ROYAUME DU MAROC

INSTITUT SUPERIEUR DE COMMERCE
ET D'ADMINISTRATION DES ENTREPRISES
CYCLE D'EXPERTISE COMPTABLE (C.E.C)

PROPOSITION D'UNE METHODOLOGIE POUR LA CONDUITE DES MISSIONS D'AUDIT INFORMATIQUE

MEMOIRE PRESENTE POUR L'OBTENTION DU DIPLOME NATIONAL D'EXPERT-COMPTABLE

PAR

M. Abdelilah TOURY

MEMBRES DU JURY

Président :	**M. Mohamed ELMOUEFFAK** **Enseignant et Directeur des études de L'ISCAE**
Directeur de Recherche :	**M. Abdelaziz AL MECHATT** **Expert-Comptable DPLE**
Suffragants :	**M. Fawzi BRITEL** **Expert-Comptable DPLE**
	M. Larbi KZAZ **Enseignant à L'ISCAE**

Mai 2006

REMERCIEMENTS

Je tiens à remercier toutes les personnes qui ont participé à la réalisation de ce travail.

J'exprime ma gratitude, particulièrement à :

- L'ensemble des enseignants à l'ISCAE, pour la qualité de la formation qu'ils m'ont assurée aussi bien pendant les quatre années du Cycle Normal que pendant les trois années du Cycle d'Expertise Comptable ;

- M. ABDELAZIZ AL MECHATT, qui a suivi de près la réalisation de ce travail ;

- M. MOHAMED MOUEFFAK, Enseignant et Directeur des études à l'ISCAE ;

- M. FAWZI BRITEL, Expert-Comptable DPLE ;

- M. LARBI KZAZ, Enseignant à l'ISCAE.

Je remercie, au même titre, M.Rachid M'RABET, Directeur de l'ISCAE, qui veille continuellement à la qualité de la formation assurée au sein de cet Institut.

TABLE DES MATIERES SIMPLIFIEE

INTRODUCTION GENERALE 2

PARTIE I :
LA COMPREHENSION DU CADRE GENERAL DE LA FONCTION INFORMATIQUE : UN PREALABLE NECESSAIRE POUR LA REALISATION DES MISSIONS D'AUDIT INFORMATIQUE 8

INTRODUCTION DE LA PREMIERE PARTIE 9

TITRE 1 :
L'ENVIRONNEMENT ET L'ORGANISATION DE LA FONCTION INFORMATIQUE 10

CHAPITRE 1 : L'ENVIRONNEMENT ET L'ORGANISATION DE LA FONCTION INFORMATIQUE DE L'ENTREPRISE 10
CHAPITRE 2 : L'ENVIRONNEMENT LEGAL DES SYSTEMES D'INFORMATION 22

TITRE 2 :
PRESENTATION DES CYCLES DE VIE DU SYSTEME D'INFORMATION DES RISQUES ET DES CONTROLES Y AFFERENTS 32
CHAPITRE 1: PRESENTATION DES CYCLES DE VIE ET DES METHODOLOGIES DE DEVELOPPEMENT D'UN SYSTEME D'INFORMATION 32
CHAPITRE 2 : IDENTIFICATION DES RISQUES ET DES CONTROLES LIES AUX CYCLES DE VIE DES SYSTEMES D'INFORMATION 37

CONCLUSION DE LA PREMIERE PARTIE 46

PARTIE II :
PROPOSITION D'UNE METHODOLOGIE POUR LA CONDUITE DES MISSIONS D'AUDIT INFORMATIQUE 48

INTRODUCTION DE LA DEUXIEME PARTIE 49

TITRE 1 :
LE PROCESSUS DE L'AUDIT INFORMATIQUE DANS LE CADRE DES MISSIONS D'AUDIT FINANCIER ET COMPTABLE 50
CHAPITRE 1 : PRESENTATION DE LA DEMARCHE DE L'AUDIT INFORMATIQUE DANS LE CADRE DES MISSIONS D'AUDIT FINANCIER ET COMPTABLE 50
CHAPITRE 2 : L'AUDIT DE LA FONCTION INFORMATIQUE (CONTROLES GENERAUX INFORMATIQUES) 60
CHAPITRE 3 : AUDIT DES APPLICATIONS INFORMATIQUES 72

TITRE 2 :
PROCESSUS DE L'AUDIT DANS LE CADRE D'AUTRES MISSIONS D'AUDIT INFORMATIQUE 87
CHAPITRE 1: PROPOSITION D'UNE APPROCHE D'AUDIT DE LA MISSION CONNEXE DU COMMISSAIRE AUX COMPTES RELATIVE A L'EXAMEN DU DOSSIER FINANCIER 88
CHAPITRE 2: PROPOSTION D'UNE METHODOLOGIE D'AUDIT DE LA SECURITE INFORMATIQUE 93

CONCLUSION DE LA DEUXIEME PARTIE 100
CONCLUSION GENERALE 101
BIBLIOGRAPHIE 105
PLAN DETAILLE 109
LEXIQUE DU SYSTEME D'INFORMATION 113
ANNEXES 122

INTRODUCTION GENERALE

1. L'enjeu économique lié à l'évolution et au rôle des systèmes d'informati un contexte de globalisation

1.1 Evolution des systèmes d'information

L'environnement actuel de l'entreprise est caractérisé par la globalisation des économies qui est facilitée par le développement accéléré des systèmes d'information. En effet, durant les vingt dernières années, ils ont connu des évolutions exponentielles grâce au développement technologique. Ainsi, nous avons observé notamment, l'explosion des micro-processeurs, le développement des réseaux, l'intégration des systèmes, l'ouverture des systèmes sur les partenaires de l'entreprise.

L'irruption de l'Internet a accéléré considérablement l'évolution des systèmes d'information, puisque son coût réduit et sa relative simplicité d'utilisation ont favorisé leur pénétration, notamment vers les petites entreprises et les consommateurs. L'économie moderne devient de plus en plus immatérielle.

Cette évolution vers la Société de l'Information n'aurait été facilitée que par le développement spectaculaire des technologies de l'information.

1.2 Rôle stratégique des systèmes d'information

Aujourd'hui, les systèmes d'information revêtent un caractère stratégique dans le monde des entreprises. En effet, les exigences de l'environnement (marchés financiers, clients, concurrence... etc.) imposent à celles-ci la performance et la réactivité. Ceci implique que le traitement de l'information soit rapide et pertinent.
Ainsi, il est primordial que les systèmes d'information permettent à l'entreprise d'une part, d'adapter en permanence sa structure aux exigences de son marché et, d'autre part, d'être en mesure, d'augmenter continuellement sa productivité.

C’est ainsi que les dirigeants des entreprises s’orientent de plus en plus vers des systèmes ouverts, modulaires, axés sur les besoins des clients et permettant la couverture de l’ensemble des besoins de l’entreprise.

2. Impacts des systèmes informatiques sur l’approche de l’audit financier

Les évolutions significatives de la réglementation, des référentiels comptables et des modes de fonctionnement des entreprises auxquelles nous avons assistées au cours de ces dernières années, ont fortement influencé la démarche de l’audit comptable et financier.

Afin de répondre aux nouvelles exigences imposées par cet environnement, l’auditeur devra revoir sa méthodologie d’audit et compléter sa formation dans le domaine de l’audit informatique de façon à prendre en considération les risques induits par les systèmes informatiques et leur impact sur le dispositif du contrôle interne.

En effet, l’ouverture et la complexité des systèmes peuvent engendrer des risques ayant des conséquences néfastes sur le bon fonctionnement de l’entreprise.

Pour faire face à ce nouveau contexte, les grands cabinets d’audit et de conseil ont adopté de nouvelles démarches d’audit qui reposent largement sur l’évaluation des risques et des contrôles informatiques. Ces nouvelles approches imposent aux auditeurs de comprendre, évaluer et tester le contrôle interne relatif à l’environnement de la fonction informatique et aux applications gérant les principaux processus des activités de l’entreprise.

3. Problématique et objectifs du présent mémoire

3.1 Problématique du mémoire

Le sujet du mémoire intitulé «proposition d’une méthodologie pour la conduite des missions d’audit informatique» est en relation directe avec les missions d’audit et de conseil de l’expert comptable.

La problématique réside dans le fait que :

- L'information comptable et financière est souvent issue des processus hautement informatisés et qu'il est par conséquent inconcevable de certifier les comptes sans auditer les systèmes informatiques ;
  En outre, les nouvelles réglementations exigent des auditeurs d'évaluer et de tester les procédures de contrôle interne y compris celles liées aux systèmes informatiques.
- Les systèmes informatiques induisent des risques spécifiques que l'auditeur doit prendre en considération dans sa démarche d'audit.

En effet, le recours aux technologies de l'information s'accompagne inéluctablement de nouveaux risques, parmi lesquels nous pouvons citer :

- L'ouverture des systèmes d'information aussi bien en interne à travers les outils d'Intranet qu'en externe à travers l'Internet ;
- L'absence de procédures de gestion et de maîtrise des risques liés à l'introduction des nouvelles technologies de l'information peut avoir des conséquences financières préjudiciables ;
- L'absence de politiques et de procédures relatives à la sécurité informatique ;
- La dépendance vis-à-vis des fournisseurs de technologie ;
- La refonte des processus suite à la mise en place de nouveaux systèmes informatiques peut affecter l'architecture des contrôles et leur capacité à couvrir les risques de l'entreprise.

Face à ce nouveau contexte, quel est l'apport de l'expert comptable ?

En effet, il sera confronté à la complexité des systèmes informatiques et aux risques qui leur sont liés. Il n'est donc pas seulement appelé à adapter sa démarche d'audit comptable et financier mais aussi à conseiller les clients en matière de gestion des risques et de mise en place des procédures de contrôle interne liées aux systèmes informatiques.

3.2 Objectifs

Les objectifs à atteindre par ce mémoire sont les suivants :

- Présenter une méthodologie claire permettant d'aider les professionnels à effectuer des missions d'audit informatique ;
- Présenter les bonnes pratiques en matière d'organisation de la fonction informatique et de management du système d'information, qui peuvent être utilisées comme un guide par les professionnels dans leurs missions de conseils en gestion des risques ou de mise en place des procédures de contrôle interne ;
- Permettre aux auditeurs financiers de comprendre les risques liés aux systèmes informatiques et de se familiariser avec la démarche de l'auditeur informatique devant leur permettre d'utiliser les résultats de ces travaux dans leur approche d'audit financier.

Sur le plan personnel, ce travail m'a permis d'approfondir mes connaissances dans un domaine stratégique qui implique nécessairement une mise à niveau du métier de l'expert comptable. En effet, celui-ci est amené de nos jours à développer une expertise dans ce domaine, afin d'élargir les champs de ses missions à l'audit et au conseil en système d'information et d'être en mesure de certifier les états de synthèse.

4. Démarche adoptée

De manière à atteindre les objectifs énoncés ci-dessus avec le maximum d'efficacité et de valeur ajoutée, la méthodologie adoptée s'articule autour des axes suivants :

- Une démarche pragmatique

Elle consiste à présenter une méthodologie pour la conduite des missions d'audit informatique, en mettant en évidence les bonnes pratiques en matière de contrôle des systèmes d'information, ainsi que les guides permettant la réalisation de ce type de mission notamment des guides spécifiques.

- Un plan structuré

Le plan de ce mémoire s'articule autour de deux grands volets :

1ère partie : La compréhension du cadre général de la fonction informatiq préalable nécessaire pour la réalisation des missions d'audit informatiq

Dans cette partie, l'attention sera portée sur :

- La compréhension du fonctionnement de la fonction informatique (son organisation, son contrôle interne et la gestion des cycles de vie des systèmes informatiques) ;
- La présentation de l'environnement légal de la fonction informatique ;
- La présentation des bonnes pratiques en matière de gestion et d'organisation de la fonction informatique, en s'appuyant sur les référentiels existants et sur l'expérience vécue ;
- La présentation sommaire des cycles de vie des systèmes informatiques ;
- L'identification des contrôles et des risques liés à la fonction informatique en s'appuyant également sur les référentiels existants et sur les expériences tirées des missions accomplies au sein du cabinet. Cette identification sera effectuée pour les différents cycles de vie des systèmes d'information.

2ème partie : Proposition d'une méthodologie pour la conduite des missions d'audit informatique.

Dans cette partie, l'accent sera mis sur :

- Le processus de l'audit informatique en tant que support aux missions d'audit comptable et financier ;
- La présentation des objectifs, des spécificités, des composantes, des phases et des outils de la démarche d'audit informatique.
- La démarche d'audit informatique dans le cadre de certaines missions spécifiques. L'accent sera mis sur les missions qui présentent un caractère obligatoire ou prioritaire pour le pilotage des systèmes d'information et la gestion des risques qui leur sont liés.

Il y a lieu de noter que nous avons joint en fin du présent mémoire, un lexique des principaux termes informatiques utilisés. Par ailleurs, nous tenons à préciser qu'actuellement les systèmes d'information des entreprises sont généralement informatisés. Ce sont ces systèmes automatisés auxquels nous faisons référence dans le présent mémoire. Les termes souvent utilisés dans notre étude sont soit les systèmes informatiques, soit les systèmes d'information (SI).

PARTIE I

LA COMPREHENSION DU CADRE GENERAL DE LA FONCTION INFORMATIQUE : UN PREALABLE NECESSAIRE POUR LA REALISATION DES MISSIONS D'AUDIT INFORMATIQUE

INTRODUCTION DE LA PREMIERE PARTIE

Le processus de libéralisation et de mondialisation des marchés entraîne une concurrence féroce sur les marchés. Ceci, amène les entreprises à maîtriser, entre autre, leur système d'information afin d'être réactives et d'être en mesure de jouer un rôle prédominant dans leurs marchés.

Face aux exigences de ce nouvel environnement, les structures des organisations notamment celles relatives à la fonction informatique, devraient évoluer de façon à permettre de raccourcir le cycle de leur processus et de réagir rapidement. Ces nécessités imposent également, une disponibilité de l'information en temps réel et une intégration des systèmes d'information et leur ouverture sur les partenaires de l'entreprise.

L'évolution et l'ouverture des systèmes sur les partenaires induisent de nouveaux enjeux et risques, ce qui pourrait se traduire par l'augmentation de la vulnérabilité des systèmes d'information. Par ailleurs, la mise en place des nouveaux systèmes informatiques intégrés et complexes s'accompagne par une refonte des processus de gestion des activités et des procédures de contrôle interne des entreprises.

Afin de prendre en considération les enjeux et les risques liés au développement des systèmes informatiques, les législateurs et les organismes professionnels ont réagi et ont adopté de nouvelles règles et normes.

Il est évident que la compréhension de l'organisation et de l'environnement légal de la fonction informatique, des cycles de vie des systèmes et des principaux risques qui y sont liés constituent un préalable nécessaire à l'accomplissement des missions d'audit informatique aussi bien dans le cadre des missions d'audit financier que des missions d'audit spécifique.

Cette partie sera donc consacrée à :

- L'environnement et l'organisation de la fonction informatique (titre 1) ;
- La présentation des cycles de vie du système d'information, des risques et des contrôles qui y sont liés (cf. titre 2).

TITRE 1 :
L’ENVIRONNEMENT ET L’ORGANISATION DE LA FONCTION INFORMATIQUE

CHAPITRE 1 : L’ENVIRONNEMENT ET L’ORGANISATION DE LA FONCTION INFORMATIQUE DE L’ENTREPRISE

L’objectif de ce chapitre est d’apporter des éléments de contexte général et de présenter l’organisation de la fonction informatique. Il sera consacré à la présentation des fonctions gravitant autour du système d’information et aux bonnes pratiques de leur organisation.

1. Rôle et caractéristiques des systèmes d’information

1.1 Rôle des systèmes d’information de gestion

Le système d’information d'une organisation est constitué d'un ensemble de moyens, de ressources, d'éléments organisés permettant de collecter, saisir, traiter, stocker et diffuser l'information. Cette dernière est nécessaire pour décider, agir, prévoir, contrôler et effectuer les activités d’une organisation.

L'amélioration de l'efficacité et de l'efficience des organisations est la préoccupation permanente des dirigeants des entreprises. Dans une économie qui se mondialise, où la concurrence devient de plus en plus féroce, les organisations cherchent à offrir davantage de services aux clients, l'information est de plus en plus une variable stratégique, essentielle et primordiale au processus de prise de décision.

Le système d'information est aujourd'hui au cœur de la création de valeur au sein des entreprises et peut constituer un avantage comparatif par rapport à la concurrence.

1.2 Caractéristiques des systèmes d'information

Actuellement, les dirigeants des entreprises sont soucieux de la rentabilité, de la capacité d'évolution, et de la fiabilité de leur système d'information. Ainsi, ils s'orientent vers des systèmes :

- Globaux devant avoir une large couverture fonctionnelle permettant de prendre en charge l'essentiel des processus et de centraliser l'ensemble des flux d'information. Ils permettront ainsi d'offrir des applications gérant les activités de l'entreprise et des outils de contrôle de gestion, de pilotage et d'aide à la décision ;
- Ouverts sur d'autres systèmes par le biais d'interfaces permettant la génération automatique des transactions et des écritures comptables, ainsi que l'échange des données informatisées avec l'ensemble des partenaires ;
- Modulaires avec une conception du système d'information selon le principe de modules métiers ;
- Orientés client permettant de disposer d'une vision globale de l'ensemble des informations des clients ;
- Fiables et sécurisés permettant de restituer des informations fiables et de protéger les données contre l'ensemble des risques pouvant menacer les systèmes d'information de l'entreprise.

2. Rôle et organisation de la fonction informatique

2.1 Rôle de la fonction informatique

Compte tenu de leur caractère stratégique, la fonction informatique doit jouer un rôle central dans le pilotage et la gestion des systèmes d'information. Elle doit notamment, assurer l'alignement de la stratégie informatique avec celle de l'entreprise.

Le rôle de la fonction informatique diffère selon la taille et le degré de maturité de l'organisation informatique. La maturité de l'organisation informatique peut être appréhendée à partir de deux aspects :

- L'aspect organisationnel : l'organisation informatique est considérée comme ayant atteint un degré élevé de maturité si d'une part, la relation entre l'informatique et les utilisateurs est régie par des contrats de services ou « Service Level Agreement - SLA » et si, d'autre part, les utilisateurs reconnaissent le rôle des directions des systèmes d'information (DSI) et s'impliquent dans les projets informatiques ;

- L'aspect fonctionnel et technologique : plus les systèmes d'information sont intégrés, ouverts sur les partenaires et utilisent les nouvelles technologies (Approche Clients Relationship Management - CRM, E-commerce, architecture client léger, Extranet… etc.), plus l'organisation est considérée comme ayant atteint un degré de maturité élevé.

Lors de ses missions d'audit et de conseil, l'expert comptable est appelé à évaluer cette maturité afin de comprendre le rôle et le positionnement de l'informatique au sein de l'entreprise, et de proposer des recommandations pratiques et adaptées au contexte de sa mission.

2.2 L'organisation de la fonction informatique

2.2.1 Structure de la fonction informatique

Afin d'accompagner le développement spectaculaire des systèmes informatiques grâce à l'utilisation des nouvelles technologies, les directions des systèmes d'information (DSI) ont dû s'adapter en élargissant les compétences de leurs ressources humaines et en se dotant d'organisations et d'outils appropriés.

En effet, l'organisation des DSI a évolué d'une architecture centralisée vers des structures plus étendues et ouvertes. La structure des DSI dépend des métiers de l'organisation et des technologies utilisées, du recours aux progiciels et des pratiques du management de l'entreprise.

Quelque soit la structure adoptée par l'entreprise pour cette fonction, deux activités principales néanmoins doivent être assurées à savoir :

- La gestion des opérations d'exploitation informatique ;
- La gestion des opérations relatives à l'acquisition, le développement et la maintenance des systèmes informatiques.

Généralement, la fonction informatique est organisée de la manière suivante :

a - Un directeur ou service informatique en charge de la supervision de la direction informatique,

b - une division ou service exploitation en charge des travaux d'exploitation des systèmes de production,

c - une division ou service études et développement en charge de la gestion des projets informatiques,

d - une division ou service systèmes en charge de la gestion et de la maintenance des systèmes informatiques.

Selon la taille de la direction des systèmes d'information et le degré de développement des systèmes informatiques de l'entreprise, nous pouvons trouver d'autres services comme par exemple :

- Le service télécommunication ;
- Le service assistance aux utilisateurs (HelpDesk) ;
- Le service administration des bases de données (DBA) ;
- Le service administration réseaux ;
- Le service administration de la sécurité informatique ;
- Le service assurance Qualité.

2.2.2 Les principales attributions de la direction des systèmes d'information

Les principaux objectifs assignés à la direction des systèmes d'information peuvent se résumer comme suit :

- Permettre à l'informatique de délivrer un bon niveau de service aux utilisateurs et de pouvoir répondre à leurs attentes (qualité, délais), en formalisant les relations et les responsabilités dans le domaine informatique des différents intervenants (personnel informatique, organisation, utilisateurs) ;
- Assurer un bon niveau de contrôle des opérations de la direction informatique, en formalisant les contrôles du personnel informatique et les tableaux de bord de la direction informatique ;
- Assurer la pérennité des opérations de la direction informatique, en formalisant les procédures informatiques.

Ainsi, la direction des systèmes d'information définit et met en œuvre les systèmes d'information, destinés au pilotage et à la gestion des différentes activités de l'organisation. A ce titre, elle est chargée de définir, de mettre en place et de gérer les moyens techniques nécessaires aux systèmes d'information et de communication, et de planifier leur évolution dans le cadre d'un schéma directeur. Elle définit et met en œuvre également les contrôles et les ressources informatiques (personnel, applications, technologie, utilitaires, données) qui permettent d'atteindre ses objectifs dans les domaines suivants :

- Le planning et l'organisation,
- L'acquisition et l'implémentation,
- L'exploitation et la maintenance,
- Le monitoring (le pilotage).

2.3 Principes de gestion et de contrôle interne relatifs à l'organisation de la fonction informatique

Avant d'aborder les principes du contrôle interne relatif à l'organisation de la fonction informatique, il est utile de rappeler ceux relatifs au contrôle interne des organisations d'une manière générale.

2.3.1 Rappel relatif au dispositif du contrôle interne

Nous rappelons ci-après d'une manière synthétique la définition et les composantes du contrôle interne :

Le système du contrôle interne selon les normes professionnelles

Au Maroc :

Le manuel des normes professionnelles marocaines en matière d'audit légal et contractuel élaboré par l'ordre des experts comptables a défini le contrôle interne comme suit :

« Le contrôle interne est constitué par l'ensemble des mesures de contrôle, comptable ou autre, que la direction définit, applique et surveille, sous sa responsabilité, afin d'assurer la protection du patrimoine de l'entreprise et la fiabilité des enregistrements comptables et des états de synthèse qui en découlent ».

Le contrôle interne ainsi défini, doit permettre d'obtenir l'assurance raisonnable que :

- Les opérations sont exécutées conformément aux décisions de la direction (système d'autorisation et d'approbation) ;
- Les opérations sont enregistrées de telle façon que les états de synthèse qui en découlent soient réguliers et sincères et donnent une image fidèle du résultat de l'exercice, de la situation financière et du patrimoine de l'entreprise (contrôles internes fiables lors du traitement des données et de l'élaboration des états de synthèse) ;

Les actifs de l'entreprise sont sauvegardés (séparation des tâches, contrôle physique sur les actifs, service d'audit interne, assurances, …etc.) ».

En France :

La norme 2.301 du CNCC (Conseil National des commissaires aux comptes) a défini le système du contrôle interne comme «l'ensemble des politiques et procédures mises en œuvre par la direction d'une entité en vue d'assurer dans la mesure du possible la gestion rigoureuse et efficace de ses activités. Ces procédures impliquent le respect des politiques de gestion, la sauvegarde des actifs, la prévention et la détection des irrégularités et inexactitudes, l'exactitude et l'exhaustivité des enregistrements comptables et l'établissement en temps voulu des informations financières ou comptables fiables. Le système de contrôle interne s'entend au-delà des domaines directement liés au système comptable. Il comprend l'environnement général du contrôle interne et les procédures de contrôle ».

Définition du contrôle interne selon le modèle COSO :

Le modèle COSO (Committee of Sponsoring Organizations) définit le contrôle interne comme suit :

« Globalement le contrôle interne est 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 d'objectifs entrant dans les catégories suivantes :

- Réalisation et optimisation d'opérations ;
- Fiabilité des informations financières ;
- Conformité aux lois et règlements en vigueur ».

Ce modèle distingue cinq niveaux de contrôle qui permettent d'atteindre les objectifs du contrôle interne cités ci-dessus. Ces niveaux sont résumés comme suit :

Niveau 1 : L'environnement de contrôle

Il constitue la base des autres éléments du contrôle interne. Il est déterminé par l'attitude et le comportement des dirigeants vis-à-vis du contrôle interne. Il couvre les domaines suivants :

- L'intégrité, l'éthique et la compétence du personnel ;
- Les responsabilités et les délégations du pouvoir ;
- La politique des ressources humaines.

Niveau 2 : L'évaluation des risques

Les risques inhérents au business et à l'organisation de l'entreprise peuvent l'empêcher de réaliser ses objectifs. Ainsi, elle doit disposer des mécanismes et des outils permettant d'identifier, d'évaluer et de gérer ces risques.

Niveau 3 : Les activités de contrôle :

Les activités de contrôle sont une partie intégrante de l'activité de l'entreprise. Elles sont définies comme l'application des normes et des procédures contribuant à réaliser les objectifs et à maîtriser les risques de l'entreprise.

Nous distinguons deux types de contrôle:

- Les contrôles de pilotage de l'activité : Ils comprennent les analyses effectuées par le management et les indicateurs de performance et de gestion liés aux activités de l'entreprise.
- Les contrôles d'application: Ils comprennent les contrôles de traitement des données, les contrôles physiques, la séparation des tâches et les confirmations externes.

Niveau 4: Information et communication

L'information revêt une importance capitale dans la mesure où sa qualité influence directement le processus de prise des décisions et des contrôles effectués.
En effet, afin de permettre au personnel d'assumer ses responsabilités, le management doit mettre à sa disposition des informations fiables et pertinentes.
Par ailleurs, la communication aussi bien interne qu'externe devra être suffisante et de qualité.

