organisation Comptable :

L'article 15 de la loi 96-112 stipule que : « lorsque l'entreprise opte pour la méthode de centralisation mensuelle des livres et journaux auxiliaires ou pour l'usage de l'informatique pour tenir sa comptabilité, il est établi un document qui prévoit l'organisation comptable et comporte notamment les intitulés et l'objet des documents utilisés pour le traitement des informations et les modalités de liaison entre ces documents et les pièces justificatives y afférentes. »

La norme générale[34] a précisé le contenu de ce document. En ce qui concerne les traitements informatisés, ce manuel doit comprendre notamment :

1. La description des procédures de collecte, de saisie, de traitement et de contrôle des informations ;
2. Le système de classement et d'archivage ;
3. Les livres comptables obligatoires et les liens entre ces livres et les autres documents et pièces comptables.

En outre, le paragraphe 49 et 50 de la norme générale stipulent que « la réalisation de tout contrôle du système de traitement automatisé suppose l'accès à la documentation relative aux analyses, à la programmation et à l'exécution des traitements en vue, notamment, de procéder aux tests nécessaires.[35]

Dans le cas d'acquisition de logiciel standard, la documentation fournie avec le logiciel peut constituer la documentation requise. »

---

[32] Dispositions prévues par le décret N°83-1020 du 29 novembre 1983 portant promulgation des obligations comptables des commerçants de certaines sociétés et par le Nouveau Plan Comptable Général homologué par l'arrêté du 22 juin 1999 (paragraphe 410-06.)

[33] Idem

[34] Deuxième partie, Paragraphe 63

[35] Même disposition que le paragraphe 410-4 du Nouveau Plan Comptable Générale Français 1999 : «L'organisation de la comptabilité tenue au moyen de systèmes informatisés implique l'accès à la documentation relative aux analyses, à la programmation et à l'exécution des traitements, en vue, notamment, de procéder aux tests nécessaires à la vérification des conditions d'enregistrement et de conservation des écritures. »

Cette documentation décrivant les procédures et l'organisation comptables est établie en vue de permettre la compréhension et le contrôle du système de traitement. Elle doit être complète, claire, précise et constamment tenue à jour. Elle est conservée aussi longtemps qu'est exigée la présentation des documents comptables auxquels elle se rapporte. Toutefois, il y a lieu de préciser qu'aucune sanction n'est prévue pour le non-respect de cette disposition.

En pratique, nous constatons que cette documentation est quasiment absente dans les entreprises ou est dans la majorité des cas obsolète. Par ailleurs, la documentation fournie avec le logiciel standard ne concerne généralement que le volet d'utilisation et d'exploitation.

3. Les pièces justificatives :

Selon le paragraphe 53 de la norme générale (partie II : dispositions relatives à l'organisation comptable) : « La pièce justificative est établie sur papier ou sur un support assurant la fiabilité, la conservation et la restitution en clair de son contenu pendant les délais requis et comporte la mention de la date ».

Cette disposition est identique à celle du paragraphe 420-3 du Nouveau Plan Comptable Général Français de 1999.

Selon le Conseil National de la Comptabilité Français[36], les résultats de traitement en amont peuvent être intégrés en comptabilité à l'aide d'écritures comptables générées automatiquement par le système, sans être accompagnées de l'émission de pièces justificatives classiques (exemple : le calcul des agios effectué par les banques).

4. Le chemin de révision :

Le Nouveau Système Comptable Tunisien stipule dans son article 12 que : « Tout enregistrement précise l'origine, le contenu et l'imputation de l'opération ainsi que les références des pièces justificatives qui l'appuient »[37].

Le paragraphe 52 de la norme générale (partie II : Dispositions relatives à l'organisation comptable) ajoute que : « à tout moment, il est possible de reconstituer à partir des pièces justificatives appuyant les données entrées, les éléments des comptes, état et renseignements soumis à la vérification, ou, à partir de ces comptes, états et renseignements, de retrouver ces données et les pièces justificatives»[38].

C'est ainsi que tout solde de compte doit pouvoir être justifié par un relevé des écritures dont il découle depuis un solde antérieur. Chacune de ces écritures doit comporter une référence permettant l'identification des données correspondantes.

5. Le caractère définitif des enregistrements :

Selon les paragraphes 56 et 57 de la norme générale (Partie II) : « le caractère définitif des enregistrements est assuré, pour les comptabilités tenues au moyen de systèmes informatisés, par la validation. Cette procédure, qui interdit toute modification ou suppression de l'enregistrement est mise en œuvre au plus tard au terme de chaque mois.[39]

Une procédure de clôture destinée à figer la chronologie et à garantir l'intangibilité des enregistrements est mise en œuvre et ce, au plus tard avant l'expiration de la période suivante, sous réserve des délais différents fixés par des dispositions légales ou réglementaires. ».

Cette mesure vise à interdire la modification ou la suppression des données sans laisser de traces. En informatique, elle est en principe assurée par la validation, la clôture et l'utilisation d'un support de sauvegarde inaltérable.

Par ailleurs, et selon le mémento comptable 2000, si l'entreprise utilise un système comptable ne garantissant pas l'absence d'altération, ceci peut remettre en cause la force probante de la comptabilité. « Une telle situation constitue pour le commissaire aux comptes un facteur de risque qu'il doit intégrer dans son approche générale d'audit et dont il doit tirer les conséquences dans son plan de mission. Par ailleurs, dans la mesure où les insuffisances du système comptable seraient de nature à enlever toute force probante aux contrôles effectués par le commissaire aux comptes, celui-ci serait conduit à formuler une réserve dans l'expression de son opinion sur les comptes. »

---

[36] Bulletin N°88 du 3ème trimestre 1991, page 4 et suivant.
[37] Disposition identique aux dispositions du paragraphe 420-2 du Nouveau Plan Comptable Général Français 1999
[38] Disposition identique aux dispositions du paragraphe 410-3 du Nouveau Plan Comptable Général Français 1999
[39] Disposition identique aux dispositions du paragraphe 420-5 du Nouveau Plan Comptable Général Français 1999

Il convient de distinguer trois phases pour apprécier la validité d'une comptabilité informatisée :

- Avant la validation comptable d'une écriture : la modification est dans ce cas permise. En effet, tant que la validation n'est pas faite, les écritures ne font pas partie du système comptable.
- La validation comptable proprement dite : Il s'agit d'une étape qui consiste à figer les différents éléments de l'écriture de façon à ce que toute modification ultérieure soit impossible. Cette étape devrait être réalisée au moins mensuellement.
- Après la validation comptable d'une écriture : Toute modification devrait être impossible.

6. Les procédés et les moyens de traitement de l'information :

Selon le paragraphe 47 de la norme comptable générale[40], « l'organisation de la comptabilité tenue au moyen de systèmes informatisés doit permettre :

- de satisfaire les exigences de sécurités et de fiabilité requises en la matière
- de restituer sur papier sous une forme directement intelligible toute donnée entrée dans le système de traitement ».

Le paragraphe 48 ajoute que : « l'identification des documents informatiques est obtenue par :

- Une numérotation des pages,
- L'utilisation de la date du jour de traitement générée par le système et qui ne peut être modifiée par l'entreprise, pour dater les documents,
- L'utilisation d'un programme interdisant l'annulation ou la modification des opérations validées ».

Sous section 2 : La réglementation fiscale

L'étude de la réglementation fiscale touchant les aspects informatiques et les nouvelles technologies couvre deux aspects :

- Le régime fiscal des opérations
- Les obligations des contribuables

1. Le régime fiscal des opérations :

Les opérations réalisées à travers Internet posent une multitude de questions fiscales dont : Les taxes de ventes, et en particulier la TVA, sont-elles applicables pour les ventes de produits à l'international ? Et comment taxer les produits immatériels, informations ou produits numériques téléchargeables (logiciels, films, musique, voyages…) ?

1.1. Pour les biens physiques :

La commercialisation de biens physiques et leur exportation ou importation n'est pas un obstacle à la perception de droits fiscaux et de droits de douanes. Bien évidemment, les réglementations douanières peuvent limiter l'expédition ou l'importation de certains produits suivant leur nature de ou vers tel ou tel pays.

1.2. Pour les biens immatériels :

Ces taxes et droits de douanes s'appliquent également aux produits immatériels, mais leur perception est quasi impossible compte tenu de la difficulté de contrôler la circulation des biens immatériels et de l'absence de « filtres douaniers » ou « guichets de douane virtuels » au sein du réseau Internet.

Afin d'officialiser cet état de fait, un moratoire a été signé par les pays membres de l'OCDE[41] à Amsterdam début mai 1998, reculant à l'an 2000 toute décision en ce domaine. Ceci est suite à la pression des Etats Unis d'Amérique qui souhaiteraient la disparition de toutes les taxes et droits de douane sur les transactions commerciales effectuées sur le réseau international de l'Internet et ce, dans un objectif de développement plus rapide de ce nouveau circuit commercial.

[40] Partie 2 de la Norme Générale : « Dispositions relatives à l'organisation comptable ».
[41] O.C.D.E. : « Organisation de Coopération et de Développement Economique » : Groupe constitué à Paris en 1961 par les dix-neuf Etats européens membres de l'ex-O.E.C.E (Organisation Européenne de Coopération Economique) et par quelques pays non européens (Australie, Canada, Etas Unis, Nouvelle zélande, Japon, Mexique) en vue de favoriser l'expansion des Etats membres et des Etats en voie de développement.

2. *Les obligations des contribuables :*

Les obligations des contribuables se présentent comme suit :

2.1. En Tunisie :

Les principales dispositions fiscales tunisiennes en la matière se résument dans ce qui suit :

A/ Dispositions en matière de comptabilité informatisée :

L'article 62 alinéa II du code de l'impôt sur le revenu des personnes physiques et de l'impôt sur les sociétés stipule que « les personnes qui tiennent leur comptabilité sur ordinateur doivent :

- Déposer, contre accusé de réception, au bureau de contrôle des impôts dont elles relèvent un exemplaire du programme initial ou modifié sur support magnétique ;
- Informer ledit bureau de la nature du matériel utilisé, du lieu de son implantation et de tout changement apporté à ces données.»[42]

Ce même article ajoute dans son alinéa IV que « les livres de commerce et autres documents comptables, et d'une façon générale, tous documents dont la tenue et la production sont prescrites en exécution du présent code doivent être conservés pendant 10 ans. »

Par ailleurs, la loi de finances pour la gestion de 1998 dans ses articles 75, 76, 77 et 78 a harmonisé les obligations comptables prévues par la législation fiscale avec les dispositions de la législation comptable des entreprises (Loi 96-112 du 30 décembre 1996). Ainsi, et sur le plan fiscal, les entreprises qui tiennent leur comptabilité sur ordinateur demeurent astreintes à la tenue des documents prescrits par la législation comptable à savoir le journal général, le grand-livre et le livre d'inventaire.

En outre, et dans le cas où la comptabilité est tenue sur ordinateur, par le moyen de logiciels informatiques destinés à l'usage collectif et élaborés par les entreprises des services informatiques, ces derniers peuvent déposer, au lieu et place de leurs entreprises clientes, une copie du programme initial ou modifié sur supports magnétiques, à condition de faire parvenir aux services du contrôle fiscal la liste de la clientèle utilisant lesdits programmes[43].

Par ailleurs et selon les dispositions de la loi N° 2000-82 du 09 août 2000 portant promulgation du code des droits et des procédures fiscaux, les personnes soumises à la tenue d'une comptabilité conformément à l'article 62 du code de l'IRPP et de l'IS, doivent communiquer, en cas de contrôle et entre autres, les programmes, logiciels et applications informatiques utilisés pour l'arrêté des comptes ou pour l'établissement de leurs déclarations fiscales.

En outre, les personnes qui tiennent leur comptabilité ou établissent leurs déclarations fiscales par les moyens informatiques, doivent communiquer, aux agents de l'administration fiscale, les informations et éclaircissements que les agents de l'administration leur demandent dans le cadre de l'exercice de leurs fonctions.

Selon l'article 97 de la loi 2000-82 précitée, toute personne qui refuse de communiquer ou qui a détruit, avant l'expiration de la durée légale de conservation, la comptabilité, les registres ou répertoires prescrits par la législation fiscale est punie d'une amende allant de 100 dinars à 10.000 dinars.

B/ Dispositions en matière de factures :

L'article 18 du code de la TVA stipule dans son alinéa III que :

« **1)** Les assujettis à la TVA sont tenus :

- d'utiliser des factures numérotées dans une série ininterrompue
- de déclarer au bureau de contrôle des impôts de leur circonscription les noms et adresses de leurs fournisseurs en factures.

2) Les imprimeurs doivent tenir un registre coté et paraphé par les services du contrôle fiscal sur lequel sont inscrits, pour toute opération de livraison, les noms, adresses et matricules fiscaux des clients, le nombre de carnets de factures livrés ainsi que leur série numérique.

[42] Article 75 de la loi N°97-88 du 29 décembre 1997 portant loi de finances pour l'année 1998
[43] Note commune 19/98

Cette mesure s'applique aux entreprises qui procèdent à l'impression de leurs factures par leurs propres moyens. »

Par ailleurs, l'administration fiscale n'a pas encore traité la dématérialisation des factures et leur transmission par voir télématique.

En outre, selon l'article 96 du nouveau code des droits et procédures fiscaux[44], « est punie d'une amende de 1.000 dinars à 50.000 dinars, toute personne qui procède à l'impression de factures non numérotées ou numérotées dans une série irrégulière ou interrompue ».

Aussi, et selon le même article, « est punie d'une amende de 50 dinars à 1.000 dinars par facture, toute personne qui utilise des factures non numérotées ou numérotées dans une série irrégulière ou interrompue. »

C/ Assouplissement pour l'accomplissement des obligations fiscales :

Les articles 57 et 58 de la loi N°2000-101 du 31 décembre 2000, portant loi de finances pour l'année 2001, ont institué des mesures d'assouplissement pour l'accomplissement des obligations fiscales.

Afin de bénéficier des nouvelles technologies de la communication et dans un souci de simplification des procédures d'accomplissement des obligations fiscales, la loi de finances pour la gestion 2001 a prévu la possibilité de dépôt des déclarations fiscales et de paiement de l'impôt par des moyens électroniques. Les procédés correspondants seront fixés par décret.

En attendant la parution de ce décret, ce qui demandera nécessairement du temps étant donné l'importance de la question, la loi de finances pour la gestion 2001 a prévu, au profit des contribuables soumis au régime réel d'imposition, la possibilité de dépôt des déclarations fiscales et autres documents sur des supports magnétiques au lieu et place des procédés classiques (sur papier). Les modalités pratiques seront, aussi, fixées par décret[45].

2.2. En France :

En France, depuis le début des années 80, la direction générale des impôts (DGI) a modernisé les procédures de transmission des informations à l'administration. Elle a développé une nouvelle application dite Transfert des Données Fiscales et Comptables (TDFC).

L'article 47 de la loi de finances rectificative pour 1990 (décret d'application n° 91-579 du 20 juin 1991) autorise la dématérialisation des factures et la transmission par voie télématique si elles répondent à certaines conditions et si l'administration a donné expressément son accord.

L'arrêté du 26 janvier 1993 admet la transmission par voie informatique de la déclaration d'échange de biens en matière douanière.

En outre, entre 1990 et 1996, plusieurs textes sont venus définir progressivement le cadre et les modalités de vérification, par l'administration fiscale, des comptabilités informatisées :

- 1990 : Définition des aspects informatiques susceptibles d'être vérifiés. « lorsque la comptabilité est tenue au moyen de systèmes informatisés, le contrôle porte sur l'ensemble des informations, données et traitements informatiques qui concourent directement ou indirectement à la formation des résultats comptables ou fiscaux et à l'élaboration des déclarations rendues obligatoires par le code général des impôts ainsi que sur la documentation relative aux analyses, à la programmation et à l'exécution des traitements. »[46]
- 1991 : Publication de l'instruction du 14 octobre 1991 précisant les modalités de conservation des informations, données et traitements, ainsi que le cadre et les conditions de contrôle des comptabilités informatisées.
- 1996 : Réaffirmation de la volonté de l'administration fiscale dans l'instruction du 24 décembre 1996 de poursuivre dans la voie de l'instruction de 1991, tout en apportant des éclaircissements et des précisions quant aux modalités d'archivage des comptabilités informatisées.
- Eléments d'actualité : « Après sept années de mise en place de ces procédures de contrôle des comptabilités informatisées, l'attitude de l'administration fiscale française semble s'orienter vers une application plus systématique des sanctions fiscales prévues par les textes (procédure d'évaluation d'office) ».[47]

[44] Code promulgué par la loi 2000 – 82 du 9 août 2000 portant promulgation du code des droits et procédures fiscaux.
[45] Décret non encore paru à la date de la rédaction du présent mémoire.
[46] Article 103 de la loi de finances pour la gestion de l'exercice 1999
[47] « Bulletin Comptable et Financier », Avril 1997, Edition Francis Lefèvre.

Les principales dispositions fiscales en France sont les suivantes :

A/ La documentation technique :

La documentation doit poursuivre un double objectif :

- Informatique : l'analyse de la documentation doit permettre aux vérificateurs de connaître et de comprendre le système d'information en vigueur au cours de la période soumise au contrôle, y compris l'ensemble des évolutions significatives.
- Fiscal : la documentation doit décrire de façon suffisamment précise et explicite les règles de gestion des données et des fichiers mises en œuvre dans les programmes informatiques et qui ont une incidence sur la formation du résultat comptable, du résultat fiscal et des déclarations rendues obligatoires par le code général des impôts.

L'instruction du 14 octobre 1991 énumère de façon exhaustive la documentation susceptible d'être vérifiée lors d'un contrôle fiscal : il s'agit de "la documentation relative aux analyses, à la programmation et à l'exécution des traitements". Ceci implique au minimum :

- Un dossier de présentation générale de l'organisation et de fonctionnement du système d'information et moyens informatiques (humains et matériels),
- Les dossiers de conception, de réalisation et de maintenance
- Les dossiers d'utilisation et d'exploitation

B/ Conservation des données et des traitements :

Les données soumises à l'obligation de conservation sont définies par leur relation avec la formation des résultats comptable et fiscal et des diverses déclarations obligatoires.

D'une façon générale, les livres, registres, documents ou pièces quelconques doivent être conservés pendant un délai de six ans.

S'il s'agit de documents établis ou reçus sur support informatique, ils doivent être conservés sur leur support original au minimum pendant trois ans. Passé ce délai, ils peuvent être conservés sur support informatique ou sur tout autre support.

La documentation relative aux analyses, à la programmation et à l'exécution des traitements doit être conservée jusqu'à l'expiration de la troisième année suivant celle à laquelle elle se rapporte.

La non-présentation des informations, données et traitements informatiques requis par l'administration ainsi que de la documentation informatique, pour quelque motif que ce soit, exemple : absence de conservation, archives détruites, archives illisibles par suite d'un changement de système, constitue une opposition au contrôle fiscal. Dans cette situation, les bases d'imposition peuvent faire l'objet de redressement selon la procédure d'évaluation d'office et entraîner l'application d'une amende de 150%.

Sous section 3 : La réglementation juridique

Ce volet représente un domaine très vaste et le présent mémoire ne peut songer à une couverture totale de tous les aspects. Nous avons essayé de présenter les principaux.

1. La réglementation juridique en Tunisie :

En Tunisie, la réglementation juridique spécifique à l'informatique se résume, essentiellement, dans ce qui suit :

1.1. Loi 94-36 du 24 février 1994 relative à la propriété littéraire et artistique :

Les grands axes de cette loi se rapportant aux logiciels sont les suivants :

- Le logiciel crée par un ou plusieurs salariés d'un organisme appartient, sauf stipulation contraire, à cet organisme employeur ;
- Sauf stipulation contraire, l'auteur ne peut s'opposer à l'adaptation du logiciel par des tiers dans la limite des droits qu'il leur a cédés ;
- Sauf stipulation contraire, toute production autre que l'établissement d'une copie de sauvegarde par l'utilisateur ainsi que toute utilisation d'un logiciel non expressément autorisée par l'auteur ou

des ayants droits, est interdite. Toute infraction est passible d'une amende de 500 à 5000 dinars et/ou d'un emprisonnement de un à six mois ;

- Les droits prévus s'éteignent à l'expiration d'une période de vingt cinq ans à compter de la date de la création du logiciel.

1.2. Loi 2000-57 du 13 juin 2000 :

Cette loi a adapté les dispositions du code des obligations et des contrats aux exigences du commerce sur Internet en introduisant l'usage légal de la signature électronique et des documents électroniques pour conclure des contrats sur Internet.

1.3. Loi 2000-83 du 09 août 2000 relative aux échanges et au commerce électronique :

Cette loi a réglementé l'activité du fournisseur de certification électronique. Elle a prévu aussi la création de l'ANCE (Agence Nationale de Certification Electronique) chargée de chapeauter les fournisseurs privés de services de certification électronique et de définir des normes pour les dispositifs de création et de vérification des signatures électroniques.

En outre, cette loi a prévu d'autres dispositions régissant les échanges et le commerce électronique dont les principales sont :

A/ Documents et signatures électroniques :

- La conservation du document électronique fait foi au même titre que la conservation du document écrit (article 4). L'émetteur s'engage à conserver le document électronique dans la forme de l'émission. Le destinataire s'engage à conserver ce document dans la forme de la réception.
- Le document électronique est conservé sur un support électronique permettant :
  1. La consultation de son contenu tout au long de la durée de sa validité
  2. Sa conservation dans sa forme définitive de manière à assurer l'intégrité de son contenu
  3. La conservation des informations relatives à son origine et sa destination ainsi que la date et le lieu de son émission ou de sa réception.
- La loi admet l'apposition d'une signature électronique sous réserve de l'existence d'un dispositif fiable dont les caractéristiques techniques seront fixées par décret.[48]

B/ Des transactions commerciales électroniques :

- Avant la conclusion du contrat, le vendeur est tenu lors des transactions commerciales électroniques de fournir au consommateur de manière claire et compréhensible toutes les informations se rattachant à la transaction et au paiement.
- La loi énumère les obligations et les droits aussi bien du consommateur que du vendeur.

C/ Protection des données personnelles :

- Le fournisseur de services de certification ne peut traiter les données personnelles qu'après accord du titulaire du certificat concerné. Auquel cas, il doit appliquer des procédures suffisantes pour la protection de ces données.
- Sauf consentement du titulaire du certificat, le fournisseur de services de certification électronique ou un de ses agents ne peut collecter les informations relatives au titulaire du certificat que dans le cas où ces informations seraient nécessaires à la conclusion du contrat, à la fixation de son contenu, à son exécution et à la préparation et l'émission des factures.

1.4. Loi N° 2001-1 du 15 janvier 2001 portant promulgation du code des télécommunications :

Le code des télécommunications a pour objet l'organisation du secteur des télécommunications. Parmi les principales sanctions prévues par ce code, nous citons :

- est puni d'un emprisonnement de 3 mois, quiconque divulgue, incite ou participe à la divulgation du contenu des communications et des échanges transmis à travers les réseaux des télécommunications.

[48] Décret non encore paru à la date de la rédaction du présent mémoire

- est puni d'un emprisonnement de six mois à cinq ans et d'une amende de 1.000 à 5.000 DT ou de l'une de ces deux peines seulement, celui qui utilise, fabrique, importe, exporte, détient en vue de la vente ou la distribution à titre gratuit ou onéreux ou met en vente ou vend les moyens ou les services de cryptologie en violation de la réglementation en vigueur.

1.5. Code pénal :

Les principales dispositions du code pénal, pouvant être appliquées dans un contexte d'environnement informatique, sont :

- Vol : Selon l'article 258 du Code Pénal « Quiconque soustrait frauduleusement une chose qui ne lui appartient pas est coupable de vol ». Il ne s'applique qu'à la soustraction de biens corporels (ordinateurs, périphériques...).
- Escroquerie : L'escroquerie est définie à l'article 291 du Code Pénal. Elle est caractérisée par une tromperie. L'auteur de l'infraction obtient de sa victime la remise de fonds, de valeurs ou de biens. En informatique, la chose remise est, la plupart des temps, des fonds.
- Abus de confiance : Il est prévu par l'article 297 du Code Pénal. A l'inverse de l'escroquerie, la chose détournée a été remise avec le consentement de la victime. L'auteur de l'infraction l'a accepté par contrat et s'est engagé à la restituer ou à en faire un usage déterminé.
- Dommages divers à la propriété d'autrui : Prévus par l'article 304 et suivant du code pénal et concernent quiconque, volontairement, cause un dommage à la propriété immobilière ou mobilière d'autrui.

2. La réglementation juridique en France :

2.1. Loi du 6 janvier 1978 « Informatique et libertés » :

Cette loi décrit les règles relatives à l'informatique, aux fichiers et aux libertés. Sa portée est limitée à la protection des données nominatives.

Son objectif est d'éviter que l'informatique ne puisse porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Elle expose les contrevenants à des sanctions allant de 2.000 à 2.000.000 Francs Français d'amende et de 6 mois à 5 ans de prison.

Par ailleurs, en date du 24 octobre 1995, le parlement européen et du conseil a promulgué la Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données entre les Etats membres.

2.2. Loi du 3 juillet 1985 : La protection des logiciels

L'objectif de cette loi est d'étendre aux logiciels le régime de protection du droit d'auteur (loi du 11 mars 1957). Ce droit doit être défini dans un cadre contractuel (incessibilité du produit, interdiction des copies, limitation du nombre de sites d'utilisation).

Il existe plusieurs types de piratage de logiciel :

- La reproduction intégrale sans l'autorisation de l'auteur (sauf copie de secours),
- La reproduction partielle ou l'imitation d'un logiciel,
- L'utilisation d'un logiciel sans licence.

Le piratage d'un logiciel constitue un acte de contrefaçon (délit pénal). Les sanctions peuvent être lourdes (jusqu'à deux ans de prison en sus d'une amende).

Du point de vue pratique, un éditeur de logiciels peut mandater un commissaire de police qui viendra à l'improviste vérifier tous les postes informatiques de l'entreprise.

2.3. La réglementation de la cryptologie :

Le décret N° 86-250 du 18 février 1986 assimile les matériels et logiciels de chiffrement à des armes de guerre, et donc les soumet au régime strict de l'autorisation préalable.

La loi du 29 décembre 1990 assouplit légèrement cette réglementation, en instituant un régime de simple déclaration préalable auprès du Service Central de la Sécurité des Systèmes Informatiques (S.C.S.S.I), si l'utilisation est faite à des fins d'authentification ou d'intégrité. L'autorisation étant maintenue dans les autres cas, c'est-à-dire chaque fois qu'il y a chiffrement de fichiers.

Les défauts de déclaration ou d'autorisation sont sanctionnés de 6.000 à 500.000 Francs Français d'amende et de 1 mois à 1 an de prison.

2.4. La loi N°88-19 du 5 janvier 1988 (Loi GODFRAIN) relative à la fraude informatique :

Par la loi GODFRAIN, un vide juridique qui persistait en matière de fraude informatique a été comblé. Cette loi punit :

- l'accès ou le maintien non autorisé dans tout ou partie d'un Système d'Information,
- le fait d'entraver ou de fausser le fonctionnement d'un Système d'Information,
- l'introduction ou la modification non autorisée des données ou leur code de traitement ou de transmission,
- la falsification des documents informatisés,
- l'usage de documents informatisés falsifiés.

Les tentatives, même infructueuses, sont passibles des mêmes sanctions, pouvant atteindre 2.000.000 Francs Français et/ou 5 ans d'emprisonnement.

2.5. La loi du 10 juillet 1991 relative à la protection des télécommunications :

Son objectif est de préserver le secret des correspondances émises par la voie des télécommunications. Elle ne concerne pas que les écoutes téléphoniques, mais aussi les transmissions de données.

Cette loi interdit l'installation d'appareils d'interception. Elle interdit, aussi, l'interception, le détournement, l'utilisation et la divulgation des informations transmises par télécommunication.

Elle prévoit des sanctions allant de 5.000 à 100.000 Francs Français d'amende et de 6 jours à 1 an de prison.

2.6. Loi MADELIN du 11 février 1994 :

Il est entendu que la preuve est libre pour les actes de commerce conclus entre commerçants.

L'article 4 alinéa I de la loi sus-visée a élargi ces possibilités en disposant que les entreprises peuvent remplacer toutes déclarations écrites par un message électronique équivalent. La conclusion d'un contrat précisant les règles en matière de preuve est nécessaire (identification de l'auteur, lisibilité, fiabilité et intégrité de la transmission, horodatation, réception et archivage).

2.7. Loi 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique 49:

La signature électronique et la valeur probante du document numérique sont reconnus par la loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

Les principales dispositions sont les suivantes :

- Art. 1316-1 : L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.
- Art. 1316-3 : L'écrit sur support électronique a la même force probante que l'écrit sur support papier.
- Art. 1316-4 : La signature, lorsqu'elle est électronique, consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.

Le Décret N° 2001-272 du 30 mars 2001, a défini les conditions de fiabilité d'un procédé de signature électronique assurant l'identité du signataire et garantissant l'intégrité de l'acte.

[49] Cette loi a été éléborée conformément à la directive 1999/93/CE du Parlement Européen et du Conseil du 13 décembre 1999 portant sur un cadre communautaire pour les signatures électroniques.

2.8. Dispositions particulières du Code Pénal :

Les dispositions du Code Pénal Français en la matière sont similaires à celles des dispositions du Code Pénal Tunisien.

Toutefois, il est utile d'ajouter qu'en matière de vol, il est admis par les tribunaux français qu'un vol est commis en cas de reproduction d'un support matériel (disquette...) alors que la chose volée est immatérielle (logiciels, données...).

2.9. Code du travail :

Dans le cadre des dispositions de l'article L321.1 du code de travail et d'après un arrêt de la cour de Cassation Sociale du 15 octobre 1992, si malgré les efforts pour assurer l'adaptation d'un employé à l'informatisation de l'entreprise, celui-ci n'a pu s'adapter ni aux nouvelles exigences technologiques de son emploi ni aux autres postes qui lui ont été proposés, le licenciement est légitime et a une cause économique.

3. La réglementation juridique aux Etats Unis d'Amérique (USA) :

Nous avons constaté que contrairement à la Tunisie et à la France, la réglementation aux USA a prévu des dispositions préventives et détectives des violations de la loi[50] et ce, outre les dispositions touchant les obligations comptables, fiscales et celles se rapportant à la protection des droits de l'individu face à l'informatique.

En effet, selon le guide de condamnation fédéral, il est exigé de chaque entreprise d'avoir un programme effectif de prévention et de détection des violations de la loi. L'absence de ce programme exposera l'entreprise à des sanctions financières importantes.

La liste des étapes à prévoir dépend de plusieurs facteurs dont notamment la taille de l'entreprise et la nature de l'activité. Le programme englobe :

- L'établissement de standards et de procédures de conformité capables de réduire le risque de toute conduite criminelle,
- La désignation d'un responsable de haut niveau chargé d'assurer la conformité avec les standards et les procédures établis,
- La non-délégation de pouvoirs discrétionnaires importants pour des personnes qui pourraient être engagées dans des activités illégales,
- La prise de mesures nécessaires pour la communication des standards et des procédures à tous les employés,
- La prise de mesures raisonnables pour s'assurer de la conformité avec les standards et les procédures en place : exemple : audit interne, système de reporting, etc.,
- La mise en place de mesures disciplinaires aussi bien pour la personne coupable que pour la personne responsable n'ayant pas détecté les infractions,
- La prise de mesures appropriées devant toute infraction et la mise en place de mesures préventives contre toute infraction similaire future.