Niveau 5: Pilotage

Le management devra mettre en place des mécanismes et des outils de pilotage des activités de contrôle de façon à garantir son fonctionnement permanent ainsi que son alignement par rapport aux objectifs et aux risques de l'entreprise. En outre, il y a lieu de procéder périodiquement à l'évaluation du contrôle interne (auto-évaluation, audit interne…etc.).

Dans le contexte actuel, la mise en place d'un système de contrôle interne est une obligation légale qui incombe aux dirigeants de l'entreprise. En effet, ces derniers doivent définir leurs objectifs, identifier les risques du business et mettre en place un système de contrôle interne. Le modèle COSO permet de décrire les composantes d'un bon système de contrôle.

Ce modèle est devenu la référence des cabinets d'audit et de plusieurs organismes professionnels à travers le monde. Ainsi, il a été retenu par le législateur Américain dans la rédaction de la loi Sarbanes oxley (exposée dans le chapitre qui suit) comme un modèle de référence du contrôle interne. Certains cabinets internationaux l'ont également intégré dans leur démarche d'audit pour la documentation du contrôle interne.

2.3.2 Le dispositif du contrôle interne relatif à l'organisation et le pilotage de la fonction informatique

Les procédures de contrôle relatives à l'organisation et au pilotage de la fonction informatique ont pour but de gérer les risques qui menacent la réalisation des objectifs de la fonction informatique. Parmi les facteurs qui peuvent engendrer ces risques nous pouvons citer:

- Mauvais environnement de contrôle;
- Faible dispositif du contrôle interne;
- Principe de séparation des tâches non respecté;
- Absence d'analyse des risques ;
- Absence de système de gestion des risques ;
- Absence de politiques relatives à la gestion des applications ;
- Les rôles et les responsabilités des utilisateurs et des informaticiens ne sont pas clairement définis ;
- Inexistence de manuel d'administration des systèmes et des applications ;
- Absence ou non mise à jour des guides d'utilisation des systèmes et des applications ;
- Incohérence des accès accordés avec le principe de séparation des tâches ;
- Absence de définition d'une charte de service entre les utilisateurs et l'informatique.

2.3.2.1 Les bonnes pratiques en matière de pilotage de la fonction informatique

Les principaux instruments de suivi et de pilotage de la fonction informatique sont le comité informatique, les tableaux de bord et la charte de service (Service Level Agreement).

Comité directeur informatique

Un comité directeur informatique est un instrument de gestion de haut niveau qui permet de s'assurer que la mission du département informatique est en harmonie avec les objectifs de l'entreprise.

L'objectif d'une telle entité est de pouvoir réunir les membres clés de l'organisation afin notamment de :

- Revoir et valider la stratégie informatique à court et à long terme ;
- Fixer les priorités en matière de développements informatiques ;
- Procéder à l'arbitrage en matière des demandes de maintenance importante ;
- Suivre l'avancement des différents grands projets ;
- Définir les grandes lignes d'une stratégie en matière de sécurité.

Ce comité pourrait se réunir par exemple semestriellement, et chaque réunion devrait faire l'objet d'un compte rendu formalisé distribué à la Direction Générale ainsi qu'aux différents responsables des départements. Ce compte rendu pourrait contenir :

- L'ordre du jour du comité ;
- Les différents points abordés ;
- Les décisions prises ;
- L'ordre du jour du comité suivant.

Les tableaux de bord

La DSI devra mettre en place des indicateurs et des outils de suivi et de mesure des performances des activités et des coûts des différentes fonctions informatiques. Les indicateurs d'évaluation des performances pourront être établis en fonction de plusieurs axes d'analyse (exemples : Contribution de la fonction informatique à la stratégie de l'entreprise, maîtrise des coûts, productivité, disponibilité, …etc.).

A titre d'exemple d'indicateurs, nous pouvons citer :

- Le taux d'avancement des projets ;
- La fréquence de maintenance corrective des applications ;
- Le turn over ;
- La part de la sous-traitance ;
- Le taux d'utilisation des applications et des systèmes ;
- Les incidents ;
- Le taux de disponibilité des applications, des systèmes et des réseaux ;
- Le nombre d'incidents par nature et par criticité ;
- Le taux de réalisation des budgets ;
- Le degré de satisfaction.

La charte de service

Une charte de service (Service Level Agreement - SLA) est un contrat de service entre les services informatiques et les utilisateurs. Ce contrat devra être établi pour chacune des prestations assurées par la DSI. Il doit également prévoir les outils de mesure et de suivi de la satisfaction des utilisateurs, notamment en ce qui concerne :

- La disponibilité des systèmes et le temps de réponse des applications ;
- La qualité du support utilisateur ;
- La continuité d'exploitation en cas de sinistre.

2.3.2.2 Le dispositif du contrôle interne relatif à l'organisation de la fonction informatique

Afin que l'informatique soit maîtrisée, la Direction Générale et les directions utilisatrices devront être impliquées dans le développement, la gestion, la mise en œuvre et le contrôle des systèmes informatiques. Ainsi, la DSI devrait être confiée à une personne ayant l'expérience et les compétences requises. Elle doit être rattachée à la Direction Générale, associée à la stratégie de l'entreprise et membre du comité informatique. Ses performances devront être régulièrement suivies et évaluées.

Il est également, recommandé de désigner un membre du directoire ou du conseil d'administration qui sera responsable du suivi et du contrôle des activités de la fonction informatique.

Les principales bonnes pratiques relatives au dispositif de contrôle interne de la fonction informatique peuvent se résumer comme suit :

- La mise à la disposition de la DSI du personnel adéquat compte tenu des missions assignées et des systèmes et technologies utilisés ;
- Les applications critiques doivent avoir un support suffisant (au moins deux personnes ayant une bonne connaissance des systèmes) ;
- La mise en place d'un plan de remplacement du personnel clé ;
- La définition et la communication d'une manière claire des rôles et des responsabilités du staff. Il est à noter que dans les organisations d'une certaine taille un organigramme doit être mis en place ;
- La désignation d'un responsable des questions et des problèmes de la sécurité ;
- La formalisation et la documentation des procédures informatiques ;
- La formation du staff de la fonction informatique sur les métiers de l'entreprise, les procédures et les technologies utilisées ;
- L'implication des utilisateurs dans le développement et la mise en œuvre des systèmes informatiques ;
- L'utilisation d'une méthodologie rigoureuse pour le développement, la mise en service des systèmes et la documentation des applications ;
- L'existence et l'application des procédures de modification des programmes ;
- L'implication de la fonction dans les projets informatiques ;
- L'existence de procédures formalisées et communiquées aux personnes concernées ;
- La séparation des tâches entre les fonctions de spécifications fonctionnelles, de développement des programmes, tests, mise en production, exploitation des applications, autorisation des transactions et de surveillance des données.

Après avoir passé en revue le rôle des systèmes d'information, l'organisation de la fonction informatique ainsi que les bonnes pratiques de contrôle interne qui y sont liées, il convient d'examiner l'environnement légal des systèmes informatiques.

CHAPITRE 2 : L'ENVIRONNEMENT LEGAL DES SYSTEMES D'INFORMATION

Face à l'évolution technologique et informatique, en plus de la réglementation existante, de nouvelles dispositions législatives sont apparues et de nombreuses cellules de réflexion ont été créées, à ce sujet, dans le cadre d'organismes professionnels. A cet effet, nous allons essayer , tout au long de ce chapitre, de comparer les réactions au Maroc par rapport à celles d'autres pays (dont, essentiellement, la France).

1. LA REGLEMENTATION COMPTABLE ET FISCALE

1.1 Au Maroc

1.1.1 La réglementation comptable

La législation marocaine ne prévoit pas des dispositions spécifiques relatives aux systèmes comptables informatisés, à l'exception de quelques dispositions implicites contenues dans les textes fiscaux, le code du commerce, la loi 9-88 relative aux obligations comptables des commerçants et le CGNC.

1.1.2 La réglementation fiscale

Les textes relatifs à l'impôt sur les sociétés (IS), la Taxe sur la valeur ajoutée (TVA) et l'impôt général sur les revenus (IGR) ont imposé aux contribuables un certain nombre d'obligations comptables. Ces obligations relatives à l'organisation et la conservation des documents comptables ont pour objectif de permettre à l'administration fiscale le droit de contrôle et de communication prévu par la loi.
En effet, les contribuables sont dans l'obligation de tenir un certain nombre de livres comptables quelque soit le système choisi (système classique, centralisateur ou informatique).

Dans le cas où la comptabilité serait tenue par des moyens informatiques, le contribuable devrait prévoir les dispositions permettant à l'administration fiscale d'exercer son droit de contrôle.
Il y a lieu de noter qu'en vertu des dispositions fiscales citées ci-dessus, les documents comptables et les pièces justificatives doivent être conservés pendant une période de dix ans.

1.2 En France

Contrairement à son homologue Marocain, le législateur français a mis à niveau sa réglementation de façon à prendre en considération les spécificités de l'environnement informatique des entreprises. Cette nouvelle réglementation prévoit de mettre en place de nouvelles modalités de transmission, de conservation et de vérification des informations communiquées à l'administration fiscale et des comptabilités informatisées en général.
Les principales dispositions fiscales prévues concernent essentiellement les aspects suivants :

- La documentation technique permettant d'une part, de comprendre le système d'information utilisé au cours de la période de contrôle et, d'autre part, de transcrire de manière précise les règles de gestion des données et des fichiers qui ont un impact direct sur la formation du résultat comptable et fiscal et des diverses déclarations prévues par la législation fiscale.

- La conservation sur support informatique des données et des traitements liés à la formation des résultats comptable et fiscal et des diverses déclarations prévues par la législation fiscale pendant une période de 3 ans.

2. LE CADRE JURIDIQUE GENERAL

La compréhension du cadre juridique de la fonction informatique constitue un préalable nécessaire pour la réalisation d'une mission d'audit informatique. Notre propos au niveau de cette partie est de présenter l'essentiel des textes applicables et

projets relatifs au domaine informatique et qui peuvent avoir un impact sur les travaux d'audit de la fonction informatique.

2.1 – Le cadre juridique au Maroc:

Les seules véritables innovations en la matière constituant l'arsenal juridique marocain, sont les suivantes :

La loi n° 2-00 du 15 février 2000

Relative aux droits d'auteur et droits voisins, cette loi consacre en effet le droit d'auteur et les sanctions civiles auxquelles les contrevenants à ce droit s'exposent (articles 62 et 64 de la loi 2-00). Par ailleurs, la protection des entreprises est assurée par la loi 11-99 du 25 juillet 1993 formant code pénal. Il y a lieu de noter que dans le cadre de l'accord du libre échange conclu entre le Maroc et les Etats-Unis d'Amérique (USA), la réglementation relative aux droits d'auteurs a été complétée et modifiée par la loi n° 34-05 de façon à la mettre en harmonie avec les standards internationaux.

Projets de lois réglementant le E-commerce

Des projets de loi visant à réglementer les aspects liés au commerce électronique ont été proposés par un comité interministériel qui avait été institué à cet effet. Ces projets de lois ont été traités dans le mémoire intitulé «Incidence de la présence d'un site de commerce électronique sur la mission d'audit» présenté par M.Adnane LOUKILI pour l'obtention du diplôme national d'expert comptable.

2.2 – Le cadre juridique en France :

Contrairement au Maroc, la France a adopté des lois réglementant les aspects liés à l'utilisation des nouvelles technologies de l'information. Les principales lois ont porté sur :

- La protection des données relatives à la vie privée des personnes ;
- La protection des droits d'auteurs en matière de production des logiciels ;
- La sanction des fraudes informatiques : Les délits sanctionnés vont de l'accès non autorisé aux informations à la falsification des données informatiques ;
- La protection de la transmission des données ;
- La reconnaissance de la signature électronique en tant que moyen de preuve ;

- La définition des conditions de fiabilité des procédés de signature électronique ;
- La possibilité de remplacer les déclarations écrites par les messages électroniques à condition de conclure un contrat qui précise les règles en matière de preuve.

3. Réglementation spécifique aux dispositifs de contrôle interne liés au rep financier

Suite aux scandales financiers qui ont secoué le marché à l'échelle mondiale, notamment aux Etats unis, les législateurs Américains et Européens ont promulgué des lois visant à rassurer les marchés financiers sur la fiabilité des reportings financiers : Sarbanes Oxley (SOX) et la loi sur la sécurité financière (LSF).
En revanche, il n'existe toujours pas au Maroc une réglementation dans ce domaine à l'exception des circulaires émises par Bank Al Maghrib et le code des assurances.

3.1 Revue du système d'information dans le cadre de la revue par le CAC du dossier financier établi par les compagnies d'assurance

L'article 245 du code des assurances a rendu obligatoire le contrôle par les CAC du Compte Rendu Statistique et Financier préparé par les compagnies d'assurance, appelé communément le « Dossier Financier » et transmis à la Direction des Assurances et de la Prévoyance Sociale (DAPS).

Le code des assurances n'a pas défini l'étendue de la mission du CAC relative à l'examen du « Dossier Financier ». Une commission ad hoc, composée des membres de l'ordre des experts comptables et des représentants de la DAPS et de la Fédération des assurances a délimité la nature et le contenu de cette mission. Ainsi, elle a été définie comme étant une mission connexe de revue du Dossier Financier.

Il y a lieu de souligner que cette mission connexe du CAC est en train d'être redéfinie afin de l'élargir à l'ensemble du dispositif du contrôle interne afférent au Dossier Financier.

3.2 Circulaire n° 6/G/2001 de Bank Al Maghrib relative au contrôle interne des Etablissements de crédit

Afin de renforcer le dispositif du contrôle interne des établissements de crédit, BANK AL-MAGHRIB a émis la circulaire n°6/G/2001. Celle-ci constitue un complément au contrôle prudentiel quantitatif, fondé sur les limites de surveillance imposées par les

ratios prudentiels (coefficient de solvabilité, coefficient de division des risques, coefficient de liquidité, règles de classification et de provisionnement des créances en souffrance).

La circulaire n° 6 a imposé aux établissements de crédit la mise en place d'un système de contrôle interne visant à maîtriser les risques qu'ils encourent. Elle a ainsi précisé, les modalités et les règles minimales que ces derniers doivent observer dans ce domaine.

Elle a également énuméré certaines catégories de risques liées aux activités des établissements de crédit et a exigé qu'ils soient suivis d'une manière permanente.

En ce qui concerne, la gestion des risques informatiques, elle a prévu dans son article 63 que le dispositif de contrôle du risque informatique doit assurer un niveau de sécurité conformément aux normes technologiques et aux exigences du métier.

Les règles à observer en matière de gestion du risque informatique, sont stipulées dans les articles 63,64 et 65 de la circulaire n° 6/G/2001 et se résument comme suit :

- **Documentation**

  Les supports de l'information et de la documentation relatifs à l'analyse et à l'exécution des programmes doivent être conservés dans des conditions présentant le maximum de sécurité contre les risques de détérioration, de manipulation ou de vol (art 63).

- **Niveau de sécurité et contrôles**

  Les systèmes informatiques doivent faire l'objet de contrôles périodiques portant sur :

  - Le niveau de sécurité qu'ils offrent (art.65) ;
  - L'existence de procédures de secours informatique (back-up) permettant d'assurer la continuité de l'exploitation en cas de difficultés graves de fonctionnement (art 64).

3.3 La loi Sarbanes-Oxley (SOX)

Cette loi vise à rassurer les marchés financiers quant à la sincérité de l'information financière. Elle s'applique aux sociétés cotées aux Etats-Unis. Elle comprend 11 thèmes dont :

- La responsabilité d'entreprise,
- L'amélioration de l'information financière.

Elle impose aux dirigeants de nouvelles obligations relatives au contrôle interne afférent au processus de production du reporting financier. Ainsi, l'évaluation du contrôle interne par les dirigeants est effectuée chaque année, sous leur responsabilité. Ils doivent également certifier que des procédures et des contrôles relatifs à l'information publiée ont été définis, mis en place et maintenus, et que l'efficacité de ces procédures et de ces contrôles a fait l'objet d'une évaluation.

Cette évaluation doit être revue par les auditeurs qui doivent produire une attestation à ce sujet.

En cas de non-respect de la loi, des peines sont prévues pouvant aller jusqu'à 20 ans d'emprisonnement et USD 20 millions d'amende.

Afin de répondre à ces nouvelles obligations, les dirigeants doivent mettre en place :

- Un système de contrôle interne,
- Un processus permettant de documenter les procédures de contrôle, et d'évaluer leur efficacité et leur fonctionnement, de documenter les faiblesses et enfin de mettre en place un plan d'action visant à corriger les faiblesses identifiées et améliorer le dispositif du contrôle interne.

3.4 Loi du 1er août 2003 sur la sécurité financière (LSF)

A l'instar du législateur Américain, la France a promulgué la loi relative à la sécurité financière dont le but est de protéger les épargnants et les investisseurs. Ainsi, elle

impose de nouvelles obligations pour les entreprises et les commissaires aux comptes. Les principales dispositions de cette loi sont relatives à :

- L'indépendance des commissaires aux comptes et à la communication sur le contrôle interne ;
- La responsabilité des dirigeants en matière de contrôle interne.

Contrairement à la loi Américaine, la LSF n'a pas clairement défini le périmètre du contrôle interne ni le référentiel à utiliser pour le documenter.

4 - Les principales positions des organismes professionnels :

Nous allons examiner au niveau de cette section les principales réflexions nationales et internationales :

4.1 - Les normes marocaines

Selon la norme 2102 du manuel marocain des normes d'audit légal et contractuel :

« L'évaluation du contrôle interne d'un système de traitement informatisé de l'information financière est effectuée selon une démarche en deux parties telle que décrite ci-dessous :

- l'évaluation du contrôle interne de la «fonction informatique » (c'est-à-dire, l'ensemble formé par le service informatique et par les utilisateurs dans leurs relations avec le service) qui a pour objectif de s'assurer que le système fonctionne de manière à garantir :
    - la fiabilité des informations produites,
    - la protection du patrimoine,
    - La sécurité et la continuité des travaux.
- l'évaluation du contrôle interne d'un système ou d'une application où sera considérée plus particulièrement :

. Les contrôles sur la préparation et la saisie des données, aussi bien au niveau des services utilisateurs qu'au niveau informatique ;
. Les contrôles sur l'exploitation : prévention contre des erreurs et des fraudes pendant le traitement ;
. Les contrôles destinés à s'assurer de l'intégrité, de l'exactitude, et de l'autorisation des opérations à enregistrer ;
. Le maintien du chemin de révision (ou système de référence) ;
. La qualité de la documentation ;
. Les modifications intervenues d'un exercice à l'autre dans les programmes, notamment pour les méthodes d'enregistrement et d'évaluation. ».

4.2 - Les réflexions internationales

4.2.1 - Les réflexions de l'IFAC (International Federation of Accountants)

L'IFAC, qui est une référence en matière de normalisation des référentiels d'audit, a élaboré plusieurs normes relatives à l'audit financier dans un environnement informatisé. Parmi celles-ci, nous pouvons citer :

- La norme Internationale relative à l'audit dans le contexte d'un système d'information informatisé,
- La directive Internationale d'Audit relative à un système d'information fondé sur un micro- ordinateur autonome,
- La directive Internationale d'Audit relative à un système d'information fonctionnant en réseau et/ou en temps réel,
- Directive Internationale d'Audit relative à un système à bases de données,
- Directive Internationale d'Audit relative à l'utilisation des techniques d'audit assistées par ordinateur.

4.2.2 - Les réflexions du Conseil National des Commissaires aux Comptes (CNCC) : En France

Le CNCC soucieux de la qualité de l'audit légal effectué par les commissaires aux comptes, a publié plusieurs normes, avis et guides relatifs à l'audit dans un environnement informatisé. Ces publications ont porté sur plusieurs sujets dont notamment la sécurité informatique, le commerce électronique, l'échange des données informatisées et l'internet.

4.3 - Autres réflexions : ISACA

L'ISACA (Information system audit and control association) est une association considérée comme le normalisateur de référence en matière d'audit informatique. Elle a élaboré des standards et des guides d'audit informatique. Les standards de l'ISACA ont porté sur la responsabilité de l'auditeur, les règles de son indépendance, le code de conduite professionnel qu'il doit respecter lors de ses missions d'audit informatique, ainsi que les connaissances et les compétences qu'il doit avoir et maintenir à travers la formation continue. Par ailleurs, l'ISACA a défini des normes de travail relatives à la planification, l'exécution et la finalisation des missions d'audit informatiques.
Elle a également développé le COBIT qui constitue un référentiel international de gouvernance, de contrôle et de l'audit de l'information et des technologies associées. Il a été conçu à partir des meilleures pratiques mondiales en audit et en maîtrise des systèmes d'information. Il est destiné à la fois à la Direction d'entreprise, aux utilisateurs et aux auditeurs.

Il comprend quatre domaines : 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.

A travers cette étude sommaire relative au cadre légal des systèmes informatiques, nous constatons l'intéressement aussi bien pour les instances législatives que les organismes professionnels.

Au Maroc, et au niveau réglementaire, nous remarquons un intéressement du Gouvernement à mettre en place une réglementation relative aux nouvelles technologies. Certainement, il y a encore beaucoup à faire dans ce domaine mais les projets de lois proposés visent notamment, à combler le vide constaté.

Au niveau des organismes professionnels, nous constatons une mise à jour des lignes directrices des normes d'audit. Ceci dénote de l'importance de l'enjeu pour l'expert comptable. En effet, ce dernier doit dans sa démarche d'audit effectuer les diligences nécessaires afin de s'assurer du respect des dispositions réglementaires relatives au domaine informatique.

TITRE 2

PRESENTATION DES CYCLES DE VIE DU SYSTEME D'INFORMATION DES RISQUES ET DES CONTROLES Y AFFERENTS

CHAPITRE 1: PRESENTATION DES CYCLES DE VIE ET DES METHODOLOGIES DE DEVELOPPEMENT D'UN SYSTEME D'INFORMATION

L'objectif de ce chapitre est de comprendre les phases du cycle de vie d'un système d'information afin de faciliter l'identification des contrôles et des risques y afférents et qui seront abordés dans le chapitre 2 qui suit.

1. LE CYCLE DE VIE D'UN SYSTEME D'INFORMATION

Avant de faire la description des phases du cycle de vie d'un système d'information il est important de faire un rappel sur la planification stratégique qui constitue un préalable à la naissance d'un système d'information.

Planification stratégique

L'objectif principal de cette étape est de définir globalement le système d'information cible de l'organisation et les moyens pour sa réalisation.
Afin d'atteindre cet objectif, il y a lieu d'analyser la situation actuelle, de définir les besoins futurs en fonction des orientations générales du management de l'entreprise.
Le principal document issu de cette étape est le plan stratégique ou le schéma directeur.
Ce plan stratégique doit définir les projets, les priorités et les actions à mener à court, moyen et long terme.
Le plan stratégique informatique, qui assure l'alignement de la stratégie des systèmes d'information avec celle de l'entreprise, devrait être approuvé par la Direction Générale ou par un comité de direction représentant de l'ensemble des utilisateurs.

1.1 Description des phases des cycles de vie d'un système d'information

Pour chacune des étapes de chaque phase du cycle de vie d'un système d'information, nous allons résumer les objectifs, la démarche à suivre ainsi que les documents ou produits issus de l'étape :

1.1.1 Phase de l'étude de faisabilité

L'objectif de cette étape est d'étudier la faisabilité technique et organisationnelle du système d'information à développer ou à acquérir et d'analyser sa rentabilité économique.

A l'issue de cette étape, un document d'étude de la faisabilité devrait être établi.

1.1.2 Phase de développement

Elle comprend les étapes de conception, de réalisation des programmes et de mise en œuvre.

1.1.2.1 Etape de Conception

Cette étape comprend deux activités principales :

- **Analyse fonctionnelle**

Les principaux objectifs de l'analyse fonctionnelle sont de spécifier les solutions retenues par domaine fonctionnel, obtenir un consensus entre les utilisateurs et les informaticiens et affiner la charge et le planning de la suite des travaux.

La démarche à suivre comprendrait notamment la description exhaustive et détaillée de la solution retenue, l'organisation des circuits d'information et les traitements à effectuer (contrôles, calculs, décisions). A l'issue de cette étape, un cahier des charges et des spécifications fonctionnelles devrait être établi.

- **Analyse technique**

Les principaux objectifs de l'analyse technique sont la préparation de la programmation, l'établissement du plan de test et la planification de la programmation.

Durant cette phase, l'architecture des programmes devrait être décrite dans des termes compréhensibles par les informaticiens chargés de la programmation.

A l'issue de cette étape, les principaux documents à établir sont : les spécifications techniques, le dossier de programmation et le plan des tests (Définition des phases, calendrier, responsabilités, standards de documentation…etc.).

1.1.2.2 Etape de réalisation des programmes

Le principal objectif de cette étape est de produire le code (programme) et la documentation associés aux spécifications tout en garantissant les critères de qualité exigés.

Lors de cette étape, les programmes devraient être testés (recettes fonctionnelle et technique) et documentés conformément aux standards requis. En outre, il y a lieu d'établir des guides d'installation, d'exploitation et d'utilisation.

1.1.2.3 Etape de mise en œuvre

Les principaux objectifs de cette étape sont la définition de l'organisation des postes et des procédures de travail, la formation du personnel à l'accomplissement de ses nouvelles tâches, la transformation des données existantes dans le format attendu par les nouveaux programmes et le lancement de la mise en production des nouveaux programmes.

Lors de cette étape, il y a lieu de décrire les fonctions des services et des postes de travail ainsi que les procédures de traitement. Par ailleurs, le plan et les supports de formation devraient être préparés et exécutés. Enfin, les travaux d'ordonnancement et les travaux nécessaires au changement du système ainsi que leur exécution devront être effectués.

A l’issue de cette étape, les principaux documents à produire sont: les fiches de poste, le manuel des procédures, le plan de formation et le plan de lancement.

1.1.3 Phase d’exploitation

L’exploitation a pour objectif d’assurer le bon fonctionnement des machines, des périphériques, des réseaux et des programmes.

Pour ce faire, il y a lieu de définir et mettre en œuvre une politique adéquate de gestion des moyens techniques et des incidents d’une part, et des procédures documentées d’exploitation des programmes d'autre part.

1.1.4 Phase de maintenance

Les principaux objectifs de la maintenance sont la correction des erreurs, l’amélioration des performances des programmes et la réalisation des modifications demandées par les utilisateurs.