Par ailleurs, la réglementation aux USA[51] prévoit des amendes et des termes d'emprisonnement à l'encontre de la direction d'une entreprise qui a fermé, ou qui a enregistré des pertes de revenus considérables, ou qui a encouru, exceptionnellement, de grosses dépenses dues à l'absence d'un plan de secours[52].

4. Les difficultés juridiques associées aux nouvelles technologies :

Certaines difficultés juridiques sont nées suite à l'utilisation des technologies de l'Internet. Ces difficultés sont dues au fait que plusieurs pays ont mis en place un système juridique régulant les affaires électroniques nationales sans que l'aspect mondial de ce genre d'affaires soit pris en compte. Exemple : Plusieurs pays ont proclamé des lois pour réguler la signature électronique sans que soit mis en place un système de signature électronique reconnu mondialement.

Parmi les difficultés, nous citons :

---

[50] « Handbook of information system auditing », paragraphe A 2.03.5b, Coopers & Lybrand, 1997
[51] Exemple : La référence pour les banques est le circulaire N°177.
[52] « Handbook of information system auditing », paragraphe D 6.02, Coopers & Lybrand, 1997

- La propriété intellectuelle : L'ensemble des règles internationales relatives à la protection intellectuelle du droit d'auteur s'applique au support multimédia que sont les sites Web, commerciaux ou non commerciaux. Mais les actions juridiques contre un serveur hébergé dans un pays tiers diffusant des créations multimédias contrefaites (son, image, texte, vidéo…), nécessitent des procédures légales difficiles à mettre en œuvre, et ne facilitant pas la suppression ou la réparation immédiate des faits délictueux constatés.
- Les disparités réglementaires concernant les noms de domaine (les adresses des sites web) posent également des problèmes. La règle est celle du premier arrivé, premier servi. Ceci a permis à des personnes, d'enregistrer légalement des noms des marques mondialement connues ou d'entreprises, soit pour les utiliser à leurs propres bénéfices, soit pour les revendre fort chers à leurs véritables titulaires (exemple : vizzavi de vivendi).

Section 2 : Les principales réactions des organismes professionnels :

Etant membre de l'IFAC, l'Ordre des Experts Comptables de Tunisie a décidé de faire des normes internationales d'audit (ISA)[53] la base des normes d'audit et de services connexes approuvés en Tunisie. Le Conseil de l'Ordre des Experts Comptables de Tunisie a décidé de les adopter à compter de l'année 2000.

Nous avons examiné au niveau de cette section les principales réflexions de l'IFAC ainsi que celles des autres principaux organismes professionnels.

Sous section 1 : Les réflexions de l'IFAC

L'International Auditing Practices Committee (IAPC)[54] a élaboré des projets de mise à jour des documents suivants :

- Norme Internationale d'Audit N°401 relative à l'audit dans le contexte d'un système d'information informatisé,
- Directive Internationale d'Audit N°1001 relative à un système d'information fondé sur un micro-ordinateur autonome,
- Directive Internationale d'Audit N°1002 relative à un système d'information fonctionnant en réseau et/ou en temps réel,
- Directive Internationale d'Audit N°1003 relative à un système à bases de données,
- Directive Internationale d'Audit N°1009 relative à l'utilisation des techniques d'audit assistées par ordinateur.

1. Le projet de la norme internationale d'audit N°401 :

Cette norme traite les principes de base régissant :

- l'impact du système informatisé sur l'approche d'audit
- la compétence et le savoir-faire nécessaires de l'auditeur
- l'utilisation des compétences de l'auditeur ou le recours à des spécialistes
- le risque inhérent et le risque lié au contrôle relatifs à l'informatique et les procédures d'audit destinées à diminuer le risque d'audit.

La structure et le contenu de ce projet sont différents de la norme actuelle. Les différents chapitres portent sur[55] :

[53] ISA : International Standards on Auditing
[54] IAPC : Comité des Normes Internationales d'Audit créée par le Conseil de l'IFAC afin d'élaborer et de publier pour son compte des normes et des directives d'audit et de services connexes.
[55]Muttiah Yogananthan, « Les projets en cours de l'IAPC », Revue Française de Comptabilité N° 16, Novembre 1999.

- Les définitions de l'infrastructure de sécurité, des contrôles informatiques, des risques relatifs à la sécurité informatique et de la configuration informatique,
- Les objectifs informatiques de l'entreprise,
- L'informatique et le management des risques,
- La compétence et le savoir-faire,
- Le recours à un spécialiste,
- Le planning,
- La connaissance de l'entreprise et de son secteur d'activité,
- La structure et l'organisation,
- L'infrastructure sécuritaire,
- Les contrôles généraux,
- Le risque inhérent et le risque lié au contrôle,
- Les rapports financiers et le contrôle interne,
- Les procédures d'audit,
- La continuité de l'exploitation.

2. Le projet de la directive internationale d'audit N°1001 :

Ce projet traite du système d'information fondé sur un micro ordinateur autonome. Il présente les arguments conduisant à affirmer qu'en général le risque lié au contrôle est plus élevé que dans le cadre d'un système plus grand. Par conséquent, il peut s'avérer plus approprié pour l'auditeur d'augmenter les contrôles substantifs, la taille des échantillons et les contrôles physiques et d'utiliser de façon plus large les techniques d'audit assistées par ordinateur.

3. Le projet de la directive internationale d'audit N°1002 :

Ce projet traite des systèmes d'information fonctionnant en réseau et/ou en temps réel. Il comporte une description de leurs caractéristiques ainsi qu'une énumération des contrôles qu'ils peuvent comporter. Il contient, aussi, une analyse de l'impact de ce type de système sur le système comptable et les contrôles internes et par conséquent, sur les procédures d'audit.

Le projet de la directive met l'accent sur le fait que les caractéristiques de ces systèmes font qu'il est plus efficace pour l'auditeur de faire une revue avant la mise en place de ces systèmes qu'après et ce afin de demander les modifications et les améliorations nécessaires en vue de renforcer les contrôles.

4. Le projet de la directive internationale d'audit N°1003 :

Ce projet traite des systèmes de base de données. Il comporte une description de leurs caractéristiques ainsi qu'une énumération des contrôles qu'ils peuvent comporter. Il contient, aussi, une analyse de l'impact des bases de données sur le système comptable et les contrôles internes ainsi qu'une appréciation de l'impact de ce type de système sur les procédures d'audit.

A l'instar de la directive 1002, le projet de la directive met l'accent sur le fait que les caractéristiques de ces systèmes font qu'il est plus efficace pour l'auditeur de faire une revue avant la mise en place de ces systèmes qu'après.

5. Le projet de la directive internationale d'audit N°1009 :

Ce projet traite des techniques d'audit assistées par ordinateur en tant qu'outils permettant d'améliorer l'efficacité et l'efficience des procédures d'audit en indiquant une description des différentes techniques et de leurs utilisations possibles. Le projet traite aussi des conditions et des modalités de mise en place de ces techniques.

Outre la mise à jour de ces normes et directives, il convient de signaler qu'il existe au sein de l'IFAC un comité des technologies de l'information (ITC : Information Technology Commitee) chargé de développer les compétences des professionnels et des gestionnaires et leurs consciences des nouveaux développements technologiques et ce, en facilitant la recherche, en renforçant les communications et en fournissant des guides sur diverses questions d'actualité.

A la date de la rédaction du présent mémoire, l'IFAC a publié cinq guides relatifs aux technologies de l'information. Ces guides sont :

1.	Gérer la sécurité de l'information (Managing Security of Information)	Janvier 1998
2.	Gérer la planification des technologies de l'information (managing Information Technology Planning for Business Impact)	Janvier 1999
3.	Acquisition des technologies de l'information (Acquisition of Information Technology)	Juillet 2000
4.	Les solutions de la mise en place des technologies de l'information (The implementation of Information Technology Solutions)	Juillet 2000
5.	La distribution et le support des technologies de l'information (IT service delivery and support)	Juillet 2000

Sous section 2 : Les différentes réflexions en France

1. Le Conseil National des Commissaires aux Comptes (CNCC) :

Le CNCC, à travers la commission informatique, traite des sujets informatiques susceptibles d'avoir un impact sur la mission du commissaire aux comptes. Dans ce cadre, cette commission mène régulièrement des réflexions sur les nouvelles technologies et ce, en :

- Formulant des avis, en diffusant des guides spécifiques de contrôle dans les entreprises informatisées (exemple : l'audit en milieu EDI, édition 1997) et en apportant des réponses aux questions techniques posées par les professionnels ;
- Elaborant des outils informatiques d'aide à l'audit et à la gestion administrative des missions ;
- Contribuant à la mise en place des actions de formation nécessaires et en organisant des manifestations sur les différents thèmes se rattachant à l'informatique.

Certains travaux ont déjà abouti à des publications spécifiques telles que les sujets traitant de la sécurité informatique, du Webtrust, du commerce électronique, de l'échange de données informatisées (EDI), des technologies de la communication, d'Internet et des services publics en ligne, etc., et aussi à des ouvrages dont par exemple « le diagnostic des systèmes informatisés : guide d'application des recommandations ».

2. L'Association Française d'Audit et du conseil en Informatique (AFAI) :

L'Association Française de l'Audit et du conseil en Informatiques a été fondée en 1982 pour :

- regrouper tous les professionnels concernés par la maîtrise des systèmes d'information,
- favoriser le développement des méthodes et des techniques d'audit et de contrôle de l'informatique,
- promouvoir l'emploi de méthodologies et de techniques contribuant à une meilleure maîtrise des systèmes d'information,
- aider à améliorer les compétences de tous les intervenants dans le domaine de l'audit et du conseil informatiques.

L'AFAI réunit, aujourd'hui, plus de 400 adhérents représentant :

- diverses fonctions au sein des entreprises : direction de l'audit, direction de l'informatique, direction financière et direction du contrôle de gestion,
- des auditeurs externes, des consultants, des experts comptables et des commissaires aux comptes, des sociétés de service et d'ingénierie informatique, des experts judiciaires, des juristes, des enseignants et des spécialistes de la sécurité informatique.

3. Le Club de la Sécurité des Systèmes d'Information (CLUSIF) :

Fondé en 1984, le Club de la Sécurité des Systèmes d'Information (CLUSIF), offre un cadre dans lequel les acteurs dans le domaine de la sécurité des systèmes d'information, responsables et prestataires de services, se rencontrent, échangent leurs points de vue, partagent leurs expériences et connaissances, travaillent et progressent ensemble.

Les travaux du CLUSIF comprennent des travaux de recherche et développement, des prises de position sur des sujets d'actualité, des guides et recommandations à caractère didactique, l'effet de l'art sur différents types de solutions, des méthodes, des enquêtes, des outils de sensibilisation, etc.

Le CLUSIF participe avec un certain nombre d'acteurs de la sécurité à la promotion de la sécurité et fait valoir les besoins et contraintes des utilisateurs auprès des instances dirigeantes.

Il s'implique activement dans le processus éducatif et de sensibilisation et ce, à travers les séances thématiques accordées aux étudiants, enseignants et membres.

Sous section 3 : Les différentes réflexions aux Etats Unis d'Amérique

Il existe une multitude d'associations aux Etats Unis d'Amérique touchant aussi bien le domaine de l'audit, de l'informatique, des nouvelles technologies, de la sécurité, etc. Nous nous sommes limités à l'AICPA[56].

L'AICPA a proposé, en novembre 2000, un projet de modification de la SAS (Statement on Auditing Standards) N°55 intitulé « Consideration of Internal Control structure in a financial statement audit ». Ce projet focalise sur l'effet de la technologie de l'information et de la communication sur le contrôle interne et sur l'évaluation des risques d'audit.

La SAS proposée traite, essentiellement, des points suivants :

- Décrire comment la technologie de l'information peut affecter le contrôle interne, les éléments probants, et la compréhension par l'auditeur du contrôle interne et l'évaluation des risques,
- Présenter un guide afin d'aider l'auditeur de déterminer s'il y a lieu de recourir à des spécialistes en technologies de l'information.

Par ailleurs, l'AICPA a traité les aspects suivants :

- Implication de l'EDI sur l'audit (Audit Implications of Electronic Data Interchange) : Produit N°021060kk
- L'âge des technologies de l'information : Les éléments probants dans un milieu informatisé (The Information Technology Age : Evidential matter in the Electronic environment) : Produit N°021068kk
- L'effet des documents électroniques sur l'audit (Audit implications of Electronic Document Management) : Produit N°021066kk
- L'audit dans un environnement informatisé (Auditing in common computer environments) : Produit N°021059kk
- L'audit au moyen de l'informatique (Auditing with computers) : Produit N°021057kk
- La structure du contrôle interne dans un milieu informatisé : Etude de cas (Consideration of the Internal Control Structure in a Computer Environment : A case study) : Produit N°021055kk

Par ailleurs, et en collaboration avec le CICA « Canadian Institute of Chartered Accountants », l'AICPA a défini les principes et les critères associés au WebTrust. Ces derniers sont applicables à partir du 28 février 2001.

Sous section 4 : Autres réflexions : ISACA

L'ISACA[57] est une association fondée en 1969 qui englobe des professionnels de la vérification, de la sécurité et du contrôle des technologies de l'information.

L'ISACA se veut la référence mondiale reconnue en gouvernance, contrôle et assurance qualité des technologies de l'information. Groupement international de 20.000 membres dans plus de 100 pays, l'ISACA organise des conférences, des cours et des séminaires, publie des informations techniques, édite des guides, développe et met à jour des normes professionnelles. Elle effectue des travaux de recherche en audit informatique et délivre la certification d'auditeur de systèmes d'information (CISA), label professionnel mondial.

[56] AICPA : American Institute of Certified Public Accountants
[57] ISACA : « Information System Audit and Constrol Association » .

L'ISACA a développé et promulgué des Normes Générales ainsi que des directives pour l'Audit des Systèmes d'Information[58]. L'objectif de ces normes et directives est de définir pour les auditeurs un niveau de diligence minimal pour répondre aux responsabilités professionnelles.

Elle a aussi développé le COBIT[59] qui constitue un référentiel international de Gouvernance, de Contrôle et de l'Audit de l'Information et des technologies associées.

COBIT a été conçu à partir des meilleures pratiques mondiales en audit et en maîtrise des systèmes d'information. Il est destiné à trois publics différents :

- La direction : pour l'aider à trouver l'équilibre entre le risque et l'investissement en contrôles,
- les utilisateurs : pour obtenir des garanties sur la sécurité et les contrôles des services informatiques fournis en interne ou par des tiers
- les auditeurs : pour justifier leur opinion et conseiller la direction sur les contrôles internes.

Le référentiel COBIT retient quatre domaines fonctionnels : Planification et Organisation, Acquisition et Mise en Place de systèmes, Distribution et Support, Surveillance. Ces domaines regroupent 34 processus principaux auxquels correspondent 302 objectifs de contrôle.

Parallèlement, l'ISACF (Information Systems Audit and Control Foundation), un organisme à but non lucratif rattaché à l'ISACA, assure la promotion de la recherche et publie différents ouvrages traitant du contrôle des technologies de l'information.

Parmi les projets en cours de l'ISACF, nous citons :

- E-commerce : Contrôle, Audit et sécurité
- L'intégrité de l'information
- Enterprise Resource Planning - SAP
- Les pratiques du contrôle des technologies de l'information

Conclusion :

A travers cette étude sommaire, nous constatons l'intéressement que revêt le sujet des nouvelles technologies de l'information et de la communication aussi bien pour les instances législatives que pour les organismes professionnels.

En Tunisie et au niveau réglementaire, nous remarquons un intéressement constant du législateur et du gouvernement à mettre en place une réglementation à la hauteur des exigences des nouvelles technologies tout en assurant les objectifs des systèmes d'information : efficacité, optimisation, confidentialité, intégrité, fiabilité, disponibilité, etc. Certainement, il y a encore beaucoup à faire étant donné le caractère embryonnaire, en Tunisie, des affaires sur Internet.

En outre, du côté de la fiscalité, nous constatons que ce volet demeure toujours rigide et nécessite par conséquent une mise à niveau aussi bien législative qu'administrative.

Par ailleurs, une approche internationale de la réglementation touchant la technologie de l'Internet est tout à fait souhaitable. A défaut, toute entreprise entrant dans le cyberespace doit savoir qu'elle prend des risques d'enfreindre par inadvertance la législation du pays où elle compte vendre ses produits ou services.

Au niveau des organismes professionnels, nous constatons une mise à jour des lignes directrices des normes de révision ainsi que des recherches constantes sur d'autres aspects se rattachant directement aux nouvelles technologies. Ceci dénote l'importance de l'enjeu pour l'expert comptable.

[58] La liste des normes générales et des directives de l'ISACA figure au niveau de la bibliographie.
[59] COBIT : Control Objectives for Information and Related Technology

Conclusion Partie I

Nous avons essayé de montrer tout au long de cette partie les différents impacts des nouvelles technologies de l'information et de la communication aussi bien sur l'entreprise que sur l'audit financier.

Il convient de noter que cette étude a été orientée « audit financier » et par conséquent, c'est la recherche de la fiabilité des états financiers qui est privilégiée. En effet, dans la mesure où le système d'information automatisé produit l'information financière, c'est la capacité de ce système à produire une information fiable qui est analysée et évaluée par l'auditeur.

De ce fait, nous n'avons pas focalisé sur les aspects d'efficacité et d'efficience des opérations touchées par les nouvelles technologies.

Face à ce nouveau contexte d'intervention caractérisé, entre autres, par la dématérialisation des informations et l'automatisation des contrôles, il est de plus en plus difficile pour l'auditeur financier de forger son opinion sans une approche approfondie du système informatique.

Par conséquent, l'audit informatique, qui consiste à émettre une opinion sur la fonction informatique et sur les traitements et les contrôles automatisés, devient, désormais, une nécessité dans le processus de l'audit financier.

La deuxième partie de ce mémoire est consacrée à l'étude des différents aspects de l'audit informatique et ce, dans un objectif de présenter la manière avec laquelle s'intègre l'audit informatique dans les différentes étapes de l'audit financier et d'anticiper le développement futur de l'audit informatique en support à l'audit financier.

Partie II : L'audit informatique dans le processus de l'audit financier

Introduction Partie II

Après avoir exposé les principaux impacts des nouvelles technologies de l'information et de la communication sur l'entreprise et sur l'audit financier, il apparaît clairement que l'audit informatique est devenu un élément nécessaire dans une mission d'audit financier.

L'audit informatique, dans son sens large, peut traiter plusieurs aspects couvrant aussi bien la fonction que les applications informatiques.

Toutefois, il est utile de préciser que, dans le cadre d'une mission d'audit financier, c'est la recherche de la fiabilité qui est privilégiée. Les autres aspects d'efficacité et d'efficience, couverts généralement par l'audit opérationnel, ne sont pas exigés par l'audit financier.

C'est ainsi que cette deuxième partie traite uniquement des aspects de l'audit informatique dans le cadre d'une mission d'audit financier.

Pour cela, nous examinons, dans un premier chapitre, la détermination du besoin de recours à l'audit informatique et à l'étude des rôles qui lui sont dévolus.

Ensuite, nous présentons, dans un deuxième chapitre, une démarche d'audit informatique qui pourrait être suivie dans le processus de l'audit financier. Cette démarche peut être aussi utilisée dans une mission spéciale d'audit informatique avec, généralement, un champ d'action plus élargi.

Enfin, nous traitons, dans un dernier chapitre, les principales évolutions prévisibles des pratiques en la matière en Tunisie.

Chapitre 1 : Le Besoin De Recours A l'Audit Informatique Et Ses Rôles Dans Une Mission D'Audit Financier

Introduction :

C'est lors de la planification de la mission d'audit financier que le besoin de recours à l'audit informatique est ressenti. Cette phase délicate de la mission est généralement conduite par le signataire du rapport ou par l'un de ses collaborateurs les plus expérimentés sous sa supervision et son entière responsabilité.

Nous rappelons dans ce chapitre la démarche à suivre pour la planification d'une mission d'audit financier et nous déterminons les cas où il y a lieu de faire recours à l'audit informatique.

En outre, nous précisons, dans une deuxième section, les rôles dévolus à l'audit informatique dans une mission d'audit financier.

Section 1 : La planification d'une mission d'audit financier et la détermination du besoin de recours à l'audit informatique

La planification d'une mission d'audit financier se compose des étapes suivantes :

- L'évaluation de l'environnement de contrôle
- La compréhension de l'activité de l'entreprise et de son secteur
- La collecte d'informations sur les systèmes et l'environnement informatique
- L'évaluation préliminaire des contrôles de direction
- La définition de la stratégie d'audit et le besoin de recours à l'audit informatique

Sous section 1 : L'évaluation de l'environnement de contrôle

L'environnement de contrôle est l'ensemble des conditions dans lesquelles fonctionnent les systèmes de contrôle. Il reflète la philosophie de la direction, son attitude et son engagement démontré à établir une atmosphère positive pour la mise en œuvre et l'exécution d'opérations bien contrôlées.

Aussi, il influence profondément le fonctionnement des systèmes de contrôle contribuant ou non à leur fiabilité.

Si l'auditeur ne peut pas mesurer avec précision les aspects de l'environnement de contrôle, il est cependant possible de déceler des facteurs plus ou moins favorables à l'exercice du contrôle interne. Il s'agit, alors, d'évaluer de manière globale si l'environnement de contrôle contribue à l'efficacité des contrôles, et donc au traitement correct des informations comptables et à la prévention ou à la détection des erreurs et irrégularités.

L'inexistence ou la faiblesse de l'un de ces aspects ne signifie pas nécessairement que l'attitude globale vis-à-vis des contrôles est négative.

Toutefois, un bon environnement de contrôle a pour conséquences :

- une approche utilisant les contrôles clefs ayant de fortes chances d'être efficaces
- l'application d'un plan d'audit comportant une rotation plus grande des secteurs contrôlés

- un niveau probable de conformité (application effective des contrôles) élevé, permettant de réduire la quantité de preuves nécessaires à la formation de la conviction sur l'efficacité des contrôles généraux et des contrôles directs.

Les aspects à évaluer sont :

- les incidences de l'organisation, des rôles et des responsabilités sur l'environnement de contrôle et ce, en évaluant :

  1. le rôle du Conseil d'Administration : l'auditeur doit s'assurer, s'il compte leur accorder un niveau de confiance, que la composition, les responsabilités et le comportement des membres du Conseil d'Administration ainsi que les informations dont ils disposent sont de nature à générer une ligne de conduite appropriée, conduisent à une réelle prise de décisions et à un contrôle effectif des opérations, et encouragent la direction à agir dans l'intérêt des actionnaires.
  2. l'efficacité de l'organisation et de l'encadrement : l'auditeur doit s'assurer, s'il compte leur accorder un niveau de confiance, que la structure de la société, les responsabilités et l'attitude de la Direction sont de nature à permettre la maîtrise et le contrôle de l'activité. Il doit aussi s'assurer que les directeurs et les cadres dirigeants, en particulier ceux qui exercent une responsabilité financière directe, ont les compétences requises et l'expérience nécessaire pour mettre en œuvre les décisions du Conseil et faire face aux changements de l'environnement.
  3. la politique et les procédures en matière de ressources humaines : l'auditeur doit évaluer et, si un niveau de confiance est accordé à ces aspects, tester si la politique et les procédures en place assurent le recrutement d'un nombre suffisant de personnes qualifiées (y compris le personnel informatique), leur épanouissement et leur fidélité, afin de favoriser l'exécution de la stratégie de l'entreprise et de prévenir les défaillances de contrôle interne ou les pertes financières.

- les incidences de l'évaluation des risques par l'entreprise sur l'environnement de contrôle et ce, en évaluant :

  1. le processus de gestion des risques par la direction : l'auditeur doit évaluer et, si un niveau de confiance est accordé à ces aspects, tester :

     - si la direction établit des objectifs clairs et met en place des procédures permettant d'identifier les risques qui compromettent la réalisation de ces objectifs et,
     - si les procédures mises en place reposent sur une information fiable, sont appliquées par des personnes compétentes, et toute action nécessaire est menée dans les temps.

     Désormais, les risques informatiques font partie de l'ensemble de ces risques.
  2. le respect des lois et de la réglementation : l'auditeur doit évaluer, et si un niveau de confiance est accordé à ces aspects, tester si la direction a une connaissance adéquate des lois et de la réglementation applicable à son activité, si elle mesure le risque de leur éventuel non-respect et si elle agit pour prévenir les infractions.

- les incidences du processus de pilotage sur l'environnement de contrôle et ce, en évaluant :

  1. la fiabilité du reporting financier : l'auditeur doit évaluer, et si un niveau de confiance est accordé à ces aspects, tester si des procédures de reporting financier sont en place pour produire les informations destinées à être revues par la direction et que cette revue permet de détecter d'éventuelles défaillances dans le contrôle interne ou des erreurs significatives et débouche sur des actions appropriées, si besoin est.
  2. la qualité des prévisions de la direction et du contrôle budgétaire : Ceci englobe, à titre indicatif, les procédures de préparation des prévisions et des budgets, leur qualité, la pertinence et la fiabilité de l'information financière produite.
  3. le rôle de l'audit interne : l'auditeur doit évaluer, et si un niveau de confiance est accordé à ces aspects, tester si l'audit interne est un rouage essentiel de l'environnement de contrôle, par sa contribution à l'évaluation des risques de l'activité (y compris les risques informatiques), et en sa qualité de garant du fonctionnement continu des règles de contrôle interne destinées à atteindre les objectifs de l'entreprise.

4. le rôle du comité d'audit : l'auditeur doit évaluer, et si un niveau de confiance est accordé à ces aspects, tester :
    - si la composition, les responsabilités et le comportement du comité d'audit, ainsi que l'information dont il dispose, débouchent sur un pilotage et une revue effectifs de la comptabilité, du contrôle interne et des procédures de reporting financier et,
    - si le comité contribue à la définition d'une ligne de conduite appropriée et au maintien d'un réseau de communication constructif avec les auditeurs internes et externes.
5. la fiabilité des estimations de la direction : l'auditeur doit évaluer, et si un niveau de confiance est accordé à ces aspects, tester si la direction, pour l'établissement d'estimations, utilise une méthodologie fondée sur des données actualisées et fiables, supervise la production des estimations, et s'appuie sur les personnes qui disposent des compétences nécessaires à l'établissement d'estimations raisonnables.

Sous section 2 : La compréhension de l'activité de l'entreprise et de son secteur

Une connaissance approfondie de l'activité de l'entreprise est indispensable pour que la planification de l'audit soit efficace. L'objectif n'est pas de devenir des experts dans le domaine de l'entreprise auditée mais de connaître suffisamment l'entreprise pour pouvoir déterminer les orientations stratégiques de la planification.

Les étapes à suivre peuvent se résumer comme suit :

- Prendre en considération les spécificités du secteur et ce, notamment, en consultant des spécialistes du secteur d'activité et d'autres sources d'information concernant ledit secteur.
- Comprendre ou mettre à jour la compréhension de l'entreprise et de son secteur d'activité, de façon à pouvoir appréhender les événements, les transactions et les pratiques qui peuvent avoir un impact significatif sur les états financiers ou sur le rapport d'audit. L'attention de l'auditeur devrait être focalisée davantage, si l'entreprise :
    - utilise l'Internet ou une autre technologie pour la conduite de son affaire. Exemples : l'entreprise achète ou vend des produits ou des services par Internet, l'entreprise procède à des actions de publicité sur son site Web, etc.
    - opère dans une industrie où les opérations sont significativement traitées par Internet (Les agents immobiliers, les agences de voyage et les tours opérateurs, etc.).
- Si l'entreprise auditée externalise certaines fonctions, focaliser l'attention sur le caractère significatif de cette externalisation et sa pertinence pour l'audit et ce, en examinant dans quelle mesure cette externalisation des services affecte la comptabilité de l'entreprise et son système de contrôle interne et en y tenant compte dans la planification de l'audit et l'élaboration du programme de travail.
- Comprendre les politiques comptables les plus significatives utilisées et considérer si elles sont appropriées pour l'entreprise auditée et en relation avec les risques que court l'entreprise et la substance économique des transactions.
- Effectuer une revue analytique préliminaire : Il s'agit d'analyser l'information financière ou non financière récente. Les procédures analytiques préliminaires sont nécessaires afin de :
    - comprendre les conditions actuelles de l'activité (cash flow, résultat d'exploitation, situation financière,…),
    - évaluer les risques de continuité d'exploitation,
    - identifier les principales activités et les comptes concernés, la nature et le volume des transactions, les soldes comptables et les éléments inhabituels ou inattendus pouvant traduire un risque de fraude ou d'erreur
    - permettre une évaluation préliminaire du seuil de signification.

Sur la base de la compréhension de l'entreprise, de son activité, de son secteur, de ses risques et des contrôles liés, ainsi que des résultats des procédures analytiques préliminaires, l'auditeur doit

identifier et documenter les risques inhérents spécifiques à chaque section d'audit significative, et en tenir compte pour l'élaboration des programmes de travail.

Sous section 3 : La collecte d'informations sur les systèmes et l'environnement informatique

La compréhension des systèmes de l'entreprise et son environnement informatique est nécessaire pour une planification efficace et efficiente. Les informations collectées seront utilisées dans un objectif de détermination du degré d'appui à placer sur le contrôle interne de l'entreprise auditée et par suite de la stratégie d'audit à adopter.

Au cours de la phase de planification, la nécessité de faire appel à des experts en révision informatique doit être considérée en cas de système complexe. L'équipe intervenante sera dans ce cas mixte.

Cette phase de la planification doit apporter à toute l'équipe d'audit une identification et une compréhension suffisante :

- des principaux cycles ainsi que des applications informatiques qui les supportent,
- de l'organisation de la fonction informatique,
- des contrôles de la direction sur la fonction informatique,
- du degré de dépendance de l'activité quotidienne sur les systèmes informatiques,
- des caractéristiques principales des systèmes et environnements,
- des changements significatifs en termes de systèmes et d'environnement informatiques,
- des problèmes antérieurs survenus au niveau des systèmes.

Elle doit permettre à l'auditeur de dégager les facteurs de risques pouvant avoir un impact sur la stratégie d'audit. Nous citons :

- L'existence éventuelle de faiblesses de contrôle relatives à la fonction informatique qui empêchent d'accorder aux contrôles un niveau de confiance déterminé ;
- L'existence de problèmes fondamentaux, concernant la qualité de l'information de gestion, qui pourraient remettre en cause la fiabilité des contrôles de pilotage et par conséquent, empêcher d'accorder à ces contrôles un niveau de confiance déterminé ;
- Les incidences des changements de systèmes ou d'environnements informatiques sur notre connaissance antérieure de la mission et par suite sur la stratégie d'audit ;
- La nécessité de faire recours à des spécialistes au cours de l'audit.

Cette étape importante de la planification fait l'objet d'une étude plus détaillée dans le chapitre suivant.

Sous section 4 : L'évaluation préliminaire des contrôles de direction

Les contrôles de direction (ou aussi les contrôles de pilotage) peuvent être définis comme étant les moyens que la direction utilise pour piloter l'affaire et en contrôler les risques, soit de façon continue tout au long de l'année, soit de façon ponctuelle. Ils peuvent être réalisés par la direction elle-même ou par la fonction d'audit interne.

Les contrôles de direction sont de nature à déceler des erreurs potentielles et/ou des fraudes qui résulteraient des défaillances des systèmes de contrôle interne (y compris les contrôles généraux informatiques) ou des systèmes comptables.

Ils peuvent procurer une certaine confiance sur les contrôles informatiques généraux ou sur les contrôles d'application. A titre d'exemple :

- La revue d'un rapport de revenu avec une connaissance globale du volume livrée
- L'examen des dépenses d'investissement sur la base d'un rapport trimestriel analysant ces dépenses par département et les comparant par rapport aux budgets

Les contrôles de direction s'apprécient au niveau d'un cycle contrairement à l'environnement de contrôle qui s'apprécie au niveau de l'entreprise dans son ensemble. Ils sont détectifs plutôt que préventifs et s'apparentent à des contrôles de vraisemblance, de cohérence, à des revues par exception, à des procédures analytiques, etc.

Les objectifs des contrôles de la direction sont variés et ne visent pas nécessairement des objectifs financiers. En particulier, ils ne visent pas directement et spécifiquement les objectifs de contrôle, mais fournissent une assurance indirecte sur la réalisation de ces objectifs.

L'évaluation préliminaire des contrôles de direction, au niveau de chaque cycle, est effectuée afin de déterminer le niveau de confiance accordé aux contrôles. A ce stade, ces contrôles sont documentés sans pour autant être testés.

Etant donné que les contrôles de direction sont moins détaillés que les contrôles d'application, ils ne peuvent fournir un niveau de confiance aussi élevé. En fait, ils permettent d'identifier qu'il y a un problème mais pas de déterminer quel objectif particulier n'est pas atteint.

En outre, il y a lieu de préciser que le niveau de confiance que l'on peut obtenir des contrôles de direction est très variable. Il dépend notamment de la compétence de la personne chargée d'effectuer le contrôle, de la rapidité avec laquelle il est effectué, de la fiabilité de l'information utilisée, de la probabilité que ce contrôle permette effectivement de déceler des défaillances, etc.

Par ailleurs, et au cas où l'entreprise auditée externalise certaines fonctions, l'auditeur devrait considérer les contrôles de direction relatifs à la fonction du prestataire de services, que ces contrôles de pilotage soient effectués par l'entreprise auditée ou par son prestataire de services.

Sous section 5 : La définition de la stratégie d'audit et du besoin de recours à l'audit informatique

Signalons tout d'abord que pour la première année ou l'année du changement, la phase de collecte d'informations est bien évidemment plus importante. En revanche, les années suivantes, compte tenu des connaissances d'audit accumulées, le processus doit être plus rapide puisque focalisé uniquement sur les changements de l'exercice.

Cette phase de collecte doit renseigner, entre autres, les éléments suivants :

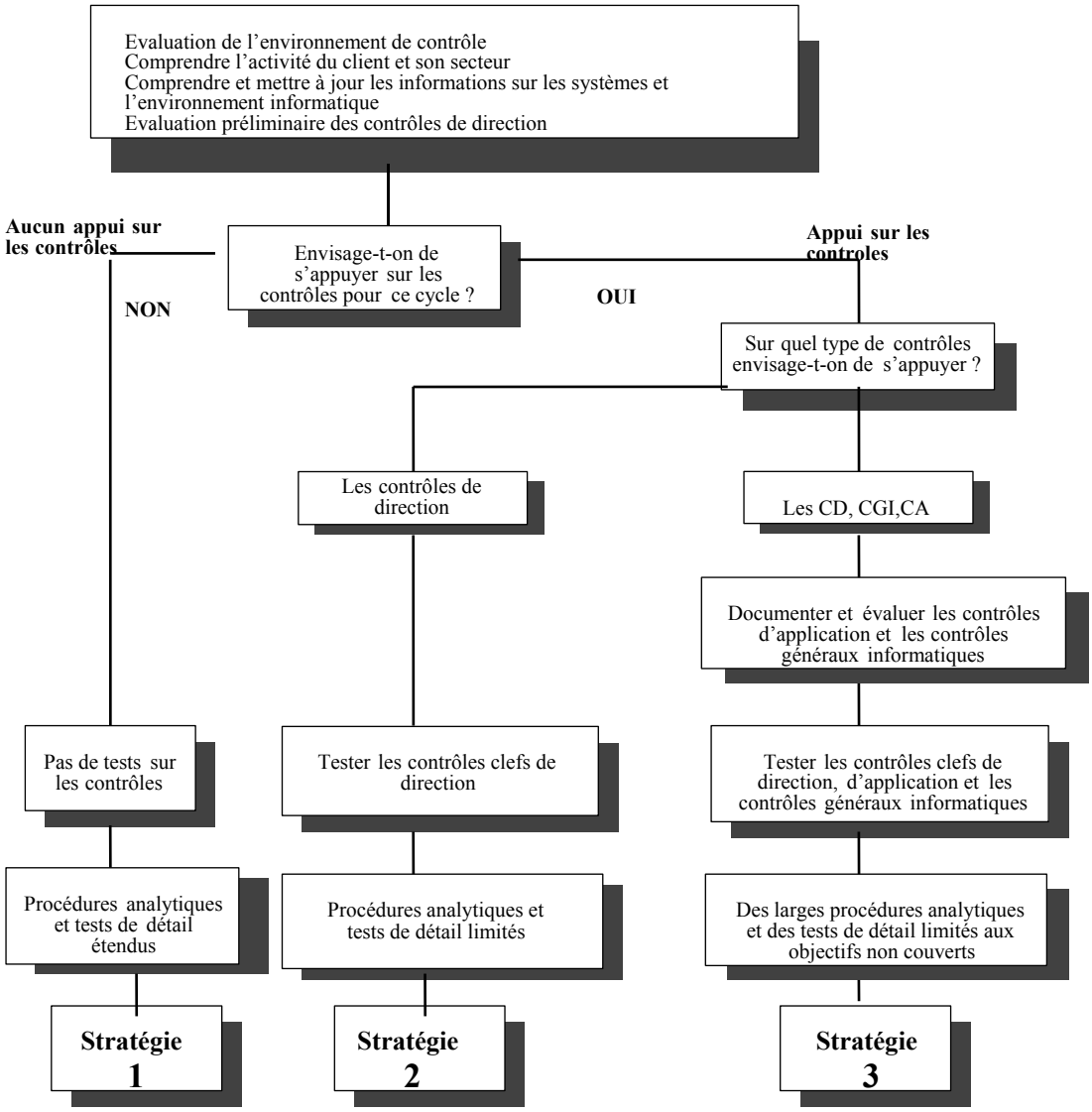
- Quels sont les cycles et comment l'audit sera organisé ?
- Quels sont les risques inhérents spécifiques à chaque section d'audit significative ?
- Quels sont les risques touchant les systèmes et les risques informatiques ?
- Quelles sont les éventuelles opérations ponctuelles à considérer (hors cycle ou hors système) ?
- Quel est l'impact de l'éventuelle externalisation de certains services ?
- Quels sont les principaux changements de l'exercice ?

Ces différentes informations recueillies permettent à l'auditeur de définir la stratégie d'audit par **cycle** compte tenu du niveau de confiance accordé aux contrôles de direction, contrôles généraux informatiques et contrôles sur d'application.

La définition de la stratégie d'audit est illustrée dans le schéma[60] suivant :

[60] Schéma inspiré de la méthodologie d'audit du cabinet international PricewaterhouseCoopers, « The PwC audit », 1999.

Les options de stratégies d'audit



CD : Contrôles de direction

CGI : Contrôles généraux informatiques

CA : Contrôles d'application

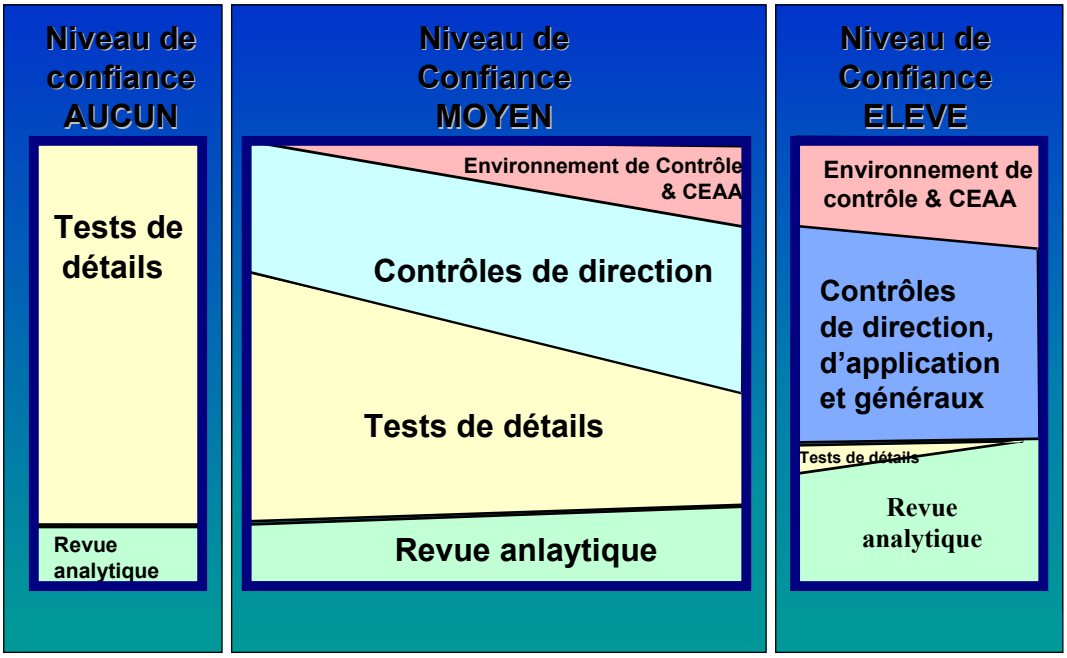
Il en découle de ce schéma que trois stratégies d'audit peuvent être envisagées. Pour chaque cycle, l'auditeur doit se poser la question suivante : ***« Compte tenu des éléments d'information préalables dont on dispose, envisage-t-on de s'appuyer sur les contrôles ? »***

Si la réponse est **non** : la stratégie retenue sera « Niveau de confiance : Aucun ». Si la réponse est **oui**, il faut ensuite se poser la question suivante : ***« Sur quel type de contrôle envisage-t-on de s'appuyer ? »***

Si on envisage de s'appuyer sur les contrôles de direction uniquement la stratégie sera « Niveau de confiance : Moyen ». Si on envisage de s'appuyer également sur les contrôles d'application et les contrôles généraux informatiques, la stratégie sera « Niveau de confiance : Elevé ».

Il convient de noter qu'en pratique la stratégie d'audit pour un cycle se positionne sur un continuum de « Aucun » à « Elevé ». L'idée générale étant : appuyons sur les contrôles clefs dés lors que c'est possible et dés lors que cet appui nous paraît optimal en terme de rapport efficacité/coût.

Par ailleurs, le choix de la stratégie d'audit constitue une décision préliminaire. Ce choix sera confirmé ou infirmé à l'occasion de la réalisation des tests sur les contrôles. Le schéma, qui suit, présente chacune de ces stratégies :



(CEAA : Connaissances et Expériences d'Audit

1. Stratégie 1 : Niveau de confiance AUCUN :

Deux types de situations peuvent conduire à ce choix : soit le cycle est mal voire pas contrôlé (mécanismes insuffisants pour assurer l'intégrité des données financières), soit des contrôles existent mais une approche substantive serait plus efficace et moins coûteuse, et donc plus appropriée en la circonstance. Exemple : des transactions individuellement significatives et peu nombreuses pouvant être vérifiées par des documents ou des confirmations.

Cette approche implique :

- une documentation très succincte des contrôles existants visant uniquement la compréhension d'ensemble de l'environnement de contrôle
- la non-réalisation de tests sur les contrôles clefs ni sur les contrôles informatiques généraux
- des travaux d'audit constitués pour l'essentiel de tests de détail ainsi que d'éventuelles procédures analytiques.

2. Stratégie 2 : Niveau de confiance : MOYEN :

Deux types de situations peuvent conduire à ce choix :

- Le cycle est contrôlé mais les contrôles clefs visant de façon détaillée les quatre objectifs de contrôle ne sont pas toujours documentés (donc difficile à tester) ou pas totalement performants. Cependant, il existe des contrôles de direction performants permettant de détecter des défaillances majeures.
- Une approche « Niveau de confiance - Moyen » est jugée plus adaptée car moins coûteuse qu'une approche « Niveau de confiance - Elevé » pour un même niveau d'efficacité. En effet, la réalisation de tests sur les contrôles de direction et des tests de détail additionnels peut être, dans certains cas, plus efficace qu'évaluer et tester les contrôles généraux informatiques et les contrôles d'application et la réalisation de tests substantifs réduits.

Cette approche implique l'appui sur les contrôles de direction qui donnent une certaine évidence qu'il n'y a pas eu de défaillances majeures et réduit l'étendue, mais en général pas la nature, des tests de détail selon la confiance que l'auditeur place sur ces contrôles. Ainsi, la démarche à suivre par l'auditeur consiste à :

- Documenter les contrôles de direction
- Tester les contrôles clefs de direction
- Ne pas tester les contrôles informatiques généraux
- Réaliser des travaux d'audit constitués pour l'essentiel de tests de détail ainsi que des procédures analytiques.

3. *Stratégie 3 : Niveau de confiance ELEVE :*

Dans ce cas des contrôles clefs existent (de direction et d'application), sont documentés, performants et couvrent de façon détaillée les quatre objectifs de contrôle. La réalisation de tests sur ces contrôles permet à l'auditeur de s'assurer de leur fonctionnement effectif et de leur permanence.

Ainsi, cette démarche consiste à :

- Documenter les contrôles de direction, les contrôles d'application et les contrôles généraux informatiques existants
- Tester les contrôles généraux informatiques
- Sélectionner et tester les contrôles clefs de direction et d'application
- Réaliser de très larges procédures analytiques. Les tests de détail ne seront déroulés que pour les objectifs d'audit non couverts par les contrôles
- Réduire les tests substantifs : L'étendue et même la nature des tests devront être réduites en conséquence selon les résultats des procédures précédentes.

Toutefois, il convient de signaler que pour la première année ou l'année de changement (exemple : installation de nouveau logiciel, modification significative d'un logiciel existant), les tests sur les contrôles clefs sont focalisés, essentiellement, sur les contrôles d'application comme base pour les années ultérieures.

Pour les années suivantes sans changements significatifs, l'étendue des tests des contrôles clés peut être réduite sur la base de la connaissance et l'expérience accumulées sur l'entreprise et sur la base de la capacité des contrôles de pilotage à détecter une défaillance au niveau des contrôles généraux informatiques ou au niveau des contrôles d'application et à détecter des problèmes existants au niveau des systèmes comptables sous-jacents. Les contrôles généraux informatiques continuent à être testés car ils permettent une assurance globale de l'intégrité de l'environnement du traitement et par suite la réduction des tests sur les contrôles clefs.

Dans un contexte de nouvelles technologies, caractérisé, entre autres, par la dématérialisation des informations, l'automatisation des contrôles et la complexité et le volume de plus en plus important des opérations, il est de plus en plus difficile pour l'auditeur financier de forger son opinion sans une approche approfondie du système informatique. Ainsi, la tendance, dans ce type d'environnement, est toujours vers une stratégie de « Niveau de confiance Elevé ».

Parmi les principaux avantages offerts par cette stratégie est qu'elle est, généralement, la plus optimale en terme de rapport efficacité / coût, en raison du fait que les tests sur les contrôles consomment, généralement, moins de temps que les tests de détail. Cette approche est d'autant plus efficace en cas d'utilisation des techniques d'audit assistées par ordinateur.

De ce fait, l'auditeur est de plus en plus confronté à mettre en œuvre une approche basée sur l'évaluation et l'examen des contrôles de direction, des contrôles généraux informatiques et des contrôles d'application.

C'est dans ce cadre qu'intervient l'audit informatique en support à l'audit financier pour assurer, entre autres, la documentation, l'évaluation et l'examen des contrôles généraux informatiques et des contrôles d'application (autres que les contrôles purement manuels).

Afin d'illustrer ces faits nous avons jugé utile de présenter l'exemple d'une Caisse de Sécurité Sociale tunisienne. Cette dernière compte des milliers de cotisants et de prestataires. Elle gère une multitude de secteurs, de régimes, de prestations etc. Le volume des opérations est important et les montants sont peu significatifs. L'ensemble des processus de gestion est automatisé : l'encaissement des cotisations, la liquidation des droits, etc., font l'objet de traitements informatiques complexes et lourds. Ainsi, une approche basée essentiellement sur les tests de détail n'est, donc, pas adaptée et ne permet pas de mettre en évidence des faiblesses de contrôle interne pouvant avoir un impact significatif sur les états financiers.

Par ailleurs, le recours à l'audit informatique peut être requis même pour une approche de « Niveau de confiance Moyen » et ce, pour s'assurer que les process de génération des rapports, sur lesquels s'exerce la fonction de pilotage, sont convenablement contrôlés.

Enfin, avant d'aborder avec plus de détails les rôles dévolus à l'audit informatique dans une mission d'audit financier, nous devons répondre à l'interrogation suivante : Quelle doit être la composition de l'équipe chargée de l'audit informatique ?

C'est suite à la phase de la collecte d'informations sur les systèmes et l'environnement informatique que l'auditeur décide si le système est considéré comme étant complexe[61] ou pas. Cette décision devrait être prise conjointement avec l'auditeur spécialiste.

Dans le cas de systèmes complexes, la composition recommandée de l'équipe pour l'exécution de la documentation, l'évaluation et l'examen des contrôles d'application est une équipe mixte d'auditeurs généraux et de spécialistes.

Toutefois, quelle que soit la complexité des systèmes, les spécialistes réservent la partie consacrée à l'examen des contrôles généraux informatiques. En effet, ce volet nécessite des compétences non évidentes chez l'auditeur financier « généraliste ».

De ce fait, dans un système de nouvelles technologies, le recours à une équipe d'audit mixte est, très souvent, nécessaire. Le tableau, qui suit, résume les situations décrites ci-dessus :

	Systèmes complexes		**Systèmes moins complexes**	
	Auditeurs	**Spécialistes**	**Auditeurs**	**Spécialistes**
Recueillir des informations sur les systèmes et l'environnement informatique.	Equipe mixte		X	*
Documenter et évaluer les contrôles d'application.	Equipe mixte		X	*
Sélectionner et tester les contrôles clefs.	Equipe mixte		X	*
Documenter, évaluer, sélectionner et tester les contrôles généraux informatiques.		X		X

(*) Des spécialistes peuvent être impliqués s'il y une incertitude quant au degré de complexité ou sur l'approche d'audit à mettre en œuvre.

Section 2 : Les rôles dévolus à l'audit informatique dans une mission d'audit financier

L'audit informatique vient supporter la mission de l'audit financier dans la mesure où il permet de :

- mettre en évidence des faiblesses de contrôle interne ayant un impact sur les états financiers et non détectables par une approche classique ;
- limiter les travaux substantifs pour les entreprises pour lesquelles l'auditeur peut s'appuyer sur les systèmes ;
- apporter une plus value à l'entreprise auditée par la mise en œuvre de travaux d'audit-conseil.

Ces objectifs sont atteints à travers la description et l'examen des contrôles généraux informatiques et des contrôles d'application.

Sous section 1 : Les tests sur les contrôles généraux informatiques

Les contrôles généraux informatiques sont les contrôles qui contribuent de manière significative à l'efficacité des contrôles directs individuels. Ils ne visent pas directement les objectifs de contrôle et ne

[61] Pour la définition de système complexe, se référer à la partie I, Chapitre II, Section 2, Sous-section 2

servent donc pas par eux même à fonder la conviction de l'auditeur, mais permettent à ce dernier de savoir si les faiblesses éventuelles dégagées ne réduisent pas l'efficacité et la fiabilité des contrôles directs.

Aussi, les contrôles généraux informatiques ne s'exercent pas au niveau d'un cycle particulier et peuvent avoir, par conséquent, une incidence diffuse sur les divers traitements réalisés par le système.

En effet, « si ces contrôles ne sont pas efficaces, des erreurs peuvent se produire et passer inaperçues dans les diverses applications. C'est pourquoi des défaillances dans les contrôles informatiques généraux peuvent empêcher de vérifier efficacement les contrôles prévus pour certaines applications »[62].

Cet aspect de l'audit informatique ne s'agit pas d'examiner les contrôles généraux de façon isolée mais lors de l'évaluation de la qualité des contrôles directs. En effet, si l'auditeur estime qu'un contrôle direct constitue un contrôle clef potentiel, il doit déterminer s'il peut aussi s'appuyer sur les contrôles généraux s'y rapportant. Ainsi, il est généralement plus efficace d'examiner les contrôles généraux une fois les contrôles directs clefs identifiés.

Faire le lien entre les risques identifiés au niveau de la fonction informatique et les risques en découlant sur les applications est une tâche assez difficile qui demande de la compétence, de l'expérience et du jugement. Exemple : En cas de contrôles insuffisants des modifications de programmes, le risque d'erreurs sur le calcul des paies est relativement faible du fait que la plupart des salariés vérifient leur bulletin de paie. Par contre le risque d'irrégularités sur les bulletins de paie est théoriquement possible.

Dans le cadre de l'audit financier, l'examen des contrôles généraux informatiques englobe, notamment, l'examen des aspects suivants :

1. Organisation générale de la fonction informatique :

Le contrôle de l'organisation générale de la fonction informatique permet, notamment, d'apprécier :

- le degré de sensibilisation au contrôle interne de la fonction,
- le degré de séparation des tâches incompatibles,
- la division des obligations et des responsabilités entre le service informatique et les différents utilisateurs.

Le contrôle de l'organisation générale de la fonction informatique ne peut donner que des indices ou des présomptions qui doivent être complétés par l'audit des différentes activités de la fonction informatique.

2. Développement, mise en place, modification et intégrité de système :

L'audit de cet aspect permet à l'auditeur de s'assurer que les systèmes sont développés en limitant au minimum les risques d'erreurs (objectif de fiabilité des traitements) et qu'ils ne peuvent être modifiés à l'insu des utilisateurs (objectif de fiabilité des traitements et de protection du patrimoine)

Les contrôles destinés à couvrir les risques liés aux modifications des programmes sont particulièrement importants du fait qu'ils affectent l'efficacité d'un bon nombre de contrôles clefs dépendants. L'existence de contrôles efficaces se rapportant aux modifications des programmes représente un moyen privilégié pour s'assurer que ces deniers restent fiables et complets.

Si ce contrôle n'est pas satisfaisant, il n'y a souvent qu'un autre moyen de savoir si les programmes qui ont été utilisés au cours de la période sont correctement approuvés et testés, c'est de les répéter à partir d'un échantillon représentatif.

3. Accès aux ressources logiques :

L'objectif de l'audit de cet aspect est de permettre à l'auditeur de porter une appréciation sur les procédures d'autorisation d'accès et de protection de l'intégrité des données.

[62] IFAC : Directive Internationale d'Audit N°1008 : « Evaluation du risque et contrôle interne : caractéristiques et considérations sur l'informatique ».

Dans la pratique, l'auditeur est confronté à de nombreux environnements où les procédures en ce domaine sont inadéquates ou insuffisantes. Dans ces environnements, l'auditeur doit apprécier, cas par cas, l'impact de ces risques sur les applications.

La nature des risques et l'existence ou non de contrôles compensatoires guident l'auditeur dans la conception, la période et l'étendue des tests sur les applications. Par exemple, pour une application imprimant des lettres chèques, un contrôle rigoureux des utilisateurs sur les séquences et le montant des lettres chèques est un contrôle compensatoire nécessaire en cas d'absence de procédures d'accès suffisamment rigoureuses évitant toute modification non contrôlée des fichiers et des programmes.

4. Sécurité physique et procédures de sauvegarde et d'urgence :

L'examen des procédures de contrôle relatives à la sécurité physique et aux procédures de sauvegarde et d'urgence permet à l'auditeur d'apprécier si la protection du patrimoine informatique, la sécurité et la continuité des travaux sont correctement assurées eu égard à la spécificité de l'entreprise.

5. Exploitation :

L'auditeur examine l'exploitation pour apprécier la façon dont cette activité satisfait aux objectifs d'autorisation, d'exhaustivité et d'exactitude.

Sous section 2 : Les tests sur les contrôles d'application

Les contrôles d'application garantissent l'intégrité de l'information. Ils peuvent être définis comme étant des contrôles assurant que seulement les données complètes, exactes et valides sont saisies et mises à jour dans le système informatique, que le traitement a été correctement accompli, que les résultats du traitement satisfont les attentes et que l'intégrité de données est maintenue.

Nous rappelons que les principales caractéristiques des contrôles d'application sont les suivantes :

- Ils s'exercent au niveau d'un cycle ou d'une transaction
- Ils visent directement et spécifiquement les objectifs de contrôle (ils peuvent également viser d'autres objectifs d'audit tel que la séparation des exercices).
- Ils peuvent être manuels ou automatisés

Les contrôles d'application qui sont couverts par l'audit informatique sont ceux portant sur les outputs des systèmes et sur les procédures de contrôles programmés et les contrôles manuels s'y rattachant.

L'assurance que les contrôles programmés sont correctement conçus peut être obtenue directement à travers la répétition ou indirectement à travers les résultats des tests sur les contrôles généraux informatiques portant sur les procédures de développement et de mise en place de nouveaux systèmes.

L'étendue des tests varie selon qu'il s'agit de la première année d'audit (ou l'année du changement) ou d'une année suivante sans changements significatifs.

1. La première année ou l'année du changement :

La première année ou l'année du changement se définit comme suit :

- nouveau mandat,
- mandat récurrent mais au cours duquel un changement s'est produit affectant le cycle de façon significative, dont par exemple :
  - changements significatifs au niveau de l'activité ou des risques de l'entreprise susceptibles d'avoir un impact sur la capacité des systèmes à traiter et à assurer la fiabilité des transactions et des soldes,
  - changement au niveau opérationnel ou au niveau des hommes,
  - installation d'un nouveau système ou logiciel,
  - modifications significatives d'un logiciel existant,
  - changements significatifs au niveau de la structure organisationnelle ou au niveau des politiques ou des procédures,

- la première année pour laquelle le niveau de confiance accordée aux contrôles est réévalué alors qu'il avait préalablement été estimé comme "Aucun" ou comme "Moyen".

Dans ces cas, il s'agit de sélectionner et tester tous les contrôles d'application clés qui permettent d'atteindre les objectifs de contrôle. Cette sélection doit être effectuée en liaison avec la sélection des contrôles de direction clés. La combinaison de ces deux types de contrôles (pilotage et applications) constitue l'ensemble des contrôles clés pour le cycle.

Généralement, l'attention est focalisée plus sur les contrôles d'application que sur les contrôles de direction et ce, en raison du fait que les contrôles d'application fournissent une assurance plus importante quant à la satisfaction des objectifs de contrôle et que la réalisation de tests sur ces contrôles constitue une base d'appui pour les années subséquentes.

2. Les années suivantes sans changements significatifs :

Les contrôles clefs identifiés durant la première année demeurent valables. Toutefois, l'étendue des tests des contrôles d'application clés peut être réduite sur la base de :

- la connaissance et l'expérience d'audit accumulées sur l'entreprise auditée,
- la capacité des contrôles de pilotage à détecter une défaillance au niveau des contrôles généraux informatiques ou au niveau des contrôles d'application, ou des problèmes existants au niveau des systèmes comptables sous-jacents.

Ainsi, dans ce cas, il y a lieu de :

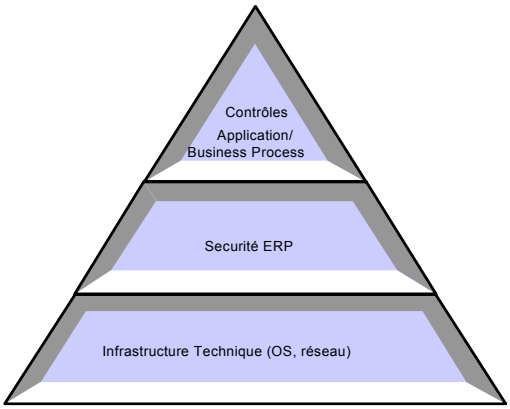
- sélectionner et tester **tous les contrôles de pilotage clés** qui permettent d'atteindre les objectifs de contrôle
- Sélectionner et tester les contrôles d'application qui permettent d'atteindre les objectifs de contrôle pour lesquels les seuls tests sur les contrôles de pilotage ne fournissent pas une assurance suffisante (en tenant compte de la connaissance et l'expérience d'audit accumulées).

L'assurance que les contrôles programmés fonctionnent correctement et d'une façon permanente tout au long de la période auditée peut être obtenue indirectement à travers les résultats des tests sur les contrôles généraux informatiques portant sur les procédures de maintenance et ceux portant sur la sécurité des systèmes et sur la sécurité de l'exploitation. En effet, l'auditeur aura toujours besoin de tester les contrôles généraux informatiques pour s'assurer qu'ils demeurent les mêmes et pour s'assurer qu'il n'existe pas de nouvelles faiblesses de nature à réduire l'efficacité et la fiabilité des contrôles directs.

Sous section 3 : Exemple des rôles dévolus à l'audit informatique dans un milieu d'ERP :

Dans un milieu d'ERP, l'audit informatique couvre, généralement, les volets suivants :

- Contrôles de l'infrastructure technique
- Sécurité ERP
- Contrôles d'application



A/ Contrôle des infrastructures techniques des systèmes d'information :

Les faiblesses éventuelles de l'infrastructure technique de l'ERP peuvent remettre en cause l'environnement de contrôle constitué au sein de l'application. Il est donc essentiel que ce domaine fasse l'objet d'une revue afin de vérifier que de tels risques sont maîtrisés et limités.

Les domaines spécifiques de cette revue comprennent notamment :

- Le système d'exploitation afin de s'assurer que l'accès aux objets, commandes et utilitaires sont convenablement protégés ;
- Les sécurités réseau afin de s'assurer que les accès à l'ERP sont protégés ;
- Les procédures de sauvegarde et de reprise afin de s'assurer que les données essentielles peuvent être récupérées en cas d'incident.

B/ Sécurité ERP :

L'auditeur doit, notamment :

- valider l'existence et la mise en place d'une politique et de procédures adéquates de sécurité des données
- vérifier que la séparation des tâches a été correctement définie dans chacun des modules de l'ERP
- vérifier que des procédures et des directives ont été définies afin d'assurer une séparation des tâches efficace et une maintenance permanente des profils.

C/ Contrôles d'application :

L'auditeur doit couvrir quatre risques liés à l'ERP. Il doit documenter les flux des processus clés de l'entreprise et doit évaluer la pertinence des contrôles exercés sur :

- la saisie des données et les interfaces avec les systèmes amont
- l'identification et la correction des erreurs
- les traitements et les états de sortie
- les procédures concernant les données permanentes

Par ailleurs, pour la première année de mise en exploitation de l'ERP, l'auditeur doit revoir les procédures et les contrôles appliqués au cours du processus de conversion, afin de confirmer que tous les soldes et les données permanentes migrés des systèmes existants vers l'ERP ont été correctement rapprochés des systèmes sources et autorisés.

Conclusion :

Nous pouvons conclure que, dans un environnement de nouvelles technologies de l'information et de la communication, l'audit informatique fait partie intégrante de l'audit financier.

Certains auteurs affirment que l'informatique doit être intégrée à la démarche professionnelle de l'auditeur et que désormais, il n'y a plus d'audit financier sans audit informatique.[63]

Une démarche de l'audit informatique en support à l'audit financier est présentée dans le chapitre suivant.

[63] Michel LEGER, Didier KING, Pierre COLL et Patrick DE CAMBOURG, « Audit financier : Faire face aux risques informatiques »; 15ème congrès de l'AFAI ; Revue « Audit et conseil informatique » N°54 ; Janvier – Mars 1998.