La démarche à suivre pour la maintenance des programmes est similaire à celle des étapes de développement mentionnées ci-dessus. Il faudrait veiller, lors de cette étape, à la mise à jour de la documentation des programmes modifiés.

2. METHODES DE CONCEPTION ET DE DEVELOPPEMENT DES SYSTEMES D’INFORMATION

Les méthodologies de développement des systèmes d’information s’inscrivent toutes dans l’ingénierie des systèmes (system engineering). Celles-ci comprennent non seulement l’analyse, le design et la programmation relatifs au développement d’un logiciel, mais aussi, la définition des postes de travail et des processus de façon à faciliter l’implémentation des solutions développées. En effet, la mise en place des nouveaux systèmes s’accompagne le plus souvent par la refonte des processus.

Il y a lieu, de faire une distinction entre une méthodologie et un modèle de développement. La première concerne la définition des étapes et des tâches de développement ainsi que la gestion des projets. En revanche, le modèle de développement concerne les éléments relatifs au développement du logiciel (langage de développement et le détail technique touchant le matériel informatique).

Par ailleurs, il existe une panoplie de méthodologies pour concevoir, développer et mettre en œuvre un système d'information. Dans le cadre de ce mémoire, nous n'allons pas aborder ces différentes méthodes.

CHAPITRE 2 : IDENTIFICATION DES RISQUES ET DES CONTROLES LIES AUX CYCLES DE VIE DES SYSTEMES D'INFORMATION

Après avoir décrit les cycles de vie des systèmes et synthétisé les bonnes pratiques y afférentes, il est nécessaire pour l'auditeur de comprendre les risques et les contrôles qui y sont liés.

1 LES RISQUES LIES AUX CYCLES DE VIE DES SYSTEMES D'INFORMATION

Préalablement à la présentation des risques liés aux cycles de vie des systèmes d'information, il est utile de rappeler la définition du risque et le facteur de risque.

1.1 Définition du risque

Le risque peut être défini comme « un péril mesurable visant des biens ou des activités précis aux conséquences économiques dommageables » (Jacques Charbonnier)

Le risque informatique est défini comme la possibilité d'un événement provoquant une réduction de l'adéquation aux besoins ou de l'efficacité/ performance ou de la fiabilité/ sécurité ou du niveau de ressources, ce qui pourrait induire la non réalisation d'un objectif de l'entreprise ou de l'une des fonctions de celle-ci.

1.2 Facteur de risque

Le facteur de risque est une cause de vulnérabilité due à une faiblesse du contrôle interne (faiblesse du processus de gestion, absence de politique de sécurité, absence de politique informatique…etc.). Le risque informatique peut avoir un impact fonctionnel (conséquence sur le fonctionnement du système d'information) ou financier.

Dans ce mémoire, le mot « risque » est utilisé par simplification à la place de facteur de risque. Les facteurs de risque ainsi que les mesures de protection proposées pour y remédier ont été développés dans le mémoire de M.Omar SEKKAT intitulé « Le rôle

de l’expert-comptable face aux risques de sécurité micro-informatique dans les PME - proposition d’une démarche ». Comme cela a été demandé par le jury qui a validé la notice du présent mémoire, nous allons nous limiter à rappeler les principaux facteurs de risque liés au cycle de vie du système d’information et aux applications informatiques.

1.3 Les risques liés au cycle de vie du système d’information

1.3.1 Risques liés à la planification

Les principaux risques associés à la planification peuvent se résumer comme suit :

- Non prise en compte de la stratégie de l’entreprise;
- Absence d’une stratégie globale de conception et de développement ou d'acquisition du système d’information;
- Non alignement de la stratégie du système d’information à celle de l’entreprise;
- Non implication du top management dans la définition de la stratégie, la conception, le développement et l’acquisition des systèmes informatiques;
- Absence d’études de rentabilité et de faisabilité des systèmes informatiques acquis ou développés;
- Absence de plan informatique;
- Absence de suivi des projets informatiques;
- Processus d’établissement des priorités non défini ;
- Processus de décision non documenté.

1.3.2 Risques liés au développement et à la mise en service des systèmes informatiques

Les principaux risques associés au développement se résument comme suit :

- Gestion de projet déficiente;
- Objectifs et périmètre du projet mal définis;
- Absence de méthodologie de développement ;
- Inadaptation des méthodes, des techniques et des outils utilisés;
- Dérapage au niveau des coûts et des délais;

- Faible adéquation des solutions développées par rapport aux besoins des utilisateurs;
- Analyse insuffisante dans la phase de conception;
- Absence des tests utilisateurs des applications développées;
- Formation insuffisante des utilisateurs;
- Documentation insuffisante des solutions développées;
- Absence de tableaux de bord et d'outils de suivi des projets de développement.

1.3.3 Risques liés à la mise en service

Les principaux risques associés à la mise en service d'un système d'information peuvent se résumer comme suit :

- Communication et coordination déficientes entre exploitation et études;
- Absence de séparation des tâches entre études et exploitation;
- Documentation technique insuffisante;
- Tests exécutés sans le recours à une méthodologie appropriée;
- Absence de plan de reprise des données;

1.3.4 Risques liés à l'exploitation

Les principaux risques associés à l'exploitation peuvent être résumés comme suit :

- Absence de procédures formalisées de gestion de l'exploitation;
- Absence de tableaux de bord et d'outils de suivi de l'exploitation;
- Programmes exécutés avec les mauvaises données;
- Programmes non exécutés;
- Programmes exécutés deux fois;
- Programmes exécutés dans le mauvais ordre;
- Exécution non autorisée des programmes (fraude);
- Répétition d'erreurs de traitement;
- Restauration incorrecte des fichiers après incidents.

1.4 Gestion des risques

Le développement des systèmes des technologies de l'information a permis aux organisations d'avoir de grandes possibilités de traitement, de stockage et de communication des informations. Toutefois, l'ouverture des systèmes sur l'environnement de l'entreprise les a rendus plus vulnérables aux accidents et malveillances (externes et internes).

Il existe deux types de risques:

Les risques physiques (incendies, dégâts des eaux, vols, …etc.);

Les risques logiques (virus, piratage, altération ou destruction de données, …etc.).

La survenance de ces risques peut avoir des conséquences lourdes sur les entreprises (perte de business suite à l'indisponibilité des systèmes, coût financier lié aux dégâts causés aux systèmes). C'est pour cela que la protection des systèmes est devenue une préoccupation majeure des dirigeants des entreprises.

Les politiques de sécurité à mettre en place doivent être en mesure de protéger les ressources sensibles de l'entreprise en prenant en considération les contraintes techniques et organisationnelles.

Les mesures de sécurité et de protection des systèmes informatiques ont été développées par M.Omar Sekkat dans le mémoire précédemment cité. Comme cela a été demandé par le jury qui a validé la notice de ce mémoire, nous n'allons pas traiter les mesures de gestion des risques. En revanche, et conformément aux recommandations du jury, nous allons nous focaliser sur la démarche de l'audit de la sécurité informatique. Ainsi, un chapitre lui sera consacré dans la deuxième partie de ce mémoire.

2 CONTROLES LIES AUX CYCLES DE VIE DES SYSTEMES D'INFORMATION

La présentation des bonnes pratiques en matière de contrôle interne relatif aux phases du cycle de vie des systèmes d'information, sera limitée principalement aux contrôles usuels et pertinents. Elle couvrira les contrôles relatifs aux aspects suivants:

- Le développement et la mise en œuvre des applications informatiques;
- La gestion des modifications des programmes et des applications;
- L'acquisition et la sélection des progiciels;
- La gestion des opérations d'exploitation informatique;
- Les procédures utilisateurs;
- Le plan secours.

2.1 Les contrôles relatifs au développement et à la mise en œuvre des applications informatiques

Afin de mieux piloter les projets informatiques, il est recommandé de mettre en place les pratiques suivantes:

- Une gestion appropriée des projets informatiques en fonction de leur importance en prévoyant les ressources et les outils nécessaires ;
- L'utilisation d'une méthodologie rigoureuse et appropriée;
- L'établissement d'un budget et des outils permettant le suivi et le pilotage des projets informatiques;
- Une division des phases des projets en des tâches bien définies avec des points de contrôle de la réalisation de ces tâches ;
- Les outils de planification et de reporting;
- L'allocation des ressources nécessaires aux projets (personnel et matériel);
- L'implication de la direction dans le pilotage et le suivi des projets informatiques;
- L'implication des utilisateurs clés dans toutes les phases des projets;
- Les besoins des utilisateurs devraient être suffisamment analysés et pris en compte dans le développement des projets;
- La prise en considération des besoins de sécurité et de contrôle interne au niveau de chaque étape du projet ;
- La réalisation des tests techniques et utilisateurs avant la mise en production de toute nouvelle application informatique;

- Une procédure d'autorisation des transferts en production des programmes développés: Cette procédure devra permettre le contrôle des transferts en production des programmes (seuls ceux testés et autorisés doivent être mis en production);
- Une documentation appropriée des applications développées (documentation technique et utilisateurs).

2.2 Les contrôles relatifs à la gestion des modifications

En matière de gestion des modifications des programmes il faudrait prévoir notamment:

- Un système de décision permettant de choisir entre maintenir un programme, le réécrire ou carrément le remplacer;
- Une procédure de demande, d'autorisation et de suivi des modifications: Celles-ci doivent être justifiées et prioritisées;
- Une méthodologie de spécification, de design, de test et de mise en production des modifications apportées aux programmes;
- Une revue des modifications: Elle doit être réalisée afin de s'assurer qu'elles ont été effectuées conformément aux standards et aux procédures de contrôle interne de l'entreprise ;
- Une mise à jour de la documentation des programmes modifiés.

2.3 Les contrôles relatifs à la sélection et à la mise en œuvre des progiciels

A l'instar du développement des applications, l'acquisition des progiciels devrait se faire selon des procédures rigoureuses dont notamment:

- La sélection des solutions connues et ayant fait leur preuve;
- Le choix des solutions en fonction de leur réponse aux besoins de l'entreprise, de leur fiabilité et de la qualité du support fourni par leurs fournisseurs: il y a lieu de souligner, que l'étude des besoins et l'établissement de cahier des charges est un préalable obligatoire;
- La Limitation des développements au minimum: En effet, la majorité des besoins devraient être satisfaite par les progiciels à acquérir. Les développements spécifiques

sont généralement limités au paramétrage de certaines fonctionnalités non prévues dans les progiciels;

- Le package choisi doit inclure les contrôles appropriés;
- Les tests techniques et utilisateurs doivent être effectués avant toute mise en production des progiciels;
- Les utilisateurs doivent être impliqués dans toutes les phases de l'acquisition jusqu'à la mise en œuvre des progiciels (définition des besoins, choix de la solution, mise en œuvre et tests);
- La rédaction de contrat prévoyant l'engagement formel des fournisseurs à assurer l'assistance aux utilisateurs et la maintenance des solutions vendues: il y a lieu de noter qu'il est préférable d'avoir un seul fournisseur responsable de l'ensemble des prestations afin d'éviter la dilution des responsabilités.

2.4 Les contrôles relatifs à la gestion des opérations d'exploitation informatique

La gestion de l'exploitation des systèmes importants est normalement assurée par des informaticiens dédiés et suivant des procédures détaillées et formalisées. En revanche, l'exploitation des petits systèmes pourrait être réalisée par un informaticien à temps partiel ou par des utilisateurs suffisamment formés.

En effet, pour les systèmes importants, il y a lieu d'établir des procédures détaillées expliquant toutes les tâches des opérateurs. Ces procédures doivent inclure aussi bien les opérations d'exploitation normale que celles relatives à la gestion des incidents.

Afin d'assurer une gestion efficace des opérations d'exploitation, il est vivement recommandé d'automatiser au maximum les opérations d'exploitation. Il est à noter que dans le cas où elles seraient automatisées, la vérification de leur fiabilité devrait être effectuée au moment de leur première mise en œuvre.

De plus, La direction informatique devrait mettre en place des indicateurs et des tableaux de bord permettant de remonter notamment les éléments suivants :

- Les incidents d'exploitation: Il faudrait documenter la nature des incidents relevés, leur impact ainsi que la manière avec laquelle ils ont été résolus;
- Le taux d'utilisation des systèmes;

- Le temps de réponse des systèmes critiques;
- Les tentatives d'accès non autorisé aux systèmes.

Par ailleurs, il y a lieu de contrôler les activités des opérateurs qui sont chargés des opérations d'exploitation des systèmes.
En outre, il faudrait prévoir des procédures appropriées de sauvegarde et de conservation des données et des programmes.

2.5 Les contrôles relatifs aux procédures utilisateurs

Afin d'assurer une bonne utilisation des systèmes, il faudrait notamment, prévoir:

- Des instructions détaillées permettant de faciliter l'utilisation et le contrôle des systèmes: Elles doivent être mises à jour à chaque changement effectué;
- Une formation appropriée des utilisateurs. Elle doit inclure des guides et des manuels relatifs à l'utilisation des systèmes ;
- La mise en place d'un service de support aux utilisateurs: Ceci est envisagé notamment dans les organisations d'une certaine taille. En revanche, dans les organisations d'une taille réduite, l'assistance aux utilisateurs est généralement assurée par le personnel de l'exploitation ou du développement des systèmes.

2.6 Les contrôles relatifs au plan de secours

Afin de se prémunir contre les dommages liés aux risques d'interruption des systèmes informatiques, un plan de secours est fortement conseillé. Il doit porter sur tous les éléments susceptibles d'être affectés par les disasters informatiques. Ce plan inclura non seulement les opérations liées aux systèmes informatiques mais aussi toutes les fonctions critiques pour la continuité du business de l'entreprise.

Il doit comprendre notamment:

- Les procédures de restauration des systèmes informatiques;
- Les méthodes d'obtention des informations nécessaires à la continuité du business;
- Les critères de sa mise en œuvre;
- Le temps nécessaire à la restauration de chaque fonction clé du business;

- Les équipements de remplacement (matériel, programmes, télécommunication);
- Les méthodes de traitement et de conservation pendant la période d'indisponibilité des systèmes;
- Le personnel responsable des différentes tâches du plan de secours;
- Les procédures de sauvegarde et de restauration des programmes et des données suite à un incident éventuel.

Afin de préparer un bon plan de secours, il faudrait bien identifier les fonctions critiques du business ainsi que les systèmes qui les gèrent.

Une fois ce plan est établi, il y a lieu de le tester régulièrement et de le mettre à jour à chaque changement des systèmes ou des opérations du business.

CONCLUSION DE LA PREMIERE PARTIE

Les systèmes d'information sont composés de plusieurs modules, sous-systèmes ou applications et des infrastructures permettant de recueillir (collecter et saisir), traiter, stocker, prendre et véhiculer l'information. Ils sont de plus en plus intégrés, ouverts et complexes et permettent de prendre en charge la majorité des processus de l'entreprise ou de l'organisation.

Dans une économie de plus en plus mondialisée et libéralisée, les systèmes d'information sont devenus un levier stratégique pour les entreprises et pourront constituer un avantage concurrentiel s'ils sont gérés d'une manière efficace et efficiente.

Face à ce nouvel environnement contraignant, l'organisation de la fonction informatique dans les entreprises performantes a été repensée de façon à être réactive et en adéquation avec la stratégie de l'entreprise.

Au cours de cette partie, nous avons exposé le rôle des systèmes d'information ainsi que l'organisation de la fonction informatique. Nos propos ont été axés sur les bonnes pratiques en matière de contrôle interne relatif à la fonction informatique.

Par ailleurs, nous avons souligné que l'évolution, la complexité et l'ouverture des systèmes d'information sur les partenaires de l'entreprise s'accompagnent le plus souvent, par de nouveaux risques. Ces derniers, qui sont liés à l'environnement et à l'organisation de l'entreprise, rendent les systèmes d'information vulnérables. En effet, s'ils ne sont pas bien encadrés par le dispositif du contrôle interne, ils peuvent engendrer de lourdes conséquences pour les entreprises. Les facteurs de ces risques ont été synthétisés dans cette première partie du mémoire.

Au cours de cette partie, nous avons également résumé les réactions des législateurs et des organismes représentant les corps professionnels de l'audit face au nouveau contexte de l'environnement de la fonction informatique.

La mission de l'audit financier, qui repose aujourd'hui largement sur le contrôle interne des entreprises, devra être adaptée et complétée de façon à prendre en

considération les risques et les contraintes imposés par le nouvel environnement des entreprises.

En effet, dans un milieu informatisé, il est devenu très difficile de certifier les états de synthèse sans auditer préalablement les systèmes informatiques.

La démarche d'audit informatique dans le cadre d'une mission d'audit financier, prenant en compte les enjeux du nouveau contexte, sera présentée dans la deuxième partie de ce mémoire.

PARTIE II

PROPOSITION D'UNE METHODOLOGIE POUR LA CONDUITE DES MISSIONS D'AUDIT INFORMATIQUE

INTRODUCTION DE LA DEUXIEME PARTIE

Dans le contexte actuel, l'environnement de l'audit financier a fortement changé et il se caractérise ainsi par:

- La complexité des modes de fonctionnement des entreprises qui deviennent de plus en plus dépendantes des nouvelles technologies;
- L'évolution de la réglementation et des référentiels comptables (Sarbanes oxley, Loi sur la sécurité financière, IFRS…etc.);
- L'exigence croissante des marchés financiers en ce qui concerne la qualité de l'information financière produite par les sociétés cotées.

Ainsi, les cabinets d'audit ont dû revoir leur méthodologie de façon à répondre aux exigences des marchés et de la réglementation, d'une part, et, d'améliorer la qualité de l'audit comptable et financier, d'autre part.

Les nouvelles démarches d'audit adoptées reposent largement sur la compréhension des risques inhérents au business et à l'organisation des entreprises ainsi que sur la qualité de contrôle interne de ces dernières.

Compte tenu du fait que les entreprises sont devenues hautement informatisées, l'évaluation des systèmes informatiques devient un axe central dans la démarche de l'audit financier.

La deuxième partie de ce mémoire, est consacrée à la présentation d'une méthodologie pour la conduite des missions d'audit informatique en tant que support à l'audit comptable et financier, ainsi que des démarches d'audit informatique dans le cadre de certaines missions spéciales.

TITRE 1
LE PROCESSUS DE L'AUDIT INFORMATIQUE DANS LE CADRE DES MISSIONS D'AUDIT FINANCIER ET COMPTABLE

CHAPITRE 1 : PRESENTATION DE LA DEMARCHE DE L'AUDIT INFORMATIQUE DANS LE CADRE DES MISSIONS D'AUDIT FINANCIER ET COMPTABLE

Afin de mieux comprendre la place de l'audit informatique dans le processus de l'audit, il y a lieu de rappeler brièvement dans ce chapitre la nouvelle démarche générale de l'audit financier, et d'exposer par la suite l'approche proposée pour la conduite des missions d'audit informatique.

1. Présentation de la nouvelle démarche générale de l'audit comptable et finan

1.1 Caractéristiques de la nouvelle approche d'audit

La démarche d'audit que nous allons présenter dans ce mémoire, s'inspire des méthodologies récemment développées par les cabinets internationaux d'audit et de conseil. Il s'agit d'une approche d'audit par les risques ; basée essentiellement sur la compréhension des activités des clients et l'évaluation de leur dispositif de contrôle interne. En effet, ces nouvelles méthodologies visent à mieux répondre au nouveau contexte de l'audit comptable et financier (exigences réglementaires: SOX, LSF et pressions des marchés financiers).

En effet, la loi Américain(SOX) stipule que l'auditeur doit examiner les états financiers et le contrôle interne. Ainsi, l'approche d'audit développée permet de:

- Certifier les états financiers;
- Donner une attestation sur la certification de l'efficacité du dispositif contrôle interne relatif au reporting financier établi par le management.

Cette nouvelle approche d'audit est une démarche intégrée. Elle ne remet pas en cause les principes fondamentaux de l'audit, mais elle constitue une évolution

méthodologique visant à se conformer au nouveau contexte de l'audit d'une part, et, à mieux gérer le risque professionnel d'audit d'autre part.

Les caractéristiques de cette nouvelle démarche peuvent se résumer ainsi:

- L'évaluation et les tests relatifs aux contrôles deviennent systématiques: Auparavant, les tests des contrôles n'étaient effectués que lorsque l'auditeur s'appuyait sur eux pour valider les comptes. Désormais, ce type de tests est préconisé par la réglementation;
- L'identification et l'évaluation des risques ne sont plus effectuées à partir des comptes mais, elles se basent sur la compréhension du business, des engagements et des opérations de l'entreprise auditée;
- L'assurance d'audit est davantage obtenue à travers l'évaluation et les tests du dispositif du contrôle interne y compris les contrôles de pilotage;
- Le lien entre les travaux sur le contrôle interne et ceux sur les comptes est mieux clarifié;
- Les recommandations d'audit ont une plus grande valeur ajoutée pour les clients puisqu'elles sont plus axées sur les vraies préoccupations du management.

1.2 Les phases de la nouvelle approche d'audit comptable et financier

La nouvelle démarche d'audit repose sur une approche intégrée dont, le cycle d'assurance d'audit est le point central. Celui-ci commence à partir des premiers entretiens avec le management. Les principales étapes de l'audit de cette démarche sont résumées comme suit :

1.2.1 Phase d'acceptation et de poursuite de la mission

Cette phase a pour objectif de décider de l'acceptation d'une nouvelle mission ou la poursuite d'une ancienne mission. L'auditeur doit évaluer le risque professionnel lié à chaque mission avant de commencer ses travaux d'audit. Sur le plan pratique, les cabinets internationaux ont développé des logiciels de scoring permettant d'aider

l'auditeur dans son processus de décision relatif à l'acceptation ou la poursuite de la mission.

1.2.2 Phase de cadrage de la mission

Elle a pour but de mieux cibler les objectifs de la mission, de structurer l'approche d'audit, de définir les rôles des membres de l'équipe et le planning d'intervention, et enfin, d'identifier les comptes significatifs et les processus qui les alimentent.

1.2.3 Phase de compréhension

Elle a pour objectif de comprendre le business du client, ses risques, son dispositif du contrôle interne, son organisation, ses sources d'information ainsi que son environnement. Cette compréhension se fait sur la base de l'analyse des activités et de l'organisation du client. Celle-ci devrait s'articuler autour de:

- Marché: la concurrence, l'environnement légal et économique;
- Stratégie : les objectifs stratégiques, le business plan, l'organisation et le mode de management;
- Activités créatrices de valeur: les clients, les ressources humaines, l'innovation, la chaîne d'approvisionnement et les systèmes d'information;
- Performance financière: la situation financière, la performance économique, l'analyse sectorielle et les politiques comptables.

1.2.4 Phase d'évaluation

Elle a pour objectif d'évaluer d'une part, l'impact éventuel des risques identifiés sur les comptes et, d'autre part, d'évaluer dans quelle mesure le dispositif du contrôle interne permet de gérer ces risques. L'auditeur devra aussi déterminer quels sont les contrôles clés sur lesquels il peut s'appuyer dans sa stratégie d'audit.

1.2.5 Phase de validation:

Elle a pour objectif de collecter les preuves d'audit quant au fonctionnement des contrôles et d'apprécier la certification du dispositif du contrôle interne relatif au reporting financier établi par le management.

La validation des comptes est effectuée en fonction de l'assurance obtenue à partir de l'évaluation finale des contrôles. En effet, si celle-ci donne une grande assurance d'audit, la validation des comptes se fera essentiellement par le biais des revues analytiques approfondies. Dans le cas contraire, où l'assurance obtenue, à l'issue de cette étape, est limitée, la validation des états financiers sera basée essentiellement, sur les tests étendus portant sur les comptes. Ces derniers sont généralement moins efficaces, car ils sont consommateurs de temps et ne permettent pas de cerner tous les risques d'audit.

En plus de l'évaluation des tests et des contrôles, l'auditeur est appelé à effectuer d'autres procédures d'audit qui peuvent varier en fonction du contexte de la mission d'audit. Parmi elles nous pouvons citer:

- La revue des contrats significatifs et des procès verbaux des conseils d'administration et des assemblées générales;
- La revue des engagements du client y compris ceux du hors bilan;
- La revue des opérations comptabilisées qui n'ont pas suivi le circuit habituel d'approbation.

2 DEMARCHE GENERALE DE L'AUDIT INFORMATIQUE

Compte tenu de la complexité des systèmes informatiques, les cabinets d'audit internationaux ont développé des méthodologies propres et des équipes spécialisées dans l'audit informatique. Dans le cadre du présent mémoire, nous présenterons une méthodologie d'audit informatique dans le cadre d'une mission d'audit comptable et financier.

La démarche d'audit informatique ne diffère pas, dans ses aspects méthodologiques, de l'approche de l'audit comptable et financier. Elle se décline en cinq phases:

- Cadrage de la mission ;
- Compréhension de l'environnement informatique ;
- Identification et évaluation des risques et des contrôles afférents aux systèmes;
- Tests des contrôles;
- Finalisation de la mission.

2.1 Cadrage de la mission

Le cadrage de la mission a pour objectif :

- De délimiter le périmètre d'intervention de l'équipe d'audit informatique. Cela peut être matérialisé par une lettre de mission, une note interne, une réunion préalable organisée entre les équipes d'audit financier et d'audit informatique;
- De structurer l'approche d'audit et organiser les travaux entre les deux équipes;
- De définir le planning d'intervention;
- De définir les modes de fonctionnement et de communication;
- De définir les délivrables.

Lors de cette phase, l'auditeur informatique prendra connaissance du dossier de l'équipe de l'audit financier (stratégie d'audit, management letter, rapports d'audit interne, points d'audit soulevés au cours des précédents audits, attentes du client... etc.).

Cette prise de connaissance permettra à l'auditeur d'orienter ses travaux lors des phases qui suivent.

2.2 Compréhension de l'environnement informatique

Elle a pour objectif de comprendre les risques et les contrôles liés aux systèmes informatiques. Elle peut se faire sur la base notamment, de la compréhension de l'organisation de la fonction informatique, des caractéristiques des systèmes informatiques et de la cartographie des applications. Elle doit permettre de déterminer comment les systèmes clés contribuent à la production de l'information financière.

2.2.1 L'organisation de la fonction informatique

Lors de cette étape, l'auditeur devra comprendre notamment :

- La stratégie informatique de l'entreprise: Il s'agit de voir d'une part, dans quelle mesure est-elle alignée sur la stratégie globale de l'entreprise? Et, d'autre part, comment est-elle pilotée? (Examen du plan informatique, du comité directeur informatique, des tableaux de bords... etc.).