Chapitre 2 : Présentation de la Démarche de l'Audit Informatique En support à l'Audit Financier

Introduction :

Le présent chapitre se propose d'apporter une contribution à la recherche d'une méthodologie d'audit informatique comme support à l'audit financier. Cette méthodologie est à développer et à adapter à chaque contexte technique rencontré. Elle peut être aussi utilisée dans une mission spéciale d'audit informatique avec, généralement, un champ d'action plus élargi.

Notons, tout d'abord, qu'en raison de la complexité croissante des systèmes, la majorité des cabinets internationaux ont développé des équipes internes spécialisées dans l'audit informatique. Dans leurs travaux, ces derniers entreprennent leur audit en réelle collaboration avec l'équipe d'audit financier mais d'une façon indépendante de point de vue formalisme[64]. La démarche présentée ci-après tient compte de ce fait.

Section 1 : La planification de la mission d'audit informatique

Sous section 1 : Le lancement de la mission d'audit informatique :

Le lancement de la mission d'audit informatique s'intègre dans celui de la mission principale d'audit financier. Son rôle de départ se limite à la collecte d'informations sur les systèmes et l'environnement informatique.

Le lancement de la mission consiste, essentiellement, à organiser une réunion de mobilisation comprenant les membres clefs de l'équipe afin d'aborder, principalement, les aspects suivants :

- Revoir les points soulevés lors de la réunion de clôture de la dernière intervention sur l'entreprise,
- Evaluer la connaissance et l'expérience d'audit accumulées sur l'entreprise et la consolider avec les connaissances acquises par l'intermédiaire des contacts réguliers avec la direction et des autres missions éventuelles menées pour l'entreprise,
- Déterminer le processus de collecte d'informations le plus optimal pour mettre à jour les informations sur le système informatique de l'entreprise. Ceci suppose au préalable une parfaite coordination avec l'équipe d'audit financier et avec les différents responsables concernés de l'entreprise,
- Envisager la coordination avec l'équipe d'audit interne,
- Examiner les problèmes de coordination en cas d'audit sur plusieurs sites.

[64] Cette séparation est, essentiellement, pour des raisons techniques et de suivi administratif du dossier.

Sous section 2 : L'information sur les systèmes et l'environnement informatique

Cette phase se compose, essentiellement, de deux principales étapes à savoir :

- L'établissement de la cartographie des fonctions et systèmes informatiques et identification des cycles
- Collecte d'informations sur les systèmes et l'environnement informatique

1. L'établissement de la cartographie des fonctions et systèmes informatiques et identification des cycles :

L'auditeur doit identifier les principaux cycles et établir la cartographie des fonctions et systèmes informatiques applicables aux sections d'audit liées à chacun de ces cycles. Ces travaux permettront de :

- déterminer la relation entre les états financiers et les fonctions et systèmes qui les génèrent
- déterminer les environnements et les applications informatiques à aborder au cours de la revue générale des contrôles généraux informatiques
- déterminer quelles fonctions et quels systèmes informatiques doivent être revus pour chaque cycle.

Ces travaux sont, généralement, menés d'une façon conjointe entre l'auditeur « généraliste » et l'auditeur « spécialiste des systèmes ».

La collecte de l'information se fait en discutant avec les responsables opérationnels, les responsables financiers et les responsables informatiques ainsi qu'en examinant la documentation correspondante existante.

La cartographie doit permettre de répondre aux questions suivantes :

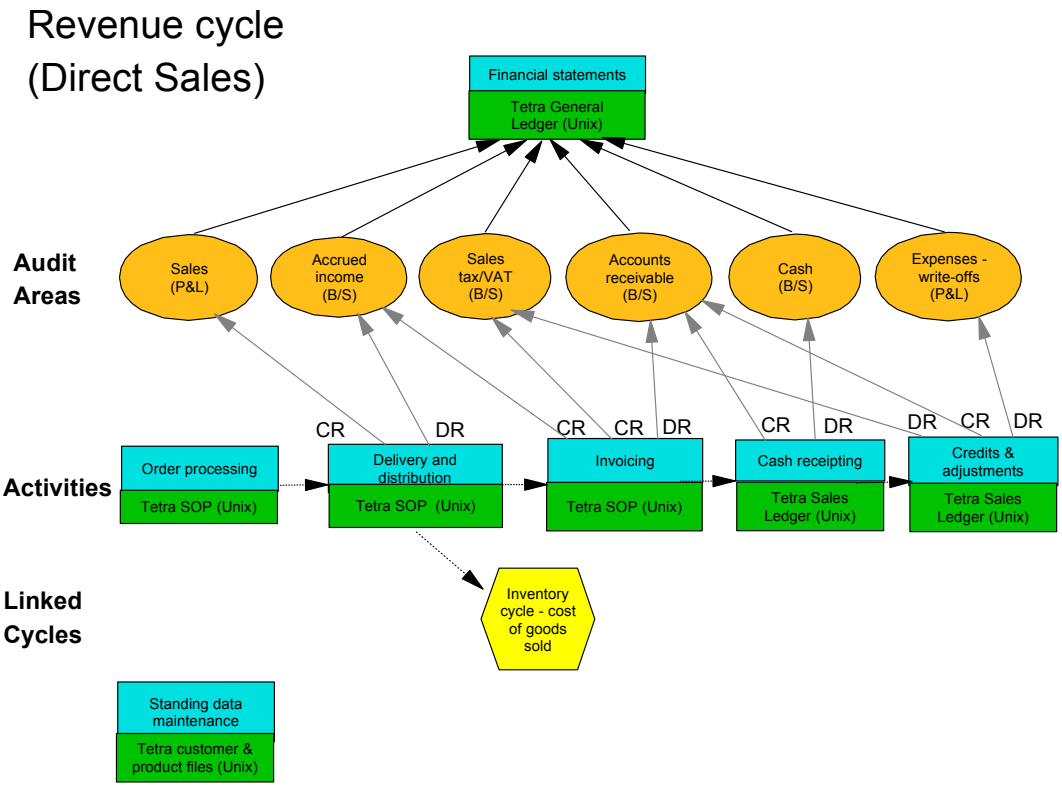
- Quels sont les principaux cycles ?
- Quelles sont les sections d'audit clés ?
- Quelles sont, parmi ces sections d'audit, celles dont les données sont principalement issues de traitements informatiques ?
- Comment les sections d'audit sont-elles reliées avec les cycles ?
- Quelles sont les principales activités au sein de chacun des cycles ?
- Comment ces activités sont-elles initiées ?
- Quels sont les documents comptables et autres documents significatifs relatifs à ces cycles ?
- Quel est le processus comptable et le processus de reporting financier de l'initiation des transactions significatives jusqu'à l'inclusion dans les états financiers ?
- Quels sont les systèmes sous-jacents de chacune des activités au sein des cycles ?
- Sur quels environnements informatiques les systèmes fonctionnent-ils ?
- Quels sont les autres systèmes à prendre en compte dans la planification de l'audit ?

Elle se présente le plus souvent sous la forme d'un diagramme ou, dans le cas de systèmes moins complexes, sous la forme d'un tableau. Toute information utile à la planification devrait y être portée, tels que les volumes, les montants et la fréquence des transactions.

Dans ce qui suit, nous présentons un exemple simple de cartographie afférent au cycle « revenu »[65] :

[65] Cartographie extraite de l'ouvrage du cabinet international PricewaterhouseCoopers, « The PwC audit », 1999.

Cycle Revenu :



2. *La collecte d'informations sur les systèmes et l'environnement informatique :*

Nous distinguons, essentiellement, les axes suivants[66] :

2.1. Appréhender l'organisation de la fonction informatique :

L'auditeur doit documenter sa compréhension de l'organisation de la fonction informatique. Il doit répondre aux questions suivantes :

- Quelle est l'organisation de la fonction informatique ?
- Les rôles et les responsabilités au sein de la fonction informatique sont-ils clairement définis ?
- Des changements majeurs sont-ils intervenus au cours de l'exercice ?
- Qui assume la responsabilité opérationnelle de la fonction informatique (Directeur Général, Directeur Financier, etc.) ? A qui est rattachée la fonction informatique ?
- Y a-t-il un Comité de Pilotage Informatique ? Comment les priorités sont-elles définies ?
- Quels sont nos principaux interlocuteurs au sein de la fonction informatique ?
- Y a-t-il d'autres départements qui assument des responsabilités en matière informatique ?

2.2. Appréhender les contrôles de la direction sur la fonction informatique :

L'auditeur doit documenter sa compréhension des contrôles effectués par la direction sur la fonction informatique. Il doit répondre aux questions suivantes :

- Quels sont les indicateurs clés de performance utilisés par le service informatique dans son reporting ? Ces indicateurs sont-ils revus par des membres appropriés de la direction ?
- Les développements informatiques sont-ils réalisés sur la base d'une méthodologie formalisée ?

[66] NB : La collecte d'informations particulières en cas d'externalisation figure au niveau de la partie I, chapitre 2, section 1, Sous section 1, paragraphe 1.4.

- La direction a-t-elle défini une procédure formelle pour piloter les interventions courantes de maintenance ?
- Une politique en matière de sécurité informatique a-t-elle été définie et communiquée au sein de la société ?
- La société a-t-elle évalué les impacts qui pourraient résulter d'une indisponibilité du système informatique ? Un plan de secours a-t-il été défini ?

2.3. Evaluer dans quelle mesure l'activité repose sur les systèmes informatiques :

L'auditeur doit documenter sa compréhension de l'importance du support informatique dans l'activité. Il doit répondre aux questions suivantes :

- Quel rôle le management attribue-t-il au département informatique dans la réalisation des objectifs de la société ?
- Quelle est l'évolution probable du département informatique dans l'organisation ? (i.e. quelle est la stratégie informatique) ?
- Comment le management évalue-t-il la qualité de sa fonction informatique par rapport à celle d'organisations similaires ?
- Quelles sont les fonctions – clés de la société qui ont une forte prédominance informatique ?
- Comment les utilisateurs perçoivent-ils le service informatique ? Comment la direction informatique mesure-t-elle cette perception ?
- Les informations issues des systèmes répondent-elles aux besoins de la direction ?
- Dans quelle mesure la société utilise-t-elle des technologies nouvelles ou émergentes, telles que le commerce électronique ?

2.4. Identifier les caractéristiques principales des systèmes et environnements :

L'auditeur doit identifier et documenter les caractéristiques principales des systèmes et environnements. Il doit répondre aux questions suivantes :

- Quels sont les systèmes que l'entreprise considère comme les plus importants pour l'activité de la société ?
- Les systèmes sont-ils essentiellement des applicatifs maisons ou des progiciels ? Dans quelle mesure les progiciels ont-ils été adaptés ? Par qui sont effectuées les modifications sur ces applicatifs (internes ou externes) ?
- Quels sont les principaux sites de traitement informatique ? Quels sont les principaux environnements hardware ?
- Comment les environnements informatiques sont-ils interconnectés ? Quelles sont les principales connexions avec des réseaux externes (Exemple : EDI, Internet) ?

2.5. Identifier les changements significatifs en termes de systèmes et d'environnement informatiques :

L'auditeur doit identifier tout changement significatif dans les systèmes et l'environnement informatiques. Il s'agit de répondre, essentiellement, aux questions suivantes :

- Quels nouveaux systèmes ont été mis en place ? Comment se sont déroulées ces opérations ?
- Quel est le volume d'interventions courantes de maintenance sur les systèmes existants ? Y a-t-il eu des interventions majeures ?
- Y a-t-il eu des migrations vers de nouveaux environnements ?
- Y a-t-il eu des mises à jour majeures du logiciel système ?
- Y a-t-il eu des changements majeurs au niveau du réseau ?
- Quelles sont les principales actions informatiques planifiées, à long terme et pour les douze prochains mois ?

2.6. Comprendre les problèmes identifiés au niveau des systèmes :

L'auditeur doit documenter les problèmes identifiés au niveau des systèmes de l'entreprise auditée. Il s'agit d'observer, essentiellement, les points suivants :

- Y a-t-il des problèmes significatifs ou des déficiences fonctionnelles au niveau des systèmes ? Quelles sont, le cas échéant, les mesures palliatives ?
- Y a-t-il eu des incidents d'exploitation majeurs ou des problèmes d'intégrité des données ?

Sous section 3 : L'organisation et la planification de la mission d'audit informatique

A l'issue des différentes étapes de la planification, la stratégie d'audit par cycle est fixée. Si le besoin éventuel de recours aux services de l'audit informatique est exprimé, le responsable de la mission d'audit informatique établira un plan stratégique et un programme de travail qui feront l'objet d'une approbation par le responsable de la mission d'audit financier pour tenir lieu de lettre de mission interne.

Le plan stratégique indique, essentiellement, les éléments suivants :

- Un résumé des principaux éléments recueillis sur le système d'information se rapportant à la structure générale de l'organisation informatique, à la configuration du système informatique, à la nature et à l'étendue du traitement informatisé de l'information, à la complexité des systèmes et des traitements, etc.
- Un plan de rotation entre les unités opérationnelles et un plan de rotation entre les composants : Dans le cas où le système de traitement des données serait décentralisé, chaque unité a sa propre organisation de la fonction informatique, ses programmes et ses applications. L'auditeur peut avoir besoin de visiter chaque emplacement potentiellement significatif pour l'audit. Même si la politique de l'entreprise dicte l'usage de procédures identiques à chaque emplacement, l'auditeur aura besoin de considérer si les procédures sont réellement appliquées.
- L'organisation générale de la mission : Ceci consiste, essentiellement, à :
  - Préparer un calendrier d'intervention qui doit contenir au minimum les dates concernant :
    a) le démarrage et la finalisation de l'audit et les étapes clés de la mission,
    b) la préparation par les responsables de l'entreprise des informations et documents importants nécessaires à l'audit et,
    c) les réunions périodiques avec l'équipe d'audit et avec les responsables de l'entreprise.

    Ce calendrier détaillé doit être discuté et accepté par le responsable de la mission d'audit financier et par les responsables de l'entreprise.
  - Prévoir des réunions d'avancement régulières avec l'équipe d'audit informatique afin de s'assurer du bon déroulement de la mission et des réunions d'avancement régulières avec l'équipe d'audit financier et, éventuellement, avec les différents responsables de l'entreprise.
  - Préparer la répartition des tâches avec un niveau de détail suffisant en prenant les dispositions nécessaires pour permettre une réalisation efficace des travaux d'audit informatique et une parfaite coordination avec l'équipe d'audit et les différents responsables de l'entreprise.
  - Préparer le budget global et par intervenant.
  - Se mettre d'accord avec l'équipe d'audit financier des procédures à suivre en cas de modifications apportées au plan d'audit informatique.
- L'évaluation des risques liés à l'environnement informatique : Il s'agit de dégager les risques liés à la fonction informatique pouvant affecter la stratégie. Exemples : des modifications ont été ou seront apportées aux systèmes informatiques durant l'exercice ; De nouveaux systèmes ou des améliorations majeures ont été ou seront mis en place pendant l'exercice.

- La démarche à suivre en cas d'externalisation : Au cas où l'entreprise externalise un ou plusieurs aspects de son système informatique, l'auditeur devrait considérer les contrôles généraux informatiques et les contrôles d'application relatifs à la fonction du prestataire de services, que ces contrôles soient effectués par l'entreprise auditée ou par son prestataire de services. En effet,
  - Si le prestataire de services procède à des contrôles généraux informatiques et à des contrôles d'applications pertinents pour l'évaluation des risques, il convient de déterminer si l'auditeur du prestataire a formalisé, dans son rapport, ses conclusions sur les tests réalisés sur ces contrôles et si ce rapport est exploitable ;
  - Si c'est l'entreprise qui effectue des contrôles généraux informatiques et des contrôles d'applications liés à la fonction du prestataire de services, l'auditeur doit tester ces contrôles ;
  - Si le rapport de l'auditeur du prestataire de services n'est pas disponible et si les contrôles effectués par l'entreprise ne sont pas suffisants, l'auditeur doit s'interroger sur la nécessité de tester les contrôles existants chez le prestataire de services.

Sous section 4 : Le dossier permanent informatique

Le dossier permanent informatique comprend les informations permanentes se rapportant au système d'information de l'entreprise. Il peut être structuré comme suit :

1. Renseignements généraux :

- Présentation générale de l'entreprise : (Raison sociale, adresse, activité, adresse du service informatique si différente, personnes à contacter, etc.)
- Renseignements internes (Associé responsable, équipe, clôture comptable, code mission, etc.)
- Organigramme de la société

2. La fonction informatique :

- Place de l'informatique dans l'organisation générale de l'entreprise :
  - Rattachement de l'informatique dans l'organigramme général, rôles et limites de la responsabilité du département ou du service informatique
  - Evolution du budget informatique sur les cinq dernières années (en valeur et en pourcentage du chiffre d'affaires)
  - Principaux axes du plan informatique.
- Structure du service ou de la direction informatique
- Schéma directeur informatique
- les comptes rendus du comité directeur informatique

3. Le (ou les) centres de traitement :

- Configuration générale
- Configuration de chaque centre de traitement : matériel, etc.

4. Les applications :

Pour chaque application en place, il y a lieu d'indiquer :

- La version
- La description : fonction, interface, etc.
- Le fournisseur
- La date d'installation de la première version
- La date de la dernière mise à jour
- Le coût de la maintenance
- Etc.

5. Historique des interventions :

- Objets de l'intervention
- Budgets
- Intervenants²

6. Cartographie et description des procédures

7. Autres informations

Section 2 : L'examen des contrôles généraux informatiques

En se basant sur les informations documentées dans la cartographie durant la phase de planification, l'auditeur sélectionne les environnements et les systèmes informatiques significatifs. Il procède, ensuite, à la documentation de ces environnements et systèmes afin de dégager les contrôles généraux informatiques clefs. Ces derniers font l'objet de tests appropriés afin d'apporter la preuve qu'ils fonctionnent réellement et d'une façon permanente. Ces travaux se font, généralement, durant la phase intérimaire.

La documentation des contrôles peut être réalisée en utilisant les questionnaires standards en la matière. Elle peut être, aussi, sous forme narrative et/ou sous forme de diagrammes.

Par ailleurs, avant la sélection des contrôles clefs, l'auditeur doit assurer sa compréhension des contrôles documentés à travers, généralement, la réalisation de tests de cheminement ou la confirmation auprès des responsables de l'entreprise.

Les contrôles généraux informatiques clefs sont des contrôles qui :

- fournissent l'assurance à l'auditeur de s'appuyer sur les contrôles automatisés sélectionnés comme des contrôles clefs d'un cycle ;
- peuvent être testés le plus efficacement possible.

En cas d'absence de changements, les contrôles généraux informatiques clefs demeurent les mêmes d'une année à l'autre. Pour les années suivantes, l'auditeur aura toujours besoin de tester ces contrôles, mais l'étendue des tests peut être réduite sur la base de l'évaluation antérieure du risque et de l'implication des dirigeants dans le domaine de la maintenance, de la sécurité des systèmes et de la sécurité de l'exploitation.

Le mix des contrôles dépend de plusieurs facteurs :

- La largeur de couverture qu'un contrôle fournit
- L'étendue de l'assurance fournie par le contrôle sur un contrôle automatisé particulier
- La compétence requise pour exécuter les tests
- Le temps exigé pour la réalisation du test
- La complexité du test
- L'ampleur du risque et l'assurance requise.

Dans ce qui suit, nous examinons, avec plus de détails, les différentes catégories de contrôles généraux informatiques et les divers indicateurs qui peuvent être considérés par l'auditeur[67].

Sous section 1 : Les contrôles portant sur la sécurité des systèmes

L'efficacité de certains contrôles automatisés et l'intégrité des données peuvent être affectées par des contrôles insuffisants au niveau de la sécurité des systèmes. Par exemple, l'utilisation de mots de passe et de menus pour assurer la séparation des fonctions peut être rendue inefficace si la sécurité globale de l'environnement informatique s'avère peu fiable.

[67] Cette section est une synthèses des différents ouvrages, articles, formations, ateliers, séminaires, etc. traitant du sujet et figurant au niveau de la bibliographie. Nous citons, essentiellement, « The PricewaterhouseCoopers Audit », Cabinet international PwC, 1999.

Ainsi, l'auditeur doit documenter, évaluer, sélectionner et tester les contrôles clefs afférents à l'administration d'ensemble et aux procédures détaillées de gestion de la sécurité de l'information.

1. Documenter, évaluer et tester l'administration d'ensemble de la sécurité de l'information :

Il s'agit d'effectuer une description générale de l'administration d'ensemble de la sécurité de l'information. En outre, et pour l'évaluation des contrôles mis en place, il y a lieu de considérer, à titre indicatif, les éléments suivants :

1.1. Administration d'ensemble de la sécurité :

La direction de l'entreprise doit établir des procédures de contrôle d'accès en fonction du niveau de risque résultant de l'accès aux programmes et aux données. Ainsi, l'auditeur doit considérer, à titre d'exemple, les indicateurs suivants :

- Quelle est l'approche de la direction pour évaluer les risques liés à la confidentialité, à l'intégrité et à la disponibilité de l'environnement informatique ?
- La direction a-t-elle clairement identifié les informations et les actifs informatiques qu'il convient de protéger ?
- La direction a-t-elle pris en compte les obligations réglementaires et légales ?
- La direction a-t-elle pris en compte le risque d'intrusion en provenance de l'extérieur y compris via des connections à des réseaux externes ?
- La direction a-t-elle pris en compte le risque de fraude informatique, les éventuels actes de sabotage ou de vandalisme sur les installations informatiques ?
- Quelle est l'attitude de la direction à l'égard de la sécurité ?
- La politique de sécurité est-elle appropriée ?
- Les descriptions de postes définissent-elles les rôles et les responsabilités en termes de sécurité informatique ?
- Quelle est la procédure de sélection des candidats à des postes impliquant un accès à des systèmes informatiques gérant des informations sensibles ?
- Les utilisateurs sont-ils soumis à une clause de confidentialité ?

1.2. Définition des rôles, des responsabilités et des procédures :

La direction de l'entreprise doit définir les rôles et les responsabilités en termes de sécurité informatique et s'assurer que les responsables mettent en place des procédures adéquates. Ainsi, l'auditeur doit considérer, par exemple, les indicateurs suivants :

- Les rôles et les responsabilités sont-ils clairement définis et compris et ce en matière de configuration des systèmes, de gestion de la sécurité, de propriété des données et de sécurité physique des installations informatiques ?
- Si la taille de l'organisation est importante, comment les mesures en matière de sécurité informatique sont-elles coordonnées et communiquées ?
- Les paramètres de configuration système sont-ils clairement documentés ?
- Les procédures d'administration de la sécurité (par exemple pour la création de nouveaux utilisateurs, la modification ou la suppression d'utilisateurs existants) sont-elles définies et communiquées ?

1.3. Sensibilisation et formation des utilisateurs à la sécurité :

La direction doit s'assurer que les utilisateurs sont suffisamment sensibilisés et formés dans le domaine de la sécurité informatique, et qu'ils comprennent les enjeux et les actions à mener. Ainsi, l'auditeur doit considérer, à titre d'exemple, les indicateurs suivants :

- La direction a-t-elle mis en place une procédure pour s'assurer que les utilisateurs ont suivi une formation de sensibilisation aux enjeux de la sécurité informatique ?
- Les formations utilisateurs sont-elles adaptées ?

1.4. Moyens informatiques à la disposition des utilisateurs :

Les moyens informatiques mis à la disposition des utilisateurs finaux ainsi que leur utilisation doivent être contrôlés de manière à assurer la compatibilité des systèmes et à garantir l'intégrité des données. Ainsi, l'auditeur doit considérer, par exemple, les indicateurs suivants :

- Comment identifie-t-on et contrôle-t-on l'utilisation des ordinateurs et des autres moyens informatiques laissés à la disposition des utilisateurs ?
- Comment est contrôlée l'acquisition des matériels et des logiciels informatiques destinés aux utilisateurs ?
- Les utilisateurs bénéficient-ils d'une formation adéquate et d'un support technique suffisant ?
- Quels contrôles ont été mis en place par la direction pour prévenir le risque de virus informatiques (y compris celui provenant de l'usage d'Internet) ?
- Quels contrôles ont été mis en place par la direction pour prévenir les risques de non-respect de la réglementation des droits sur les licences de progiciels ?

1.5. Contrôle des incidents en matière de sécurité et du respect des procédures :

La direction doit contrôler les incidents liés à la sécurité ainsi que le respect des procédures de sécurité. L'auditeur doit considérer, par exemple, les indicateurs suivants :

- Comment sont répertoriés les incidents ou les événements survenant dans le domaine de la sécurité ? Comment la direction en est-elle informée ? Ces événements et ces incidents font-ils l'objet d'un suivi ?
- Combien d'incidents ou d'événements liés à la sécurité se sont-ils produits au cours de la période auditée ?
- Quelles sont les vérifications régulières effectuées sur les paramètres de configuration du système, afin de s'assurer de leur conformité ?
- Quel type de contrôle (ou procédure d'audit) garantit l'efficacité du processus d'administration de la sécurité ?
- Des problèmes de non-respect des procédures de la sécurité se sont-ils produits ?

2. Documenter, évaluer et tester les procédures détaillées de gestion de la sécurité de l'information :

Après avoir effectuer une description générale des procédures détaillées de gestion de la sécurité de l'information, l'auditeur doit documenter et évaluer les contrôles mis en place et ce en considérant, à titre indicatif, les éléments suivants :

2.1. Administration de la sécurité logique des accès utilisateurs au système d'exploitation :

L'accès des utilisateurs au système d'exploitation et aux programmes doit être contrôlé. L'auditeur doit considérer, par exemple, les indicateurs suivants :

- Les utilisateurs et les administrateurs ont-ils un identifiant spécifique (ID) ?
- Quelle procédure permet de contrôler la création d'un nouvel identifiant ?
- Existe-t-il des procédures assurant une mise à jour rapide des autorisations d'accès en cas de changement, d'affectation ou de départ du personnel ?
- Quelles mesures permettent de prévenir les accès non autorisés suite à l'utilisation d'identifiants par défaut (par exemple, identifiants créés automatiquement lors de la mise en place du système d'exploitation) ?
- Quelles mesures permettent d'identifier les identifiants inactifs et de minimiser le risque d'accès non autorisés liés à l'utilisation de ces identifiants ?
- Quels sont les contrôles périodiques effectués afin de garantir l'adéquation du profil d'accès des utilisateurs avec leurs fonctions ?
- La saisie des mots de passe est-elle obligatoire pour l'ensemble des identifiants ?

- Quelle est la longueur minimale des mots de passe ? Et quelles mesures permettent de prévenir l'utilisation de mots de passe faciles à deviner ?
- Quelle est la périodicité de renouvellement des mots de passe ?
- Quel est le niveau de protection du fichier contenant les identifiants et les mots de passe ?
- Quelles sont les mesures permettant d'empêcher l'accès aux commandes des systèmes par les utilisateurs ?
- La structure de détermination des groupes d'identifiants est-elle appropriée et l'affectation d'un utilisateur à un groupe est-elle pertinente ?
- Quel est le processus de connexion ?
- Quels sont les messages d'avertissement lancés au moment de la connexion, afin de prévenir tout accès non autorisé dans l'environnement ?
- Quelles sont les procédures permettant d'éviter l'usurpation des mots de passe par essais successifs ou à la suite d'une erreur ?
- Y a-t-il des procédures d'identification de terminal permettant d'authentifier les postes sur lesquels sont effectuées les connexions ?
- Le nombre de connexions simultanées par utilisateur est-il limité à un ?
- Existe-t-il des restrictions d'accès des utilisateurs en termes de nombre de connexions par jour, ou de jours par semaine, ou d'horaires ?
- Y a-t-il une procédure de déconnexion automatique ou de mise en veille des écrans inactifs après une période de non-utilisation ?

2.2. Administration de la sécurité logique des données :

L'accès aux données doit être contrôlé de manière adéquate. L'auditeur doit considérer, par exemple, les indicateurs suivants :

- Comment les fichiers systèmes/répertoires sont-ils protégés contre des modifications non autorisées ?
- Les droits d'accès accordés par défaut sur les nouveaux fichiers sont-ils pertinents ?
- Les droits en création/modification sur les répertoires sont-ils justifiés ?
- Comment les droits d'accès des utilisateurs sur les fichiers sont-ils contrôlés ?

2.3. Administration de la sécurité au niveau applicatif :

Les moyens informatiques et les procédures en place doivent permettre de restreindre les accès aux différentes fonctions applicatives (par exemple : approbation des règlements fournisseurs) afin d'assurer une séparation des tâches adéquates et d'empêcher les accès non autorisés. Dans ce cadre, l'auditeur doit considérer, par exemple, les indicateurs suivants :

- Comment les accès utilisateurs sont-ils limités au sein des applications ?
- La gestion des mots de passe au sein des applications est-elle efficace ?
- Quelle est la qualité des "pistes d'audit" issues des systèmes ?
- Comment le paramétrage de nouveaux utilisateurs est-il contrôlé ?
- Existe-t-il des procédures assurant une mise à jour rapide des autorisations d'accès en cas de changement d'affectation ou de départ de personnel ?
- Quels contrôles réguliers permettent de garantir l'adéquation des profils d'accès des employés avec leurs fonctions ?

2.4. Administration des systèmes et des profils privilégiés :

L'utilisation de ressources sensibles, telles que les mots de passe système, les utilitaires puissants et les outils de gestion du système, doit être contrôlée de façon appropriée. A cet effet, l'auditeur doit considérer, par exemple, les indicateurs suivants :

- Le nombre de personnes ayant des profils d'administrateurs système est-il approprié ?
- Comment l'activité des administrateurs système est-elle contrôlée ?
- Quelle est la fréquence de renouvellement des mots de passe pour les administrateurs système ?
- Le nombre de profils privilégiés est-il approprié ?
- Comment l'usage des profils privilégiés est-il contrôlé ?

2.5. Sécurité physique :

L'accès physique aux installations informatiques et aux données doit être contrôlé de manière appropriée. A cet effet, l'auditeur doit, à titre indicatif, considérer les indicateurs suivants :

- Comment l'accès au site/bâtiment comportant les installations informatiques est-il restreint ?
- Comment l'accès à la salle informatique est-il contrôlé ?
- Comment les supports informatiques (cassettes, cartouches, etc.) sont-ils protégés ?
- Comment les documents confidentiels sont-ils classés et protégés ?
- Comment la documentation relative aux systèmes est-elle protégée ?
- Comment la mise au rebut des équipements informatiques et des supports de données est-elle sécurisée (destruction, reformatage des supports physiques) ?

2.6. Contrôle des accès réseaux informatiques / accès distants :

Les accès distants aux systèmes informatiques, via des connexions par réseau informatique ou téléphonique, doivent être restreints de façon appropriée. A ce niveau, l'auditeur doit considérer, par exemple, les indicateurs suivants :

- Comment les connexions avec des sites distants sont-elles authentifiées ?
- Si le réseau est étendu, est-il divisé entre plusieurs domaines distincts ? Si oui, quels sont les contrôles permettant de s'assurer que les utilisateurs n'accèdent qu'aux domaines relevant de leurs fonctions ?
- Comment les transferts de données par les réseaux sont-ils protégés ?
- Le nombre d'utilisateurs ayant un accès distant est-il approprié ?
- Comment ces utilisateurs sont-ils authentifiés ?
- La disponibilité des connexions distantes au réseau est-elle limitée à certaines périodes de la journée /semaine ?
- Quels sont les contrôles mis en place sur la télémaintenance ?

2.7. Contrôle des connexions avec des réseaux externes (par exemple : Internet, EDI, etc.) :

Les connexions avec des réseaux externes doivent être convenablement protégées. Des contrôles doivent être mis en place afin de prévenir le risque d'une faille dans la sécurité du système. A titre indicatif, les indicateurs suivants devraient être considérés par l'auditeur :

- Des conditions de sécurité adéquates ont-elles été définies dans les contrats signés avec des tiers concernant les transferts de données via des réseaux externes ?
- Quel est le niveau de sécurité de la messagerie électronique ?
- Comment le point d'entrée entre l'environnement informatique de la société et le réseau Internet est-il contrôlé ?
- Comment les connexions externes utilisées pour des liaisons EDI sont-elles protégées ?
- La société utilise-t-elle l'encryptage ou toute autre procédure de sécurité équivalente pour assurer l'intégrité des transactions réalisées à travers Internet et pour protéger les transmissions de l'authentification de l'utilisateur et des informations de vérification ?
- Des tests périodiques de pénétration sont-ils réalisés ? (Ces tests utilisent les mêmes méthodes de pénétration que celles des pirates informatiques).

Sous section 2 : Les contrôles portant sur la sécurité de l'exploitation

L'examen des contrôles portant sur la sécurité de l'exploitation nécessite la documentation, l'évaluation et l'examen de l'administration d'ensemble de l'exploitation des systèmes d'une part, et des procédures détaillées de l'exploitation d'autre part.

1. Documenter, évaluer et tester l'administration d'ensemble de l'exploitation des systèmes :

L'auditeur doit effectuer une description générale de l'administration d'ensemble de l'exploitation des systèmes informatiques relative à tous les environnements. Il doit documenter et évaluer les contrôles mis en place par l'entreprise. Pour cela, il doit considérer, à titre indicatif, les éléments suivants :

1.1. Définition des rôles, des responsabilités et des procédures :

La direction doit définir les rôles et les responsabilités des personnes chargées de l'exploitation et s'assurer que les procédures sont clairement définies et comprises.

L'auditeur doit s'assurer que les rôles, les responsabilités et les procédures relatifs aux domaines suivants sont clairement définis et compris :

- Les traitements
- Les traitements des sauvegardes et des restaurations
- La maintenance des logiciels systèmes

Par ailleurs, l'auditeur doit s'assurer que le personnel impliqué dans l'exploitation informatique a reçu une formation adéquate et dispose d'une documentation appropriée.

1.2. Procédures de continuité d'exploitation :

Des plans de continuité d'exploitation couvrant tous les aspects de la fonction informatique doivent être en place. Pour cela, l'auditeur doit considérer par exemple les indicateurs suivants :

- La direction a-t-elle évalué le risque qui pourrait résulter des défaillances des équipements ou d'un sinistre ?
- Existe-t-il un plan de secours servant à limiter les pertes tangibles et intangibles associées à une interruption ou catastrophe majeure et à planifier le retour aux opérations normales ?
- Le plan de secours fait-il l'objet d'une procédure d'actualisation et de test ?

1.3. Gestion du réseau :

Les réseaux hardware et software doivent être conçus de façon adéquate afin de répondre aux besoins de disponibilité, de performance et d'adaptabilité. Ainsi, l'auditeur doit considérer, par exemple, les indicateurs suivants :

- Quelle est la documentation réseau disponible ?
- Quelle est la procédure d'approbation, de contrôle et de test des modifications apportées au réseau ?
- Quelles sont les procédures en place en matière de gestion de la capacité et de suivi du niveau de performance ?

1.4. Suivi des performances opérationnelles et du respect des procédures :

La direction doit assurer le suivi des performances et contrôler le respect des procédures d'exploitation. Ainsi l'auditeur doit considérer, par exemple, les indicateurs suivants :

- Sur la base de quelles informations la direction contrôle-t-elle les opérations d'exploitation et le bon déroulement des traitements « batch » ?
- Selon quelle fréquence la direction dispose-t-elle de ces informations ?
- Y a-t-il eu des problèmes dans la performance du système ou dans le bon déroulement des traitements « batch » ?
- Quel type de contrôle (ou procédure d'audit) garantit l'efficacité du processus d'exploitation ?
- Des problèmes de non-respect des procédures d'exploitation se sont-ils produits ?

2. Documenter, évaluer et tester les procédures détaillées de l'exploitation :

L'auditeur doit effectuer une description générale des procédures détaillées de l'exploitation. Ensuite, il procédera à la documentation et à l'évaluation des contrôles mis en place. A titre indicatif, les éléments suivants peuvent être étudiés :

2.1. Planification, préparation et exécution des traitements batch :

Les traitements batch qui doivent être exécutés à des périodes définies (quotidiennement, hebdomadairement, mensuellement, annuellement) doivent être documentés, planifiés et mis à jour régulièrement. A titre indicatif, les indicateurs suivants peuvent être considérés :

- Les opérateurs d'exploitation disposent-ils de consignes d'exploitation documentées ?
- Quelles procédures garantissent la qualité de la planification et de l'ordonnancement des traitements batch ?
- Comment s'assure-t-on que les données nécessaires à l'exécution des traitements batch sont effectivement disponibles (par exemple : disponibilité au début de traitement de données provenant de différents sites) ?
- Existe-t-il des comptes-rendus de traitement permettant d'assurer aux opérateurs le suivi de l'exécution et le contrôle de l'exécution ?
- Comment s'assure-t-on que l'activité des opérateurs est conforme à leur définition de fonction ?

2.2. Sauvegarde :

Des sauvegardes à jour des programmes et des données doivent être disponibles pour assurer la continuité de l'exploitation en cas de besoin. L'auditeur doit examiner, à titre indicatif, les points suivants :

- Les procédures de sauvegarde des données et des programmes sont-elles satisfaisantes ?
- Les supports de sauvegarde sont-ils répertoriés et conservés dans un lieu sûr ?
- Quelles sont les procédures garantissant le bon fonctionnement des sauvegardes et la reprise des données ?

2.3. Gestion des incidents :

Des procédures doivent être définies afin de garantir que les incidents d'exploitation (par exemple : crash de disques, défaillances des programmes) sont identifiés et résolus de manière adéquate.

A titre indicatif, l'auditeur doit observer les indicateurs suivants :

- La protection physique des équipements est-elle correctement assurée (par exemple : contre le feu, la fumée, l'eau, les poussières, les éléments chimiques, les radiations électromagnétiques) ?
- Les équipements informatiques bénéficient-ils d'une maintenance adéquate ?
- Quels sont les contrôles permettant d'éviter la survenance d'incidents opérationnels liés au matériel ?
- Comment l'alimentation électrique des équipements informatiques est-elle sécurisée ?
- Quelles sont les procédures permettant d'assurer l'adéquation des niveaux de ressources et des performances avec les besoins de l'entreprise ?
- Comment les incidents sont-ils répertoriés ?
- Quelles sont les procédures permettant de résoudre les incidents opérationnels ?

2.4. Mise à jour des logiciels systèmes :

La sélection de nouveaux logiciels systèmes et la mise à jour des logiciels existants (par exemple : système d'exploitation et tout autre logiciel système dans les domaines de la sécurité) ne doivent pas causer d'incidents de traitements ou déstabiliser les mécanismes de contrôle des systèmes.

L'auditeur doit, par conséquent, considérer les indicateurs suivants :

- Comment le processus de sélection / mise à jour des versions des logiciels systèmes est-il contrôlé ?
- Qui est habilité à effectuer la maintenance des logiciels systèmes ?
- Quelles procédures garantissent que seules les mises à jour appropriées sont effectuées sur les logiciels maintenus en interne ?

- Comment les modifications apportées aux logiciels de base maintenus en interne sont-elles testées avant leur mise en exploitation ?
- Comment s'assure-t-on que les nouveaux logiciels ou les mises à jour ont été testés de manière appropriée avant transfert dans l'environnement d'exploitation ?
- Des procédures sont-elles prévues pour permettre le retour à l'ancien environnement en cas de problème survenu lors de la mise en place d'une nouvelle version d'un logiciel ?

Sous section 3 : Les contrôles portant sur les procédures de maintenance des applications informatiques

Les procédures de maintenance en place doivent permettre, essentiellement, d'assurer le contrôle que les programmes modifiés opèrent comme prévu et qu'ils ne peuvent être manipulés pour des raisons non autorisées durant le processus de maintenance.

En terme d'audit, ces procédures sont importantes pour assurer la pérennité des contrôles automatisés. Ainsi, l'auditeur doit documenter et évaluer les activités de maintenance des systèmes et sélectionner et tester les contrôles clés correspondants en considérant, à titre indicatif, les éléments suivants :

1. La gestion de la maintenance :

La direction doit établir une procédure dès lors que des modifications de système sont envisagées et s'assurer du respect de cette procédure. Dans ce cadre, l'auditeur peut examiner les indicateurs suivants :

- La direction a-t-elle mis en place une procédure afin de contrôler les modifications apportées aux systèmes informatiques ?
- La direction est-elle impliquée dans la revue et l'approbation des changements relatifs aux systèmes informatiques ?
- La direction effectue-t-elle une revue régulière de ces changements ?
- Lorsque la maintenance de la nouvelle application est assurée directement par le fournisseur, quelles précautions sont prises dans le cas où celui-ci ne serait plus en mesure de fournir ce service ?
- Les qualités fonctionnelles et opérationnelles des systèmes sont-elles mesurées et suivies par la direction informatique ?
- Le management opérationnel dispose-t-il de rapports et de statistiques pour apprécier les qualités opérationnelles des systèmes ?
- Le management opérationnel est-il directement impliqué dans le test des modifications apportées au système ?
- La direction dispose-t-elle de rapports sur les résultats de ces tests ?

2. La définition, l'autorisation et la gestion des demandes de modifications

Les demandes de modifications de programmes informatiques doivent être correctement examinées et traitées. Ainsi, l'auditeur doit examiner, par exemple, les indicateurs suivants :

- Les équipes de développement sont-elles en liaison étroite avec les utilisateurs ?
- Comment les demandes de modifications sont-elles transmises aux équipes de développement ?
- Quelles procédures permettent d'assurer que les équipes de développement ont bien compris les besoins des utilisateurs avant d'entamer toute modification des systèmes ?
- Existe-t-il une procédure adéquate permettant de répertorier et de suivre les demandes de modifications ?
- Qui approuve et hiérarchise les demandes de modifications ? Dans quelle mesure l'ordre de réalisation des modifications est-il conforme à l'ordre des priorités qui leur a été affecté ?
- Quelles sont les procédures permettant, d'une part d'assurer que les modifications approuvées sont mises en œuvre dans les délais impartis et d'autre part de suivre l'avancement des projets ?
- Le nombre de programmeurs est-il suffisant pour assurer la maintenance des systèmes ?

- Les programmeurs ont-ils les compétences nécessaires pour assurer la maintenance des systèmes ?
- Les programmeurs ont-ils une compréhension suffisante des enjeux liés aux systèmes d'information de l'entreprise ? Depuis combien de temps les programmeurs assurent-ils la maintenance des systèmes ?

3. *Les tests unitaires, les tests d'intégration et les tests utilisateurs :*

Les modifications apportées aux programmes doivent être testées pour s'assurer qu'elles répondent aux attentes des utilisateurs et qu'elles n'ont pas d'incidences négatives sur les traitements existants. A titre indicatif, les indicateurs suivants devraient être considérés par l'auditeur :

- La séparation des environnements informatiques de développement, de test et d'exploitation est-elle respectée ?
- Quelle est la nature et l'étendue des tests réalisés par l'équipe de développement préalablement aux tests d'intégration dans le système et aux tests utilisateurs ?
- Quelle est la nature des tests d'intégration et des tests utilisateurs réalisés sur les changements applicatifs mineurs et sur les changements applicatifs majeurs ?
- Les utilisateurs sont-ils en nombre suffisant pour assurer un contrôle adéquat sur les systèmes ?
- Quelles procédures permettent de s'assurer qu'aucune modification non autorisée ne peut être effectuée entre la phase des tests et la mise en production des programmes ?
- Quels contrôles permettent de s'assurer que la version de code source utilisée est la plus récente et que les modifications faites par plusieurs programmeurs sont coordonnées ?

4. *L'autorisation de mise en production :*

Seuls les changements dûment autorisés et testés doivent être transférés dans l'environnement d'exploitation. A titre d'exemple, l'auditeur doit examiner les indicateurs suivants :

- Qui réalise les migrations courantes (pour les modifications routinières) ?
- Dans quelle mesure les développeurs peuvent-ils avoir accès à l'environnement d'exploitation ?
- Une procédure d'autorisation pour les corrections urgentes de programmes ou de données est-elle définie ?
- Garde-t-on la trace des accès à l'environnement d'exploitation par les programmeurs dans le cadre de corrections urgentes ?
- Comment s'assure-t-on que les mises à jour sont réalisées sur les bonnes bibliothèques de programmes et avec la dernière version des programmes développés ?
- Lorsque les applications sont installées sur plusieurs sites, quelles procédures permettent d'assurer la correcte mise à jour des programmes sur l'ensemble des sites concernés ?

5. *La formation et la mise à jour de la documentation technique et de la documentation destinée aux utilisateurs :*

La documentation technique doit être mise à jour en fonction des modifications effectuées. Quand les modifications affectent les procédures utilisateurs, la documentation qui leur est destinée doit également être mise à jour et, si nécessaire, une formation devait leur être assurée ainsi qu'au personnel informatique.

L'auditeur doit considérer, par exemple, les indicateurs suivants :

- La documentation utilisateur et le manuel de procédures sont-ils facilement accessibles et exploitables ? Couvrent-ils tous les aspects du système ?
- Existe-t-il des procédures de mise à jour de la documentation utilisateur lorsque des modifications sont effectuées ?
- La documentation technique relative au système est-elle facilement accessible et exploitable ?
- Quelle est l'étendue du domaine couvert par la documentation technique ?
- Existe-t-il des procédures de mise à jour de la documentation technique lorsque des modifications sont effectuées ?
- Les utilisateurs ont-ils reçu une formation appropriée pour exploiter les systèmes ?

6. La gestion des bases de données (si applicable) :

Les bases de données alimentant les systèmes doivent être gérées de façon à ce que l'intégrité des données soit assurée. L'auditeur doit examiner, par exemple, quelles sont les procédures mises en place pour assurer l'intégrité des données ?

Il y a lieu de rappeler que pour les auditeurs, les contrôles portant sur les procédures de maintenance des applications informatiques sont des contrôles importants. En effet, en l'absence de contrôles appropriés sur les changements des programmes, il peut être difficile, pour l'auditeur, de s'assurer par d'autres moyens que les contrôles programmés et les fonctions de traitement informatisées fonctionnent d'une façon efficace et permanente tout au long de la période examinée.

Par ailleurs, un facteur important à considérer lors de l'évaluation des risques et des contrôles est que, dans la majorité des cas associés aux nouvelles technologies, le personnel de l'entreprise n'a aucune participation directe dans le développement ou la maintenance du logiciel (ou uniquement une participation limitée) de source extérieure.

En effet, souvent, il est stipulé dans les contrats d'achat que la maintenance est fournie par le vendeur du logiciel. Dans cette situation, l'entreprise ne peut pas apporter des changements au logiciel (l'accès au code source est non fourni). En conséquence, le risque que des changements non autorisés soient apportés aux programmes peut être jugé faible. Toutefois, l'auditeur doit obtenir l'assurance que les changements réalisés par le vendeur sont testés par l'entreprise d'une façon appropriée.

Enfin, il est à noter que l'auditeur est souvent confronté à des environnements qui ne satisfont pas, ou qui ne satisfont que partiellement, les éléments étudiés ci-dessus. Dans ce cas, l'auditeur peut faire recours à des tests alternatifs destinés à dégager les éventuelles modifications apportées. Nous citons, à titre d'exemple, le rapprochement, par des outils informatiques d'aide à l'audit, la version utilisée et une copie de contrôle et l'identification des modifications qui feront l'objet d'une investigation par l'équipe d'audit.

Sous section 4 : Les contrôles portant sur les procédures de développement et de modification des applications

La mise en place de contrôles portant sur les procédures de développement et de modification des applications permet à la direction de s'assurer que les nouveaux systèmes ou les améliorations importantes introduites sont convenablement conçus, testés et mis en exploitation et que des contrôles appropriés ont été prévus.

L'auditeur, à travers l'examen de ces contrôles, vise à s'assurer que les systèmes, une fois mis en exploitation, incluent des contrôles appropriés et fonctionnent comme prévu. Il doit effectuer, au préalable, une description générale des procédures de développement et de mise en exploitation. Par ailleurs, il doit documenter et évaluer les contrôles dans les domaines suivants :

1. Le lancement du projet :

La direction doit s'assurer que seuls les projets adéquats sont initiés et que la structure de ces projets est appropriée. A titre d'exemple, l'auditeur peut considérer les indicateurs suivants :

- Quelle procédure garantit la planification de l'ensemble des étapes nécessaires au projet (par exemple : utilisation d'une méthodologie de développement) ?
- Quelles procédures assurent le contrôle de l'avancement du projet (par exemple : structure de projet, procédures de reporting) ?
- A-t-on défini des objectifs opérationnels clairs pour ce projet ?
- Quelles études de faisabilité ont été engagées préalablement au démarrage du projet ?
- Le projet a-t-il été placé sous la responsabilité d'un membre de l'équipe de Direction ? Des objectifs en termes de résultats à atteindre ont-ils été assignés ?
- Quelles procédures garantissent que les chefs de projet disposent du niveau de compétence nécessaire ?
- Les utilisateurs sont-ils suffisamment impliqués dans la gestion du projet ?
- Existe-t-il un pôle indépendant d'assurance qualité sur le projet ?
- Quelles procédures ont étés mises en place pour maîtriser les aléas du projet (dérapages dans les dates de livraison,...) ?

2. *Les spécifications du projet :*

Les spécifications doivent inclure de façon suffisamment détaillée et pertinente la description des fonctionnalités, les performances, les sécurités et les dispositifs de contrôle interne. L'auditeur doit considérer par exemple les indicateurs suivants :

- Comment s'assure-t-on que les spécifications des besoins et des contrôles applicatifs sont correctement définies ?
- Comment les différentes demandes, y compris les demandes conflictuelles, sont-elles hiérarchisées ?
- La direction, les utilisateurs et les équipes informatiques sont-ils suffisamment impliqués dans la phase de spécification ?
- Comment les modifications apportées aux spécifications en cours de projet sont elles validées et contrôlées ?

3. *La conception de projet en interne/ mise en place de progiciel externe :*

Les développements internes et les logiciels externes doivent répondre aux besoins de l'entreprise. L'auditeur doit considérer, par exemple, les indicateurs suivants :

- Pour les développements internes, les membres de direction concernés, les utilisateurs et les informaticiens ont-ils été impliqués dans la définition des spécifications détaillées ou dans le prototypage du système ?
- Pour les progiciels externes, quel a été le processus de sélection du produit ? Le produit est-il largement répandu et reconnu sur le marché ?
- Quel est le processus de contrôle et de validation des modifications introduites en phase de conception détaillée ?
- Quelles procédures garantissent l'adéquation de l'application à la configuration des matériels et au système d'exploitation actuels ou envisagés ?
- Quelles procédures garantissent la prise en compte des contrôles applicatifs définis lors de la phase de conception (par exemple : les rapports d'exception)?
- Pour les progiciels, le paramétrage est-il contrôlé de manière appropriée ?
- La Direction effectue-t-elle des revues d'avancement du projet ?

4. *Les tests unitaires, les tests d'intégration et les tests utilisateurs :*

Les tests doivent permettre de vérifier que le système qui a été livré est conforme aux spécifications fonctionnelles et aux exigences de contrôle interne. L'auditeur doit observer, par exemple, les indicateurs suivants :

- Pour les développements internes, des tests appropriés ont-ils été menés par les équipes de développement et les utilisateurs de façon à détecter les erreurs de programmation ?
- Pour les progiciels externes, comment s'assure-t-on que les options d'installation retenues et les paramètres définis répondent aux besoins de l'activité et garantissent un niveau de contrôle suffisant ?
- Existe-t-il des procédures de tests par les équipes informatiques et par les utilisateurs permettant d'assurer le bon fonctionnement du nouveau système ?
- Comment s'assure-t-on que les modifications apportées après la période de tests sont elles-mêmes soumises aux procédures de tests ?
- Comment s'assure-t-on qu'aucun changement non autorisé n'est effectué entre la fin de la phase de tests et la mise en exploitation ?

5. *La migration des données :*

La migration des données doit garantir l'exactitude et l'exhaustivité du transfert des données issues de l'ancien système dans la nouvelle application et empêcher les changements non autorisés. Ainsi, et à titre d'exemple, les indicateurs suivants doivent être considérés :

- 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-t-il des procédures pour s'assurer que les données sont correctement vérifiées par les utilisateurs et les équipes informatiques ?

6. La mise en exploitation :

La décision de mise en exploitation doit être prise par la direction sur la base d'informations appropriées. L'auditeur doit examiner, par exemple, les points suivants :

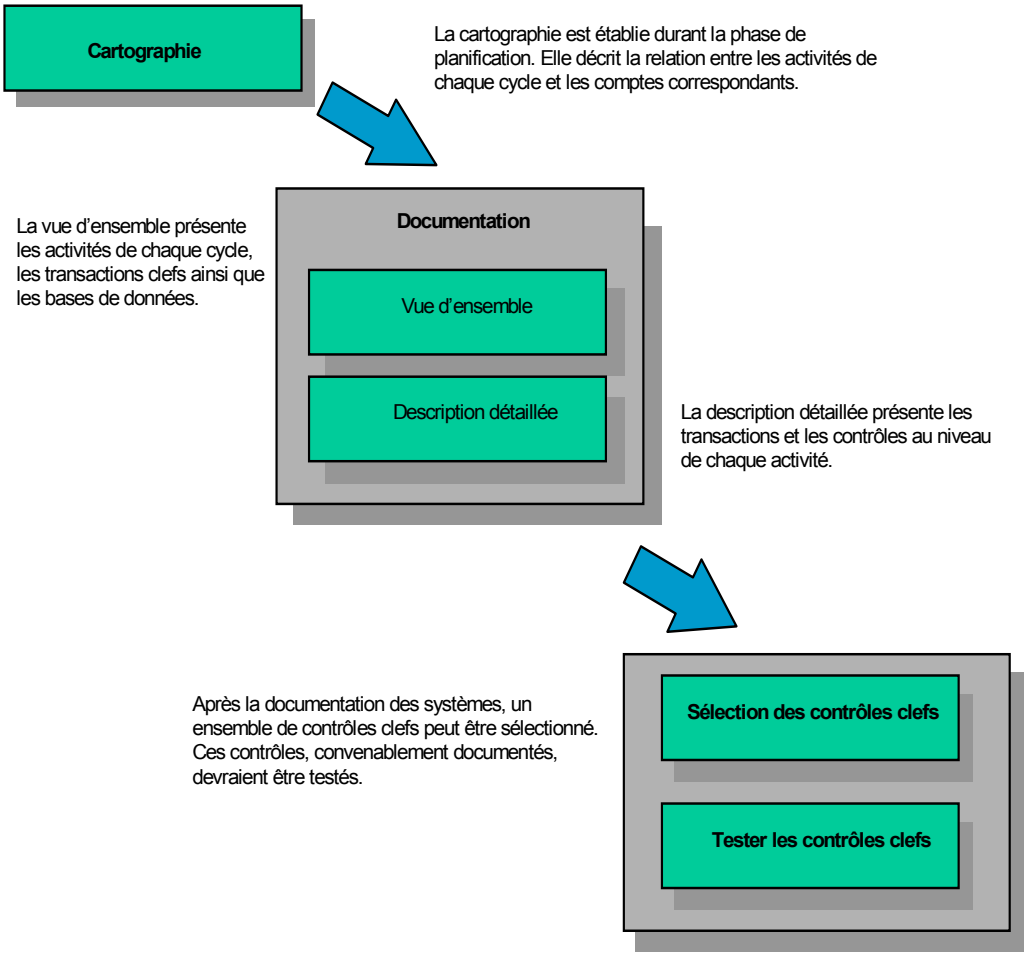
- Qui décide de la mise en exploitation ?
- Sur la base de quelles informations la décision de mise en exploitation est-elle prise ?
- Un planning de déploiement a-t-il été défini ?
- Existe-t-il des procédures permettant de s'assurer que seuls les programmes dûment testés, revus et approuvés sont transférés en environnement d'exploitation ?
- Lorsque les applications sont installées sur plusieurs sites, quelles procédures permettent d'assurer la correcte mise en place des nouveaux systèmes sur les différents sites ?
- Une revue post mise en exploitation est-elle prévue ?

7. La documentation et la formation :

Les utilisateurs doivent posséder les compétences nécessaires à une bonne utilisation du nouveau système. La documentation doit permettre de sous-tendre les opérations quotidiennes, la réduction des problèmes et la maintenance du système. Ainsi, les éléments suivants devraient être examinés :

- Les utilisateurs sont-ils suffisamment et correctement formés ?
- La documentation utilisateur est-elle adaptée ?
- La documentation utilisateur est-elle disponible dès la mise en exploitation de l'application ?
- La documentation technique permet-elle de fournir un support adéquat aux équipes chargées de la maintenance de l'application ?

Section 3 : L'examen des contrôles d'application



L'audit informatique n'est pas censé examiner tous les contrôles d'application. Son champ d'action est déterminé en commun accord avec l'équipe d'audit financier. Toutefois, dans la majorité des cas, l'équipe d'audit informatique sera chargée de l'audit des contrôles d'applications programmés et des suivis manuels rattachés.

L'examen des contrôles d'application se divise en trois étapes détaillées dans le schéma qui suit :

- La documentation des transactions et des process
- L'identification des contrôles clefs d'application
- Les tests portant sur les contrôles d'application clefs

Sous section 1 : La documentation des transactions et des process

La documentation des transactions et des process constitue une étape préalable pour l'examen des contrôles d'application (et aussi des contrôles de direction). Elle doit permettre aux lecteurs de comprendre de manière claire et sans ambiguïté le processus revu et aux auditeurs d'identifier les contrôles clés ainsi que les zones de risques.

Pour réaliser cette documentation, et en plus des interviews avec les différents responsables de l'entreprise, l'auditeur peut examiner les dossiers de correspondance, les statistiques clefs, l'organigramme, les rapports d'audit interne, les rapports de consultant, les manuels de procédures et les anciens rapports d'audit externes y compris les anciens commentaires de la direction.

La documentation doit indiquer :

- Les entrées, leur forme (papier, écran, support magnétique...), leur origine (utilisateur ou autre application en amont), les modes d'autorisation, les contrôles de validité faits par les utilisateurs et les contrôles automatisés ;
- Les fichiers : il s'agit des fichiers qui sont utilisés ou mis à jour par l'application. En général, il n'est pas tenu compte des fichiers intermédiaires mais seulement des fichiers principaux. Pour chacun, il y a lieu de connaître son contenu, son utilisation et les contrôles qui assurent son intégrité.
- Les traitements : il s'agit de recenser les principales fonctions et leur fréquence et d'identifier les procédures de contrôles informatisées et manuels
- Les sorties, leur forme (états, fichiers magnétiques...), leur contenu, les contrôles exercés notamment sur le chemin de révision.

La nature et l'étendue de la documentation propre à chaque cas dépendent de nombreux facteurs parmi lesquels :

- Le degré de fiabilité que l'auditeur pense accorder aux contrôles et aux fonctions de traitement informatisées
- Le risque propre à chaque composant et son importance relative
- L'existence ou non de documentations préparées par l'entreprise sur les systèmes
- La complexité des systèmes : s'ils sont particulièrement compliqués, une documentation détaillée, comprenant également des organigrammes, sera de circonstance
- Le degré d'utilisation et de sophistication du système informatique
- La nature de l'activité : dans certains industries spécialisées, les contrôles utilisés sont souvent spécifiques et les questionnaires généraux peuvent être mal adaptés.

Par ailleurs, la documentation peut revêtir de nombreuses formes dont les plus communes sont :

- Les organigrammes ou diagrammes de flux (Flowchart)
- Des descriptions sous forme narrative
- Des questionnaires spécialement adaptés

Aujourd'hui, la technique de documentation la plus utilisée est le « flowcharting » du fait que les auditeurs la trouvent de plus en plus efficace de part sa simplicité. Plusieurs logiciels informatiques se sont développés aidant non seulement à l'élaboration de flowcharts mais aussi à l'identification des contrôles clés potentiels.

Le flowcharting est une technique de description de procédures qui se base essentiellement sur des formes géométriques généralement standardisées (accompagnés le plus souvent par des notes écrites).

Il existe plusieurs techniques de flowcharting, dont les principales sont :

1. La technique horizontale : Dans ce cas, le flux des transactions est présenté de gauche à droite sur chaque page.
2. La technique horizontale par organisation : Le flux des informations est, dans ce cas, présenté de gauche à droite par sous unités organisationnelles. Pour chaque sous unité organisationnelle, les procédures ou les opérations s'y rattachant sont présentées verticalement. Le flowchart serait présenté du côté haut gauche au côté bas droit de la page.
3. La technique de présentation verticale : Dans ce cas, le flux des transactions est présenté de haut en bas selon une simple ligne, présentant les opérations séquentielles affectant chaque transaction avec les documents et les fichiers nécessaires à chaque opération.

C'est cette dernière technique qui semble la plus utilisée par les auditeurs. En outre, et lors de la préparation des flowcharts, il conviendrait de suivre les règles suivantes :

- Présenter le flux principal des activités et des contrôles sur une ligne verticale au milieu du diagramme
- Du côté gauche du flowchart, il convient d'ajouter les principales entrées (input) : documents, fichiers informatiques, etc.

- Du côté droit du flowchart, il convient d'ajouter les principales sorties (output) : documents, fichiers informatiques, etc.
- La séquence des activités devrait courir du haut en bas
- Chacun des flowcharts devrait être présenté sur une seule page. Si la présentation excède la page, alors il serait pertinent de regrouper les activités en processus plus élevés, pour pouvoir les détailler par la suite.

En outre, le flowchart doit pouvoir être lu à plusieurs niveaux :

- Vue d'ensemble : Elle permet d'avoir une vue globale de chaque cycle montrant les activités principales, les transactions les plus importantes, les bases de données utilisées et mises à jour et les principales entrées et sorties des différentes activités.