- Le mode de gestion et d'organisation de la fonction informatique : Il s'agit notamment de comprendre dans quelle mesure la structure organisationnelle de la fonction informatique est adaptée aux objectifs de l'entreprise. En outre, il faudrait apprécier si la fonction informatique est sous contrôle du management. A cet effet, il faudrait examiner les aspects suivants:

  - L'organigramme de la fonction informatique (son adéquation par rapport aux objectifs assignés à la fonction, la pertinence du rattachement hiérarchique de la fonction, le respect des principes du contrôle interne);
  - La qualité des ressources humaines (compétence, expérience, effectif, gestion des ressources, formation);
  - Les outils de gestion et de contrôle (tableaux de bord, reporting, contrôles de pilotage);
  - Les procédures mises en place (leur formalisation, leur respect des principes de contrôle interne, leur communication au personnel);
  - La délimitation des rôles et des responsabilités, le respect du principe de séparation des tâches.

2.2.2 Caractéristiques des systèmes informatiques

L'auditeur devra se focaliser sur les systèmes clés de façon à identifier les risques et les contrôles y afférents. Ainsi, il faudrait documenter l'architecture du matériel et du réseau en précisant:

- Les caractéristiques des systèmes hardware utilisés (leur architecture, leur procédure de maintenance, les procédures de leur monitoring).

- Les caractéristiques des systèmes software (systèmes d'exploitation, systèmes de communication, systèmes de gestion des réseaux, de la base des données et de la sécurité, utilitaires).

2.2.3 Cartographie des applications clés

La documentation des applications clés devrait être effectuée de préférence, conjointement par l'équipe de l'audit financier et celle de l'audit informatique. Les auditeurs financiers identifient les comptes significatifs compte tenu du seuil de matérialité de la mission. Les deux équipes recensent les processus qui alimentent ces comptes. Il reviendra par la suite, à l'équipe d'audit informatique d'inventorier les applications informatiques utilisées dans ces processus ainsi que leurs caractéristiques (langage de développement, année de développement, bases de données et serveurs utilisés…etc.).

Il y a lieu également de préciser :

- Le lien entre les applications ;
- Les interfaces ;
- Le mapping des processus d'initialisation des opérations jusqu'à leur comptabilisation dans les états financiers ;
- Les applications critiques ;
- Les états et les rapports permettant d'effectuer des contrôles et des tests d'audit.

La documentation de la cartographie des applications peut être effectuée en utilisant des diagrammes ou des tableaux complétés par des narratifs. En annexe 6 nous avons présenté un exemple schématique de cartographie d'une compagnie d'assurance marocaine.

2.3 Identification et évaluation des risques et des contrôles afférents aux systèmes

En plus des risques inhérents au business de l'entreprise recensés par l'auditeur financier, il y a lieu d'identifier les risques liés aux systèmes informatiques et au contrôle dans un environnement informatisé. Ils concernent aussi bien les risques liés

aux contrôles généraux informatiques que ceux liés aux applications. Les principaux facteurs de ces risques ont été évoqués au niveau de la première partie de ce mémoire.

Il y a lieu de noter qu'il faudrait se focaliser sur les risques ayant un impact direct ou indirect sur la fiabilité des états financiers. Les risques liés à la fonction informatique sont relatifs à l'organisation de la fonction informatique, au développement et mise en service des applications, à la gestion de l'exploitation et à la gestion de la sécurité. Ces risques ont été abordés dans le chapitre du titre 2 de la première partie.

Une fois ces risques recensés, l'auditeur devra évaluer les contrôles mis en place par l'entreprise pour gérer ces risques.

L'identification des risques et l'évaluation des contrôles peuvent être récapitulées sous la forme d'un tableau reprenant les éléments suivants:

- Les objectifs du business;
- Les risques de ne pas atteindre ces objectifs et les risques d'audit;
- Les contrôles mis en place pour limiter ces risques;
- L'évaluation par l'auditeur de l'alignement ou adéquation du contrôle par rapport aux risques;
- Les réponses apportées en terme de démarche d'audit;
- Les commentaires et recommandations à formuler au client.

2.4 Tests des contrôles

Les tests des contrôles informatiques peuvent être effectués en utilisant aussi bien des techniques spécifiques aux environnements informatisés (contrôles assistés par ordinateurs, revue des codes, jeux de tests…etc.) que des techniques classiques (re-performance, examen des pièces et documents, observation…etc.).

Ces tests portent sur les contrôles généraux informatiques et les contrôles d'application. Ces derniers seront traités dans le chapitre 3 de cette partie.

En revanche, les contrôles généraux informatiques sont détaillés dans le chapitre 2 a section qui suit.

2.5 Finalisation de la mission

Une fois les travaux achevés et revus, les conclusions de ces travaux doivent faire l'objet de communications ultérieures au client et à l'équipe d'audit. En effet, à l'issue des travaux, l'auditeur évalue l'impact des anomalies relevées sur la fiabilité des états financiers et éventuellement les travaux d'audit spécifiques qu'il y a lieu d'accomplir afin d'obtenir une assurance raisonnable sur les états financiers.

Dans tous les cas, les conclusions doivent être communiquées à l'équipe d'audit sous forme d'un mémorandum comprenant les éléments suivants :

- Un rappel du cadre et des modalités d'intervention (date, durée de la mission, personnes rencontrées, …etc.) ;
- Un rappel des objectifs validés avec le client ;
- La description des travaux réalisés et leur conclusion, notamment en terme d'impact sur la stratégie d'audit ;
- Les points relevés ;
- Les objectifs éventuellement non atteints (cause, impact) ;
- Les éléments connus à prendre en compte pour les interventions futures (migration technique annoncée…etc.) ;
- Les opportunités de missions spéciales.

De même, les faiblesses de contrôle interne doivent être transmises au client sous forme de lettre de contrôle interne comprenant les éléments suivants :

- La synthèse des points relevés ;
- Le cadre de l'intervention ;
- Les remarques sur le pilotage de la fonction informatique ;
- Les remarques sur les contrôles détaillés.

Les points relevés peuvent être présentés de deux manières différentes :

1 er mode de présentation :

- **Appréciation générale de l’environnement ;**
- **Pour chaque domaine couvert :**
  - Points forts;
  - Opportunités d’amélioration.

2 ème mode de présentation :

- **Sommaire des zones d’amélioration potentielles dans le domaine concer**
- **Pour chaque point relevé:**
  - Description du problème;
  - Risque induit;
  - Recommandations.

CHAPITRE 2 : L'AUDIT DE LA FONCTION INFORMATIQUE (CONTROLES GENERAUX INFORMATIQUES)

Les contrôles généraux informatiques sont ceux relatifs à l'environnement général de la fonction informatique. Ils contribuent de manière significative au renforcement du niveau de contrôle interne. Leur qualité conditionne la fiabilité des contrôles automatisés et par conséquent le degré de confiance que l'auditeur financier peut avoir dans ce type de contrôles.

La revue est effectuée dans le cadre des travaux d'audit des comptes qui ont pour but de former une opinion sur les comptes de la société auditée. Elle ne permet pas d'identifier toutes les améliorations du contrôle interne qu'une revue spéciale plus approfondie pourrait permettre.

Par ailleurs, cet aspect de l'audit informatique est planifié généralement avant la fin de l'exercice comptable, lors de la mission d'évaluation des procédures et du niveau de contrôle interne au sein de l'entreprise. La conclusion de l'auditeur informatique permettra à l'équipe d'audit financier, selon la démarche décrite ci-dessus, de mener un travail plus ou moins détaillé lors des travaux de vérification des comptes en fin d'exercice.

Il convient de souligner aussi que la revue des contrôles généraux informatiques est souvent suivie par un audit d'application notamment dans les sociétés où le degré d'automatisation est très élevé. En général, si les contrôles généraux ne sont pas bons, ils impacteront de manière indirecte et inévitable les contrôles d'application. De plus, selon les constats relevés lors d'une mission de revue des contrôles généraux informatiques, l'auditeur pourrait effectuer d'autres missions d'audit informatique.

Nous citons, à titre d'exemple les audits suivants :

- Audit des projets informatiques ;
- Audit de la sécurité informatique ;
- Audit d'application informatique.

Dans le cadre de l'audit financier, la revue des contrôles généraux informatiques couvre les aspects suivants :

- Organisation, planification et management de la fonction informatique ;
- Développement, acquisition, implémentation et maintenance des applications et programmes informatiques ;
- Exploitation informatique ;
- Sécurité des actifs informatiques et des accès aux ressources informatiques ;
- Plan de secours informatique.

1 Organisation, planification et management de la fonction informatique

L'examen de l'organisation, de la planification stratégique et du management de la fonction informatique permet à l'auditeur informatique de vérifier l'alignement de la stratégie des Systèmes d'Information (SI) à celle de l'entreprise et d'apprécier la qualité du pilotage de la fonction informatique.

1.1 Planification stratégique et management de la fonction informatique

L'auditeur informatique doit s'assurer notamment de l'existence d'une planification stratégique qui doit définir les projets, les priorités et les actions à mener à court, à moyen et à long terme dans l'objectif de répondre aux besoins métiers de l'entreprise. Il doit également :

- Vérifier que le plan informatique est approuvé par le top management ou par le comité informatique et qu'il est en ligne avec la stratégie de l'entreprise ;
- Vérifier qu'un comité informatique regroupant les différentes directions de l'entreprise a été créé. Ce comité doit recenser les besoins, valider les choix informatiques, gérer les priorités et assurer le suivi et le contrôle de la réalisation des projets informatiques ainsi que les performances et la qualité des prestations;
- Examiner les PV de ce comité et évaluer son rôle ;
- S'assurer que les directions utilisatrices sont impliquées dans la conception, le développement des systèmes informatiques, la validation des traitements, les tests des nouvelles versions et l'analyse des risques et la classification des informations ;

- Vérifier l'existence de contrats de services (Service level agreement : SLA) pour chacune des prestations de la DSI ;
- S'assurer que la DSI établit des indicateurs de performance et des tableaux de bord, et apprécier leur pertinence.

1.2 Audit de l'organisation de la DSI

L'audit de l'organisation de la DSI permet entre autres d'apprécier :

- L'environnement général de contrôle de la DSI et le niveau de risque associé à l'organisation informatique ;
- Le degré de sensibilisation au dispositif du contrôle interne ;
- La répartition des tâches entre les utilisateurs et les informaticiens.

L'auditeur doit vérifier notamment :

- L'existence d'un organigramme à jour de la DSI ;
- L'existence d'une définition claire des fonctions ;
- L'adéquation des effectifs informatiques aux besoins ainsi que de leurs qualifications ;
- L'existence de procédures formalisées ;
- Le respect du principe de séparation des tâches.

2 Développement, acquisition, implémentation et maintenance des applic des programmes informatiques

L'audit de cet aspect en cas de conclusion positive permet à l'auditeur financier de :

- S'appuyer sur les contrôles automatisés au sein des systèmes afin de valider l'information financière issue de l'application auditée ;
- S'assurer que les systèmes ont été développés suivant une méthodologie permettant de limiter les risques d'erreurs et qu'ils ne peuvent être modifiés sans autorisation.

Lors de cette étape, l'auditeur devra notamment :

- Déterminer les composantes, les objectifs et les besoins des utilisateurs afin d'identifier les aspects qui nécessitent un niveau de contrôle important. Cette action est effectuée par des entretiens avec les utilisateurs clés et les membres du projet de développement ;
- A travers ces entretiens, déterminer les zones de risques relatives aux développements réalisés et identifier les contrôles mis en place pour réduire le niveau des risques identifiés ;
- S'assurer que les contrôles ont été implémentés et que les développements réalisés correspondent bien aux besoins des utilisateurs ;
- Revoir la méthodologie de développement qui a été suivie et s'assurer que toutes les étapes ont été correctement documentées ;
- Evaluer et tester les procédures de maintenance standards des systèmes pour s'assurer que toutes les modifications ont été correctement autorisées et documentées.

Un guide récapitulant les principaux travaux à effectuer sur les aspects relatifs au développement, acquisition, implémentation et maintenance des applications et des programmes informatiques est présenté en annexe1.

3 Exploitation informatique

L'audit de l'exploitation a pour objectif d'apprécier la qualité de la planification des opérations et des procédures d'exploitation d'une part, et la capacité du département informatique à gérer les incidents y afférents, d'autres part.
Dans son examen de la planification et gestion des travaux d'exploitation informatiques, l'auditeur doit vérifier notamment :

- La capacité de l'organisation à répondre aux besoins de l'entreprise ;
- La maîtrise des technologies utilisées;
- L'existence des points de contrôle relatifs à l'exploitation;
- L'existence de manuels d'exploitation des différentes applications nécessitant des travaux batchs;

- La qualité de la planification des opérations d'exploitation ;
- Le suivi des incidents d'exploitation suite à l'arrêt d'un programme par exemple ;
- La mise en œuvre de tableaux de bord d'exploitation.

L'auditeur doit également vérifier que :

- Les traitements sensibles peuvent faire l'objet d'un retour en arrière ;
- Tout rejet est identifié et fait l'objet d'un recyclage approprié ;
- Les applications et les systèmes génèrent des fichiers exploitables ;
- Les alertes sont remontées en temps réel à la console d'administration.

4 La sécurité des actifs informatiques et des accès aux ressources informa

L'objectif de l'audit de cet aspect est de permettre à l'auditeur de porter une appréciation sur :

L'existence d'une politique de sécurité adoptée et approuvée par le top management portant aussi bien sur la sécurité logique que la sécurité physique;

- En ce qui concerne, la sécurité logique relative aux procédures d'autorisation d'accès et de protection de l'intégrité des données, l'auditeur informatique doit s'assurer de:

  - L'existence et la bonne application d'une procédure d'accès aux ressources informatiques (création autorisée des accès au système et des mots de passe, définition autorisée du périmètre d'accès des utilisateurs, définition autorisée des habilitations en consultation, modification ou suppression des transactions).
  - L'existence et la bonne application d'une procédure de suppression des accès aux systèmes suite aux départs des employés. Dans le cas d'existence de comptes dormants, il convient de souligner que les risques encourus sont importants car les comptes dormants sont considérés comme des cibles privilégiées pour des personnes souhaitant s'introduire de manière frauduleuse dans un système d'information ;
  - L'existence d'une procédure de gestion et de changement des mots de passe. Un mot de passe est la clé d'entrée d'un utilisateur dans le système, d'où son caractère confidentiel et important. Il est donc recommandé que ce dernier ne

soit pas facile à deviner (alphanumérique et supérieur à cinq caractères) ni difficile à mémoriser (ne doit pas dépasser 12 caractères). De plus, il est également important de procéder au changement périodique du mot de passe, car en cas de non-modification régulière des mots de passe, il existe un risque de divulgation qui affecte leur caractère confidentiel. Par conséquent, la fiabilité du système de sécurité, basée sur la confidentialité des mots de passe, est remise en cause.

- S'agissant de la sécurité physique des actifs informatiques (serveurs gros systèmes, mini-ordinateurs, équipements réseaux et télécoms, micro-ordinateurs), elle concerne notamment:
  - Les procédures d'accès physique au bâtiment de l'entreprise;
  - Les procédures d'accès spécifiques aux zones protégées (salles "machines", imprimantes systèmes, lieu d'emplacement des cartouches de sauvegardes, …etc.).

5 Plans de sauvegardes et de secours informatique

5.1 Plan de sauvegardes

La sauvegarde du patrimoine informatique relève de la pérennité du système d'information de la société. L'auditeur informatique doit donc s'assurer que :

- Des sauvegardes quotidiennes des données d'exploitation sont effectuées selon un cycle de cinq ou six jours sur sept. Ces sauvegardes doivent être placées dans un endroit protégé (dans un coffre ignifuge par exemple) ;
- Des sauvegardes mensuelles doivent être également effectuées, pour garder une image mensuelle des données d'exploitation et surtout des données comptables ;
- Des sauvegardes annuelles et décennales effectuées notamment pour les besoins légaux ;
- Des sauvegardes des programmes sources et objets à chaque changement de version ou chaque modification de programme ;
- Une sauvegarde externe doit être prévue et placée dans un endroit sécurisé (dans le coffre fort d'une banque par exemple).

5.2 Plan de secours

L’auditeur informatique doit s’assurer de l’existence d’un plan de secours, c'est à dire le document listant l'ensemble des opérations devant permettre à la société de pouvoir restaurer son système d'information de manière intègre en cas de sinistre informatique grave.

En effet, en l’absence d’un plan de secours et en présence d’un sinistre informatique grave, la société pourrait ne pas pouvoir disposer de son système d'information pendant une certaine durée. Ceci pourrait être préjudiciable pour la gestion de l'entreprise.

Par ailleurs, la non-préparation à ce type d'éventualité peut déboucher, dans un cas de sinistre, à l'exécution d'opérations incorrectes impactant ainsi l'intégrité des données à caractère comptable.

De même, le DMI (Délai Maximum d’Indisponibilité) doit être identifié par application. A titre d’exemple, les applications d’une salle de marchés d’une banque sont des applications critiques, et ne peuvent en aucun cas être indisponibles. Par contre, une application de gestion de courrier n’étant pas critique peut avoir un délai d’indisponibilité plus important.

Un plan de secours informatique, doit prévoir, entre autres, un site de backup qui doit définir, selon la criticité des applications, les modalités de back up/restauration.

Un site de back up est :

- Soit un « hot site » qui est un site de backup ayant des serveurs avec les mêmes performances du site réel et des connexions réseaux disponibles. L’avantage d’un tel site est sa rapide disponibilité en cas de sinistre, notamment pour les applications critiques ayant un faible DMI ;
- Soit un « Warm site » qui est un site de backup ayant uniquement des connexions réseaux disponibles mais sans la présence des serveurs ;
- Soit un « cold site » qui est un site disposant uniquement d’électricité et de climatisation.

En cas de présence du plan de secours, l'auditeur informatique doit vérifier si ce plan est revu annuellement et s'il a fait l'objet de tests. En effet, un plan de secours non mis à jour est par conséquent obsolescent. De même, un plan non testé n'est pas de nature à garantir les résultats escomptés. Au-delà du facteur technique, il est très important de mesurer et connaître la réaction des employés face à une situation de sinistre.

6 Présentation d'un cas de revue des contrôles généraux informatiques

Nous avons effectué une revue de la fonction informatique d'une compagnie d'assurance de la place. Cette revue a été effectuée dans le cadre de nos travaux d'audit des comptes qui ont pour but d'exprimer une opinion sur les comptes de la dite société.

La plate-forme informatique de la société auditée s'articulait principalement autour d'une machine AS/400 et d'un système d'information basé sur des applications développées en interne.

6.1 Etendue et objectifs de la mission

L'intervention a été réalisée au siège de la société et avait pour principal objectif la revue des contrôles généraux informatiques. Elle a couvert les domaines suivants :

- **L'organisation de la direction informatique :** s'assurer que la direction informatique dispose d'une structure permettant une bonne séparation des tâches;
- **L'exploitation informatique** s'assurer que les opérations d'exploitation sont correctement définies, planifiées et suivies;
- **Le développement des applications :** s'assurer que les procédures de développement et de modification des programmes sont correctement définies et appliquées;
- **La sécurité :** s'assurer que les accès aux données et aux transactions sont correctement autorisés;

- **Le plan de secours et les sauvegardes :** s'assurer que des mesures ont été mises en plac
afin d'assurer la restauration du système d'information en cas de sinistre informatique.

6.2 Notre démarche

Concernant l'organisation de la direction informatique, nous avons dans un premier temps effectué des entretiens croisés avec les personnes clés de la direction informatique (IT Manager, Responsable de la division études et développements, responsable d'exploitation, Responsable réseaux, Helpdesk) afin de prendre connaissance du système d'information de la société, de son plan stratégique informatique ainsi que des différentes attributions de chaque membre du personnel du département informatique. Dans un deuxième temps, nous avons effectué une revue de la documentation existante qui matérialise les aspects du management de la fonction informatique (schéma directeur, plan d'action, comptes-rendus du comité informatique, fiches de fonction du personnel informatique, …).

En ce qui concerne les travaux d'exploitation informatique, nous avons interviewé les différentes personnes du service d'exploitation qui sont responsables de la planification, de l'exécution des batchs et des tâches d'exploitation qui concernent la préparation des fichiers, l'exécution des programmes, le suivi des incidents ou problèmes d'exploitation. Ces entretiens ont été complétés par une revue de la documentation d'exploitation existante (manuel d'exploitation, registre des incidents, …).

En ce qui concerne les développements informatiques, notre démarche a été de prendre connaissance de la cartographie des applications informatiques, de vérifier l'existence de méthodologie des développements menés en interne et de revoir la documentation fonctionnelle et technique de certaines applications (application de la production automobile et application des sinistres maladies). Nous avons également vérifié l'existence d'une procédure formalisée de modification des programmes suite à une maintenance corrective ou évolutive, ainsi qu'une procédure de mise en production (les développeurs ne doivent en aucun procéder eux-mêmes à la mise en production des programmes).

En ce qui concerne les aspects de sécurité des actifs informatiques de la société, nous avons commencé par les aspects physiques, nous avons en compagnie du personnel informatique visité la salle "machines" et vérifié l'application des normes standards de la sécurité notamment les règles d'accès à la salle (badges magnétiques, registre manuel pour les visiteurs), l'existence de climatiseurs, détecteurs de feu, extincteurs de feu automatique, onduleurs, instrument de mesure de température et d'humidité, …). Nous avons également vérifié que la salle machines n'est pas visible de l'extérieur et qu'il y a une séparation physique entre les serveurs et les imprimantes systèmes.

Nous avons ensuite abordé les aspects de sécurité logique et interviewé le responsable d'administration du système d'exploitation (AS/400), ainsi que les responsables d'administration des différentes applications de la société. L'objectif de ces entretiens était de :

- S'assurer de l'existence de procédures de création, modification ou suppression de profils utilisateurs tant au niveau de la couche système (AS/400), qu'au niveau des applications développées en interne ;
- S'assurer du respect du principe de séparation des tâches eu égard aux droits et habilitations des utilisateurs ;
- S'assurer de l'existence de revue périodique des profils utilisateurs afin d'assainir et éliminer les profils dormants (personnes ayant quitté la société), les profils en double (plusieurs login pour la même personne) ;
- S'assurer de la bonne gestion des mots de passe.

Nous avons ensuite revu la documentation existante et réalisé des tests de comparaison des profils utilisateurs existant dans le système avec la liste du personnel de la société. Nous avons également effectué des tests par sondage pour s'assurer de la bonne application des procédures de création, modification et suppression des profils utilisateurs.

Enfin, en ce qui concerne les aspects du plan de secours et des sauvegardes nous avons demandé à obtenir le contingency plan de la société et demandé à connaître les procédures de sauvegarde et de backup du système d'information de la société (sauvegarde selon un cycle quotidien, hebdomadaire, mensuel et annuel, sauvegarde externe, placement des cartouches dans un endroit sécurisé, …).

6.3 Notre conclusion

Nous n'avions pas décelé au cours de nos travaux de faiblesses alarmantes pour que le cabinet, en tant qu'auditeur externe, ne puisse pas s'appuyer sur le système d'information pour valider les états financiers de la dite société. Néanmoins, nous avions considéré que le niveau de contrôle général de la fonction informatique était insuffisant et qu'il devait être renforcé.

Pour ce dossier d'audit, nous avons retenu un niveau de confiance moyen dans les systèmes.

6.4 principaux points relevés lors de notre mission

La sécurité logique de l'AS/400 de production est insuffisante, nous n'avons pas relevé de plan de sécurité permettant d'identifier les données stratégiques gérées par le système d'information ni les moyens de protection. Par ailleurs, nous avons noté que la liste des utilisateurs n'était pas à jour. Enfin, nous avons estimé que les droits de certains informaticiens et utilisateurs étaient trop importants, ce qui était préjudiciable à une correcte séparation des tâches.

A ce niveau, nos recommandations étaient de :

- Revoir la liste des utilisateurs ;
- Nommer un Responsable de la Sécurité des Systèmes d'Information (RSSI), indépendant des départements études et exploitation informatique ;
- Mettre en place un plan sécurité.
- Il n'y avait pas un standard de documentation des développements entrepris sur l'AS/400 (S36, AGL LANSA). Ainsi, il existait un risque que la maintenance des

applications soit plus difficile à posteriori, et pouvant même entraîner des anomalies non détectées en production.

- La société ne disposait pas de procédure de mise en production formalisée. Les mises en production étaient effectuées par les développeurs aussi bien pour les applications métiers en environnement AS/400 (LANSA) que pour quelques applications en environnement NT/SQL. Il existait, donc, un risque que les programmes mis en production n'aient pas été autorisés. Nous avions recommandé à ce qu'une limitation très stricte d'accès à l'environnement de production soit adoptée et des moyens de contrôle mis en place.

- Il n'existait pas de plan de secours informatique opérationnel pour la société, ce qui faisait courir des risques d'interruption de la continuité d'activité en cas de sinistre informatique important. Dans ce cadre, un plan de secours devrait être défini, mis en place et testé.

CHAPITRE 3 : AUDIT DES APPLICATIONS INFORMATIQUES

Il existe deux types de mission d'audit d'applications informatiques:

- L'audit de fiabilité et de sécurité;
- L'audit d'efficacité et de performance.

L'audit de fiabilité et de sécurité vise d'une part à identifier les risques d'erreur et de fraude, et d'autre part à évaluer la qualité du contrôle interne de l'application et de son environnement afin de s'assurer de la fiabilité des informations produites par l'application en question.

En revanche, les objectifs et le périmètre de l'audit d'efficacité et de performance d'une application sont variables et définis au cas par cas (Audit sur mesure).

Un audit complet d'une application couvre les deux volets. Dans ce chapitre, nous allons nous limiter à l'audit de fiabilité et de sécurité des applications en raison de son importance capitale pour l'expert comptable dans sa mission de certification des états de synthèse.