  La vue d'ensemble devrait contenir les éléments suivants :

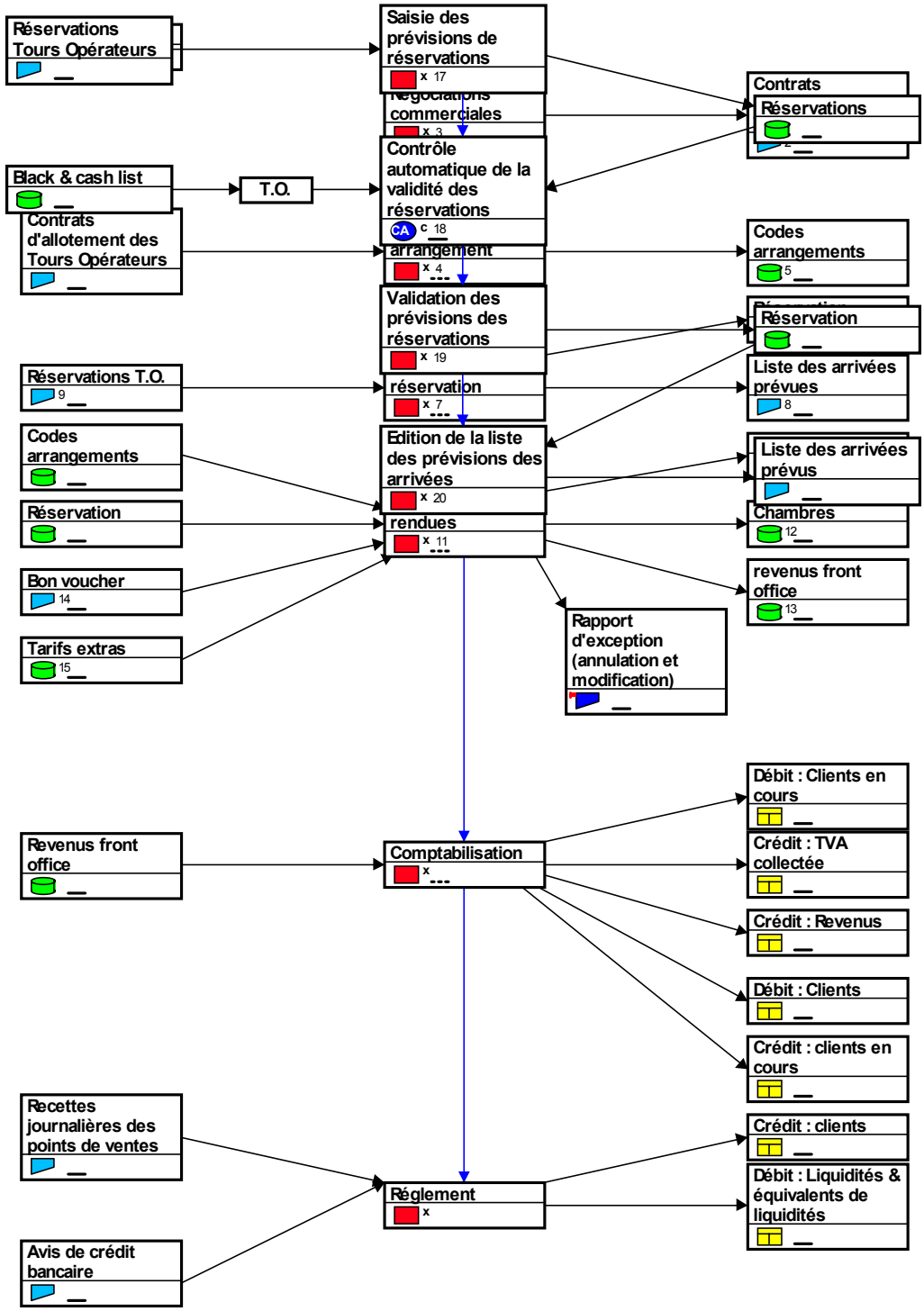
  - Tous les documents saisis dans le système
  - Les principales étapes de traitement et les principales activités
  - Les documents et les fichiers informatiques utilisés par plus que d'un process
  - Les comptes mouvementés suite à l'enregistrement des opérations
  - Eventuellement, la taille et le volume des transactions ainsi que les soldes des comptes correspondants (Cette information est utile pour l'évaluation de l'impact des faiblesses de contrôle interne soulevées)
  - Un sommaire des rapports produits par le système informatique. Ces rapports sont de deux types : les rapports de routine[68] et les rapports d'exception[69].
- Vue détaillée : Une fois le flowchart décrivant la vue d'ensemble a été achevé, la prochaine étape consisterait à fournir de plus amples détails et ce, en préparant des flowcharts pour chacune des activités principales.

[68] Les rapports de routine sont afférents aux transactions normales
[69] Les rapports d'exception (Audit log) concernent les transactions ou les opérations ne correspondant pas à une opération ou à une situation courante (exemple : stock négatif, marge inhabituelle etc.)

Exemple de flowcharts[70] du cycle revenus/clients d'une entreprise hôtelière :

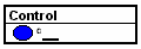
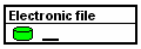
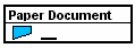
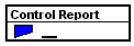
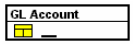
Vue d'ensemble :

Vue détaillée (prévisions de réservation) :



[70] Ces flowcharts ont été réalisés à l'aide d'un software d'aide à la documentation propre au cabinet international PricewaterhouseCoopers.

La signification de chaque symbole utilisé est :

Explications	Symboles
Activités : (Les activités peuvent être manuelles, automatisées ou mixtes).	
Contrôle	
Fichier électronique	
Documents Papier	
Rapport de contrôle	
Comptes comptables	
Eléments de données	

N.B : Les chiffres à l'intérieur des symboles font référence à des annotations explicatives et à des informations utiles au lecteur (volume des opérations, leurs montants, etc.).

Généralement, après la préparation ou la mise à jour de la documentation des systèmes, l'auditeur doit confirmer sa compréhension des procédures à travers la réalisation de tests de cheminement. Cependant, il peut être plus efficace de réaliser ces tests et de préparer la documentation correspondante en même temps.

Les tests de cheminement doivent porter aussi bien sur les procédures manuelles que sur les procédures automatisées. Dans la pratique, concernant les procédures automatisées, les problèmes suivants peuvent être rencontrés :

- Les transactions sont parfois groupées en batchs avant leur traitement par l'ordinateur. Habituellement, un résumé des procédures appliquées au groupe est rapporté sans que des évidences du traitement de chaque transaction individuelle ne soient documentées.
- Les procédures programmées peuvent consister en un ou plusieurs programmes complexes et englober une multitude de fichiers informatiques.

Parmi les types de tests de cheminement concernant les procédures automatisées, nous citons :

- La répétition des procédures automatisées : Cette méthode n'est possible que dans les systèmes informatiques simples où toutes les informations nécessaires pour la répétition du traitement sont disponibles.
- La revue de la documentation des programmes : Si la documentation est suffisante et correspond à la version de l'application utilisée, l'auditeur peut la revoir afin de confirmer sa compréhension des procédures automatisées
- La revue limitée du code source : Ceci peut être appliquée si la documentation existante ne décrit pas convenablement les procédures automatisées, si elle est incomplète ou non à jour et si elle ne peut être utilisée dans la confirmation de la compréhension des procédures.

Sous section 2 : L'identification des contrôles d'application clefs

Un contrôle clé est un contrôle qui permet de couvrir un ou plusieurs objectifs de contrôles et qui peut en même temps être testé d'une façon efficiente.

Pour chaque cycle donné, les contrôles clés sont toutes combinaisons de contrôles de direction et de contrôles d'application. Pour des raisons d'efficacité, leur identification se fait en collaboration avec l'équipe d'audit financier.

L'identification des contrôles clés se fait généralement en utilisant l'information obtenue durant la documentation de chaque cycle ou processus. En effet, durant cette phase plusieurs contrôles

auraient été découverts. Le travail le plus difficile serait de procéder à l'évaluation de chaque contrôle pour être en mesure d'identifier uniquement les contrôles clés.

Ceci fait appel au jugement de l'auditeur, qui examine :

- Quels sont les contrôles qui seuls ou combinés permettent de couvrir les risques inhérents au composant et donc, de fonder la conviction de l'auditeur au sujet des assertions de base ;
- L'impact de l'environnement dans lequel s'exerce le contrôle interne ;
- L'impact des contrôles généraux informatiques ;
- L'avantage retiré de l'utilisation du contrôle comme source de conviction.

Exemples de contrôles d'application automatisés clefs :

Parmi les contrôles d'application automatisés se rapportant au cycle revenu et pouvant être jugés clefs, nous citons à titre indicatif :

- Le système refuse au moment de la validation ou pendant l'exécution des traitements, les données ayant des numéros redondants.
- L'application permet l'édition de rapports d'exception, qui font l'objet d'un suivi manuel approprié, tels que :
  - Etat des avoirs et des annulations de revenus
  - Etat des bons de livraison annulés
  - Etat des modifications apportées aux fichiers des données permanentes (prix, remise, plafond de crédit, régime fiscal, etc.)
  - Etat des marchandises livrées et non facturées
  - Etat des factures éditées dont les marchandises correspondantes n'ont pas encore été livrées
  - Etat des marchandises retournées n'ayant pas encore fait l'objet d'un avoir.
- Contrôles par rapprochement avec d'autres données stockées sur fichiers : Exemple : l'enregistrement comptable d'une facture n'est possible qu'à la condition préalable de l'existence d'un bon de livraison correspondant dans le fichier des livraisons ;
- L'annulation des bons de livraison est protégée par un mot de passe et limité à un seul responsable.
- Contrôle par encodage/décodage permettant de protéger la réalité du transfert des données par télécommunication

Sous section 3 : Les tests portant sur les contrôles d'application clefs

La mission d'audit informatique est généralement chargée de la réalisation des tests portant sur les contrôles clefs d'application automatisés et les suivis manuels correspondants.

Les tests ont pour objet de s'assurer que les contrôles fonctionnent réellement et d'une façon permanente.

Plusieurs techniques sont plus spécifiques à l'informatique. Nous citons, à titre d'exemple :

- Les techniques des jeux d'essai : L'auditeur saisie des données dans le système et vérifie le fonctionnement des procédures de contrôle. Ce test suppose l'accord préalable de l'entreprise et, pour être efficace, doit être répété périodiquement tout au long de l'exercice comptable.
- Examen à posteriori des listes d'anomalies produites par le système : La mise en œuvre de ce type de tests permet de s'assurer que les contrôles programmés fonctionnent comme décrits dans la documentation et sont périodiquement analysés. La fiabilité de cet examen dépend largement de l'appréciation des contrôles généraux informatiques.

- Examen des programmes sources où sont codés les contrôles : La mise en œuvre de ce type de test rencontre plusieurs difficultés dont par exemple la nécessité pour l'auditeur d'avoir une expertise très approfondie des techniques de programmation.

Signalons à ce niveau que l'examen des contrôles d'application automatisés exige, généralement, de la part de l'auditeur l'utilisation des techniques d'audit assistées par ordinateur (TAAO) non seulement pour des besoins d'efficience mais aussi pour des besoins d'efficacité.

Si une faiblesse a été relevée lors de l'examen des contrôles d'application, les étapes suivantes devraient être observées :

- Déterminer s'il existe une autre combinaison de contrôles (de direction et d'application) qui constitue des contrôles compensatoires
- Déterminer s'il y a lieu de tester ces nouveaux contrôles
- Déterminer si les faiblesses de contrôle devraient être communiquées à la direction de l'entreprise

Tout objectif de contrôle non observé et touchant un cycle significatif aura un impact potentiel sur l'existence d'erreurs significatives au niveau des états financiers.

En outre, l'auditeur doit vérifier que le logiciel ou le module comptable (en cas d'ERP) :

- Permet l'attribution de mots de passe à chaque utilisateur les limitant à certains travaux ;
- Effectue certains contrôles tels que, par exemple, l'existence des numéros de comptes saisis, l'égalité des mouvements débit et crédit, la vraisemblance des dates saisies ;
- Autorise la validation des écritures seulement en l'absence d'anomalies ;
- Laisse la trace des annulations et des suppressions des écritures ;
- Interdit la suppression d'un compte mouvementé sur l'exercice (même soldé) ;
- Ne permet pas la modification d'un numéro de compte,
- N'autorise aucune création de comptes ayant des numéros identiques ;
- Lors du traitement de clôture, édite les états financiers et les états spécifiques (balance de clôture, etc.), archive les écritures clôturées, sauvegarde les fichiers, remet des comptes de produits et charges à zéro et inscrit le résultat dans le compte approprié ;
- Après clôture, interdit la passation d'écritures sur l'exercice clôturé ou la réouverture d'un exercice clos.

Section 4 : La phase de finalisation

Cette phase représente l'analyse des résultats des tests sur les contrôles d'application et des tests sur les contrôles généraux informatiques clefs.

Si des faiblesses ont été notées, l'auditeur doit considérer :

- Les types d'erreurs qui pourraient se produire dues à chacune des faiblesses
- Si l'erreur pourrait avoir un effet significatif sur la fiabilité des états financiers
- Si la faiblesse est en rapport avec les contrôles généraux informatiques, s'il existe des contrôles d'application compensatoires

Par ailleurs, s'il est établit que les contrôles et les fonctions de traitement informatisées sont inefficaces à un moment donné, il est probable qu'un certain nombre de transactions seraient affectées.

En outre, concernant les contrôles clefs manuels (y compris ceux associés aux contrôles d'application automatisés), l'auditeur ne doit pas s'attendre à ce qu'ils soient toujours efficaces. L'auditeur doit évaluer les déviations détectées au cours des tests de conformité et déterminer si le taux effectif de déviation et inférieur au taux de déviation admissible déterminé durant la phase de planification.

Suite à l'analyse des résultats, l'auditeur doit considérer si les procédures d'audit planifiées donneront une assurance suffisante pour déterminer si la faiblesse dégagée pourrait résulter, ou a résulté, en une erreur significative dans les états financiers. Dans certains cas, il peut juger nécessaire de concevoir une procédure d'audit spécifique. Si par suite de ce processus, l'auditeur détermine que les objectifs de contrôle demeurent assurés, il doit considérer d'informer l'entreprise de la faiblesse concernée.

Dans ce qui suit, nous présentons des exemples de faiblesses pouvant être relevées ainsi que les risques correspondants :

1/ Organisation :

Faiblesses	Risques
Absence de séparation des tâches entre les départements des études informatiques et de l'exploitation.	Accès direct des développeurs à l'environnement de production et modification des données avec des outils de développement
Absence de responsable de la sécurité informatique (physique, logique, plan de secours)	Stratégie de sécurité de l'entreprise non adaptée aux besoins de la société et entraînant des failles importantes dans le dispositif de sécurité

2/ Développement et maintenance des systèmes :

Faiblesses	Risques
Absence de méthodologie de conception ou d'acquisition de systèmes	Prise en compte incorrecte des besoins des utilisateurs, lenteur des développements, qualité insuffisante de la documentation rendant difficile la pérennité des systèmes
Absence de procédures de demande de changement	Des changements de programmes non autorisés peuvent causer des erreurs au niveau des états financiers
Absence de méthodologie de tests	Tests insuffisants entraînant des anomalies en production.
Test dans l'environnement de production	Des données de test peuvent être prises en compte dans les états financiers

3/ Exploitation :

Faiblesses	Risques
Absence de revue des travaux d'exploitation	Anomalies d'exploitation non détectées et donc non corrigées et pouvant porter atteinte à l'intégrité des données de l'entreprise
Absence de Plan de Continuité d'Exploitation	Arrêt des activités critiques de l'entreprise en cas de sinistre informatique important
Des procédures de sauvegarde et de restauration inadéquates	Risque de pertes de données et incapacité de restaurer les systèmes et/ou leurs données. Le coût de restaurer les données peut être élevé.

4/ La sécurité physique et logique :

Faiblesses	Risques
Sécurité insuffisante : Absence de contrôles logiques et physiques sur les accès (Exemple : absence de Firewall contrôlant l'accès des tierces personnes via Internet)	Des mises à jour non autorisées des bases de données, une mauvaise utilisation ou une destruction des données, la perte de la confidentialité, etc. Intrusion de personnes étrangères (surtout dans le cas d'EDI, d'E-commerce, E-business, etc.)
Absence de revue régulière des profils utilisateurs et de leurs habilitations	Utilisation de profils "dormants" pour entreprendre des opérations frauduleuses (saisie de données, diffusion d'informations confidentielles, etc.)
Documentation inadéquate	Dépendance sur une personne clef. Les changements du système peuvent être difficiles, chers ou impossibles.

5/ Interfaces :

Faiblesses	Risques
Sécurité absente ou insuffisante des interfaces	Altération des données
Vérification insuffisante des données reçues par rapport aux données envoyées (exemple : entre le site Web et le back-office)	Les données financières peuvent être perdues ou altérées lors du transfert.

6/ Séparation des tâches :

Faiblesses	Risques
Le personnel informatique peut avoir accès à des transactions utilisateurs	Les utilisateurs et le personnel de support informatique peuvent créer des fournisseurs et des clients, créer des bons de commande, recevoir des biens, entrer des données en comptabilité générale, effectuer des paiements, etc. (risque de fraude, de divulgation d'informations confidentielles, etc.…) De telles possibilités affectent la crédibilité des données financières.
Des utilisateurs peuvent avoir accès à des fonctions élevées d'administration du système	
Les utilisateurs et le personnel informatique ont des tâches incompatibles avec leurs fonctions.	
Des droits étendus ou inappropriés peuvent être donnés à des personnes non autorisées Un manque de standard dans la dénomination des profils	Certains profils peuvent être utilisés pour valider des transactions non autorisées. Certains profils peuvent permettre d'effectuer la quasi-intégralité des fonctions, sans nécessairement respecter la séparation des tâches.

7/ Contrôles d'application :

Faiblesses	Risques
Les personnes chargées de la validation peuvent avoir accès à la maintenance des tables.	Les employés ayant les autorisations pour maintenir les tables peuvent outrepasser les limites d'approbation.
Insuffisance des contrôles programmés lors de la saisie de données	Erreurs sur les montants saisis, enregistrement dans une mauvaise période, imputation incorrecte
Absence de procédures automatiques de réconciliation entre une facture fournisseur et un bon de commande	Enregistrement de facture non réelle, double enregistrement de facture
Le système est configuré pour n'afficher qu'un message d'alerte quand un paiement est saisi deux fois dans le système.	Les factures peuvent être payées plusieurs fois si le contrôle n'est pas bloquant.
Absence de procédure de revue du listing des règlements	Enregistrement d'opérations de règlements non autorisées
Les factures, chèques et journaux peuvent être entrées dans le système pour toutes les périodes ouvertes.	Les écritures sont saisies sur les mauvaises périodes comptables générant des problèmes de cut-off.

Ces faiblesses et leurs impacts sur la stratégie d'audit font l'objet d'un compte rendu à l'attention de l'équipe d'audit financier. En outre, un rapport de contrôle interne peut aussi être adressé à l'attention de la Direction Générale.

Sous section 1 : Le compte rendu à l'attention de l'équipe d'audit

Après l'achèvement de ses travaux, l'auditeur informatique doit élaborer un compte rendu à l'attention de l'équipe d'audit financier. Ce compte rendu doit indiquer clairement :

1. Les objectifs et les limites de l'intervention :

Le compte rendu rappelle les objectifs et les limites de la mission d'audit informatique engagée dans le cadre de l'audit financier ainsi que les conditions d'exécution.

2. Les travaux effectués :

Il s'agit de décrire les étapes, l'étendue (système d'information, applications, etc.), les cycles et les comptes comptables couverts par l'audit informatique. Il y a lieu de rappeler que les cycles et les comptes comptables à auditer sont déterminés lors de la phase de la collecte d'informations sur les systèmes et l'environnement informatique en commun accord avec l'équipe d'audit financier.

En outre, l'auditeur doit indiquer, éventuellement, les limitations de l'étendue de ses travaux imposées par l'entreprise auditée.

3. Les principaux points et les conclusions :

Il s'agit de décrire les points susceptibles de modifier la stratégie d'audit, les faiblesses de contrôle, le niveau de risque, et les points à reporter à la Direction de l'entreprise. Il convient de signaler que l'obtention des commentaires de la direction sur les points dégagés peut être utile à l'équipe de l'audit financier.

Par ailleurs, sur la base des travaux entrepris, l'auditeur doit évaluer les assertions sous-jacentes à chaque cycle et à chaque compte comptable.

L'auditeur doit aussi indiquer, à ce niveau, les cas relevés de non-respect par l'entreprise des dispositions informatiques prévues par la réglementation comptable, juridique et fiscale. Ceci est d'autant plus important en cas d'une mission de commissariat aux comptes où l'obligation de révélation des faits délictueux est entière.

4. L'impact sur l'audit :

Sur la base des faiblesses relevées et des risques induits, l'auditeur informatique recommande, à l'équipe d'audit financier, les tests de détails nécessaires à entreprendre, lors de l'audit final des comptes, pour valider les assertions non couvertes.

Sous section 2 : Le rapport sur les faiblesses de contrôle interne

L'auditeur informatique peut présenter à la Direction Générale de l'entreprise auditée un rapport de contrôle interne indiquant les insuffisances des procédures et des contrôles relevées au cours de l'audit. Ce rapport peut, aussi, indiquer les grandes lignes des moyens à mettre en œuvre avec l'ordre de priorité selon lequel chaque élément devrait être pris en considération et ce, pour ramener le risque à un niveau acceptable compte tenu des contraintes spécifiques à l'entreprise.

La structure du rapport de contrôle interne est critique pour une communication effective des résultats de l'audit. A titre indicatif, le rapport doit inclure les éléments suivants :

- L'étendue des travaux d'audit
- Les domaines ou les comptes examinés
- Une description sommaire de la méthodologie suivie
- L'opinion sur les systèmes objets de la revue
- Un sommaire des faits constatés
- La présentation détaillée des faits constatés
- Une présentation des recommandations, des actions à mener et l'ordre de priorité correspondant à chacune des recommandations et actions

Par ailleurs, l'auditeur informatique doit préciser que les situations décrites dans son rapport sont celles observées dans le cadre des travaux d'audit financier et, par conséquent, les commentaires ne comportent pas nécessairement une description de toutes les situations qui mériteraient une amélioration et qui auraient été mises en évidence par une étude plus spécifique et détaillée.

Sous section 3 : Le dossier de synthèse

Le dossier de synthèse afférent à l'intervention de l'audit informatique dans le cadre de l'audit financier peut contenir, essentiellement, les éléments suivants :

- La synthèse de fin de mission
- Les rapports et les comptes rendus émis
- Le plan stratégique et le programme de travail
- Les procès verbaux des réunions internes de l'équipe d'audit informatique
- Les procès verbaux des réunions avec l'équipe d'audit financier

- Les procès verbaux des réunions avec les différents responsables de l'entreprise auditée
- L'équipe intervenante, le budget, les temps consommés
- La cartographie
- La documentation des systèmes

Conclusion :

L'évolution croissante des technologies de l'information et de la communication élargit de plus en plus le champ et les domaines d'intervention de l'audit informatique en support à l'audit financier.

Par ailleurs, la démarche présentée, tout au long de ce chapitre, peut être appliquée dans le cadre d'une mission d'audit informatique indépendante non rattachée à une mission d'audit financier ou dans le cadre d'une mission d'audit interne informatique. Dans ces cas, le champ d'action est généralement plus élargi et la responsabilité et l'autorité de la mission doivent être définies de façon appropriée dans une lettre de mission ou une charte d'audit.

Aussi, est-il nécessaire de rappeler que l'auditeur informatique est tenu de respecter les règles d'éthique d'indépendance, d'intégrité, d'objectivité, de compétence professionnelle, de confidentialité, de professionnalisme et de respect des normes techniques et professionnelles.

L'auditeur informatique doit être indépendant de l'entité auditée en attitude et en apparence. Il doit aussi être suffisamment indépendant du domaine audité pour permettre une réalisation objective de l'audit.

Chapitre 3 : Les Principales Evolutions Prévisibles des Pratiques en la Matière en Tunisie

Introduction

Au niveau des chapitres précédents, nous avons identifié les principaux impacts des nouvelles technologies de l'information et de la communication sur le système comptable et les contrôles internes de l'entreprise ainsi que sur l'audit financier. Nous avons montré la nécessité de faire impliquer davantage l'audit informatique dans le processus d'audit financier.

Aussi, nous avons passé en revue la réglementation comptable, juridique et fiscale aussi bien en Tunisie qu'à l'étranger et les réactions des organismes professionnels destinées à réglementer et à contrôler certains aspects des systèmes informatisés.

A travers ces études, nous avons noté certains domaines d'évolutions nécessaires en Tunisie que nous allons détailler dans ce chapitre. Nous devons, toutefois, préciser que notre analyse sera focalisée uniquement sur les aspects se rattachant à la mission d'audit financier.

Nous couvrirons :

- L'évolution du cadre juridique et technique
- L'évolution de l'approche et des procédures d'audit
- La mise à niveau de la formation des auditeurs

Section 1 : L'évolution du cadre juridique et technique

En raison de la nature dynamique des technologies de l'information et de la communication, les cadres juridique et technique devraient être en état de mise à niveau continue.

En Tunisie, il y a un effort certain de réglementation de ces nouvelles technologies. Toutefois, il reste encore beaucoup à faire pour adapter le cadre juridique à toute nouvelle technologie.

«C'est une impérative obligation pour que le droit des affaires réponde aux besoins du commerce. L'informatique, c'est la mort du papier, et se trouve en conflit avec les traditions juridiques rigoureuses»[71].

Ainsi, certaines dispositions comptables, juridiques et fiscales devraient être actualisées ou prévues. Nous citons à titre d'exemple :

- Comptable : Faut-il abroger l'obligation de la tenue d'un livre journal et d'un livre d'inventaire coté et paraphé malgré que le procédé de la cote et du paraphe n'apporte pas de garantie réelle contre la falsification et ne s'adapte pas à la progression des technologies de l'information ?
- Juridique : Faut-il prévoir une réglementation plus spécifique de la fraude informatique ?
- Fiscale : L'administration fiscale tunisienne doit-elle autoriser, comme c'est le cas en France, la dématérialisation des factures et leur transmission par voie télématique ?

Par ailleurs, étant donné que les garanties de régularité de la comptabilité pourront s'appuyer sur le contrôle interne et des moyens informatiques appropriés[72], faut-il alors prévoir des dispositions légales préventives sur ces domaines ?

[71] Michel LESOURD, « Communication informatique : administration / entreprise », Revue Française de Comptabilité N°199, Mars 1989.

Exemple 1 : Exiger des entreprises informatisées, sous peine de sanctions financières importantes, d'avoir un programme effectif de prévention et de détection des violations de la loi (comme c'est le cas aux Etats Unis).

Exemple 2 : Imposer pour les entreprises appartenant à certains secteurs sensibles (exemple : le secteur bancaire et le secteur des assurances) un contrôle périodique de la sécurité de leur système d'information par un organe indépendant.

Parallèlement, il est certain que les nouveaux textes juridiques sur l'informatique créent pour l'entreprise des obligations nouvelles, dont le non-respect peut entraîner des sanctions pénales et/ou fiscales. L'auditeur, et plus particulièrement le commissaire aux comptes, doit tenir compte de ces dispositions dans le cadre de ses contrôles.

En effet, selon l'article 270 du nouveau code des sociétés commerciales, les commissaires aux comptes doivent signaler à l'assemblée générale les irrégularités et les inexactitudes relevées par eux au cours de l'accomplissement de leur mission. En outre, ils sont tenus de révéler au procureur de la république les faits délictueux dont ils ont eu connaissance.

Toutefois, certains aspects juridiques, tels que l'audit des contrats relatifs à l'informatique (achat de progiciel, contrat de travail avec les informaticiens, traitements à façon, etc.) n'entrent pas dans le champ de l'audit financier et peuvent être retenus dans le cadre d'un audit opérationnel réalisé par un auditeur interne ou externe.

Quant au cadre technique, la majorité des organismes professionnels ont procédé à la révision de leurs normes d'audit pour tenir compte des nouveaux aspects engendrés par les nouvelles technologies. En outre, une panoplie de réflexions a été publiée représentant des aides aussi bien pour le chef d'entreprise que par l'auditeur, dont par exemple : le référentiel COBIT (Control Objectives for Information and related Technology) mis en place par l'ISACA et qui répond à l'impératif de contrôle et de maîtrise de l'informatique.

Par ailleurs, de nouvelles normes comptables ont été élaborées par certains organismes professionnels pour définir les nouvelles règles de prise en compte et d'évaluation des opérations affectées par les nouvelles technologies de l'information et de la communication.

Par conséquent, il est nécessaire pour l'expert comptable tunisien de se familiariser davantage avec ces normes, réflexions et outils techniques. L'Ordre des Experts Comptable de Tunisie a un rôle important à jouer.

A l'instar des autres organismes professionnels, il doit mener régulièrement des réflexions sur les nouvelles technologies et ce, en :

- Formulant des avis, en diffusant des guides spécifiques de contrôle dans les entreprises informatisées (complémentaires à ceux de l'IFAC) et en apportant des réponses aux questions techniques posées par les professionnels ;
- Contribuant à la mise en place des actions de formation nécessaires et en organisant des manifestations sur le thème de l'informatique.

Sous section 1 : Les obligations et les responsabilités de l'entreprise

Les obligations et les responsabilités de l'entreprise les plus essentielles, actuelles et futures au vu de l'évolution prévisible du cadre juridique et technique, peuvent se résumer comme suit :

1. Le respect de la réglementation en vigueur :

Il est évident que l'entreprise doit veiller au respect de la réglementation en vigueur[73]. En effet, les sanctions peuvent parfois être lourdes et peuvent, même, engager la responsabilité pénale des dirigeants (surtout en cas de faillite).

En pratique, nous constatons, souvent, les faits suivants :

---

[72] En l'absence de preuve écrite préconstituée, ce sont des indices qui permettront d'emporter la conviction du juge. Exemple : Une bonne sécurité informatique

[73] Pour de plus amples détails sur la réglementation comptable, juridique et fiscale, se référer au chapitre III de la première partie.

- Le livre journal et le livre d'inventaire ne sont pas tenus ou ne sont pas à jour ;
- Absence d'une documentation à jour et absence de traçabilité de l'exploitation, des développements et des maintenances : Le chef d'entreprise et le responsable informatique doivent prendre au sérieux cette obligation ;
- Piratage de logiciels : Le parc informatique n'est pas vérifié régulièrement par les dirigeants des entreprises. Chaque utilisateur devrait être responsabilisé que l'installation de copies pirates est constitutive de faute grave.
- L'application ou le module comptable utilisé n'offre pas toutes les exigences de sécurité et/ou ne respecte pas les dispositions légales. Exemple : l'application ou le module comptable :
    1. Ne permet pas l'attribution de mots de passe à chaque utilisateur les limitant à certains travaux,
    2. Ne laisse pas une trace des annulations et des suppressions des écritures,
    3. N'interdit pas la suppression d'un compte mouvementé sur l'exercice (même soldé),
    4. Après clôture, n'interdit pas la passation d'écritures sur l'exercice clôturé ou la réouverture d'un exercice clos.

2. La mise en place et le maintien d'un système de contrôle interne adéquat :

La Direction Générale d'une entreprise est chargée de mettre en place et de maintenir un système comptable et un système de contrôle interne assurant la fiabilité des états financiers et la prévention et la détection de la fraude.

Il est de la responsabilité des dirigeants des entreprises de mettre en place et d'assurer le suivi de certaines règles dont les principales sont :

- Des responsabilités clairement définies et une séparation convenable des tâches : Ceci touche aussi bien le personnel informatique que les différents utilisateurs. Les sécurités d'accès logiques devraient être paramètrées en conséquence.
- Des contrôles généraux informatiques suffisants et appropriés : sécurité physique, sauvegarde, gestion du changement, etc.
- Des contrôles directs (contrôles de direction, contrôles manuels et contrôles programmés) appropriés : Ces contrôles devraient être convenablement documentés et coordonnés pour assurer les objectifs de contrôle.

En outre, la définition des responsabilités de chacun des intervenants, concernés par le fonctionnement des applications (la Direction Générale, les utilisateurs et les informaticiens), est essentielle. A titre indicatif :

- Les utilisateurs, qui ne s'impliquent pas lors des modifications de programmes en définissant les fonctions et les contrôles nécessaires et en exécutant les tests nécessaires et appropriés avant la mise en production de ces modifications, engagent leur responsabilité en cas d'anomalie de fonctionnement.
- Les informaticiens qui ne documentent pas leur système ou ne forment pas les utilisateurs sont responsables de la mauvaise utilisation d'une application.
- La Direction générale qui n'anime pas les relations entre les utilisateurs et les informaticiens et délègue toutes les décisions est responsable des dépassements de budget et de temps, voire des échecs liés à des orientations inappropriées.

La mise en place des directives efficaces et des contrôles adéquats s'intègre dans une approche globale de gestion des risques. Pour cela, la Direction Générale a besoin d'avoir une appréciation et une compréhension de base des risques et contraintes liés aux technologies de l'information et de la communication. Elle doit procéder à des arbitrages constants entre le coût de la mise en œuvre d'une décision et les avantages attendus ou le risque qu'elle est disposée à accepter.

Pour réduire les risques à un niveau acceptable, la Direction peut s'appuyer sur des outils techniques reconnus et éprouvés. Parmi ces outils, nous citons le référentiel COBIT (Control Objectives for Information and related Technology)

Quelle est la situation dans la pratique ?

Beaucoup d'entreprises présentent des insuffisances importantes au niveau de la sécurité informatique et ce, malgré la conscience des chefs d'entreprise de son importance en tant que moyen permettant de garantir la protection des personnes et du patrimoine sans nuire au bon fonctionnement de l'entreprise. En effet, la sécurité informatique est encore fragmentée et vécue comme une contrainte technique, au lieu d'être intégrée dans la stratégie de l'entreprise.

C'est aux chefs d'entreprise de veiller à ce que les principes généraux de sécurité soient respectés et mis en œuvre quels que soient les environnements, les implantations géographiques, la taille des équipements informatiques, les applications, les types de matériels, etc. Tout le personnel de l'entreprise, utilisateurs, administrateurs ou dirigeants, doit être concerné par la sécurité, car une seule personne qui n'applique pas les mesures de protection peut fragiliser tout le système, d'où l'importance d'instaurer une culture de sécurité au sein de l'entreprise.

En outre, la sécurité doit être liée de façon étroite et permanente à la dynamique d'évolution de l'architecture de l'entreprise et de son système d'information, car la nature et l'importance des risques évoluent sans cesse, notamment du fait du développement des nouvelles technologies et de la révolution Internet.

Exemple : Dans un environnement d'E-commerce, toute personne cherchera à obtenir l'assurance que l'entreprise, avec laquelle elle compte réaliser une transaction quelconque, a mis en place des contrôles efficaces pour assurer l'intégrité des opérations.

Quatre piliers sont nécessaires à l'élaboration et à la mise en place réussies d'un programme de sécurisation de l'entreprise :

- Une stratégie et une vision de la sécurité (l'état d'esprit) : La direction générale se doit d'avoir une démarche proactive en matière de stratégie sécuritaire intégrée dans la stratégie globale de l'entreprise.
- Un engagement de la Direction Générale (la volonté) : Passer d'une sécurité vécue comme une contrainte à une sécurité pleinement intégrée à la stratégie de l'entreprise ne demande qu'une volonté de la direction. Mais, la mise en œuvre de cette volonté dans une architecture opérationnelle nécessite un engagement constant et durable de la part des dirigeants et un investissement en temps, compétences et moyens financiers à la hauteur de cette vision.
- Une structure de la direction sécurité de l'information (l'organisation) : Le rôle de cette direction consiste non seulement à développer, mettre en place et maintenir la sécurité de l'information, mais aussi à accompagner les objectifs économiques de l'entreprise tout en gérant les risques.
- Une formation et une veille technologique permanentes (le savoir) : Les employés sont des éléments clés dans un programme global de sécurité de l'information. Il faut donc régulièrement les tenir informés des évolutions de la politique de sécurité. Le message essentiel à leur faire passer est que la Direction se préoccupe de la sécurité et par conséquent, tous les employés de la société sont concernés.

3. Faire recours à l'audit informatique (interne ou externe) :

La pratique de l'audit informatique est encore très insuffisamment développée dans nos entreprises tunisiennes. Il doit être intégré, principalement, dans les moyennes et les grandes entreprises, dans un schéma directeur de la sécurité informatique.

L'audit informatique peut être réalisé par le service d'audit interne de l'entreprise. Auquel cas, le personnel dudit service doit avoir les compétences et les connaissances nécessaires en la matière et doit être indépendant du volet audité. L'audit informatique peut aussi être réalisé en faisant recours à des cabinets externes spécialisés.

Sous section 2 : Les diligences et les responsabilités de l'auditeur

Nous avons déjà étudié les nouvelles diligences de l'auditeur financier dans un environnement de nouvelles technologies de l'information et de la communication. Il en découle que l'auditeur doit faire évoluer son approche et ses procédures d'audit pour couvrir les nouveaux aspects. Il lui est aussi

nécessaire d'avoir une formation informatique appropriée. Ces deux aspects font l'objet d'une étude plus détaillée dans les sections qui suivent.

En outre, dans un milieu de nouvelles technologies, les obligations incombant à l'auditeur mettent en jeu sa responsabilité professionnelle dans un cadre différent de celui des autres missions traditionnelles. La responsabilité de l'auditeur peut être mise en cause pour les raisons suivantes :

- La non mise en œuvre des diligences minimales d'audit : l'auditeur n'a vis-à-vis de son client qu'une obligation de moyens. Il doit justifier qu'il a mis en œuvre les connaissances suffisantes en informatique et les principes généraux d'organisation et de contrôle interne. L'analyse des diligences appliquées mettrait en évidence l'insuffisance des travaux et justifierait la poursuite du professionnel au titre de son obligation de moyens.
- L'incompétence de l'auditeur : Dans ce cas, l'obligation de moyens ne sera pas remplie, étant donné que la compétence du professionnel des aspects de la mission fait partie des moyens qu'un professionnel diligent met en œuvre avant l'acceptation de la mission.
- L'inexpérience de l'auditeur : l'auditeur peut être tenu pour responsable au cas où il n'a pas fait recours à des spécialistes. Toutefois, ses connaissances en informatique doivent être telles qu'il puisse comprendre et contrôler les travaux du spécialiste. En effet, il ne s'agit pas d'une délégation de responsabilité.
- Non révélation des faits délictueux informatiques : Dans le cadre d'une mission de commissariat aux comptes, l'auditeur est tenu de révéler au procureur les faits délictueux informatiques dont il a eu connaissance.

En France, l'OECCA oblige les auditeurs financiers de souscrire une assurance spécifique qui couvre les missions ou les aspects informatiques[74].

1. La révision de l'indépendance de l'auditeur :

L'auditeur ainsi que ses collaborateurs doivent respecter les règles d'indépendance vis-à-vis de l'entité auditée. Pour les auditeurs informatiques, l'indépendance doit s'étendre :

- aux membres du service informatique de l'entité auditée
- aux membres de l'équipe du projet de développement, d'acquisition, de mise en place ou de maintenance de logiciels (même ceux externes à l'entité)
- aux dirigeants du service bureau (en cas d'externalisation)

Au cas où l'auditeur a été impliqué avec la société, avant sa nomination en tant qu'auditeur, dans une revue de développement, d'acquisition, de mise en place ou de maintenance d'une application, son indépendance n'est pas mise en cause une fois le projet est mis en exploitation[75].

En outre, l'auditeur peut être amené à assister l'entreprise lors de la mise en place de son nouveau système d'information afin de s'assurer que les procédures et les contrôles nécessaires ont bien été prévus dés le départ. Toutefois, cette assistance ne devrait pas être rémunérée.

2. Les diligences particulières en cas de présentation électronique du rapport d'audit :

Avec le développement des nouvelles technologies de la communication, beaucoup d'entreprises veulent publier leur rapport d'activité ainsi que leurs états financiers audités accompagnés du rapport d'audit sur leur propre site Web et ce, afin d'assurer un accès plus élargi du public.

Ce nouvel aspect n'a pas été encore totalement réglementé. Certains organismes professionnels, dont l'« Australian Accounting Research Foundation »[76] ont traité ce volet[77]. Ce point sera très prochainement d'actualité en Tunisie.

---

[74] CNCC, « Le diagnostic des systèmes informatisés : Guide d'application des recommandations », Conseil supérieur de l'OECCA, page 22.

[75] Position de l'ISACA (Information System Audit and Control Association) dans sa directive d'audit des systèmes d'information « Organisational relationship and indépendance », septembre 2000.

[76] L'«Australian Accounting Research Foundation » a été fondé par l'«Australian Society of Certified Practicing Accountants » et l'« Institute of Chartered Accountants in Australia ».

[77] AGS (Auditing Guidance Statement) N°1050, « Audit issues relating to the electronic presentation of financial reports », publié le 1er décembre 1999.

En attendant, nous recommandons à l'auditeur financier de suivre ce qui suit[78] :

- La responsabilité incombe à la direction de l'entreprise pour veiller à la sécurité et à l'intégrité des informations publiées. L'examen des contrôles associés à la présentation électronique des états financiers audités dépasse l'étendue de la mission d'audit financier. Toutefois, l'auditeur doit veiller au respect par l'entreprise de règles appropriées assurant que le rapport d'audit ne soit pas associé à des informations non auditées.
- L'auditeur doit mentionner cette responsabilité de l'entreprise dans la lettre de mission. Il doit aussi y inclure que l'examen des contrôles associés à la présentation électronique dépasse l'étendue de sa mission.
- L'auditeur doit estimer si les mesures de sécurités et d'intégrité mises en place par l'entreprise sont satisfaisantes. S'il juge ces mesures non satisfaisantes, il doit refuser la publication de son rapport sur le site Web et de faire référence à l'information financière publiée comme étant une information auditée. Le recours à la justice doit être rendu possible si l'entreprise n'observe pas la décision de l'auditeur.
- L'auditeur doit veiller à l'obtention d'une lettre d'affirmation dans laquelle la Direction affirme que les versions électroniques présentées sont identiques à la version originale, qu'elle a mis en place les dispositions nécessaires pour différencier les informations auditées des informations non auditées et qu'elle a mis en place les moyens de sécurité et les contrôles nécessaires pour assurer la sécurité et l'intégrité des informations publiées.
- L'auditeur peut juger nécessaire d'élaborer un rapport d'audit spécial pour la présentation électronique mentionnant, entre autres, que c'est le rapport sur papier qui fait foi.

Enfin, il y a lieu de noter que ces recommandations sont loin d'être exhaustives. Nous avons, juste, voulu faire référence dans le présent mémoire mais le sujet est grand ouvert pour le débat et la recherche.

Section 2 : L'évolution de l'approche et des procédures d'audit

L'audit financier est appelé à évoluer afin de s'adapter aux besoins des entreprises et de leurs actionnaires. Cette évolution devrait être au rythme des technologies.

Dans un contexte caractérisé essentiellement par la dématérialisation des informations et l'automatisation des contrôles, l'auditeur aura de plus en plus de difficultés à forger son opinion sur les états financiers sans une approche approfondie du système informatique. D'où la nécessité d'application de l'audit informatique comme support à l'audit financier.

En outre, ce nouveau contexte contraint l'auditeur à développer et à mettre en application de nouveaux outils de révision dont, essentiellement, les techniques d'audit assistées par ordinateur.

Sous section 1 : L'application de l'audit informatique comme support à l'audit financier

Rappelons que les nouvelles technologies de l'information et de la communication entraînent une modification de l'organisation du contrôle interne. Cette organisation est basée sur des contrôles généraux informatiques et sur de plus en plus de contrôles programmés que de contrôles manuels.

Ainsi, l'audit informatique revêt, désormais, une place importante dans une mission d'audit financier[79].

En effet, l'application de l'audit informatique comme support à une mission d'audit financier est une sorte d'intégration de l'informatique dans la démarche de l'audit financier.

[78] Recommandations inspirées de l'AGS 1050 précité.

[79] C'est l'approche basée sur les contrôles qui est la plus adaptée et la plus efficace dans un environnement de nouvelles technologies. L'audit informatique comprend d'une part, l'examen de la fonction informatique et d'autre part, l'examen des contrôles d'applications automatisés et les contrôles manuels rattachés.

Toutefois, une sensibilisation des dirigeants, des cadres d'entreprises et des auditeurs sur les avantages supplémentaires procurés par l'audit informatique dans le processus de l'audit financier est nécessaire.

L'attention peut être focalisée sur les avantages suivants :

- Une meilleure maîtrise du coût de l'audit
- Même approche pour des systèmes similaires
- Une plus grande pertinence dans l'appréciation des risques de l'entreprise
- Davantage de recommandations ayant un impact opérationnel
- Produire une réelle valeur ajoutée reconnue de l'entreprise par l'identification des risques induits par les technologies de l'information

Chaque cabinet d'audit doit s'organiser comme il l'entend et doit définir les moyens qu'il juge nécessaires à mettre en place. Chacun doit être convaincu que l'application de l'audit informatique dans le processus de l'audit financier n'est ni un choix, ni un luxe mais une obligation.

Ainsi, chaque cabinet lui appartient de savoir s'il doit disposer d'équipes informatiques en interne ou s'il est préférable de faire appel à des équipes informatiques externes. Avec le développement constant des technologies de l'information et de la communication, la mise en place d'un service interne est recommandée. Le recours à des ressources externes peut être nécessaire si le sujet traité nécessite une expertise technique assez pointue.

Enfin, il convient de signaler qu'actuellement, certains cabinets recommandent l'application de l'audit informatique dans toute mission d'audit financier se rapportant à des sociétés opérant dans certains secteurs sensibles tels que les banques, les compagnies d'assurance, etc.

Sous section 2 : Le développement et la mise en application de nouveaux outils de révision

Dans un environnement de nouvelles technologies, la dématérialisation des informations et l'automatisation des contrôles nécessitent le développement et la mise en application de nouveaux outils de révision. Ces outils sont généralement des techniques d'audit assistées par ordinateur (TAAO).

1. Description des techniques d'audit assistées par ordinateur :

Les deux techniques d'audit assistées par ordinateur les plus répandues sont les logiciels d'audit et les jeux d'essai (ou données fictives de sondages).

1.1. Les logiciels d'audit :

C'est un programme spécial ou un ensemble de programmes désigné pour auditer des données conservées dans des fichiers informatiques. Il s'agit, essentiellement, des progiciels, des programmes spécifiques et des programmes utilitaires :

- Les progiciels : Ce sont des programmes d'application générale destinés à exécuter certaines fonctions de traitement des données
- Les programmes spécifiques : Ce sont des programmes préparés par l'auditeur, l'entité ou par un spécialiste informatique extérieur auquel l'auditeur a fait appel et spécifiques à l'entreprise concernée.
- Les programmes utilitaires : Ils permettent un traitement d'ordre général tel que l'extraction des données, le tri etc.

Les principaux avantages de l'utilisation des logiciels d'audit sont les suivants :

- Les résultats des tests sont plus concluants étant donné que toutes les données dans le fichier sont examinées et non uniquement un échantillon
- La répétition peut être plus étendue, plus simple et efficace étant donné que tous les calculs et les autres procédures seront réalisés par l'application

- La capacité d'identifier les données répondant à une ou plusieurs conditions particulières est améliorée
- La réalisation des procédures d'échantillonnage, que ce soit statistiques ou non statistiques, est plus rentable
- Le budget temps de la mission peut être affecté à l'examen des éléments identifiés comme nécessitants une attention particulière
- Une fois le logiciel d'audit est mis en place, les coûts d'exécution subséquents sont raisonnables et les gains de temps sont souvent considérables. En effet, le même programme peut être utilisé pour chaque audit sauf changement majeur dans le système.

Exemples de logiciels d'audit pour tester des contrôles d'intégrité :

- Des logiciels qui analysent les programmes d'exploitation de l'entreprise et les comparent avec des copies conservées. Ces logiciels permettront à l'auditeur de s'assurer que les modifications autorisées ont été correctement effectuées et qu'aucune modification non autorisée n'est intervenue.
- Des logiciels qui interrogent les bibliothèques contenant les programmes exécutables et éditent des informations qui permettent à l'auditeur d'identifier les modifications apportées.

1.2. Les jeux d'essai :

Les jeux d'essai consistent à introduire des données dans le système informatique et de comparer les résultats obtenus avec les résultats attendus. On peut citer à titre d'exemple les jeux d'essai destiné à contrôler les droits d'accès.

L'utilisation des jeux d'essai implique que :

- Le contrôle est réalisé sur une application à un moment donné dans le temps et que dans le cas où les programmes auraient été modifiés, les jeux d'essai peuvent ne plus correspondre aux nécessités du contrôle
- Le contrôle porte sur la procédure de traitement et non sur les données entrées. Ainsi, des contrôles supplémentaires devraient être prévus pour ces dernières.

2. Domaines d'application des TAAO :

Les Techniques d'audit assistées par ordinateur peuvent être utilisées pour la réalisation de multiples procédures d'audit. Nous citons, à titre d'exemple :

- Tests sur les contrôles généraux informatiques : Exemple : Tester les procédures d'accès ;
- Tests sur les contrôles d'application automatisés : Exemple : Tester le fonctionnement d'une procédure programmée ;
- Procédures d'examen analytique : identification des variations anormales et des éléments inhabituels, analyse de régression, etc.
- Tests de détails sur les transactions et les soldes : exemple : recalcul des intérêts, techniques d'échantillonnage, etc.

Exemple de TAAO relatives aux comptes clients :

- Stratification des soldes ou des transactions par âge (servant, par exemple, à la détermination de la provision pour dépréciation des comptes clients)
- Identification des soldes clients dépassant la limite du crédit et détermination du montant réel des dépassements
- Identification des comptes avec des limites de crédit inhabituelles ou sans limites de crédit
- Identification des transactions inhabituelles (Exemple : des ventes importantes vers la fin de l'exercice, des transferts inter-comptes)
- Identification des transactions non rapprochées (exemple : recouvrement sans facture)
- Identification des données permanentes inhabituelles (exemple : Taux de remise importants)

3. Eléments à prendre en compte lors de l'utilisation des TAAO :

Le recours aux techniques d'audit assistées par ordinateur implique la prise en compte d'un certain nombre d'éléments à savoir :

- Les connaissances, l'expérience et la maîtrise par l'auditeur des instruments informatiques ;
- La disponibilité des techniques d'audit assistées par ordinateur et d'installations informatiques adaptées et satisfaisantes ;
- L'impossibilité d'exécuter manuellement certains contrôles (inexistence de traces matérielles visibles, etc.) ;
- La recherche de l'efficacité et de l'efficience : l'utilisation des techniques d'audit assistées par ordinateur peut améliorer l'efficacité des procédures d'audit et réduire le temps consacré à l'obtention et à l'évaluation des éléments probants.

Toutefois, il convient de signaler que l'inexistence de contrôles généraux informatiques appropriés peut mettre en cause l'intégrité des techniques d'audit assistées par ordinateur. Dans ce cas, et selon l'ampleur des faiblesses, l'auditeur doit chercher des procédures alternatives telles que l'enregistrement des données et la réalisation des tests sur un autre environnement.

Section 3 : La mise à niveau de la formation des auditeurs

L'évolution des technologies de l'information et de la communication et les changements conséquents ont créé un nombre important de défies que toute la profession comptable doit y faire face. Cette dernière doit s'assurer que :

- les nouveaux candidats qui rejoignent la profession possèdent les compétences et les connaissances nécessaires en la matière
- après leur diplôme universitaire, ses membres sont à jour des nouveaux développements et outils correspondants.

Ainsi, l'impact se situe à deux niveaux : la formation universitaire et la formation post universitaire ou professionnelle.

La qualification universitaire et l'admission à un organisme professionnel est une reconnaissance au candidat d'avoir satisfait aux exigences de leur environnement à une date donnée.

Toutefois, dans un environnement caractérisé par des mutations rapides et constantes, les experts comptables doivent admettre que la formation continue est une nécessité et une exigence de la profession. En effet, « il y a une différence majeure entre la compétence d'une personne qui se suffit de la formation dispensée à l'université et la compétence d'une personne qui se prend en charge. Le constat est d'autant plus évident que l'université n'est relativement qu'un passage de courte durée alors que la nécessité de formation est à vie »[80].

En Tunisie, les réactions universitaires et professionnelles face à ces changements importants sont à ce jour très timides. A notre avis, l'Ordre des Experts Comptables de Tunisie en association avec les enseignants universitaires est appelé à gérer ces changements en imposant la couverture universitaire de certains concepts des technologies de l'information et de la communication et en imposant aux professionnels une formation professionnelle continue en la matière.

Alors, quelles sont les dispositions et quels sont les moyens à mettre en œuvre ?

Pour pouvoir répondre à cette question, nous nous sommes inspirés des guides internationaux d'éducation de l'IFAC (IEG[81]) et essentiellement IEG 11 intitulé « Information Technology in the accounting curriculum ».

L'IEG 11 a été développé par l'IFAC pour servir de guide à ses membres (dont l'Ordre des Experts Comptables de Tunisie) dans le développement de programmes de renforcement des compétences de leurs membres actuels et futurs en matière de technologies de l'information. Ce guide est révisable tous les deux années pour tenir compte des changements constants en la matière.

[80] Abderraouf YAICH, « La profession comptable et les Nouvelles Technologies de l'Information et de la Communication», Revue Comptable et Financière N°53, Troisième trimestre 2001.
[81] IEG : « International Education Guideline », Guides d'éducation de l'IFAC.

Selon l'IEG 11, la formation des experts comptables doit englober cinq axes :

1. Les généralités sur les technologies de l'information
2. L'expert comptable en tant qu'utilisateur des technologies de l'information
3. L'expert comptable en tant que gestionnaire des technologies de l'information
4. L'expert comptable en tant que concepteur des technologies de l'information
5. L'expert comptable en tant qu'auditeur des technologies de l'information

L'attention sera focalisée, essentiellement, sur la formation de l'expert comptable en tant qu'auditeur des technologies de l'information. Toutefois, nous avons jugé utile de décrire brièvement les autres axes parce qu'ils complètent la formation de l'auditeur en lui fournissant les outils et les notions fondamentales.

C'est comme si on ne peut être auditeur financier sans avoir une connaissance des normes comptables, sans pouvoir définir les politiques et les choix comptables et sans maîtriser les opérations d'inventaire nécessaires à l'arrêté des comptes.

Sous section 1 : La mise à niveau de l'éducation universitaire : Formation initiale

Il est vrai que des cours portant sur le système d'information et les nouvelles technologies sont déjà prévus pour les étudiants en expertise comptable et que certaines universités ont introduit un diplôme d'études supérieures spécialisées (DESS) en la matière. Toutefois, ceci demeure insuffisant.

Dans ce qui suit, nous présentons ce que les cours sur les technologies de l'information doivent fournir aux étudiants en termes de connaissances et de compétences. Ces cours devraient être toujours révisés pour tenir compte des technologies émergentes.

L'objectif recherché est que l'étudiant en expertise comptable ait des connaissances solides en informatique sans lui demander d'être un informaticien en plus d'un expert en comptabilité.

L'éducation universitaire doit porter sur :

1. Des généralités relatives aux technologies de l'information :

L'IEG 11 a prévu dans son paragraphe 40 que les étudiants en expertise comptable doivent acquérir des connaissances générales portant sur les aspects suivants :

1. Les concepts des technologies de l'information (hardware, software, gestion des données, réseau, transfert électronique de données, etc.)
2. Le contrôle interne dans un milieu informatisé[82]
3. Les normes de développement
4. La gestion des mises en place et de l'utilisation des technologies de l'information
5. Evaluation des systèmes informatisés : Evaluation des objectifs, des méthodes et des techniques, etc.

2. Le rôle d'utilisateur :

Comme utilisateur des technologies de l'information, les experts comptables s'exposent à une variété très large d'architectures de systèmes d'information, de hardware, de software et des méthodes de gestion des données.

Il n'est pas question de devenir un expert dans chaque type de système mais l'éducation universitaire doit permettre, uniquement, d'avoir les connaissances et les compétences de base nécessaires, dont à titre d'exemple :

- Mesures de sécurité à mettre en place pour prévenir les systèmes contre tout risque de perte, de fraude, d'accès non autorisé, etc.
- Aptitude à l'utilisation d'un progiciel de traitement et de gestion des données, d'un progiciel comptable, etc.
- Aptitude à utiliser la messagerie électronique, accéder et charger des informations des bases de données locales ou en ligne.

[82] Ce point mérite une connaissance plus approfondie. Il représente le contre d'intérêt des auditeurs.

3. *Le rôle de gestionnaire :*

L'expert comptable peut être amené, par exemple, à :

- Participer dans une planification stratégique associée à l'utilisation des systèmes d'information pour supporter les objectifs de l'entité
- Evaluer les investissements potentiels en technologie de l'information
- Exercer un contrôle sur la productivité des systèmes d'information

Ainsi, l'éducation universitaire doit permettre à l'expert comptable d'avoir une compréhension conceptuelle des technologies de l'information et particulièrement sur les points suivants :

- Considérations stratégiques dans le développement des technologies de l'information
- Aspects administratifs (organigramme, fiches de fonction, procédures de recrutement, etc.)
- Contrôle financier sur les technologies de l'information (budget informatique et contrôle des coûts)
- Aspects opérationnels (architecture, moyens de communication, etc.)
- Gestion de l'acquisition, du développement et de l'implémentation des systèmes
- Gestion de la maintenance et des changements de système
- La gestion des utilisateurs finaux (sécurité, assistance, etc.)

4. *Le rôle de concepteur :*

L'expert comptable est toujours sollicité pour la conception de système comptable et financier. De nos jours, cette conception est à réaliser dans un contexte de nouvelles technologies de l'information.

L'éducation universitaire doit permettre à l'étudiant en expertise comptable d'avoir des connaissances sur les étapes basiques suivantes :

- Le rôle de l'information dans l'organisation
- Les techniques de conception de système
- Les différentes phases et les différentes tâches de développement des systèmes (exemple : introduction des contrôles dans les systèmes, maintenir le contrôle sur les différentes étapes de développement)

5. *Le rôle d'auditeur :*

Le rôle d'auditeur englobe, aussi bien, les fonctions d'auditeur interne qu'externe. Dans ce cadre, l'éducation universitaire doit permettre à l'étudiant en expertise comptable de prendre connaissance des normes d'éthique, des normes d'audit traitant des technologies de l'information, de la réglementation correspondante en vigueur, etc.

En outre, l'étudiant doit pouvoir distinguer entre les objectifs d'évaluation des systèmes d'information, dont à titre d'exemple :

- Evaluation de l'efficacité, de l'efficience et de l'économie associée à l'utilisation des technologies de l'information
- Evaluation de la conformité avec la politique de la direction, la réglementation en vigueur, etc.
- Evaluation du contrôle interne dans un milieu informatisé
- Evaluation de la fiabilité des états financiers et de l'exactitude et de l'exhaustivité des enregistrements comptables.

Par ailleurs, et étant donné que les procédures d'évaluation dans le contexte des technologies de l'information peuvent nécessiter le recours aux techniques et outils assistés par ordinateur, l'étudiant en expertise comptable doit avoir une idée sur les différentes techniques et outils disponibles, leurs forces, leurs limites, comment les exécuter et contrôler leurs résultats.

Enfin, nous pouvons conclure qu'à l'instar des autres organismes professionnels, tels que l'institut canadien CGA (Certified General Accountant's association) et l'AICPA (American Institute of Certified Public Accountants), l'OECT devrait prendre les mesures nécessaires à la mise en place de l'IEG 11 «Information technology in the accounting curriculum» et ce, en collaboration avec les enseignants

universitaires, les différentes commissions et associations nationales, les instances gouvernementales, etc.

Aux Etats Unis d'Amérique, l'examen du diplôme d'expertise comptable de 2003 sera totalement informatisé. « La compétence technologique du candidat sera indispensable au déroulement de l'épreuve. L'objectif de l'examen sera revu en conséquence : On n'attend plus du candidat qu'il ait la réponse à toutes les questions mais qu'il ait la compétence pour trouver les réponses pertinentes sur Internet.

L'examen testera la capacité du candidat à gérer une grande quantité d'informations et à dénouer la complexité et l'abondance de la littérature professionnelle pour résoudre un problème pratique. »[83]

Sous section 2 : La formation post-universitaire ou professionnelle : Formation continue

Selon le code d'éthique de l'IFAC[84], les professionnels de la comptabilité ont une tâche continue pour le maintien de leur connaissance et de leur compétence à un niveau leur permettant d'assurer à leurs clients ou employeurs l'avantage du service d'un professionnel compétent et à jour des nouveaux développements.

Dans le contexte des nouvelles technologies de l'information et de la communication, l'université n'est plus qu'un outil de soutien ou un portail vers le savoir. La formation est l'œuvre de la personne elle-même qui, afin de maintenir ses compétences, doit satisfaire une formation professionnelle continue.

Ceci peut être assurée par l'auto-éducation, les lectures, les publications, les participations dans les ateliers de travail, les séminaires et les conférences, les associations professionnelles, les programmes de formation interne des sociétés et des cabinets d'expertise comptable, etc.

L'IFAC recommande que la formation professionnelle continue dans chaque pays membre soit pilotée par l'organisme professionnel comptable local soit, en Tunisie, l'Ordre des Experts Comptables de Tunisie (OECT).

L'objectif de cette formation continue est de s'assurer que tous les professionnels gardent un minimum de connaissances et de compétences en tant qu'utilisateur des technologies de l'information et cherchent à développer un ou plusieurs des rôles de gestionnaire, de concepteur et d'auditeur.

Il est utile d'évoquer à ce niveau le concept de spécialisation. En effet, vu les nouveautés continues dans le domaine des technologies de l'information et de la communication, comme par ailleurs dans d'autres domaines, l'expert comptable ne peut pas développer une expertise dans n'importe quel domaine sans une vraie spécialisation.

Cette spécialisation est la résultante de la combinaison d'une éducation théorique, d'un développement de la compétence pratique et de l'expérience spécifique dans un domaine de travail spécialisé.

L'Ordre des Experts Comptables de Tunisie peut prévoir une sorte de reconnaissance des experts comptables ayant acquis une spécialisation dans les technologies de l'information et de la communication en leur délivrant des certificats de spécialiste[85] ou tout autre moyen de reconnaissance.

Dans un cadre plus général, le guide international d'éducation (IEG) N°2 « Continuing Professional Education » de l'IFAC oblige ses associations membres, dont l'OECT, à établir et à mettre disponible des programmes d'éducation professionnelle continue qui :

- Maintiennent et améliorent les connaissances techniques et les compétences professionnelles de leurs membres ;
- Assistent leurs membres à l'application de nouvelles techniques, à la compréhension des nouveaux développements économiques ainsi qu'à la maîtrise des nouvelles responsabilités ;
- Assurent les utilisateurs du service de leurs membres que ces derniers possèdent les connaissances et les compétences requises.

[83] Abderraouf YAICH, « Actualités tunisiennes et internationales : Le diplôme d'expertise comptable US version 2003 », Revue Comptable et Financière N°53, Troisième trimestre 2001, Extrait de « Journal Of Accountancy » N°3, Mars 2001.
[84] Paragraphe 16 du Code d'Ethique, IFAC.
[85] L'AICPA vient de mettre en place le CITP (Certified Information Technology Professional) comme reconnaissance de l'expert comptable spécialiste dans les technologies de l'information.

Les nouvelles technologies de l'information et de la communication doivent faire partie des programmes de formation continue.

En outre, le même guide admet que l'expert comptable doit y participer avec un minimum de 30 heures par an ou 90 heures par 3 ans. Cette participation peut être réalisée à travers des programmes courts tout au long de la période.

Encore, les associations membres de l'IFAC, dont l'Ordre des Experts Comptables de Tunisie, doivent exiger de leur membre la réalisation d'un minimum d'éducation professionnelle continue comme condition d'adhésion à l'association et/ou du droit d'exercer. De ce fait, un système de suivi des participations par individu ainsi qu'un système de sanction doivent être mis en place.