1. Démarche générale d'un audit d'application

La démarche de l'audit d'une application dans le cadre d'une mission d'audit comptable et financier peut s'articuler autour des axes suivants :

- Prise de connaissance du cadre général de l'application étudiée ;
- Analyse des risques et des contrôles ;
- Identification et évaluation des risques et des contrôles d'application
- Test des contrôles d'application ;

1.1 Prise de connaissance du cadre général de l'application

Cette phase a pour objectif de comprendre l'environnement général dans lequel l'application a été développée ou acquise, mise en service et exploitée. Ceci permet de cerner l'environnement de contrôle de l'application. Cette prise de connaissance portera notamment, sur :

- Les systèmes sur lesquels l'application est installée;
- La méthodologie utilisée pour son développement et sa mise en service ;
- Le langage utilisé pour son développement, ses interfaces, sa portabilité, son intégration avec les autres systèmes et applications de l'entreprise;
- Ses programmes sources.
- La nature, la qualité et la fiabilité du hardware et du système d'exploitation utilisé (Micros, client serveur, mainframe) ;
- Le mode de fonctionnement de l'application (on line, batch) ;
- Les données, les fichiers et les tables clés utilisés par l'application ;
- Les flux de traitement des informations (données en entrée, traitement et sorties…) ;
- Les contrôles d'accès à l'application ainsi que l'adéquation des habilitations accordées aux utilisateurs avec leur profil ;
- Le mode de contrôle de l'exécution des programmes ;
- Le système du back up et de la restauration des données et des programmes ;
- La période de conservation des données ainsi que l'implication des utilisateurs ;
- La détermination de la période des données à conserver ;
- L'implication des utilisateurs dans le système de protection des données et de la maintenance des programmes.

En outre, l'auditeur devra apprécier la compétence et la qualité de l'éditeur et/ou les informaticiens de l'entreprise ayant développé et mis en service l'application étudiée. Dans le cas où celle-ci aurait été acquise, l'auditeur devra s'assurer que l'entreprise a pris les garanties nécessaires lui permettant d'assurer son exploitation normale (pérennité de l'éditeur, transfert des programmes sources, transfert des compétences en interne…).

En revanche, si l'application a été développée en interne, une attention particulière devra être portée notamment, sur la méthodologie utilisée ainsi que sur la compétence des informaticiens et les utilisateurs clés ayant été impliqués dans le processus de son développement.

La revue préliminaire portera aussi sur l'examen des interfaces. En effet, il y a lieu d'obtenir le détail des applicatifs qui sont interfacés avec l'application étudiée et de documenter les données échangées entre elles, et de vérifier si ces interfaces sont contrôlées.

Par ailleurs, l'auditeur devra revoir la documentation relative à l'application étudiée dont notamment les manuels d'utilisation ; les flowcharts, les schémas fonctionnels, les tables de décision. Il examinera aussi les définitions des données, les entrées, les traitements, les sorties, la séquence des opérations, ainsi que les procédures d'utilisation, de transmission, de contrôle, d'identification et de correction d'erreurs.

Une fois la revue préliminaire a été effectuée, l'auditeur doit effectuer des tests de cheminement (walk through) afin de confirmer sa compréhension des processus de traitement des transactions, des contrôles mis en place et des risques potentiels.

A l'issue de cette étape, l'auditeur devra établir des flowcharts ou overviews ou des narratifs synthétiques lui permettant d'identifier les risques afférents à l'application étudiée et d'analyser les contrôles mis en place en vue de gérer ces risques.

1.2 Identification et évaluation des risques et des contrôles d'application

Avant d'aborder l'analyse des risques et des contrôles liés aux applications, il y a lieu de rappeler les objectifs de contrôle qui permettent de valider les assertions relatives aux états financiers. Ces objectifs sont généralement au nombre de quatre :

- Exactitude des enregistrements : Tous les éléments des transactions traitées par le système sont corrects, (montant, compte…) ;
- Exhaustivité : Toutes les transactions réalisées par l'entreprise sont traitées d'une manière exhaustive par le système;

- Validité des enregistrements : Toutes les transactions et les données permanentes sont autorisées et sont réelles (absence de double traitement et/ou des opérations fictives).
- Accès restreint aux actifs et aux enregistrements : Les actifs et les données sont protégés contre les accès non autorisés.

1.3 Analyse des risques et des contrôles

Cette étape a pour objectif de:

- Recenser les risques, évaluer leur impact potentiel sur les éléments financiers, évaluer la probabilité de leur survenance et les classer selon leur degré d'importance (impact et probabilité de survenance);
- Identifier les contrôles, analyser leur pertinence par rapport aux risques identifiés et dégager les risques résiduels (non couvert par les contrôles).

L'analyse des risques et des contrôles permet de cibler l'approche d'audit. En effet, les travaux d'audit seront focalisés sur les tests des contrôles clés et sur l'évaluation de l'impact des risques non couverts par le contrôle interne sur les états financiers.

L'identification des risques sera réalisée en prenant en compte la compréhension du business du client, des processus gérés par l'application étudiée et des facteurs de risques y afférents. Parmi ces risques nous pouvons citer:

- La possibilité de saisie des données erronées ou non autorisées ;
- La possibilité de modifier, supprimer ou d'ajouter des données sans autorisation ;
- L'absence de procédure d'identification, de correction et de recyclage des données rejetées ;
- Le traitement erroné ou incomplet des données ;
- L'exécution de traitement non autorisée ;
- L'absence de contrôle d'intégrité des données saisies, traitées et éditées ;
- L'absence de contrôle du contenu et de la destination des résultats des états de sortie ;
- L'absence de contrôle sur le traitement et la transmission des fichiers.

A l’issue de cette étape, l’auditeur établira un programme de travail ciblé en vue de tester les contrôles d’application identifiés et d’évaluer l’impact éventuel des risques résiduels sur les états financiers.

Par ailleurs, il devra aussi identifier les risques non couverts par les contrôles (programmés ou manuels). En effet, les risques non contrôlés feront l’objet d’une attention particulière par l’auditeur financier lors de ses travaux de validation des comptes.

1.4 Test des contrôles d’application

Une fois les risques et les contrôles d’application ont été identifiés et évalués. Il y a lieu de procéder aux tests de ces contrôles afin de s’assurer de la permanence de leur fonctionnement. En effet, si les tests mettent en évidence que les contrôles sont opérationnels, l’auditeur financier peut s’appuyer sur ces contrôles dans sa démarche de validation des comptes. Dans le cas contraire, ils seront considérés comme inexistants, et par conséquent, il adoptera une approche basée essentiellement sur des tests substantifs des comptes (examen étendu de la majorité des transactions).

Avant d’aborder les contrôles d’application, il est utile de les définir.

1.4.1 Définition et caractéristiques des contrôles d’application

Les contrôles d’application sont conçus et mis en place afin d’assurer l’intégrité des enregistrements, ils peuvent être manuels ou automatiques, préventifs, détectifs ou correctifs.
Les contrôles préventifs ont pour objectif de prévenir la survenance d’anomalies d’erreurs ou de fraude aussi bien au niveau des entrées et des traitements qu’au niveau des sorties. En revanche, les contrôles détectifs permettent l’identification de ce type d’événements.

Les contrôles correctifs visent à minimiser l’impact des erreurs ou anomalies et fraudes découvertes. Ils permettent non seulement de les corriger et de les recycler mais aussi de modifier les processus du système de façon à éviter qu’elles se reproduisent dans l’avenir.

Contrairement aux contrôles généraux informatiques qui s'exercent au niveau global de la fonction informatique, les contrôles d'application opèrent au niveau des transactions. En effet, ils procurent une assurance d'audit direct quant à la fiabilité des enregistrements.

Par ailleurs, il y a lieu de noter l'interconnexion de ces deux types de contrôles. En effet, si les contrôles généraux informatiques ne fonctionnent pas correctement, ceci conduira forcément à l'inefficacité des contrôles d'application. C'est pour cela que l'auditeur devra normalement tester les premiers et conclure qu'ils fonctionnent correctement avant de procéder à la revue des contrôles d'application.

Ces derniers sont conçus et mis en place au niveau de chaque phase logique d'une application. Nous allons donc les passer en revue au niveau des principales étapes des processus d'une application à savoir : entrées, traitement, sorties, recyclage des rejets et des erreurs.

1.4.2 Contrôle des entrées

L'auditeur devra s'assurer que les procédures de contrôle sont mises en œuvre afin de garantir l'autorisation, l'exactitude, l'existence, et l'exhaustivité des transactions et des données permanentes. Ainsi, il est appelé à vérifier notamment

- Les procédures de contrôle d'accès ;
- Les procédures de la collecte et la saisie des transactions et des données ;
- Les procédures de traitement des données rejetées.

1.4.3 Contrôle d'accès

L'auditeur doit s'assurer que les contrôles prévus et mis en œuvre dans le système permettant de restreindre l'accès aux données, aux programmes et aux transactions aux seules personnes y habilitées. Parmi ces contrôles nous pouvons citer :

- Une gestion appropriée des mots de passe définie en fonction des ressources à partager (unicité de l'identifiant, absence de compte générique, longueur des mots de passe et leur changement périodique).
- Des procédures de détection et de contrôle des tentatives infructueuses des accès non autorisés ;

- Le respect du principe de séparation des tâches ;
- Des procédures de partage de l'accès aux données et aux transactions en fonction des profils et des tâches des utilisateurs et des informaticiens.

1.4.4 Contrôle de la collecte des données

L'auditeur devra vérifier l'existence et le fonctionnement des contrôles relatifs à la préparation et la collecte des données. En effet, des procédures devraient permettre de s'assurer que toutes les transactions et les données nécessaires sont collectées d'une manière exhaustive et qu'elles sont enregistrées d'une manière exacte et exhaustive.

Il y a lieu de souligner que dans les systèmes intégrés, les sorties générées par un module ou une application sont les entrées d'un autre module ou d'une autre application. Dans ce cas, l'auditeur doit vérifier les rapports d'intégrité du système.

1.4.5 Contrôle de l'enregistrement des données

L'auditeur devra vérifier les contrôles automatiques et manuels relatifs à l'enregistrement des données (autorisation, exactitude, et exhaustivité des données saisies et validité des données, identification et correction des erreurs et anomalies…etc.). Ainsi, il doit s'assurer notamment de l'existence et du fonctionnement des contrôles relatifs à:

- L'autorisation de toutes les données et les transactions enregistrées dans le système (génération des rapports de données nécessitant l'autorisation, définition d'un work-flow des processus prévoyant la validation des données avant le traitement par le système…) ;
- Changement des données validées et saisies dans le système ;
- L'interdiction de la saisie des données non valides (Exemple : mise en place de format des données permettant de limiter la saisie des données non valides);
- La détection des doubles-saisies, des saisies incomplètes, et des incohérences ;
- La réconciliation des brouillards de saisie avec les documents sources ;
- La saisie des données permanentes ;
- La garantie de l'unicité de la saisie des données ;
- Les rapprochements automatiques des données avec celles déjà saisies;
- La vérification de la séquence numérique;

- La réconciliation des totaux des données saisies (réconciliation annuelle ou automatique) ;
- La mise à jour des fichiers ;
- La vérification de l'exhaustivité et exactitude des fichiers ou entrées (tout fichier transmis doit contenir des zones de contrôle de l'exhaustivité et l'exactitude des données transmises : (contrôle des doublons, des trous, de la longueur et nombre des transactions)).

Il y a lieu de noter qu'il existe plusieurs types de contrôle des enregistrements que les entreprises peuvent mettre en place au niveau des applications informatiques. Parmi ces contrôles, nous pourrons citer à titre d'exemple :

- Les contrôles batchs : Ils permettent le contrôle des totaux et ils peuvent porter sur un total monétaire, le nombre d'articles ou le total des documents saisis ;
- Les contrôles de la séquence: Ils sont conçus de façon à ce que seules les données comprises dans la séquence prévue soient admises et que les doublons soient rejetés ;
- Les contrôles de limite : Ils sont conçus de façon à ce que seules les transactions n'excédant pas une certaine limite puissent être traitées ;
- Les contrôles d'intervalle : Ils sont conçus de façon à ce que seules les données comprises dans un certain intervalle soient admises;
- Les contrôles selon certains paramètres : Les données sont acceptées par le système selon des critères prédéterminés (masculin, féminin, … etc.)
- Les contrôles de double-saisie : La nouvelle transaction est comparée avec celle ou celles déjà saisie (s). Si une redondance est détectée, elle sera rejetée ;
- Les contrôles de vraisemblance : la vraisemblance des données est contrôlée selon une logique prédéterminée.

Lors de cette étape l'auditeur devra également s'assurer de l'existence et du fonctionnement des procédures de contrôles relatifs au traitement des données rejetées. En effet, il faudrait prévoir des procédures permettant la conservation, la vérification, l'analyse et le recyclage des données rejetées par le système.

1.4.6 Contrôle des traitements et des sorties des données

L'auditeur devra examiner l'existence et le fonctionnement des contrôles relatifs aux traitements. Ces contrôles ont pour objectif d'assurer l'exhaustivité et l'exactitude des données accumulées (résultats des traitements…). L'auditeur devra s'assurer notamment que :

- Toutes les opérations traitées sont journalisées ;
- Les totaux de fin de traitement sont comparés aux totaux de contrôle ;
- L'intégrité des données est assurée ;
- La piste d'audit est prévue dans le système.

Il y a lieu également de vérifier l'existence et le fonctionnement des procédures de contrôle permettant le bon déroulement des programmes selon la logique prévue (respect des séquences de traitement, utilisation des bons programmes et des bons fichiers).

En ce qui concerne les sorties de données, Il faudrait s'assurer notamment que:

- La distribution des états est contrôlée ;
- Les états de sorties sont testés avant leur distribution ;
- Les résultats des sorties sont validés par les utilisateurs ;
- L'intégrité, l'exhaustivité et l'exactitude des données transmises entre les différents modules d'une application sont systématiquement contrôlées.

Il faut noter qu'il existe plusieurs types de contrôles des traitements que les entreprises peuvent mettre en place au niveau des applications. Parmi ces contrôles de traitement, nous pouvons citer à titre d'exemples :

- Recalcule manuel : Sélectionner un échantillon des transactions et recalculer manuellement et comparer le résultat avec le traitement du système ;
- Programme d'audit : Il peut être utilisé pour vérifier le bon déroulement des traitements ;
- Contrôle de limite;
- Contrôle de vraisemblance;
- Rapports d'exception: Un rapport d'exception qui génère les données erronées compte tenu de certains critères prédéfinis.

2. CAS PARTICULIER DE LA REVUE D'UN PROGICIEL INTEGRE (ERP : ENTREPRISE RESSOURCES PLANNING) JDEDWARDS

Avant d'aborder les particularités de la revue des contrôles d'application dans l'environnement des progiciels intégrés, il est utile de rappeler leurs caractéristiques ainsi que les principales zones de risque.

- **Rappel des principales caractéristiques des progiciels :**

L'évolution de l'information a connu ces dernières années une croissance exponentielle en matière de traitement de l'information comptable et de gestion. Cette évolution a engendré en conséquence des problèmes d'hétérogénéité des systèmes et des applications informatiques.

Pour remédier à cette situation, les éditeurs de logiciels ont mis en place des systèmes intégrés appelés ERP (entreprise ressources planning) qui englobent l'ensemble des besoins fonctionnels (immobilisations, achats, ventes, production et gestion de stocks, logistique).

Ces logiciels intégrés permettent d'avoir une vue unique et cohérente de l'information grâce à une base de données commune et à une intégration des différents modules de L'ERP. En outre, ces progiciels sont diffusés en nombre important ce qui implique :

- Une meilleure qualité des développements a priori : la revue application portera généralement sur les aspects recettes, exploitation et contrôles applicatifs ;
- L'existence des guides d'audit (SAP, Oracle financial, JDE, …etc.) ;

Par ailleurs, ils offrent plusieurs avantages dont notamment :

- Une adaptation d'implémentation dans différents secteurs d'activité grâce à la flexibilité de leur système de paramétrage;
- La mise en place d'un ERP engendre une revue des chaînes de valeur en vue de les optimiser et d'éliminer les tâches et les contrôles redondants. Cela doit s'accompagner par un redéploiement des effectifs et une revue des procédures de contrôle et des fiches de fonction;

- La richesse des fonctionnalités et des contrôles prévus dans les ERP permettent d'intégrer l'ensemble des besoins de l'entreprise et renforcer le dispositif du contrôle (rapprochement automatique des comptes bancaires, gestion de l'inventaire physique, automatisation des écritures comptables, génération automatique des factures, des règlements…etc.) ;
- L'harmonisation des procédures et des règles de gestion entre les différentes unités du business.

- **Les principales zones de risque :**

Les principaux risques que nous pouvons rencontrer dans un environnement ERP sont généralement les suivants:

- Progiciels en phase de prototype ou peu diffusés;
- Etude des besoins insuffisante ;
- Prise en compte des contraintes de l'organisation insuffisante ;
- Dépendance vis-à-vis des fournisseurs ;
- Non prise en compte des besoins du contrôle interne au moment de la refonte des processus lors de la mise en place d'un ERP: En effet, comme cela a été signalé ci-dessus, l'implémentation d'un ERP s'accompagne par la refonte des processus ce qui pourrait se traduire par des suppressions des contrôles clés. Afin d'éviter ce type de risque, de nouvelles dispositions doivent être prises en compte et adaptées à l'environnement de l'ERP mis en place.

Afin de mieux illustrer la spécificité de l'approche d'audit dans un environnement ERP, nous présenterons ci-après la méthodologie de revue des contrôles d'application dans l'environnement JDE World (version qui tourne sous l'environnement du système d'exploitation AS400 : système mini d'IBM).

La revue de l'ERP JDEdwards dans le cadre des missions d'audit comptable et financier couvre deux aspects :

- La revue des contrôles relatifs à l'intégrité, la sécurité et le master data (données permanentes) ;
- La revue des contrôles relatifs aux processus.

2.1 La revue des contrôles relatifs à l'intégrité, la sécurité et le master data

Ces contrôles sont communs à tous les modules de JDE. Leur bon fonctionnement conditionne la fiabilité des données produites par l'ERP. Il est donc capital de vérifier le design et le fonctionnement de ces contrôles.

2.1.1 Revue des rapports d'intégrité

Il est vital que toutes les transactions soient saisies d'une manière exacte et exhaustive dans les comptes. Les rapports d'intégrité sont des outils de contrôle de l'exhaustivité et l'exactitude de l'enregistrement des données dans le module de la comptabilité générale (GL : general ledger accounts). En effet, les transactions enregistrées dans les sous modules doivent être conformes à celles déversées dans le module de la comptabilité générale. Ces outils de contrôle sont disponibles au niveau de JDE et doivent être édités et contrôlés régulièrement. Toute différence identifiée dans ces rapports peut avoir un impact significatif sur la fiabilité des états financiers.

La plupart des rapports clés d'intégrité sont pré-configurés et fournis avec JDE. Mais, quelques-uns uns doivent être créés et implémentés. En revanche tous les rapports d'intégrité nécessitent une configuration propre afin de s'assurer qu'ils sont reliés aux bons fichiers et qu'ils incluent le bon rang de l'objet compte (Object account) par exemple. « accounts payable to general ledger».

Compte tenu que, la revue des rapports d'intégrité nécessite l'intervention d'un spécialiste JDE. L'auditeur avec l'assistance de cet expert devra s'assurer notamment que :

- Les rapports standards d'intégrité (cf. annexe 2) ont été mis en place ou créés et correctement configurés. Les objets comptes doivent pointer aux bons fichiers (la vérification de ceci nécessite l'assistance d'un spécialiste JDE) ;
- Les rapports sont régulièrement édités, contrôlés et les éventuelles différences corrigées ;
- La nature et l'évolution des différences sont analysées et suivies. Les rapports d'intégrité doivent être édités, même si les différences sont nulles ou non significatives.

Après avoir vérifié la configuration et l'exploitation des rapports d'intégrité, il y a lieu d'éditer, de tester et d'analyser les résultats de ces rapports sur plusieurs jours. Ceci permettra d'apprécier leur fonctionnement et d'analyser l'évolution des éventuelles différences identifiées.
Dans le cas où des erreurs seraient identifiées au niveau des rapports d'intégrité cela pourrait avoir un impact significatif sur les états financiers. Par conséquent, l'auditeur doit évaluer l'impact de ce type d'erreurs sur l'opinion d'audit, ainsi que sur les travaux d'audit à effectuer sur les comptes.

Il faut noter que si l'exercice comptable a été clôturé, il n'est possible d'éditer les rapports d'intégrité c'est pour cela que l'auditeur devra les demander avant la clôture de l'exercice.

2.1.2 Revue de la sécurité (JDE World)

En plus de l'audit des aspects de la sécurité évoqués dans le précédent chapitre, il y a lieu de revoir les éléments spécifiques à l'environnement JDE. Cette revue devra permettre de s'assurer que les paramètres de la sécurité de JDE ont été correctement configurés. Le paramétrage de la sécurité doit garantir le respect du principe de séparation des tâches. Le respect de ce principe est un objectif central de la sécurité des applications dans l'environnement JDE, et il est difficile à atteindre.

En effet, une bonne implémentation de la sécurité prévue par JDE permet de garantir le respect du principe de séparation des tâches. Ainsi, l'auditeur devra revoir la manière dont les paramètres et les standards de la sécurité JDE ont été mis en œuvre.

En outre, il est important de s'assurer que l'accès aux menus, commandes et fonctionnalités critiques ont été restreints aux personnes appropriées.

Par ailleurs, l'auditeur devra également vérifier que les constantes de sécurité du système ont été bien implémentées et que les procédures de leur mise à jour sont prévues et fonctionnent correctement.

2.1.3 Revue du master data (JD Edwards World)

Le Master Data constitué des données et des règles permanentes dont les principales sont les suivantes :

- Les données permanentes relatives à la base de données commune(Adress Book) qui permet de partager les informations entre tous les modules de JDE, d'éliminer les redondances des données et réduire les erreurs ;
- Les règles de gestion ;
- Les données et les règles relatives à la sécurité ;
- Les données comptables (instructions de comptabilisation automatique, plan comptable…etc.) ;
- Les données et les règles relatives à la gestion des stocks (inventaires, tarifs…etc.)

Il y a lieu de souligner que dans le cas où des faiblesses auraient été identifiées au niveau des contrôles relatifs au master data cela pourrait affecter la fiabilité des états financiers.

Afin d'assurer l'exactitude et l'exhaustivité des transactions traitées et des données permanentes, il faudrait veiller à la garantie de la fiabilité du master data. La réalisation de cet objectif dépend largement de la qualité des procédures de contrôle interne portant sur :

- La mise en place de JDE ;
- La migration des données ;
- La maintenance du master data.

Lors de sa revue du master data l'auditeur devra s'assurer que:

- Les procédures de contrôles de création des données dans le master permettent de garantir l'exactitude et l'exhaustivité de ces données ;
- Tous les changements affectant les données du master data sont autorisés et revus ;
- Les tâches relatives aux opérations touchant chaque catégorie des données du master data (clients, tarification, crédit client, contrôle des paiements,

banques…etc.) sont attribuées de façon à permettre de respecter le principe de séparation des tâches ;

- Les opérations relatives à la gestion du plan comptable et des instructions de comptabilisation automatiques ne sont pas accessibles aux utilisateurs (limitation à une personne habilitée).

2.2 La revue des processus (business process)

Les processus gérés par JD Edwards comprennent :

- Les achats et les comptes fournisseurs (purchases & payables) ;
- Les ventes et les comptes clients (revenues & receivables) ;
- Les stocks (inventories) ;
- Les immobilisations (fixed assets) ;
- La comptabilité générale (general ledger) ;

Il y a lieu de souligner que si les procédures de contrôle relatives à la sécurité, à l'intégrité et au master data ne sont pas fiables, il sera inapproprié de tester les contrôles relatifs aux processus. Il est plus judicieux dans ce cas de remédier d'abord aux faiblesses identifiées à ces niveaux là avant de procéder aux tests des contrôles relatifs aux processus.

Par ailleurs, il y a lieu de noter que les principes des contrôles relatifs aux processus dans le cadre de l'environnement JDE sont similaires à ceux gérés sous d'autres environnements. La différence réside dans les possibilités offertes par JDE pour concevoir et mettre en place ces principes de contrôle

Dans le cadre de ce mémoire nous avons présenté en annexe3 les principaux travaux de revue à effectuer sur les processus achats-fournisseurs, ventes-clients, immobilisations et comptabilité générale.

TITRE 2 : PROCESSUS DE L'AUDIT DANS LE CADRE D'AUTRES MISSIONS D'AUDIT INFORMATIQUE

L'évolution informatique offre à l'expert comptable, qui se spécialise dans l'audit informatique, de nouvelles opportunités professionnelles. Dans le chapitre 1, nous allons présenter d'une manière synthétique l'approche d'audit informatique dans le cadre d'une mission spéciale qui présente une obligation réglementaire (revue du dossier financier des compagnies d'assurances). Nous allons proposer également dans le chapitre 2, une méthodologie pour l'audit de la sécurité dans le cadre d'une mission de revue des domaines informatiques (Trust domaine).

CHAPITRE 1: PROPOSITION D'UNE APPROCHE D'AUDIT DE LA MISSION CONNEXE DU COMMISSAIRE AUX COMPTES RELATIVE A L'EXAMEN DU DOSSIER FINANCIER

L'objectif de ce chapitre est de proposer une démarche pour la conduite de la revue des systèmes informatiques dans le cadre de l'examen limité du compte rendu statistique et financier.

En effet, conformément aux dispositions de l'article 245 du code des assurances, les commissaires aux comptes sont appelés à procéder à l'examen du dossier financier, préparé par les compagnies d'assurances et envoyé à la Direction des Assurances et de la Prévoyance sociale (DAPS).

Les modalités pratiques de l'exécution de cette mission telles que définies par le procès verbal (cité dans le paragraphe 3.1.1 du chapitre 1 du titre1 de la première partie) prévoient la revue des systèmes informatiques. Les travaux effectués par les commissaires aux comptes dans le cadre de cette mission sont définis par la norme internationale relative aux missions d'examen sur la base des procédures convenues

1 Approche d'audit de l'évaluation du système d'information dans le cadre mission du CAC de revue du dossier financier

Compte tenu du fait que les informations figurantes dans les états du dossier financier sont générées par des systèmes informatisés, l'évaluation de ces dernières est une étape obligatoire de la mission de revue du Dossier Financier.

Les travaux de la revue informatique dans le cadre de l'examen du Dossier Financier doivent porter sur les volets suivants :

- Prise de connaissance de l'environnement informatique,
- Revue des systèmes contribuant à la production du dossier financier,
- L'analyse des données et les tests (éventuellement).