Ainsi, il ressort de cette disposition que l'IFAC qualifie d'obligatoire l'éducation professionnelle continue et non de volontaire et ce, pour :

- Résoudre le problème d'implication irrégulière et indisciplinée de certains experts comptables ;
- Convaincre la société en générale de l'engagement de toute la profession à l'éducation professionnelle continue et à la compétence professionnelle ;
- Renforcer le développement et la coordination mondiale de la profession comptable avec des normes harmonisées.

Enfin, notons que le respect de ce guide par l'Ordre des Experts Comptables de Tunisie nécessite un effort considérable en moyens humains et matériels.

Sous section 3 : Le recours à la certification CISA

La certification CISA (Certified Information Systems Auditor)[86] est un titre professionnel introduit en 1978 et géré par l'ISACA. Elle est de plus en plus reconnue comme un standard international de connaissance en matière d'audit, de gestion, de gouvernement et de sécurité des systèmes d'information.

La certification CISA continue de gagner le respect et la reconnaissance des associations comptables, des gouvernements et des universités à travers le monde entier. Actuellement, 10 000 auditeurs sont certifiés CISA à travers le monde.

Les exigences pour ce titre sont la réussite de l'examen CISA, cinq années d'expérience, l'adhésion au code d'éthique ainsi que la formation continue.

1. L'examen CISA :

L'examen CISA est administré annuellement dans neuf langues et offerts dans plus de 120 villes autour du monde.

L'examen couvre tous les domaines de l'Audit des Systèmes d'Information, des aspects les plus techniques aux aspects les plus organisationnels. Ces domaines sont les suivants :

- Normes d'audit des systèmes d'information et pratiques en matière de contrôle et de sécurité des systèmes d'information : l'objectif de ce domaine est de s'assurer que l'auditeur en systèmes d'information adhère aux normes généralement appliquées en matière d'audit des Systèmes d'information, ainsi qu'aux règles de l'art et pratiques en matière de contrôle et de sécurité des Systèmes d'information.
- Audit du management et de l'organisation du système d'information : l'objectif de ce domaine est d'analyser et d'évaluer la stratégie, les politiques et les procédures, les pratiques de management ainsi que l'organisation du Système d'Information.
- Audit des ressources du système d'information : l'objectif de ce domaine est l'analyse et l'évaluation des différents processus associés aux systèmes d'information.
- Audit de la disponibilité, de l'intégrité et de la confidentialité des systèmes d'information : l'objectif de ce domaine est l'analyse et l'évaluation des contrôles logiques, physiques, d'environnement, de validation, de traitement et de réconciliation de données et du plan de secours.

[86] Traduction française : « certificat d'Audit des Systèmes d'Information »

- Audit de la continuité des opérations : l'objectif de ce domaine est l'analyse et l'évaluation des règles et des procédures concernant le plan de secours afin de s'assurer de la capacité de l'organisation à répondre efficacement aux désastres et autres situations d'urgence.
- Audit du développement, de l'acquisition et de la maintenance des systèmes d'information : l'objectif de ce domaine est l'analyse et l'évaluation des règles et des procédures concernant la sécurité et le contrôle du développement, de l'acquisition et de la maintenance des systèmes d'information.
- Audit des systèmes d'application : l'objectif de ce domaine est l'identification, l'analyse et l'évaluation des forces et des faiblesses ainsi que l'efficience et l'efficacité des systèmes d'application existants.

2. La formation continue :

La politique de formation continue des diplômés CISA consiste en la réalisation d'un minimum d'heures de formation continue par an et par une période de 3 ans comme suit :

- Atteindre un minimum annuel de vingt (20) heures de formation continue
- Atteindre un minimum de cent vingt (120) heures de formation continue pour une période de trois années

La non observation de ces dispositions résultera en la révocation du membre concerné.

Par ailleurs, pour contrôler le respect par ses membres des exigences de la formation continue, un échantillon des diplômés CISA est sélectionné chaque année pour audit. Ces diplômés choisis doivent fournir des évidences écrites des activités de formation précédemment rapportées. Le comité d'audit déterminera l'acceptation ou non des heures.

Conclusion

Les nouvelles technologies sont des cibles en mouvement. C'est ainsi que l'enjeu est important pour l'expert comptable, pour la profession comptable en général sous l'égide de l'Ordre des Experts Comptables de Tunisie et pour le législateur. Chacun a un rôle à jouer. Mais l'action devrait être rapide et continue.

Conclusion Partie II

Il apparaît clairement que dans un contexte de nouvelles technologies, il est de plus en plus difficile pour l'auditeur financier de forger son opinion sans une approche approfondie du système informatique. En outre, l'utilisation des travaux d'audit informatique dans le cadre d'une mission d'audit financier permet de :

- mettre en évidence des faiblesses de contrôle interne ayant un impact sur les états financiers audités non détectables par une approche classique
- limiter les travaux substantifs pour les entreprises pour lesquelles l'auditeur peut s'appuyer sur les systèmes
- apporter une plus value à l'entreprise par la mise en œuvre de travaux d'audit - conseil.

La mise en œuvre de l'audit informatique exige :

- une répartition convenable des tâches et une coordination continue entre les membres de l'équipe d'audit informatique et ceux de l'équipe d'audit financier. Ceci constitue une des conditions essentielles du succès de l'audit ;
- une compétence et une expérience à la hauteur des difficultés rencontrées et de l'efficacité nécessaire ; la formation permanente en séminaires et sur le terrain doit constituer un investissement important ;
- le recours à des spécialistes en cas de domaine informatique pointu ou complexe.
- une recherche permanente des méthodes et techniques nouvelles et mieux adaptées.

Par ailleurs, face à l'évolution continue et complexe des nouvelles technologies, l'auditeur ne peut développer une vrai expertise sans une vraie spécialisation.

Une question se pose : Faut-il former un auditeur à l'informatique ou un informaticien à l'audit ? Chaque possibilité a ses partisans. L'informaticien, ou l'auditeur, qui s'apprête à accepter ce genre de spécialisation doit préalablement prendre en compte l'effort que demande le maintien d'une double compétence.

Vu l'élargissement des domaines d'intervention de l'expert comptable, doit-on aussi commencer à réfléchir sur le concept d'expert comptable spécialisé ?

Conclusion Générale

Les technologies de l'information et de la communication ne touchent pas uniquement les grandes entreprises mais aussi les petites et moyennes entreprises. En effet, le degré d'informatisation n'est plus fonction de la taille de l'entreprise. Exemple : Le commerce électronique a permis à de nombreuses petites sociétés un rayonnement mondial.

Face à la complexité croissante des systèmes (intégration, décentralisation, dématérialisation des informations, automatisation des contrôles, etc.), les grandes sociétés de développement informatique ont dépensé des sommes considérables pour prévoir les sécurités nécessaires au niveau des applications. En outre, les entreprises sont de plus en plus conscientes de la nécessité d'une gestion appropriée des risques.

Ainsi, conduire un audit informatique dans le cadre d'une mission d'audit financier n'a plus rien d'exceptionnel. A terme, nous parlerons peut être non plus des auditeurs financiers et des auditeurs informatiques mais des auditeurs tout simplement, chacun ayant une compréhension globale de l'entreprise[87].

Ce n'est pas à un changement de métier, mais à une évolution des méthodes et des outils de travail que doit se préparer l'auditeur.

En outre, les nouvelles technologies sont en train de rendre disponible une quantité de plus en plus importante d'informations à un nombre croissant d'utilisateurs et ce, selon une périodicité beaucoup plus fréquente.

Ces utilisateurs, pour pouvoir prendre leur décision, ont de plus en plus besoin d'une information auditée. Ainsi, l'auditeur doit s'attendre à être contraint d'exercer un contrôle de plus en plus permanent.

Dans ce cadre d'idée, des recherches sont en train d'être entreprises par la CICA (Canadian Istitute of Chartered Accountants) et l'AICPA[88] (American Institute of Certified Public Accountants) sur ce qu'on appelle « l'audit continu »[89] et aussi « l'audit en ligne continu »[90].

Un audit continu est une méthodologie qui permet aux auditeurs indépendants de fournir l'assurance sur un sujet particulier d'une façon simultanée ou peu de temps après sa réalisation. L'audit continu peut aussi être appelé « l'audit instantané ».

L'audit en ligne continue est un audit continu avec une connexion en ligne permanente entre l'audité et l'auditeur.

Parmi les conditions préalables de faisabilité de l'audit continu, nous citons :

- L'usage par l'entité auditée de systèmes hautement automatisés
- Des outils d'audit intégrés à différents niveaux du système de l'entreprise
- Un haut niveau de compétence de l'auditeur sur les différents aspects des technologies de l'information

[87] Michel LEGER, Didier KING, Pierre COLL et Patrick DE CAMBOURG, « Audit financier : Faire face aux risques informatiques »; 15ème congrès de l'AFAI ; Revue « Audit et conseil informatique » N°54 ; Janvier – Mars 1998.
[88] Un premier rapport a été publié en 1999 qui a défini le cadre conceptuel de l'audit continue et qui a dégagé les difficultés potentielles possibles
[89] En anglais : Continuous auditing
[90] En anglais : Continuous On-line auditing.

En outre, des recherches supplémentaires sont en train d'être menées pour savoir si l'audit continue affecte la détermination des aspects fondamentaux de l'audit tels que la matérialité, les risques d'audit, la détermination de la nature, le calendrier et l'étendue des procédures substantives, etc.

Outre cette nouveauté et dans un contexte plus général, il y a lieu de préciser que les nouvelles technologies de l'information viennent éliminer de la profession comptable certains domaines d'intervention dont, à titre indicatif, la tenue de la comptabilité, l'élaboration des déclarations fiscales et sociales, etc.

Toutefois, ils viennent de créer pour les experts comptables de nouvelles opportunités professionnelles, dont à titre d'exemple :

- La gestion des systèmes d'information : Elaboration d'un schéma directeur informatique, analyse des investissements informatiques, gestion des risques informatiques, assistance à la définition des procédures de migration des données, etc.
- Mise en place de nouveaux systèmes : Ceci comprend la revue du système avant le démarrage, la définition de la sécurité et des contrôles et la revue du système après démarrage.
- Sécurité informatique : Mise en place d'une politique et de procédures de sécurité informatique, définition et mise en œuvre du paramétrage de la sécurité, diagnostic de la sécurité informatique, sécurité Internet et tests de pénétration, etc.
- Plan de continuité d'activité : analyse d'impact sur l'activité, détection d'une stratégie appropriée, développement d'un plan de continuité, maintenance et tests, évaluation du plan.

En matière d'audit, nous citons, à titre d'exemple, les nouvelles opportunités professionnelles suivantes :

- Revue de l'adéquation de la conception et de l'efficacité du fonctionnement des contrôles : Cette revue est entreprise sur les contrôles propres au service bureau en vue d'être utilisée par les auditeurs de ses entreprises clientes. Ce genre de revue est de plus en plus nécessaire avec le E-commerce et l'E-business.
- SysTrust : C'est une initiative parrainée par l'AICPA et le CICA. Il s'agit de rapporter sur la fiabilité des systèmes (hardware, software, staff, données, etc.) par référence aux quatre principes essentiels de fiabilité définis par l'AICPA à savoir la disponibilité, la sécurité, l'intégrité et la maintenabilité[91].
- WebTrust : C'est aussi une initiative parrainée par l'AICPA et le CICA. Le service est basé sur des attestations standards, mais désigné spécifiquement autour des contrôles en rapport avec un environnement interconnecté.

  La certification WebTrust peut être exercée par le commissaire aux comptes. Il s'agit alors d'une intervention dite conventionnelle, connexe à sa mission générale.

  En effet, les procédures de l'entité liées aux ventes font partie du champ des investigations du commissaire aux comptes, que ces ventes soient réalisées via le commerce électronique ou des circuits plus traditionnels. Une analyse de ces procédures en fonction des risques qui y sont attachés fait partie du déroulement classique de la méthodologie d'audit et constitue le point de départ d'investigations spécifiques plus approfondies exigées par l'intervention WebTrust. Ce faisant, cette dernière est de nature à renforcer l'efficience et la valeur ajoutée de la mission générale.

  L'intervention WebTrust se fonde sur une information déclarative de l'entité affirmant qu'elle respecte bien les principes WebTrust (transparence des pratiques en matière de commerce et de confidentialité de l'information, intégrité des transactions, protection de l'information).

  L'intervention du commissaire aux comptes d'une entité, en vue de l'obtention par celle-ci du sceau " WebtTrust " sur son site de commerce électronique, a pour objectif d'apprécier la sincérité de cette déclaration.

Enfin, il y a lieu de signaler que pour la conquête de ces nouvelles opportunités, les experts comptables doivent avoir les moyens pour résister à une forte concurrence à laquelle ils peuvent être confrontés (consultant en nouvelles technologies, banques, etc.). Cela va de leur survie.

[91] Traduction anglaise : Maintainability

Les experts comptables qui se cantonneront à la comptabilité seront progressivement ravalés à un rôle secondaire et risquent de voir restreindre leurs interventions à quelques opérations de haute technicité comme le bouclage d'un bilan, ou la préparation des déclarations fiscales ou sociales spécifiques[92].

La profession comptable en Tunisie est consciente des opportunités mais aussi des menaces. Elle doit arrêter un plan d'action afin de jouer un rôle majeur dans tous ces nouveaux domaines, et rehausser encore plus son rang dans la société toute entière.

[92] inspiré des Propos de William Nahum, président du Conseil régional des experts comptables de l'Ile-de-France, recueillis par Anne-Chantal De Divonne, Les Echos, Dossier management, Mardi 21 mars 2000.

Bibliographies

I - Textes législatifs et réglementaires :

1 - En Tunisie :

- Code de commerce
- Nouveau code des sociétés commerciales (Promulgué par la loi N° 2000-93 du 3 novembre 2000)
- Loi 96-112 du 30 décembre 1996, relative au système comptable des entreprises
- Décret N°96-2459 du 30 décembre 1996, portant approbation du cadre conceptuel de la comptabilité
- Le code de la Taxe sur la Valeur Ajoutée
- Le code de l'impôt sur les revenus des personnes physiques et de l'impôt sur les sociétés (IRPP & IS)
- Le code pénal
- Loi 94-36 du 24 février 1994 relative à la propriété littéraire et artistique
- Loi 2000-57 du 13 juin 2000 (portant modification de certains articles du code des obligations et des contrats)
- Loi N° 2000-82 du 09 août 2000 portant promulgation du code des droits et des procédures fiscaux
- Loi N° 2000-83 du 09 août 2000 relative aux échanges et au commerce électronique
- Loi N° 2000-84 du 24 août 2000 relative au brevet d'invention
- Loi N° 2001-1 du 15 janvier 2001 portant promulgation du code des télécommunications
- Note commune N° 98/19 portant commentaire des dispositions des articles 75 à 78 du 29 décembre 1997 portant loi de finances pour l'année 1998.

2- En France :

- Code de commerce (modifié par la loi du 30 avril 1983)
- Code Général des Impôts
- Nouveau Plan Comptable Général : règlement N° 99.03 du 29 avril 1999 du comité de la réglementation comptable homologué par l'arrêté du 22 juin 1999.
- Loi « Informatiques et libertés » du 06 Janvier 1978 décrivant les règles relatives à l'informatique, aux fichiers et aux libertés
- Décret N° 83-1020 du 29 Novembre 1983 portant obligations comptables des commerçants et de certaines sociétés
- Loi sur la protection des logiciels et progiciels du 3 Juillet 1985
- Loi N° 88-19 du 5 janvier 1988 sur la fraude informatique (loi GODFRAIN)
- Loi du 10 Juillet 1991 relative à la protection des télécommunications

- Loi MADELIN du 11 Février 1994
- Directive 95/46/CE du parlement européen et du conseil, du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
- Le nouveau Code pénal
- Loi N° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique
- Décret N° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique

II - Normes et Directives :

1/ I.F.A.C : International Federation of accountants :

A/ Normes internationales d'audit (ISA : International Standards on Auditing)

- ISA 300 : Planification des travaux
- ISA 400 : Evaluation du risque et contrôle interne
- ISA 401* : Audit réalisé dans un environnement informatique

  (Auditing in a computer information system environment)

  (*) En cours de révision
- ISA 402 : Facteurs à considérer pour l'audit d'entités faisant appel aux services bureaux (Audit consideration relating to entities using service organizations)
- ISA 500 : Eléments probants
- ISA 620 : Utilisation des travaux d'un expert

B/ Directives Internationales d'Audit (IAPS : International Auditing Practice Statements) :

- IAPS 1001* : Environnement informatique : Micro-ordinateurs autonomes

  (CIS environments – Standalone microcomputers)
- IAPS 1002* : Environnement informatique : Systèmes d'ordinateurs interconnectés

  (CIS environments – On line computer systems)
- IAPS 1003* : Environnement informatique : Systèmes de bases de données

  (CIS environments – Database systems)
- IAPS 1005 : Remarques particulières relatives à l'audit des petites entreprises

  (Particular consideration in the audit of small businesses)
- IAPS 1008* : Evaluation du risque de contrôle interne – Caractéristiques et considérations sur l'informatique

  (Risk assessment and Internal control : EDP characteristics and consideration)
- IAPS 1009* : Techniques d'audit assistées par ordinateur

  (Computer Assisted Audit Techniques CAAT's)

  (*) En cours de révision

C/ International Information Technology Guideline :

- N°1 : Managing Security of Information, Janvier 1998
- N°2 : Managing Information Technology planning for business impact, janvier 1999
- N°3 : Acquisition of Information Technology, juillet 2000

- N°4 : The Implementation of Information Technology Solutions, juillet 2000
- N°5 : IT service delivery and support, juillet 2000

D/ International Education Guideline (IEG) :

- N°2 : Continuing Professional Education (projet)
- N° 9 : Pre-qualification, Education, assessment of professional competence and experience requirements of professional accountants.
- N° 10 : Professional Ethics for accountants : The education challenge and practical application
- N° 11 : Information Technology in the accounting curriculum.

2/ O.E.C.C.A. : L'Ordre des Experts Comptables et des Comptables Agréés :

- Recommandation N°22.07 : « La révision en milieu informatisée ».
- Recommandation N°23.03 : « Diagnostic des systèmes informatisés ».

3/ C.N.C.C : Conseil National des Commissaires aux Comptes :

- Recommandation 5.16 : « Contrôle des entreprises informatisées » ; délibération du 7 Juillet 1983.

4/ A.I.C.P.A : American Institute of Certified Public Accountants :

- SAS N° 22 (Statement on Auditing Standards) : « Planning and supervision ».
- SAS N° 31 : « Evidential Matter ».
- SAS N° 47 : « Audit risk and materiality in conducting an Audit ».
- SAS N° 48 : « The effects of Computer Processing on the Examination of Financial Statements ».
- SAS N° 94 : « The Effect of Information Technology On the Auditor's Consideration of Internal Control in a Financial Statement Audit » modifiant le SAS N° 55 : « Consideration of the Internal Control Structure in a Financial Statement Audit ».

5/ I.C.A.E.W : Institute of Chartered Accountants of England and Wales :

- Auditing guideline 407 : « Auditing in a computer environment », 20 juin 1984.

6/ Information System Audit and Control Association :

A/ Code of Professional Ethics for Information System auditors

(Code d'éthique professionnelle des auditeurs des systèmes d'information)

B/ Normes générales pour l'audit des systèmes d'information :

- 010 Charte d'audit
- 020 Indépendance
- 030 Ethique et normes professionnelles
- 040 Compétence
- 050 Planification
- 060 Réalisation du travail d'audit
- 070 Rapport
- 080 Activités de suivi

C/ Directives d'audit des systèmes d'information :

- « audit charter », Septembre 1999
- « Audit Documentation », Mars 2000
- « Audit Consideration for Irregularities », Septembre 1999
- « Audit evidence requirement », Décembre 1998

- « Audit sampling », Mars 2000
- « Corporate Governance of Information Systems », Juin 1998
- « Due professional care », Septembre 1999
- « Effect of Involvement in the Development, Acquisition, Implementation or Maintenance Process on the IS Auditor's Independance », Mars 2000
- « Effect of pervasive IS Controls », Mars 2000
- « Materiality Concepts for Auditing Information Systems », Septembre 1999
- « Organisational Relationship and Independance », Septembre 2000
- « Outsourcing of IS Activities to other Organisations », Septembre 1999
- « Planning the IS Audit », Juin 1998
- « Report Content and Form », Décembre 1998
- « Use of Computer Assisted Audit Techniques », Décembre 1998
- « Use of Risk Assessment in Audit Planning », 1 Septembre 2000
- « Using the work of other auditors and experts », Juin 1998

III - Ouvrages :

- AICPA, « Audit and accounting guide », American Institute of Certified Public Accountants.
- Armand ST-PIERRE, « De la comptabilité manuelle à la comptabilité informatisée", Editions agence d'ARC; Collection Micro-informatique, Télématique, Robotique et Bureautique, 1994.
- Befec – PricewaterhouseCoopers, « Mémento Comptable 2000 », Edition Francis Lefebvre.
- Conseil supérieur de l'ordre des experts comptables et des comptables agrées, « Le diagnostic des systèmes informatisés : Guide d'application des recommandations », O.E.C.C.A.
- Commission bancaire, « Le livre Blanc sur la sécurité des systèmes d'information », 2ème Edition, 1996.
- CLUSIF : Club de la sécurité informatique français, « Evaluation des conséquences économiques des incidents et sinistres relatifs aux systèmes informatiques, France 1996 », Février 1997.
- Coopers & Lybrand , « Handbook of Information Technology Auditing », édition interne Coopers & Lybrand, 1997.
- Gérard PETIT, Daniel JOLY, Jocelyn MICHEL, « Guide pour l'audit financier des entreprises informatisées », ATH : Association Technique d'Harmonisation des cabinets d'audit et conseil, édition CLET , 1985.
- I.S.A.C.A. (Information Systems audit and control association), « The Certified Information Systems Auditor : Continuing Professional Education », 1999.
- ISACA, « CISA : Certified Information Systems Auditor », review manual, 2000.
- I.S.A.C.F. (Information systems audit and control foundation), « COBIT : Control Objectives for Information and Related Technology », Avril 1998.
- Price Waterhouse, « Audit Guidance Series : Computerised Information systems », édition interne de Price Waterhouse, 1988.
- Price Waterhouse World Firm, « System Management Methodology : Information System Risk Management », version 1.0, Edition interne 1994.
- PricewaterhouseCoopers, « The PricewaterhouseCoopers audit », édition interne de PricewaterhouseCoopers, 1999.
- PricewaterhouseCoopers world firm technology center, « Technology Forecast 2000 », Edition interne PwC, 2000.

- Ulric J.Gelinas, Jr. et Allan E.Oram, « Accounting Information Systems », International Thomson Publishing,1996.
- « Mémento Fiscal 2001 », Edition Francis Lefebvre.

IV - ARTICLES :

- « Incidences du milieu informatique sur l'évaluation du système de contrôle interne », Bulletin des commissaires aux comptes N° 61, mars 1986.
- Mohamed BENLAHSEN TLEMCANI et Sofiane TAHI, GRECOS, université de Perpignan, « De l'Enterprise Resource Planning au Supply Chain Management », Institut Supérieur de Gestion : for a renewal of a management education, CPU Press 1999.
- Alain BOUSQUET, « Les risques lors de l'installation d'un système ERP », Revue Française de Comptabilité N°316, Novembre 1999.
- Dominique CHESNEAU, associé chez PricewaterhouseCoopers, « Vers une nouvelle approche des risques », Les Echos, L'art de la gestion des risques, 13 décembre 2000.
- Denis CORMIER, « L'évaluation du risque dans les missions d'audit externe : L'approche nord américaine », Revue Française de Comptabilité N°221, Mars 1991.
- François-Xavier DEBROSSE et Josselin DU PLESSIS, « L'audit des mesures prises pour assurer la continuité du système d'information », Revue Française de Comptabilité N°316, Novembre 1999.
- Sylvain FAURIE : directeur de mission à KPMG, « L'audit informatique : une nécessité tant pour l'entreprise que pour l'auditeur financier », Revue « Economie et comptabilité » N°176 ; Septembre 1991.
- Valérie FLAMENT-CHABBERT et Tuyen VU, « D'une sécurité virtuelle à une sécurité réelle », PricewaterhouseCoopers, Les Echos, L'art de la gestion des risques, 22 novembre 2000.
- Daniel JOLY, « Les progiciels intégrés et les nouveaux outils informatiques vont-ils changer l'approche d'audit ? », Revue Française de Comptabilité N° 316, Novembre 1999.
- Michel KARMA, Ecole centrale de Paris, « Une nouvelle approche de conception des systèmes d'information », Revue Française de Comptabilité N°234, Mai 1992.
- Jacqueline KIPFER, Expert comptable diplômé, conseil en système d'information, « La mutation des systèmes d'information comptable : Une perspective de renouvellement pour la profession comptable ? », Revue Française de Comptabilité N°222, Avril 1991.
- Hélène LAPORTE et Philippe PRUDHOMME, « Audit informatique dans les entreprises : évaluation du contrôle interne et contrôle des comptes », Revue Française de Comptabilité N° 316, Novembre 1999.
- Michel LEGER (Barbier FINAULT et Associés), Didier KLING (CNCC), Pierre COLL (Befec-Price waterhouse) et Patrick DE CAMBOURG (Mazars et Guérard), « Audit Financier : Faire face aux risques informatiques », XV^{ème} Congrès de l'AFAI, Revue Française de l'audit et du conseil informatique N°54 ; janvier- Mars 1998.
- Stéphane LIPSKI, « Le commissariat aux comptes et l'évolution de l'informatique », Revue Française de Comptabilité N° 316, Novembre 1999.
- Judith MERRYWEATHER, consultant de l'institut des experts comptables australiens sur le chapitre afférent aux technologies de l'information, « Ethics in a Cyber World : Ethical considerations and Electronic Commerce », mai 2000.
- William NAHUM, président du conseil régional des experts comptables d'Ile de France, « Les experts comptables à l'heure de la spécialisation et du travail en réseau », Les échos, mardi 21 Mars 2000.
- Adil OUAZZANI, « Audit informatique : Le cas d'une entreprise du secteur public au Maroc », Revue Française de Comptabilité N° 316, Novembre 1999.
- Duc PHAM-HI et Valérie FLAMENT-CHABBERT, « Les E-catastrophes », les Echos (supplément 18.270), jeudi 2 novembre 2000.

- Julian RANDALL & Bridget TREACY, « Les risques juridiques pour les aventuriers de la toile », les Echos (supplément 18.270), jeudi 2 novembre 2000.
- Philippe TROUCHAUD, « Appréciation du contrôle interne informatique des grandes entreprises et impact sur le contrôle des comptes », Revue Française de Comptabilité N° 316, Novembre 1999.
- Leslie WOLLCOCKS & Chris SAUER, « Externaliser les technologies de l'information », les Echos (supplément 18.270), jeudi 2 novembre 2000.
- Abderraouf YAICH, « Actualités Tunisiennes et internationales : Le diplôme d'expertise comptable US version 2003 », Revue Comptable et Financière N°53, Troisième trimestre 2001, extrait du « Journal of Accountancy », (N°3, Mars 2001).
- Abderraouf YAICH, « La profession comptable et les NTIC », Revue Comptable et Financière N°53, Troisième trimestre 2001.
- Muttiah YOGANANTHAN, « Les projets en cours de l'IAPC », Revue Française de Comptabilité, N°316, Novembre 1999.

V - MEMOIRES :

- Yves BEGON, « Les professionnels des comptes et l'informatique : Risques et principes de sécurités », Mai 1997.
- Atef BEN SALAH, « La sécurité de l'information face aux risques informatiques : approche méthodologique de diagnostic », Novembre 1995.
- Michel FINANCE, « La révision en milieu informatisé, nécessité d'une approche intégrée : exemple comparatif de trois nouvelles missions », 1987.
- Mohamed Hichem RAIES, « Les aspects juridiques et techniques des recours aux spécialistes dans les missions d'audit », Avril 1987.
- Raja ISMAIL, « L'audit des systèmes informatiques et de leur sécurité », Décembre 1997.
- Nadia JEDDI, « La responsabilité civile et pénale du commissaire aux comptes », 1991.
- Pierre MEUNE, « La responsabilité du commissaire aux comptes et de l'expert comptable en matière de diagnostic des systèmes informatisés et ses limites », 1989.
- Philippe SARRET, « Le réviseur comptable face aux systèmes informatisés : Evaluation des risques et approche d'audit », 1986.
- Luc THEROND, « Proposition d'une méthodologie d'audit dans le cadre de l'évaluation du contrôle interne des entreprises informatisées », 1994.

VI - SEMINAIRES & ATELIERS DE TRAVAIL :

- « ERP & E-Business : Les systèmes d'Information et la Gestion du changement », Séminaire organisé par PricewaterhouseCoopers Tunis et la Société Tunisienne de l'Electricité et du Gaz, le 13 et le 14 décembre 1999.
- « L'audit de la sécurité informatique », séminaire organisé par SOGENOR (Société Générale d'Organisation Scientifique, le 18 et le 19 Octobre 1999, animé par monsieur Jean-Marc BOST.
- « Royal Dutch Shell Group : Client service Workshop », Miami du 5 au 9 Juillet 1999, organisé par PricewaterhouseCoopers.
- « Evolution technologique : ERP, E-business & E-government », séminaire organisé par François MAUBOUCHER, Sénior Partner Afrique Francophone, PricewaterhouseCoopers, Octobre 1999.

VII - FORMATION :

- « Rôle du CIS (Computer information systemn) dans la gestion de la mission d'audit », Formation interne 1994, Befec – Price Waterhouse.
- « Introduction to Information System Security », Computer Information System Audit Self Training, Price Waterhouse World Firm.

- « Computer Assurance Service Joiners course : Initiation à l'assurance des systèmes », PricewaterhouseCoopers, Prague, Novembre 1998.
- « Utilisation de l'informatique dans la révision des comptes », Université de Tunis, Formation animée par Ernest & Young, Avril 1995.
- « Global Risk Management Solutions Joiners course », Initiation à la gestion du risque management, PricewaterhouseCoopers, Marburg-Allemagne 2000.

VIII - SITES INTERNET :

- **International Federation of Accountants (IFAC) :** www.ifac.org
- **ISACA (INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION)** : WWW.ISACA.ORG
- **INSTITUTE OF INTERNAL AUDITORS :** WWW.ITAUDIT.ORG / WWW.THEIIA.ORG
- **L'INSTITUT FRANÇAIS DES AUDITEURS CONSULTANTS INTERNES :** WWW.IFACI.COM
- **ASSOCIATION FRANÇAISE DE L'AUDIT ET DU CONSEIL EN INFORMATIQUE :** WWW.AFAI.ASSO.FR
- **AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS :** WWW.AICPA.ORG
- **CONSEIL NATIONAL DES COMMISSAIRES AUX COMPTES (FRANCE) :** WWW.CNCC.FR
- **PRICEWATERHOUSECOOPERS :** WWW.PWCGLOBAL.COM / WWW.EBUSINESSISBUSINESS.COM
- **ERNST & YOUNG :** WWW.EY.COM
- **ARTHUR ANDERSON :** WWW.ARTHURANDERSON.COM
- **COSO (COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION) :** WWW.COSO.ORG
- **CLUSIF :** WWW.CLUSIF.ASSO.FR
- **COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (CNIL – FRANCE) :** WWW.CNIL.FR
- WWW.JURISCOM.NET
- WWW.LEGALIS.NET
- WWW.TELECOM.GOUV.FR