1.1 L'évaluation de l'environnement informatique

Il y a lieu de noter que les travaux relatifs à cette phase sont effectués lors de la mission de certification des états financiers. Ils seront mis à jour lors de cette mission connexe. Nous rappelons que ces travaux ont pour objectif d'apprécier dans quelle mesure les systèmes informatiques influencent les risques d'audit (risques inhérents et de contrôle). Ils portent sur les aspects suivants :

- L'organisation, la planification de la fonction informatique ;
- Le développement, l'acquisition, l'implémentation et la maintenance des applications et programmes informatiques ;
- L'exploitation informatique ;
- La sécurité des actifs informatiques et des accès aux ressources informatiques.

La revue de ces aspects a été développée dans le chapitre 1 du titre 1 de cette partie (voir ci-dessus).

1.2 Evaluation des applications informatiques contribuant à la génération du dossier financier

Cette étape a pour objectif d'identifier les processus informatiques concourant à la production du dossier financier et d'évaluer les contrôles y afférents.

1.2.1 Identification des processus informatiques significatifs

Il s'agit d'identifier les processus informatiques qui contribuent à l'élaboration du dossier financier et dont l'évaluation des contrôles y afférents est nécessaire. Il y a lieu de noter que les tests informatiques sont plus efficaces sur les systèmes traitant un volume important de transactions. Ainsi, ils porteront notamment sur les processus métiers (sinistres et production). En revanche, pour les autres processus qui sont généralement peu informatisés (réassurance, recouvrement et placement) les tests manuels sont privilégiés.

1.2.2 Tests des contrôles afférents aux processus métiers (production et sinistres)

Ces tests ont pour objectif de s'assurer que les données traitées par un processus sont exhaustives, exactes, et réelles. Ils seront axés sur les volets suivants :

- Le contrôle permanent des données et des traitements afin de s'assurer qu'ils sont correctement saisis, revus et conservés ;
- La gestion de la sécurité logique applicative ;
- Le contrôle des sorties et des données rejetées.

2 Présentation d'un cas pratique de revue des systèmes informatiques da de l'examen du dossier financier

2.1 Objectif de la mission :

Notre mission avait pour objectif d'apprécier les informations contribuant à l'élaboration du dossier financier. Elle a porté sur l'évaluation de l'environnement informatique et sur la revue des applications informatiques qui génèrent les informations servant à la production du dossier financier.

2.2 Evaluation de l'environnement informatique :

Lors de cette étape nous avons procédé à une revue des contrôles généraux informatiques. Ces derniers ont été développés dans le chapitre 1 du titre 1 de la deuxième partie.

2.3 Revue des applications informatiques :

Lors de cette étape, nous avons identifié les principaux processus et les contrôles clés y afférents dans un premier temps et par la suite nous avons procédé aux tests de ces contrôles.

2.3.1 Identification des processus et des contrôles y afférents

Afin d'identifier les processus significatifs, nous avons élaboré la cartographie des flux d'information de la compagnie et avons analysé la provenance des données servant à l'élaboration du dossier financier. Ainsi nous avons retenu deux grands processus à savoir:

- La gestion des sinistres;
- La gestion de la production.

En effet, le dossier financier est établi sur Excel (processus manuel qui est décrit dans l'annexe…). Mais la majorité des informations proviennent des deux processus cités ci-dessus et certaines données proviennent directement de la comptabilité.

Les processus de la production et des sinistres sont gérés par un progiciel dont le noyau a été acquis par la compagnie à la fin des années 80 et qui a été complété par des développements spécifiques effectués par l'équipe interne.

Lors de cette intervention, nous avons établi le mapping de ces processus et de leurs sous processus ce qui nous a permis d'identifier (voir annexe 6) :

- Les entrées ;
- Les traitements;
- Les sorties ;
- Les contrôles ;
- Les interfaces.

2.3.2 Tests des contrôles identifiés

Une fois les contrôles clés identifiés, nous les avons testés. Ces derniers ont été mis en ouvre de façon à s'assurer de:

- L'exhaustivité, l'exactitude et la réalité des données saisies et des traitements ;
- La sécurité logique relative aux applications;
- L'exhaustivité et l'exactitude des sorties;

2.4 Résultat des travaux et conclusions

A l'issue de nos travaux, nous avons conclu que les données produites par les systèmes métiers sont globalement fiables. Toutefois, nous avons relevé des faiblesses aussi bien au niveau de l'environnement informatique qu'au niveau des applications.

2.4.1 Faiblesses relatives à l'environnement informatique

Principaux points faibles sur le plan technique :

- Système d'information coûteux en termes de maintenance matériel et logiciel;
- Non ouvert en terme d'architecture;
- Forte dépendance vis-à-vis de l'éditeur;
- Structure en fichiers plats rendant difficile la restitution rapide de l'information à l'aide d'outils standards de type SQL ou Query ;
- Toute demande de modification spécifique nécessite un programme en Cobol.

Principaux points faibles sur le plan de la sécurité :

- Absence d'un plan de sécurité définissant la politique de sécurité informatique et les procédures de sa revue ;
- Absence d'un responsable dédié à la sécurité des systèmes d'information ;
- Les dispositions de la sécurité physique relative à l'accès aux salles des machines informatiques sont perfectibles ;
- Absence de procédures de revue des profils utilisateurs ;
- Absence de changement régulier des mots de passe au niveau de certaines applications ;

2.4.2 Faiblesses relatives aux applications

Principaux points faibles relatifs à la production des états du dossier fina

- Le processus d'établissement des états du dossier financier est manuel (tableur Excel) ;
- Non respect du principe de séparation des tâches (la même personne établit un état et procède à son contrôle).

Principaux points faibles relatifs aux applications informatiques en amon dossier financier

- Absence de procédures de saisie/validation et de l'annulation des quittances ;
- Absence d'interface entre le suivi des primes et les mises en demeure ;
- Absence du suivi de la compensation des sinistres (risque du double règlement des sinistres).

CHAPITRE 2: PROPOSTION D'UNE METHODOLOGIE D'AUDIT DE LA SECURITE INFORMATIQUE

Face à l'ampleur des risques qui menacent aujourd'hui les systèmes d'information des entreprises, les dirigeants sont devenus plus préoccupés par cette problématique et demandeurs de missions d'audit et de conseil dans ce domaine.

Ce chapitre est consacré à la présentation d'une méthodologie pour la conduite d'une mission d'audit et au rappel des bonnes pratiques de politique et d'organisation de la sécurité du système d'information.

1. Démarche d'audit de la sécurité informatique

La démarche suivie par l'auditeur informatique lors d'une mission de revue des aspects de sécurité d'un système d'information s'articule généralement autour des étapes suivantes **:**

- Prise de connaissance ;
- Analyse des risques ;
- Evaluation de la sécurité des systèmes ;
- Elaboration de recommandations.

En annexe 4, nous avons repris l'exemple d'un programme de travail que nous avons déroulé lors d'une mission d'audit de sécurité d'un environnement de confiance (Trust Domain) d'une société de la place. Ce programme reprend les diligences d'audit mentionnées dans les paragraphes 1.1, 1. 2 et 1. 3 du présent chapitre.

1.1 Prise de connaissance

Cette étape a pour objectif d'avoir une vue systémique du système d'information de la société, et de recenser tous les standards et les règles de sécurité en vigueur.

A partir des documents de l'entreprise, des entretiens et des visites des locaux, l'auditeur informatique doit collecter l'information relative :

- Aux matériels: serveurs, stations de travail, équipements réseaux, firewalls;
- Aux logiciels: systèmes d'exploitation, applications de gestion, ERP ;
- Aux communications: architecture du réseau (topologie), plan de câblage et connexions avec l'extérieur;
- A l'organisation:
  - Politique de sécurité;
  - Normes et standards en vigueur;
  - Personnes et équipes impliquées dans la fonction informatique;
  - Définition des responsabilités;
  - Procédures appliquées,
  - Plans des sauvegardes, d'archivage de secours, de reprise, …etc.
- Volumétrie: Nombre d'utilisateurs, volume de données en production et taille des données sauvegardées.

A l'issue de cette étape, et selon le périmètre de la mission d'audit de sécurité, l'auditeur informatique peut faire appel à des experts spécialisés dans la revue de sécurité des :

- Systèmes d'exploitation comme l'AS/400 ou l'Unix ;
- ERP comme JD Edwards ou SAP ;
- Matériels et logiciels réseaux LAN et WAN ;
- Matériels et logiciels Internet : firewall, IDS (Intrusion Detection Systems), …etc.

Nous avons présenté en annexe 5 un exemple des travaux d'audit relatifs aux aspects de la sécurité dans l'environnement de JD Edwards world. Ils ont été réalisés par un expert spécialise de la sécurité sous environnement JDEdwards et I Series (AS 400 : système d'exploitation IBM).

1.2 Analyse des risques

Cette étape a pour objectifs d'évaluer les enjeux de la sécurité du système, et notamment :

- Identification des scénarios de menace ;
- Evaluation de l'impact de ces scénarios sur les actifs, le patrimoine et l'activité de l'entreprise de la survenance de ces scénarios.

Cette analyse des risques permet donc de :

- Classer selon leur degré d'importance, les vulnérabilités qui seront identifiées ;
- Justifier le coût des actions correctives (comparaison du coût de la réalisation de la recommandation par rapport au coût de survenance de la menace) ;
- Hiérarchiser les recommandations.

Parmi les scénarios de menace associés à la sécurité d'un système d'information, nous pouvons citer :

- Interruption ou dysfonctionnement du réseau ;
- Interruption ou dysfonctionnement du serveur ;
- Perte de données ;
- Perte d'intégrité des données ;
- Divulgation d'information confidentielle ;
- Attaque des logiciels (infections logiques par des virus) ;
- Risques juridiques ;
- Répudiation ;
- Ecoute du réseau ;
- Saisie de transactions non autorisées ;
- Pénétration du site central par le réseau.

1.3 Evaluation de la sécurité du système

Cette étape a pour objectif de s'assurer que les contrôles mis en œuvre au sein ou autour du système audité sont en mesure de garantir une couverture suffisante des risques pesant sur le système.

Les principaux points à contrôler sont :

- Sécurité physique ;
- Sécurité de continuité d'exploitation ;
- Sécurité logique : contrôle des accès et des habilitations ;
- Existence d'un système de self assessement (audit et contrôle) ;
- Prise en compte de la sécurité dans les projets informatiques ;
- Respect de la réglementation et des lois en vigueur.

1.4 Emission de recommandations

Cette étape a pour objectifs de présenter un plan d'action sécurité qui devrait :

- Proposer une recommandation corrective pour chaque vulnérabilité identifiée et qui correspond à un risque ;
- Hiérarchiser les recommandations en fonction de l'importance du risque (application des résultats de l'étape d'analyse des risques) ;
- Définir un calendrier et un échéancier de réalisation des recommandations et désigner les responsabilités du personnel opérationnel de l'entreprise.

Les recommandations les plus fréquentes qui découlent d'un audit de sécurité sont résumées dans les points suivants :

1.4.1 Politique de sécurité

- Formalisation d'un document définissant la politique de sécurité;
  - Implication de la Direction Générale;
  - Cohérence de la sécurité ;
  - Définition claire des responsabilités.

- Existence d'une organisation dédiée à la sécurité :
  - Nomination d'un RSSI (Responsable de Sécurité du Système d'Information) ;
  - Séparation exploitation/administration de la sécurité.

- Sensibilisation du personnel à la sécurité de l'information (informaticiens et utilisateurs) :
  - Guides, communications, formation ;
  - Protection du SI de l'entreprise ;
  - Signature d'une convention de confidentialité de l'information par tout le personnel de l'entreprise (confidentiality agreement) ;
  - Prévention de la fraude (dont piratage) ;
  - Tout incident de sécurité causé par un employé pourrait être considéré comme une faute grave.

1.4.2 Sécurité Physique :

- Accès aux serveurs :
    - Installation des serveurs dans une salle machines munie d'un minimum de standards de sécurité (climatisation, ondulation, extincteurs de feu, détecteurs de feu, instruments de mesure de la température et de l'humidité, …etc.).

- Stockage des sauvegardes :
    - Placement des supports de sauvegardes dans un lieu sécurisé (coffre ignifuge) ;
    - Disponibilité d'une sauvegarde externe des données d'exploitation (dans le coffre fort d'une banque par exemple) ;
    - Périodicité de renouvellement des sauvegardes stockées à l'extérieur.

1.4.3 Sécurité logique :

- Contrôle d'accès logique :
    - Formalisation d'une procédure d'accès des utilisateurs aux ressources informatiques ;
    - Identification, authentification et autorisation de tous les utilisateurs ;
    - Mise en veille/déconnexion automatique après une période d'inactivité ;
    - Désactivation automatique des comptes utilisateurs en cas de tentatives infructueuses ;
    - Responsabilisation des utilisateurs.

- Gestion des mots de passe :
    - Caractère confidentiel et personnel du mot de passe ;
    - Règles de construction du mot de passe (longueur, composition, robustesse) ;
    - Règles de gestion (changement régulier des mots de passe, non réutilisation) ;
    - Procédures de réinitialisation en cas de perte de mots de passe.

- Mise à jour des habilitations accordées :
    - Cohérence entre les effectifs de l'entreprise et le fichier ID des utilisateurs ;
    - Prise en compte des changements de fonction des utilisateurs ;

- Procédures relatives à l’habilitation du personnel n’appartenant pas à l’entreprise (stagiaires, contractants, consultants et sous-traitants).

- Accès et habilitations du personnel
  - Revue des autorisations d’accès aux ressources sensibles ;
  - Les développeurs informatiques ne doivent pas être autorisés à accéder à l’environnement de production ;
  - Revue régulière par les propriétaires du SI, des autorisations à partir des données et des systèmes ;
  - Revue régulière des habilitations des utilisateurs par l’audit interne ou par le responsable sécurité (contrôle de la séparation des fonctions) ;
  - Revue régulière des accès pour détecter et analyser les tentatives de violation répétées et l’accroissement injustifié des accès réalisés sur des ressources sensibles.

2. Présentation d'un cas d'audit de la sécurité

Nous avons effectué pour le compte d'une grande filiale de multinationale une mission de revue de la sécurité de son système d'information. Cette mission s'insère dans un projet global de certification des systèmes d'information des sociétés du groupe et avait pour principal objectif l'évaluation de la conformité du système d'information de la société aux standards de sécurité adoptés par le groupe.

Notre démarche pour cette mission s'articulait autour des étapes suivantes :

- Planning : Dans cette étape, nous avons revu et validé le scope du projet de certification du SI de la société et avons défini le planning de notre intervention ;
- Revue de l'auto-évaluation (Self-assessment) : Dans cette étape, nous avons revu les travaux d'auto-évaluation effectués par l'équipe de contrôle interne de la société. Ces travaux ont été effectués sur la base d'entretiens et de revue de documentation ;
- Revue des déviations des standards de sécurité : Dans cette étape, nous avons identifié toutes les déviations par rapport aux standards établis et avons revu le bien fondé des raisons de ces déviations,
- Revue de l'implémentation des standards de sécurité : Dans cette étape, nous avons déroulé le questionnaire présenté en annexe 4, et avons vérifié la conformité du SI de la société par rapport à ces déviations ;
- Finalisation et rédaction du rapport : Dans cette étape, tous les points soulevés sont discutés avec le management de la société, documentés dans le dossier d'audit et repris dans le rapport final à destination de la direction du groupe.

Conclusion : Notre revue n'a pas révélé des points de non conformité significatifs.

Le guide d'audit que nous avons utilisé dans notre mission est présenté en annexe 4**.**

CONCLUSION DE LA DEUXIEME PARTIE

L'audit informatique dans le cadre des missions d'audit financier devient une exigence imposée par les normes professionnelles, mais il est également une nécessité en raison de l'évolution du contexte des organisations. En effet, dans le contexte actuel où les systèmes informatiques sont prépondérants dans la majorité des processus des entreprises il n'est plus possible de certifier les états financiers sans évaluer les systèmes d'information. La démarche des auditeurs devra donc être adaptée pour refléter cette nouvelle réalité. L'audit informatique en tant que support à l'audit financier est axé sur la fiabilité des informations financières produites par les systèmes. Il porte sur les contrôles généraux informatiques et les applications.

L'approche d'audit relative à ces deux aspects a été développée dans la deuxième partie de ce mémoire.

Par ailleurs, l'expert comptable en tant que commissaire aux comptes est appelé à effectuer des missions connexes qui impliquent la revue des systèmes d'information (examen du dossier financier, évaluation du contrôle interne des établissements de crédit y compris les aspects liés aux systèmes d'information). Dans le présent mémoire nous avons exposé une démarche pour la revue des systèmes dans le cadre de l'examen du dossier financier et nous avons illustré notre propos par un cas pratique.

L'expert comptable, en tant que conseiller de l'entreprise, est souvent appelé à assister le management dans la mise en place des procédures et outils permettant de gérer les risques. Une des missions le plus souvent demandée est celle relative à la revue des aspects de la sécurité. Le dernier chapitre de ce mémoire a été consacré à cet aspect.

CONCLUSION GENERALE

Aujourd'hui le monde économique est caractérisé par la libéralisation et la globalisation. Cette dernière est rendue encore plus rapide par les réseaux informatiques. En effet, la mondialisation s'accélère avec la capacité d'utiliser des moyens de transmettre des informations ou d'y accéder. Comme tout changement, cette évolution entraîne la modification des modèles de fonctionnement des entreprises.

Pour être compétitives dans l'environnement économique actuel, les entreprises marocaines sont appelées à opérer de profondes mutations tant au niveau de leurs stratégies qu'au niveau de la mise à niveau de leurs modes de gestion. Le processus de changement qui est enclenché par ce nouveau contexte les amène à maîtriser leurs systèmes d'information afin d'être compétitives et réactives.

En effet, les systèmes d'information sont devenus des leviers stratégiques qui accompagnent les entreprises dans leur mise à niveau et leur développement en leur permettant d'être performantes et réactives. Ceci implique une excellence dans la rapidité et la pertinence du traitement de l'information ce qui conduit le plus souvent à une refonte complète du système d'information et une redistribution des activités et des tâches aux différentes structures de l'organisation.

La dépendance croissante des entreprises de l'information et des systèmes qui la délivrent augmente avec le développement des technologies qui changent radicalement les organisations et les pratiques des affaires.

Il est évident que les systèmes d'information permettent à l'entreprise d'être performante et réactive, mais leur mise en place s'accompagne le plus souvent par une refonte des processus de l'organisation, ce qui pourrait se traduire par la suppression de certains contrôles clés dans la gestion des risques de l'entreprise.

Aujourd'hui, nous assistons à une forte intégration des systèmes et à leur ouverture sur les partenaires de l'entreprise. Ceci augmente considérablement la vulnérabilité des systèmes d'information et engendre de nouveaux risques.

Il y a lieu de noter que les risques inhérents aux systèmes d'information augmentent avec l'ouverture de ces derniers aussi bien en externe avec Internet qu'en interne à travers les outils d'Intranet.
Les entreprises doivent être conscientes des risques liés aux systèmes d'information et mettre en place les outils et les procédures de contrôle permettant d'empêcher leur survenance ou limiter leur impact.

Les législateurs ont émis de nouvelles dispositions visant à se prémunir contre les risques liés à l'utilisation des nouvelles technologies de l'information. Ils ont également imposé aux auditeurs d'évaluer et de tester les contrôles, y compris ceux liés aux systèmes informatiques.

Pour répondre aux nouvelles exigences réglementaires et aux contraintes et risques induits par les systèmes informatiques (intégration, ouverture, automatisation des contrôles, …etc.), les organismes professionnels de l'audit comptable et financier ont dû revoir leurs normes et méthodologies d'audit de façon à prendre en compte les enjeux de ce nouveau contexte.

Dans l'environnement actuel, où les systèmes informatiques sont devenus prépondérants et l'information comptable et financière est issue directement de ces systèmes il est inconcevable de certifier les comptes sans procéder à un audit de ces derniers.

Face à ce nouveau contexte, les cabinets d'audit ont procédé à une mise à niveau de leur méthodologie d'audit de façon à se conformer aux nouvelles normes professionnelles et dispositions réglementaires. Les nouvelles démarches proposées par les cabinets d'audit reposent largement sur la compréhension et l'évaluation des contrôles liés aux systèmes informatiques et sur les tests des contrôles programmés (contrôles automatisés).

Compte tenu que la compréhension de la fonction informatique et de son environnement est un préalable pour la réalisation des missions d'audit informatique nous avons exposé un aperçu relatif à :

- L'organisation, et l'environnement légal de la fonction informatique ;
- Aux phases du cycle de vie des systèmes informatiques ;
- Aux contrôles et risques liés aux systèmes informatiques.

La présentation de ces aspects a pour but de comprendre la manière dont les systèmes informatiques affectent le traitement de l'information et le contrôle interne de l'entreprise d'une part et d'idenfiter les risques liés aux systèmes informatiques d'autre part.

Par la suite nous avons proposé une approche d'audit pragmatique pour la réalisation des missions d'audit informatique en tant que support à l'audit comptable et financier. La démarche d'audit présentée a porté non seulement sur l'audit des contrôles généraux et les applications informatiques classiques mais aussi sur le cas particulier des progiciels intégrés dont la diffusion au sein des entreprises devient de plus en plus grande.

Nous avons également présenté des démarches pour la réalisation de certaines missions spéciales d'audit ou de revue informatique qui présentent soit un caractère obligatoire (mission de revue du dossier financier) ou un caractère prioritaire pour la gestion des risques informatiques (audit de la sécurité).

Nos propos ont été illustrés par des cas pratiques .

Par ailleurs, il y a lieu de souligner que les missions dans le domaine de l'audit et la gestion des risques informatiques sont nombreuses et variées. Ceci permet à l'expert comptable d'élargir le champ de ses missions et de se positionner en tant que conseiller et interlocuteur privilégié du management de l'entreprise.

Une des missions le plus souvent mandatée par le management de l'entreprise, en raison de son caractère prioritaire, est l'audit informatique opérationnel.
La démarche pour la réalisation de l'audit informatique opérationnel dépend des objectifs assignés à la mission et demande une plus grande expérience et expertise à l'auditeur. Généralement elle porte sur:

- L'évaluation de la rentabilité et la performance du SI ;
- L'appréciation de l'adéquation du SI aux besoins de l'entreprise ;
- L'évaluation de la pérennité du SI ;
- L'évaluation de la capacité d'évolution du SI.

Afin de se conformer aux règles de la loi Américaine Sarbanes Oxley, le management des filiales des multinationales cotées sur le marché Américain(USA) sollicite de plus en plus des missions d'audit et d'assistance relatives à l'évaluation, au design, à la documentation et aux tests des contrôles informatiques.

Compte tenu de l'importance de ces deux types de missions, les démarches d'audit y afférentes pourraient faire l'objet d'autres mémoires.

Par ailleurs, Il faut souligner qu'il existe de nombreuses autres missions dans le domaine de l'audit et le conseil en matière des procédures de contrôle et de gestion des risques informatiques, parmi ces missions nous pouvons citer :

- Mission d'audit informatique dans le cadre de la circulaire n°6 de BANK AL MAGHRIB ;
- Assistance à la définition des procédures de migration des données ;
- Revue de la gestion des projets informatiques.

Pour faire face aux nouvelles contraintes et saisir les opportunités de missions créées par l'utilisation des nouvelles technologies de l'information, l'expert comptable devra investir dans l'acquisition des compétences dans ce domaine.

BIBLIOGRAPHIE

A. Ouvrages :

Coopers & lybrand et L'IFACI : La nouvelle pratique du contrôle interne (les éditions d'organisation 1994)

G. Benedit/R.Keravel: Mission de révision: Evaluation du contrôle interne (entreprise et expertise comptable, édition Foucher)

Henry c. Lucas, jr : information technology for management (irwin mcgraw-hill : 7ième édition).

Steven alter information systems 'a management perspective' (the bengamin/cummings publishing company inc :2ième édition).

James e. Goldman : applied data communications 'a business-oriented approach' (John wiley & Sons :2ième édition).

Marc Thorin : audit informatique (3 ème édition Masson).

Brian jenkins & anthony pinkney : audit des systèmes et des comptes gérés sur informatique (édition publi-union).

Jean-patrick matheron : comprendre, merise 'outils conceptuels et organisationnels' (édition eyrolles).

Commission bancaire livre blanc sur la sécurité des systèmes d'information (2 ième édition).

Olivier lemant pour l'institut français des auditeurs consultants internes
conduite d'une mission d'audit interne (édition clet).

- ISACA, « CISA : Certified Information Systems Auditor », review manual, 2002.
- I.S.A.C.A. Guide cobit : Third edition
- PriceWaterhouseCoopers : technology forecast : 1998 (price waterhouse global technology center).

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
- 09 Irrégularités et actes illégaux
- 10 Gouvernance des systèmes informatiques
- 11 L’utilisation de l’évaluation des risques dans la planification de l’audit.

C Séminaires :

- Security and controls : Audit des contrôles dans l’environnement JDE : PriceWaterhouseCoopers, 2001

- Audit de la fonction informatique : animé par Françoit Vaillant (Directeur de l’audit informatique Groupe accord et enseignant à l’université de Paris dauphine) 2002, organisé par consilium

- Audit de la sécurité informatique organisé par consilium et animé par associé chez Deloitt Paris

- Audit des réseaux et télécommunications organisé par consilium et animé par Renaud Guillemot

- "L’audit informatique : concepts, méthodes, outils actuels, démarches pratiques" par claude salzman, mars 2002

- "computers assurance training 1" : PricewaterhouseCoopers, juillet 1997

- "computers assurance training 2" : PricewaterhouseCoopers, juillet 1998
- "Audit de la sécurité dans l'environnement as400" : PricewaterhouseCoopers, mai 1998
- "System analysis et design" : université de macgill Montréal 2000
- "Informatique system administration" : université de macgill Montréal 2000
- Audit de la sécurité

D Mémoires :

- Luc THEROND, « Proposition d'une méthodologie d'audit dans le cadre de l'évaluation du contrôle interne des entreprises informatisées », 1994 ;
- Omar SEKKAT « Le rôle de l'expert-comptable face aux risques de sécurité micro-informatique dans les PME - proposition d'une démarche » (mémoire d'expertise comptable), novembre 2002.
- Adnane Loukili, « incidence de la présence d'un site électronique sur la mission d'audit » mai 2005
- Mohamed Lassâd Borgi, « L'évolution des technologies de l'information et de la communication : Impact sur l'audit financier ». Année universitaire 2000-2001

F Principaux sites consultés

- www.IASACA.org
- www.clusif.asso.fr
- www.pwc.com (knowledgecurve.com)

PLAN DETAILLE

INTRODUCTION GENERALE 2

1. L'enjeu économique lié à l'évolution et au rôle des systèmes d'information dans un contexte de globalisation 2
1.1 Evolution des systèmes d'information 2
1..2 Rôle stratégique des systèmes d'information 2
2. Impacts des systèmes informatiques sur l'approche de l'audit financier 3
3. Problématique et objectifs du présent mémoire 3
3.1 Problématique du mémoire 3
3.2 Objectifs 5
4. Démarche adoptée 6

PARTIE I :

LA COMPREHENSION DU CADRE GENERAL DE LA FONCTION INFORMATIQUE : UN PREALABLE NECESSAIRE POUR LA REALISATION DES MISSIONS D'AUDIT INFORMATIQUE 8

INTRODUCTION DE LA PREMIERE PARTIE 9

TITRE 1 :

L'ENVIRONNEMENT ET L'ORGANISATION DE LA FONCTION INFORMATIQUE 10

CHAPITRE 1 : L'ENVIRONNEMENT ET L'OGANISATION DE LA FONCTION INFORMATIQUE DE L'ENTREPRISE 10

1. Rôle et caractéristiques des systèmes d'information 10
1.1 Rôle des systèmes d'information de gestion 10
1.2 Caractéristiques des systèmes d'information 11
2. Rôle et organisation de la fonction informatique 11
2.1 Rôle de la fonction informatique 11
2.2 L'organisation de la fonction informatique 12
2.2.1 Structure de la fonction informatique 12
2.2.2 Les principales attributions de la DSI 14
2.3 Principes de gestion et de contrôle interne relatifs à l'organisation de la fonction informatique 14
2.3.1 Rappel relatif au dispositif du contrôle interne 15
2.3.2 Le dispositif du contrôle interne relatif à l'organisation de la fonction informatique 18
2.3.2.1 Les bonnes pratiques en matière de pilotage de la fonction informatique 19
2.3.2.2 Le dispositif du contrôle interne relatif à l'organisation et le pilotage de la fonction informatique 20

CHAPITRE 2 : L'ENVIRONNEMENT LEGAL DES SYSTEMES D'INFORMATION 22

1. LA REGLEMENTATION COMPTABLE ET FISCALE 22
1.1 Au Maroc 22
1.1.1 La réglementation comptable 22
1.1.2 La réglementation fiscale 22
1.2 En France 23
2. LE CADRE JURIDIQUE GENERAL 23
2.1 – Le cadre juridique au Maroc 24
2.2 – Le cadre juridique en France 24
3. Réglementation spécifique aux dispositifs de contrôle interne liés au reporting financier 25
3.1 Revue du système d'information dans le cadre de la revue par le CAC du dossier financier établi par les compagnies d'assurance 25
3.2 Circulaire n° 6/G/2001 de Bank Al Maghrib relative au contrôle interne des Etablissements de crédit 25
3.3 La loi Sarbanes-Oxley (SOX) 27
3.4 Loi du 1er août 2003 sur la sécurité financière(LSF) 27

4. Les principales positions des organismes professionnels 28
4.1 Les normes marocaines 28
4.2 Les réflexions internationales 29
4.2.1 Les réflexions de l'IFAC (International Federation of Accountants) 29
4.2.2 Les réflexions du Conseil National des Commissaires aux Comptes (CNCC) en France 30
4.3 Autres réflexions : ISACA 30

TITRE 2 :

PRESENTATION DES CYCLES DE VIE DU SYSTEME D'INFORMATION DES RISQUES ET DES CONTROLES Y AFFERENTS 32

CHAPITRE 1: PRESENTATION DES CYCLES DE VIE ET DES METHODOLOGIES D'UN SYSTEME D'INFORMATION 32
1 LE CYCLE DE VIE D'UN SYSTEME D'INFORMATION 32
1.1 Description des phases des cycles de vie d'un système d'information 33
1.1.1 Etape d'étude de faisabilité 33
1.1.2 Phase de développement 33
1.1.2.1 Etape de conception 33
1.1.2.2 Etape de réalisation des programmes 34
1.1.2.3 Etape de mise en œuvre 34
1.1.3 Phase d'exploitation 35
1.1.4 Phase de maintenance 35
2. METHODES DE CONCEPTION ET DE DEVELOPPEMENT DES SYSTEMES D'INFORMATION 35

CHAPITRE 2 : IDENTIFICATION DES RISQUES ET DES CONTROLES LIES AUX CYCLES DE VIE DES SYSTEMES D'INFORMATION 37
1. LES RISQUES LIES AUX CYCLES DE VIES DES SYSTEMES D'INFORMATION 37
1.1 Définition du risque 37
1.2 Facteur de risque 37
1.3 Les risques liés au cycle de vie du système d'information 38
1.3.1 Risques liés à la planification 38
1.3.2 Risques liés au développement et à la mise en service des systèmes informatiques 38
1.3.3 Risques liés à la mise en service 39
1.3.4 Risques liés à l'exploitation 39
1.4 Gestion des risques 40
2 CONTROLES LIES AUX CYCLES DE VIE DES SYSTEMES D'INFORMATION 40
2.1 Les contrôles relatifs au développement et à la mise en œuvre des applications informatiques 41
2.2 Les contrôles relatifs à la gestion des modifications 42
2.3 Les contrôles relatifs à la sélection et à la mise en œuvre des progiciels 42
2.4 Les contrôles relatifs à la gestion des opérations d'exploitation informatique 43
2.5 Les contrôles relatifs aux procédures utilisateurs 44
2.6 Les contrôles relatifs au plan de secours 44

CONCLUSION DE LA PREMIERE PARTIE 46

PARTIE II

PROPOSITION D'UNE METHODOLOGIE POUR LA CONDUITE DES MISSIONS D'AUDIT INFORMATIQUE 48

INTRODUCTION DE LA DEUXIEME PARTIE 49

TITRE 1
LE PROCESSUS DE L'AUDIT INFORMATIQUE DANS LE CADRE DES MISSIONS D'AUDIT FINANCIER ET COMPTABLE 50

CHAPITRE 1 : PRESENTATION DE LA DEMARCHE DE L'AUDIT INFORMATIQUE DANS LE CADRE DES MISSIONS D'AUDIT FINANCIER ET COMPTABLE 50
1. Présentation de la nouvelle démarche générale de l'audit comptable et financier 50
1.1 Caractéristiques de la nouvelle approche d'audit 50

1.2 Les phases de la nouvelle approche d'audit comptable et financier 51
1.2.1 Phase d'acceptation et de poursuite de la mission 51
1.2.2 Phase de cadrage de la mission 52
1.2.3 Phase de compréhension 52
1.2.4 Phase d'évaluation 52
1.2.5 Phase de validation 53
2 DEMARCHE GENERALE DE L'AUDIT INFORMATIQUE 53
2.1 Cadrage de la mission 54
2.2 Compréhension de l'environnement informatique 54
2.2.1 L'organisation de la fonction informatique 55
2.2.2 Caractéristiques des systèmes informatiques 55
2.2.3 Cartographie des applications clés 56
2.3 Identification et évaluation des risques et des contrôles afférents aux systèmes 56
2.4 Tests des contrôles 57
2.5 Finalisation de la mission 58
CHAPITRE 2 : L'AUDIT DE LA FONCTION INFORMATIQUE (CONTROLES GENERAUX INFORMATIQUES) 60
1. Organisation, planification et management de la fonction informatique 61
1.1 Planification stratégique et management de la fonction informatique 61
1.2 Audit de l'organisation de la DSI 62
2 Développement, acquisition, implémentation et maintenance des applications et des programmes informatiques 62
3 Exploitation informatique 63
4 La sécurité des actifs informatiques et des accès aux ressources informatiques 64
5 Plans de sauvegardes et de secours informatique 65
5.1 Plan de sauvegardes 65
5.2 Plan de secours 66
6 Présentation d'un cas de revue des contrôles généraux informatique 67
6.1 Etendue et objectifs de la mission 67
6.2 Notre démarche 68
6.3 Notre conclusion 70
6.4 Principaux points relevés lors de notre mission 70
CHAPITRE 3 : AUDIT DES APPLICATIONS INFORMATIQUES 72
1. Démarche générale d'un audit d'application 72
1.1 Prise de connaissance du cadre général de l'application 73
1.2 Identification et évaluation des risques et des contrôles d'application 74
1.3 Analyse des risques et des contrôles 75
1.4 Test des contrôles d'application 76
1.4.1 Définition et caractéristiques des contrôles d'application 76
1.4.2 Contrôle des entrées 77
1.4.3 Contrôle d'accès 77
1.4.4 Contrôle de la collecte des données 78
1.4.5 Contrôle de l'enregistrement des données 78
1.4.6 Contrôle des traitements et des sorties des données 80
2. CAS PRTICULIER DE LA REVUE DU PROGICIEL INTEGRE (ERP : ENTREPRISE RESSOURCES PLANNING) JDEDWARDS 81
2.1 La revue des contrôles relatifs à l'intégrité, la sécurité et le master data 83
2.1.1 Revue des rapports d'intégrité 83
2.1.2 Revue de la sécurité (JDE World) 84
2.1.3 Revue du master data (JD Edwards World) 85
2.2 La revue des processus (business processes) 86

TITRE 2 : PROCESSUS DE L'AUDIT DANS LE CADRE D'AUTRES MISSIONS D'AUDIT INFORMATIQUE 87
CHAPITRE 1: PROPOSITION D'UNE APPROCHE D'AUDIT DE LA MISSION CONNEXE DU COMMISSAIRE AUX COMPTES RELATIVE A L'EXAMEN DU DOSSIER FINANCIER 88
1. Approche d'audit de l'évaluation du système d'information dans le cadre de la mission du CAC de revue du dossier financier 88
1.1 L'évaluation de l'environnement informatique 89
1.2 Evaluation des applications informatiques contribuant à la génération du dossier financier 89
1.2.1 Identification des processus informatiques significatifs 89
1.2.2 Tests des contrôles afférents aux processus métiers (production et sinistres) 89
2 Présentation d'un cas pratique de revue des systèmes informatiques dans le cadre de l'examen du dossier financier 90
2.1 Objectif de la mission 90
2.2 Evaluation de l'environnement informatique : 90
2.3 Revue des applications informatiques : 90
2.3.1 Identification des processus et des contrôles y afférents 90
2.3.2 Tests des contrôles identifiés 91
2.4 Résultat des travaux et conclusions 91
2.4.1 Faiblesses relatives à l'environnement informatique 91
2.4.2 Faiblesses relatives aux applications 92
CHAPITRE 2: PROPOSTION D'UNE METHODOLOGIE D'AUDIT DE LA SECURITE INFORMATIQUE 93
1. Démarche d'audit de la sécurité informatique: 93
1.1 Prise de connaissance 93
1.2 Analyse des risques 94
1.3 Evaluation de la sécurité du système 95
1.4 Emission de recommandations 96
1.4.1 Politique de sécurité 96
1.4.2 Sécurité physique 97
1.4.3 Sécurité logique 97
2. Présentation d'un cas d'audit de la sécurité 99
CONCLUSION DE LA DEUXIEME PARTIE 100
CONCLUSION GENERALE 101
BIBLIOGRAPHIE 105
PLAN DETAILLE 109
LEXIQUE DU SYSTEME D'INFORMATION 113
ANNEXES 122

LEXIQUE DU SYSTEME D'INFORMATION

L'informatique est définie par le dictionnaire de la langue française comme suit : « Science et technique du traitement automatique de l'information au moyen des ordinateurs ». En effet, c'est un ensemble d'outils et de méthodes qui permettent de saisir, stocker et échanger les données, et de traiter ces dernières afin d'obtenir des résultats pertinents à un problème donné ;

Le système d'information (SI) est constitué d'un ensemble de moyens, de ressources et d'éléments organisés en vue de recueillir, traiter, stocker et diffuser l'information. C'est un ensemble complexe, souvent hétérogène car constitué d'éléments qui se sont juxtaposés au fil du temps au gré des choix stratégiques, des évolutions technologiques des systèmes informatiques en place, et du développement de l'organisation elle-même.

Le système d'information peut aussi être, considéré aujourd'hui comme un ensemble cohérent composé :

- de plusieurs modules, sous-systèmes ou applications permettant ou facilitant l'automatisation de certains processus de l'entreprise ou de l'administration,
- d'une infrastructure permettant de véhiculer l'information entre ces sous-systèmes.

Aujourd'hui les SI des entreprises sont généralement informatisées. Ce sont ces systèmes automatisés auxquels nous faisons référence dans le présent mémoire qui font l'objet. Les termes souvent utilisés dans notre étude sont soit les systèmes informatiques soit les systèmes d'information.

L'audit informatique est effectué par une ou des personnes indépendantes internes ou externe à l'entreprise, en vue de donner une assurance sur la réalisation des objectifs du contrôle interne de la fonction informatique, et des conseils visant à améliorer le fonctionnement des systèmes d'information.

Le contrôle interne relatif à la fonction informatique est défini dans première partie (titre :1 chapitre 1 : 3.2).

L'audit comptable et financier est défini par le manuel des normes professionnelles marocaines, comme une mission ayant pour objectif de permettre à l'auditeur d'exprimer une opinion selon laquelle les états de synthèse ont été établis, dans tous leurs aspects significatifs, conformément à un référentiel comptable identifié et qu'ils traduisent d'une manière régulière et sincère la situation financière de la société, ainsi que le résultat de ses opérations et les flux de sa trésorerie.

Application

Programme contenant les traitements à appliquer aux données d'entrée (input) pour obtenir un résultat désiré (output).

Architecture à trois niveaux *Three Tiers Architecture*

Génération récente de l'architecture Client Serveur qui comporte trois composants (un pour les données, un pour les traitements, un pour la présentation) pouvant résider dans des endroits différents. Typiquement : les données sur un mainframe central, les traitements sur un serveur local, la présentation sur le PC (attention : l'expression "trois tiers" est un faux ami).

Architecture Client Serveur (*Client-Server Architecture)*

Architecture informatique qui vise à utiliser au mieux les ressources en puissance de traitement et en mémoire pour l'exécution des applications, en tirant parti des moyens disponibles sur les PC. Typiquement, les données sont concentrées sur le mainframe, la présentation est faite par le PC, les traitements sont répartis entre les deux. Cf. architecture à trois niveaux.

ERP : 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.

Base de données (*Database)*

Logiciel qui permet de stocker, classer, retrouver des données, et de réaliser des calculs sur ces données.

Base documentaire (*Documentary Database)*

Logiciel qui permet de stocker, classer, retrouver des documents.

Bureautique *Office Automation*

Ce terme a d'abord désigné l'équipement électronique de bureau (photocopieuses, machines à calculer). Puis il s'est appliqué au micro-ordinateur et à ses premières applications (traitement de texte, tableur, grapheur) ainsi qu'aux imprimantes. Avec la mise en réseau des PC, on est passé à la fin des années 80 à la " bureautique communicante " dont les premières applications ont été la messagerie et l'agenda partagé. La bureautique communicante a été vers 1992 englobée sous le concept de groupware.

Cellule d'assistance à maîtrise d'ouvrage (*Business Technology Unit)*

Entité qui, à l'intérieur d'une maîtrise d'ouvrage, a la responsabilité de la définition, du développement et de l'utilisation d'un système d'information correspondant aux missions de cette maîtrise d'ouvrage.

Circuit intégré (*Integrated Circuit)*

Ensemble de composants électroniques fixés, ainsi que leurs interconnexions, sur une " puce " (le plus souvent en silicium).

Client

Dans le langage de l'informatique, un " client ", ce n'est pas une personne, mais le PC de l'utilisateur. C'est ainsi qu'il faut comprendre l'expression " client-serveur ".

Commerce électronique (*Electronic Commerce)*

Réalisation du processus de la relation commerciale par voie électronique (réseau, ordinateurs) : présentation des produits, prise de commande, paiement, gestion de la logistique de livraison. Dans le cas des documents ou des logiciels, la livraison elle-même peut se faire par voie électronique.

Disque dur (*Hard Disk)*

Mémoire de masse d'un ordinateur, à accès lent, résidant sur un support magnétique.

Donnée *Data*

Une donnée, c'est un couple logique formé par (a) une définition, (b) la spécification d'une méthode de mesure, d'observation ou de calcul (" Métadonnée"). Réaliser la mesure (ou l'observation pour les données qualitatives ou le calcul pour les données agrégées) permet de connaître la valeur prise par la donnée dans un contexte particulier (lieu, date).

EDI (Echange de données informatisées) *(Electronic Data Interchange)*

Communication entre applications informatiques d'entreprises différentes ou non, par le moyen de messages dont le format et le codage auront été fixé par un accord d'interchange. La norme Edifact définit le format général des messages. L'EDI facilite les échanges répétitifs d'information (commande, facture, etc.) entre un fournisseur et un client assidu. L' " EDI-ouvert " procure une norme pour décrire les rôles de diverses entreprises dans les montages complexes d'ingénierie d'affaire, et garantit que leurs applications sont capables de communiquer par messages EDI.

Extranet

Mise en réseau de plusieurs entreprises qui connectent leurs Intranets. L'Extranet est le moyen idéal pour les relations avec les partenaires, fournisseurs et clients.

Indicateur (*Indicator)*

Donnée ou agrégat de données sélectionné pour son intérêt économique, mis sous forme de série chronologique, corrigé des variations saisonnières après interprétation des incidents, ayant fait l'objet d'une modélisation économétrique permettant de l'interpréter et de fournir des prévisions tendancielles (ou extrapolations). La production d'un indicateur est une opération relativement coûteuse : seules certaines données choisies méritent d'être élevées au statut d'indicateur.

Information

Une information, c'est une donnée observée par un acteur que cette donnée intéresse. L'observation par un acteur implique la comparaison au moins implicite à d'autres données, car sans comparaison il n'y a pas d'interprétation possible. Passer du rang de *donnée* à celui d'*information* suppose que la connaissance de la donnée contribue à l'action de celui qui l'observe : la notion d'information recèle donc un côté subjectif et un côté objectif.

Interface

Mise en forme des données permettant leur passage d'une étape à l'autre du traitement. Equipement assurant la transcription des données d'un langage dans un autre. L'interface homme-machine assure la communication entre l'homme et l'ordinateur grâce à des supports (écran, clavier, haut-parleurs) accessibles aux sens de l'être humain. L'interface graphique (Graphical User Interface ou GUI), qui permet d'afficher et de créer des images, fait partie de l'ergonomie standard en 1997.

Internet

Réseau d'interconnexion d'ordinateurs utilisant le protocole de transmission de données TCP/IP (qui permet aussi le transfert des images, fixes ou animées, et du son). Efficace, robuste et peu coûteux grâce aux qualités de TCP/IP, l'Internet a été d'abord utilisé par des chercheurs, puis a servi de support à des services devenus populaires (messagerie, forums, Web, commerce électronique, téléchargement de logiciels) qui ont fait de lui un phénomène de société. C'est désormais *le* réseau mondial de communication électronique.

Intranet

Utilisation de l'Internet à des fins internes à une entreprise. L'Intranet permet à l'entreprise de bénéficier de l'économie d'échelle acquise par les logiciels sur l'Internet, et d'outils de développement orientés-objet comme Java. On peut réaliser maintenant sur l'Intranet la totalité des applications de groupware. L'Intranet nécessite toutefois une administration soigneuse des droits d'accès, et la mise en place de " Firewalls " pour protéger les données de l'entreprise.

Firewall

Logiciel (pare-feu) qui sert à protéger un réseau contre les tentatives d'intrusion.

Langage de programmation (*Programming Language)*

L'ordinateur ne comprend que des instructions simples : chercher des données dont il connaît l'adresse en mémoire, faire une opération arithmétique sur ces données, stocker le résultat de cette opération en mémoire, etc. Le langage qui permet d'écrire ces instructions est le *langage machine*.

Programmer en langage machine serait une tâche fastidieuse pour un être humain. Les langages de programmation offrent des instructions plus synthétiques et commodes. En fait, l'exécution d'un programme écrit en " langage de haut niveau " (Visual Basic, Java, C++ etc.) nécessite une cascade de traducteurs et interpréteurs pour aboutir à des instructions exécutables par la machine.

Les langages de programmation sont ainsi plus proches du langage " naturel " (ou de sa représentation graphique). Ils restent cependant très conventionnels, et leur utilisation experte suppose une formation approfondie.

Mémoire (*Memory)*

Support magnétique ou électronique comportant des zones dotées d'adresses, et où un ordinateur peut stocker données et programmes. Une mémoire est d'autant plus chère que son accès est plus rapide (d'où l'utilisation d'un disque dur à accès lent pour la mémoire de masse, et d'une RAM à accès rapide pour les travaux en cours).

Messagerie électronique (*E-mail)*

Système d'adressage et de stockage permettant à des utilisateurs d'échanger des messages en mode asynchrone : le message est stocké dans la " boîte aux lettres " (BAL) de l'utilisateur en attente de sa consultation. L'introduction d'une messagerie a un effet puissant sur l'organisation d'une entreprise.

Micro-ordinateur (*Micro Computer)*

Ordinateur dont l'unité centrale est constituée d'un microprocesseur. Le micro-ordinateur contient d'autres circuits intégrés réalisant des fonctions de mémoire et d'interface.

Microprocesseur (*Micro Processor)*

Circuit intégré contenant les circuits arithmétiques, logiques et de contrôle nécessaires pour réaliser les fonctions de l'unité centrale d'un ordinateur.

Modèle conceptuel de données (MCD)

Catalogue des définitions mettant en évidence les liens logiques entre les diverses données de l'entreprise : découpage des nomenclatures sans double compte ni omissions, documentation des agrégats, ratios et autres données dérivées par le calcul des données d'observation directe. La rédaction du MCD est une étape importante de l'administration des données.

Multimédia (*Multimedia)*

Ce terme s'applique aux interfaces de communication qui utilisent (presque) toutes les possibilités sensorielles : caractères d'imprimerie, images fixes ou animées, son, voire sensations tactiles et vues en trois dimensions dans les espaces virtuels. Il s'applique aussi aux logiciels qui utilisent ces interfaces, et aux PC disposant de lecteurs de CD-Rom, de cartes graphiques, de cartes son, de micros, de haut-parleurs.

Ordinateur (*Computer)*

Appareil électronique capable de recevoir des données et d'exécuter sur ces données des instructions programmées à l'avance.

(Orienté-objet) : langage (*Object-Oriented Language)*

La tradition du développement voulait que l'on sépare les données et leur traitement, réalisé par les applications. Puis il est apparu judicieux de rapprocher dans un même petit programme certaines données et certains traitements qui leur sont souvent associés. Ce petit programme, appelé " objet ", est par la suite plus facile à réutiliser que les lignes de code des anciennes applications.

A la limite, le travail fait autrefois par une application est fait désormais par des objets qui communiquent en s'échangeant des messages.

L'offre d'outils de développement orientés-objet n'est pas stabilisée, mais ce type de langage semble devoir s'imposer pour des raisons économiques et logiques.

(Orienté-objet) : modèle (*Object-Oriented Model)*

La définition des données (modèle conceptuel de données) est complétée, dans les modèles orientés-objet, par celle des activités qui utilisent les données (" use case ") et par celle des objets que ces activités manipulent. Il sera utile de pousser le modèle conceptuel de données jusqu'à ce degré de précision, même si ensuite les contraintes techniques ne permettent pas de tout réaliser avec un langage orienté-objet.

Personal Computer (PC)

Nom du micro-ordinateur lancé par IBM en 1981 pour faire face à la concurrence des micro-ordinateurs d'Apple. Le PC est devenu un standard qu'on utilise souvent comme synonyme de micro-ordinateur (nous le faisons dans certaines de nos définitions).

Processus *Process*

Succession ordonnée des opérations nécessaires à l'exécution d'une tâche.

Reporting

Document périodique d'une forme convenue à l'avance, par lequel une entité de l'entreprise rend compte de son activité à une autre entité.

Réseau local de PC (RLPC) (*Local Area Network (LAN))*

Un réseau local ou RLPC, permet à plusieurs ordinateurs de communiquer entre eux dans le même bâtiment ou le même campus.

Serveur (*Server)*

Ordinateur connecté à un réseau et qui met à la disposition d'autres ordinateurs ses ressources de mémoire et de puissance ou qui sert de support au déroulement d'un programme. Exemple: serveurs de messagerie, de base de données, de calcul etc.

Système d'exploitation (*Operating System (OS))*

Logiciel qui exécute les tâches relatives à la création, l'ouverture, la fermeture, la copie, la destruction de fichiers contenant des programmes ou des données, ainsi qu'au lancement des programmes et à leur exécution, à la gestion des interruptions etc.

Transmission Control Protocol / Internet Protocol (TCP/IP)

Protocole de transmission de données en mode paquet. Mis au point pour répondre à une demande de l'armée Américaine, il est construit pour être indestructible en cas d'attaque nucléaire : pas d'administration centralisée, propagation des tables d'adressage entre serveurs par réplication de proche en proche, routage très simple exigeant le minimum de puissance des ordinateurs. C'est ce protocole qui a permis de construire le réseau Internet. TCP/IP s'impose comme *le* standard universel de la transmission de données.

Unified Modelling Language (UML)

Langage qui vise à rassembler les meilleurs procédés (" best practices ") dans les modèles conceptuels de données orientés-objet, et qui ambitionne de devenir un standard en unifiant les autres langages.

Wide Area Network (WAN)

Un WAN permet à plusieurs ordinateurs de communiquer entre eux dans une même zone géographique.

Liste des annexes

N° de l'annexe	Intitulé de l'annexe
1	Guide pour l'audit du développement, acquisition et maintenance
2	JDE WORLD :Rapports d'intégrité
3	La revue des processus (business process JDE)
4	Programme de travail de la revue de sécurité dans un environnement de confiance (Trust Domain)
5	Exemple d'un programme d'audit de la sécurité spécifique à l'ERP JD Edwards (Version World sous AS/400)
6	Description des process contribuant à l'élaboration du dossier financier et l'identification des contrôles y afférents
7	Lexique français-Arabe

ANNEXE 1

GUIDE POUR L'AUDIT DU DEVELOPPEMENT, ACQUISITION ET MAINTENANCE

1 Gestion de projet

A travers le processus de gestion de projet, l'auditeur informatique doit analyser les risques inhérents à chaque phase du cycle de vie de l'application informatique et doit s'assurer que des contrôles appropriés ont été mis en œuvre pour minimiser ces risques. Il faudrait bien entendu éviter d'implémenter des contrôles dont le coût est plus important que le risque associé.

Lors de la revue du processus SDLC (System Development Life Cycle), l'auditeur informatique doit obtenir la documentation des différentes phases du projet et les comptes-rendus de réunions. Il doit évaluer la performance de l'équipe de projet à produire à temps les livrables clés.

L'auditeur informatique doit revoir l'adéquation des aspects suivants :

- Niveau de monitoring du projet et implication du comité de projet et du comité de pilotage ;
- Méthode d'évaluation du « risk management » du projet ;
- Processus de reporting au top management ;
- Processus de contrôle des changements ;
- Revue de la documentation des phases du projet, relative :
    - aux objectifs définissant ce qui devra être accompli durant chaque phase du projet,
    - aux livrables clés de chaque phase désignant clairement les responsables directs de ces livrables,
    - au planning détaillé de chaque phase définissant notamment les dates de finalisation des livrables clés,
    - au suivi budgétaire des coûts de réalisation de chaque phase.

2 Audit de la phase d'étude de faisabilité

L'auditeur informatique doit effectuer les travaux suivants :

- Revoir la documentation produite durant cette phase ;
- Déterminer si tous les coûts et bénéfices ont été étudiés et évalués ;
- Identifier et déterminer la criticité des besoins ;

- Déterminer si tous les scénarios de développement ont été examinés ;
- Déterminer et justifier le scénario ou le choix retenu.

3 Audit de la phase d'expression des besoins et de conception générale

L'auditeur informatique doit effectuer les travaux suivants :

- Obtenir le document détaillé d'expression des besoins et vérifier son adéquation par des entretiens croisés avec les utilisateurs clés ;
- Identifier les membres de l'équipe de projet et vérifier que les départements utilisateurs concernés sont tous correctement représentés ;
- Vérifier que l'initiation du projet et l'estimation du budget ont été approuvés par le management ;
- Revoir la conception générale et s'assurer :
    - qu'elle est en adéquation avec les besoins des utilisateurs,
    - que des contrôles appropriés ont été définis.

- En cas de sous-traitance, s'assurer que le périmètre et l'étude d'expression des besoins ont été communiqués à un nombre raisonnable de prestataires.

4 Audit du processus d'acquisition de progiciels

L'auditeur informatique doit effectuer les travaux suivants :

- Analyser la documentation de la phase d'étude de faisabilité pour déterminer si le choix d'acquisition de progiciel était approprié ;
- Revoir le document d'appel d'offres RFP (Request For Proposal) pour s'assurer de son exhaustivité ;
- Déterminer si le prestataire retenu répond correctement aux spécifications fonctionnelles et techniques de l'appel d'offres ;
- Revoir le contrat signé avec le prestataire et s'assurer qu'il a inclu toute la liste des fonctionnalités de l'appel d'offres ;
- S'assurer que le dit contrat a été revu par un juriste.

5 Audit de la phase de conception détaillée

L'auditeur informatique doit effectuer les travaux suivants :

- Revoir les différents flowcharts et leur adéquation avec la conception générale.
- Vérifier que chaque changement constaté par rapport à la phase de conception générale a été correctement discuté et approuvé par le management des départements concernés ;
- Revoir les inputs, traitements, contrôles et outputs qui ont été conçus et s'assurer qu'ils sont appropriés ;
- Interviewer les utilisateurs clés en vue d'évaluer leur compréhension du futur fonctionnement du système et leur degré d'implication dans la conception des écrans et des états de sorties ;
- Revoir le résultat de la revue assurance qualité qui doit être effectuée à l'issue de cette phase.

6 Audit de la phase de programmation

L'auditeur informatique doit effectuer les travaux suivants :

- Vérifier l'intégrité des calculs et traitements ;
- Evaluer l'adéquation des pistes d'audit en vue de maintenir la traçabilité des transactions enregistrées dans le système ;
- Vérifier que le système peut identifier les données rejetées.

7 Audit de la phase de tests

La phase de tests est cruciale pour s'assurer de l'adéquation du système par rapport aux besoins et son acceptation par les utilisateurs. Ainsi, il est très important d'impliquer l'auditeur informatique dans cette phase. Il doit effectuer les travaux suivants :

- Revoir le plan et les dossiers de tests pour :
    - Vérifier leur exhaustivité et leur adéquation par rapport aux fonctionnalités décrites dans le document d'expression des besoins;
    - Matérialiser l'approbation des utilisateurs clés.
- Revoir les rapports d'erreurs lors du déroulement des tests et s'assurer qu'ils sont correctement suivis ;
- Vérifier le bon fonctionnement des traitements directement impactés ainsi que ceux qui le sont indirectement (par exemple, les traitements cycliques de fin de période) ;

- Interviewer les utilisateurs finaux sur leur compréhension du fonctionnement du système, des nouvelles façons de travailler et des procédures opérationnelles ;
- Revoir le résultat des tests en fonctionnement parallèle ;
- Vérifier que les aspects de sécurité des accès ont été correctement prévus et testés ;
- Revoir la complétude de la documentation de la phase de tests (dossiers de tests signés, PV d'acceptation,…etc.).

8 Audit de la phase d'implémentation

Cette phase ne peut être initiée que si la phase de recette des systèmes est concluante. Le nouveau système devra être mis en place selon la procédure de contrôle des changements et de mise en production. L'auditeur informatique doit s'assurer qu'une demande de mise en production a été correctement signée par les départements utilisateurs concernés. De plus, il est important de :

- Revoir les procédures et les étapes ordonnancées de mise en production ;
- Revoir toute la documentation et s'assurer qu'elle a été correctement mise à jour à l'issue de la phase de tests ;
- S'assurer de l'exhaustivité et de la qualité de toutes les données migrées.

9 *Audit de post- implémentation*

Après la stabilisation du nouveau système dans l'environnement de production, une revue post- implémentation devrait être réalisée. Dans cette revue, l'auditeur informatique doit effectuer les travaux suivants :

- S'assurer que le nouveau système a atteint ses objectifs en adéquation avec les besoins des utilisateurs. Durant cette phase, il est important de mesurer le degré de satisfaction des utilisateurs. Cet indicateur permettra de s'assurer de la bonne réussite du projet d'implémentation ;
- Déterminer si les coûts/bénéfices identifiés dans la phase d'étude de faisabilité ont été correctement mesurés, analysés et reportés au management ;
- Revoir le nombre et les procédures de demande de changement opérées durant la réalisation du projet d'implémentation. Cet indicateur permettra de connaître les types de changements effectués et leur timing par rapport à la conception générale ou détaillée, et par rapport aussi à l'interprétation des besoins utilisateurs ;

- Revoir les contrôles mis en œuvre dans le nouveau système pour s'assurer que ces contrôles correspondent bien à ce qui a été prévu dans la phase de conception ;
- Revoir les rapport de loging du nouveau système pour déterminer l'existence de quelconque problème au niveau applicatif ou système d'exploitation. Cet indicateur permettra de savoir si la phase de tests a été correctement menée avant mise en production ;
- Revoir les données en entrées et en sorties, éditer les états et vérifier le bon fonctionnement du système.

10 Audit des procédures de changements et des processus de migration

Après son implémentation, le nouveau système entre dans la phase de maintenance. Il s'agit de la :

- Maintenance corrective où des changements sont effectués pour corriger des erreurs ou des bugs de programmes;
- Maintenance évolutive où les changements opérés concernent des évolutions du système suite à de nouveaux besoins.

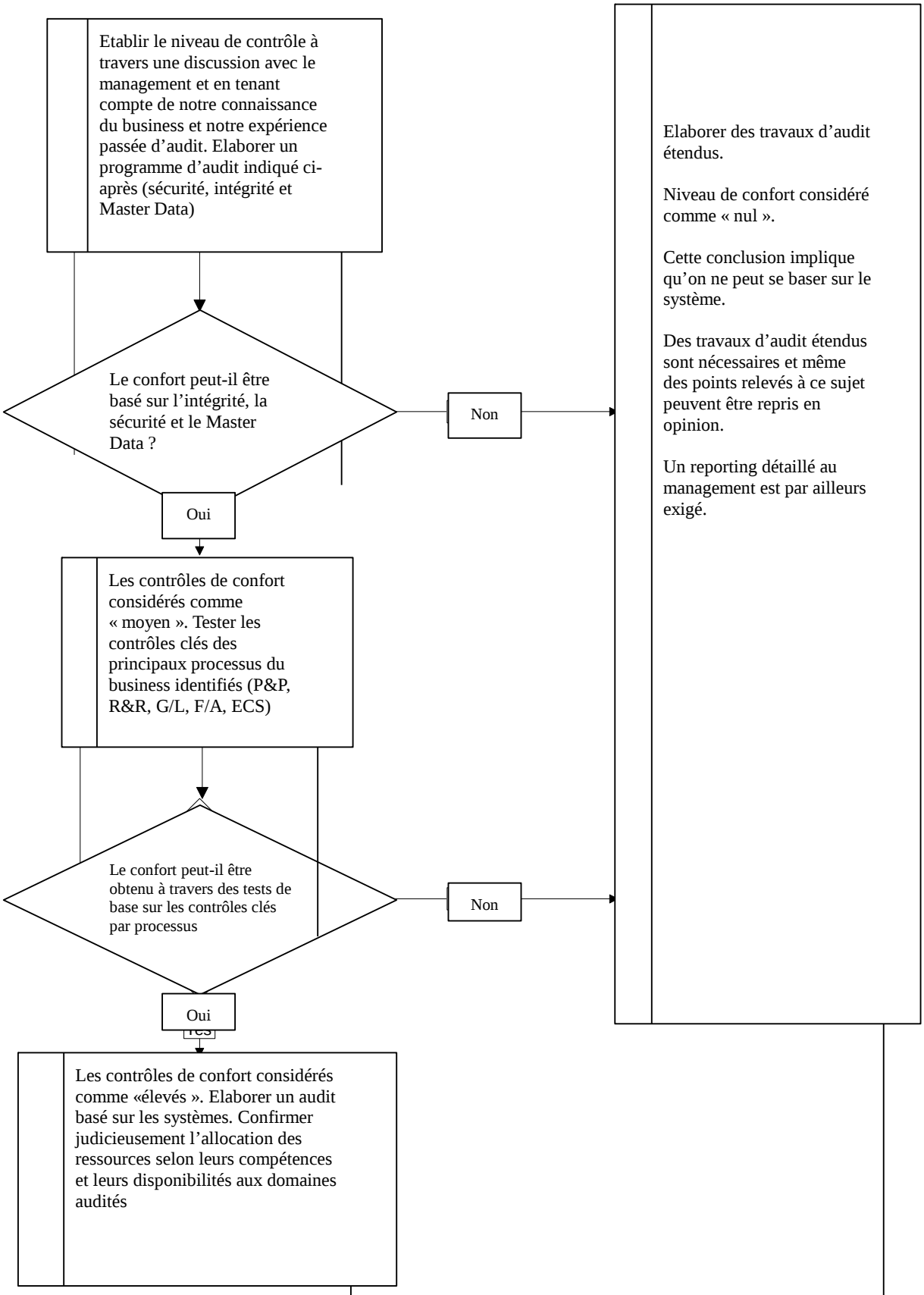
L'auditeur informatique devra considérer et revoir les aspects suivants:

- L'existence et la bonne application d'une procédure d'autorisation, l'évaluation des priorités et le suivi des demandes de modification;
- Le traitement particulier des demandes de changement à caractère urgent;
- L'existence de la documentation de tous les changements opérés dans le système;
- Le respect de la méthodologie d'implémentation (expression des besoins, conception, développement, test et mise en production);
- L'évaluation de la satisfaction des utilisateurs et les coûts de maintenance;
- Le bon suivi des versions et la correspondance entre les programmes sources et les programmes objets;
- L'adéquation des aspects de sécurité par la restriction des accès aux librairies des programmes sources et objets.

ANNEXE 2

RAPPORTS D’INTERGRITE DE JDE WORLD

1. Le processus de la détermination et la mise en œuvre de la stratégie d'



JDE WORLD : Rapport d'intégrité

Les rapports clés d'intégrité que l'auditeur externe doit tester sont les suivants :

Intégrité	Comptes de fournisseu	férence d'intégration
P047001 - A/P vers G/L	Ce rapport compare le compte A/P (F0411) avec la balance figurant dans la table des comptes de la balance (F0902).	La balance auxiliaire des fournisseurs ne sera pas cadrée par rapport à la balance générale
P04701 - A/P vers G/L par traitement Batch	Ce rapport vérifie que les totaux de chaque batch dans la table grand livre A/P (F0411) sont équilibrés avec les montants correspondants dans la table du compte comptable	Les comptes auxiliaires fournisseurs ne seront pas égaux aux comptes de la balance générale.
	Ce rapport permet également de vérifier les rejets de paiement pour chaque opération de règlement.	Une transaction totale ou partielle pourrait éventuellement échapper au processus de traitement pour paiement
P04702 - Paiements A/P vers G/L par traitement Batch	Ce rapport vérifie que pour chaque batch A/P, le détail des documents de rapprochement (F0414) relatifs aux paiements est en équilibre avec les montants des comptes généraux en traitement batch (F0911).	Le sous compte fournisseur ne sera pas équilibré avec le compte général.

Intégrité	Comptes clients	férence d'intégration
P037001 - A/R vers G/L par	Ce rapport compare les montants intégrés dans la table des transactions A/R avec les montants mis à jour dans la table de la balance des comptes (F0902).	Le sous compte clients ne sera pas équilibré avec le compte général
P03702 - AR vers GL des réceptions intégrées	Ce rapport compare les totaux intégrés par traitement batch dans l'application des réceptions (F0314) avec le compte général (F0911).	Le sous compte clients ne sera pas équilibré avec le compte général
P03701 - A/R vers G/L par traitement	Ce rapport vérifie que chaque batch des totaux intégrés dans le compte A/R (F0311) est équilibré	Le sous compte clients ne sera pas équilibré avec le compte général

Batch	avec les montants correspondants dans le compte général (F0911).	

Intégrité	Immobilisations	d'intégration	éférence
P127011 - F/I vers G/L	Ce rapport compare les enregistrements dans le fichier des immobilisations (F1202) avec les entrées dans le compte des immobilisations de la comptabilité générale (F0902).	Le sous compte des actifs immobilisés ne sera pas équilibré avec les comptes généraux de la comptabilité générale	
P12301 Immobilisations non affectées	Ce rapport identifie toutes les transactions intégrées dans le grand livre, mais qui ne sont pas encore validées dans le sous-compte immobilisations (fixed asset).	Le sous compte pourrait ne pas contenir toutes les transactions(il peut ne pas être exhaustif).	

Intégrité	ECS	d'intégration	éferenc
P41543 - registre des articles/compte Rapport d'intégrité (Cardex vers GL)	Ce rapport édite toutes les incohérences entre le registre des articles (F4111) et le compte général (F0911) : - Registre des articles existe en détail sans correspondance avec le détail du compte général. – Le registre des articles ne s'équilibre pas avec le détail du compte général.	La balance auxiliaire des stocks pourrait ne pas s'équilibrer avec la comptabilité générale.	
P41544 - Article Balance/Grand livre Integrity Report	Ce rapport édite les incohérences aussi bien pour les quantités que pour les valeurs entre la balance des stocks (F41021) et la comptabilité (F4111).	Le compte des stocks pourrait ne pas être intrinsèquement correct : i.e. coût unitaire multiplié par quantité pourrait ne pas être égal à la valeur globale.	

Intégrité	Comptabilité général	d'intégration	éferenc
P007011 – Traitements batches non intégrés	Ce rapport édite une liste de tous les batchs non intégrés sur la base de la table de contrôle des batchs (F0011)	Le compte général pourrait ne pas être exhaustif.	
P007021 – Transaction sans en-tête de batch	Ce rapport montre la liste des transactions sans sauvegarde de l'en-tête de batch dans le registre des contrôles Batch. Le rapport inclut les transactions non intégrées avec un batch statué en	Le compte général pourrait ne pas être exhaustif.	

	D. les tables utilisées sont F03B11, F0411, F0911	
P007031 – Traitements Batch à détailler et à intégrer sans équilibre	Ce rapport liste les lots déséquilibrés qui ont été intégrés. Si le montant net est différent de zéro (total débit différent du total crédit), la différence nette est incluse dans le rapport.	La balance générale et le grand livre peuvent ne pas être concordants
P097001 – Solde des compagnies	Ce rapport édite une balance par compagnie. Il identifie les règlements inter-compagnies non répertoriés ou les ajustements comptabilisés sur exercices antérieurs non inclus dans la balance.	Les compagnies structurées selon une comptabilité par filiale peuvent faire apparaître des déséquilibres entre les balances
P09706 – Compagnie par lot déséquilibré	Ce rapport montre les montants en déséquilibre par compagnie pour chaque batch.	Les compagnies structurées selon une comptabilité par filiale peuvent faire apparaître des déséquilibres entre les balances
P09705 – comptes rapprochés avec les transactions	Ce rapport montre les incohérences sur une base périodique entre la balance des comptes (F0902) et le grand livre table (F0911)	Les comptes de la balance peuvent ne pas correspondre à la somme du détail de transactions qui le composent
P097021 – Transaction sans Rapport sur le compte principal	Ce rapport montre pour la société les incohérences de comptes entre le compte comptable (F0911) et la table des comptes principaux (F0901).	Le grand livre ne sera pas exhaustif
P097031 - Balance des comptes sans compte principal	Ce rapport montre les incohérences comptables entre le compte principal (F0901) et la table des balances des comptes (F0902)	Le grand livre ne sera pas exhaustif
P097041 – Comptes sans affectation de la Business Unit	Ce rapport vérifie que la business unit (ainsi que son code) existe pour chaque enregistrement comptable dans la table des comptes principaux (F0901). Si le code de la business unit ou de la société n'existe pas dans la table des comptes principaux, le rapport édite la business unit, l'objet du compte, la filiale, et la compagnie pour chaque compte dans la business unit manquante.	Le grand livre ne sera pas exhaustif.

ANNEXE 3

La revue des processus (business process JDI

La revue des processus

Les processus gérés par JD Edwards comprennent :

- Les achats et les comptes fournisseurs (purchases and payables) ;
- Les ventes et les comptes clients (revenue and receivables) ;
- Les stocks (inventory) ;
- Les immobilisations (fixed assets) ;
- La comptabilité générale(general ledger) ;

1 Les achats et les comptes fournisseurs (Purchases and payables)

Les contrôles et les traitements standards dans le module achats – fournisseurs de JDE sont conçus pour un processus d'achat classique où les commandes sont lancées avant la réception et la facturation des achats. Ainsi cela suppose que les commandes sont autorisées avant la réception des biens et services. les factures doivent être contrôlées avant leur traitement, les défaillances de contrôles à ce niveau pourraient avoir un impact sur le processus de contrôle des entrées.

Lors des sa revue de ce processus l'auditeur devra notamment s'assurer que :

- Les commandes d'achats sont effectuées avant la réception des biens et des services et avant le traitement des factures des achats ;
    - Les commandes en instance sont régulièrement investiguées et apurées en utilisant le rapport disponible dans JDE (P43525) ;
    - Les commandes achats sont autorisées conformément aux pouvoirs de décision prévus dans le manuel des procédures de la société ;
    - Les factures fournisseurs reçues sont saisies en utilisant la fonctionnalité prévue dans JDE à cet effet (JDE invoice logging functionality) ;
    - Les factures d'achats sont correctement codifiées et approuvées dans les délais appropriés. Le rapport P43428 (Logged Voucher Detail Report) doit être régulièrement édité et revu ;
    - Les différences entre les rapports des commandes et des réceptions sont analysées ;
    - Le rapport des marchandises reçues mais non facturées est revu et apuré régulièrement ;

- Le document de contrôle des paiements est édité et revu pour tous les règlements ;
- Les taxes (notamment TVA…) sont correctement comptabilisées ;
- L'édition automatique des chèques est contrôlée ainsi que les chèques non utilisés ;
- Les paiements cash et les paiement urgents sont contrôlés ;
- Les contrôles qui permettent d'empêcher les doubles paiements sont effectués et revus régulièrement (Le rapport P04601 doit être édité et revu régulièrement) ;
- Les pouvoirs de signature des chèques sont bien définis et contrôlés.

2 Revue des revenus et des créances (JDE World)

Comme indiqué ci-dessus, la fiabilité de ce processus est dépendant des contrôles relatifs à la séparation des tâches au Master Data et le contrôle de l'intégration des données entre les modules SOM (sales order management : gestion des commandes de vente), A/R (accounts receivables : comtes clients) et G/L (general ledger : comptabilité générale.

Lors de sa revue de ce processus l'auditeur devra notamment s'assurer que:

- Toutes commandes de vente sont enregistrées dans JDE dès leur réception ;
- Les règles de gestion appliquées aux commandes des ventes sont adaptées au business du client ;
- Le système est utilisé de façon systématique et régulière pour toutes les activités de chargement et de livraison ;
- Le rapport des commandes de vente ouvertes (P42620) est édité et revu quotidiennement ;
- Le (Rapport P42801 d'erreur de mise à jour des ventes) est édité et revu quotidiennement ;
- Les règlements sont enregistrés d'une manière exhaustive et exacte et ils sont correctement affectés aux clients correspondants facture par facture. Le non fonctionnement de ce contrôle sur une base régulière peut se traduire par l'inexactitude des comptes clients dont le redressement nécessitera un effort significatif. Il est donc nécessaire que les règlements reçus au comptant ou non identifiés soient apurés en un temps raisonnable ;

- Tous les avoirs sont analysés, autorisés et comptabilisés ;
- toutes les créances sont justifiées, revues et donnent lieu à un suivi régulier ;
- le provisionnent des créances est adéquat.

3 Immobilisations JDE World

Comme indiqué ci-dessus, l'efficacité des contrôles relatifs à ce processus dépendent des contrôles relatifs à la séparation des tâches, au Master Data l'intégration des données entre F/A et G/L.

L'auditeur devra notamment s'assurer que:

- La méthode employée pour la création d'immobilisations et pour la codification des immobilisations est appropriée ;
- Que les instructions de comptabilisation automatique relatives aux immobilisations ont été mises en service ;
- Les immobilisations en cours sont revues régulièrement et que leur fichier est mis à jour en fonction des mises en service des immobilisations ;
- Les cessions sont autorisées et correctement comptabilisées (dans bonne la période et dans les bons comptes) ;
- Le fichier des immobilisations est régulièrement revu et mis à jour : Un inventaire des immobilisations devrait être réalisé selon une périodicité propre à chaque entreprise (en fonction des ses procédures, la nature des immobilisations gérées et le risque y afférent …etc.).

4 Comptabilité générale (JDE World)

En plus des contrôles évoqués ci-dessus, il y a lieu de s'assurer que :

- Les réconciliations et les analyses de comptes sont effectuées régulièrement particulièrement pour les banques, les comptes en suspens, les factures à établir ou à recevoir, les différence de change et les dépréciations ;
- La limitation des accès aux journaux de comptabilisation avec notamment l'octroi de mots de passe appropriés au personnel de la Direction Financière. Les autorisations d'accès sont de la responsabilité du Directeur financier ;
- L'enregistrement des opérations diverses (journal des OD) est strictement contrôlé ;La comptabilisation des éléments récurrents y compris ceux relatifs à

la fin d’année est correctement mise en place et tout changement est soumis à un contrôle strict.

ANNEXE 4

Programme de travail de la revue de sécurité da
environnement de confiance (Trust Domain)

Domaine	Questions d'audits	Procédure d'audit
Politique, organisation et administration de la sécurité	**Structure et gestion de la sécurité informatique**	**Structure et gestion de la sécu informatique**
	1.1 Politique de la sécurité informatique	**1.1 Politique de la sécurité informatique**
	1.1.1. Existe-t-il une politique de sécurité informatique écrite ?	1.1.1 Vérifier l'existence d'une politique de sécurité informatique écrite
	1.1.2 Est-ce que cette politique de sécurité informatique requiert-elle l'intervention des parties appropriées de l'organisation conformément aux normes de confiance du domaine ?	1.1.2 Obtenir une copie de cette politique. Examiner le contenu de cette politique et s'assurer qu'elle répond aux exigences de la sécurité informatique.
	1.1.3 Le document de la politique informatique est-il disponible à tout le personnel concerné ?	1.1.3 S'assurer de la disponibilité du document au personnel concerné.
	1.2 Répartition des responsabilités	**1.2 Répartition des responsabil**
	1.2.1 Les responsabilités de la sécurité des ressources informatiques sont-elles attribuées et documentées ?	1.2.1 Obtenir la documentation relative à la sécurité des ressources informatiques et s'assurer que les responsabilités ont été correctement assignées.
	1.2.1 Les responsabilités sont-elles communiquées au personnel approprié ?	1.2.1 Demander aux personnes concernées si elles ont été informées de leur responsabilité et /ou confirment la réception de la documentation appropriée. (Briefings, mails, etc.)
	1.3 Evaluation par rapport aux normes de confiance du domaine	**1.3 Evaluation par rapport aux normes de confiance du domaine**
	1.3.1 Existe-t-il des revues et des évaluations des mécanismes mises en œuvre pour l'identification des déficiences ou des non-conformités avec les normes de confiance du domaine ?	1.3.1 Vérifier l'existence des revues et des évaluations des mécanismes en examinant les procédures mises en place.
	1.3.2 Existe-t-il un processus pour s'assurer que les déficiences	1.3.2 S'assurer de l'existence de ces procédures par la revue de la

Domaine	Questions d'audits	Procédure d'audit
	identifiées sont corrigées ?	documentation et / ou des interviews avec le personnel concerné/
	1.4 Accord de confidentialité avec le personnel	**1.4 Accord de confidentialité avec le personnel**
	1.4.1 La société a-t-elle établit un accord de confidentialité (non-divulgation des informations de l'entreprise) avec tout le personnel ?	1.4.1 Obtenir une copie de l'accord de confidentialité (non-divulgation des informations de l'entreprise).
	1.4.2 Les accords de confidentialité sont-ils tous signés par le personnel ?	1.4.1 S'assurer sur la base d'un sondage que les accords de confidentialité sont bien signés par le personnel concerné.
	1.5 Formation et éducation sur la sécurité informatique	**1.5 Formation et éducation sur la sécurité informatique**
	1.5.1 Existe-t-il des programmes d'éducation sur la sécurité informatique, les normes et les procédures associées aux domaines ?	1.5.1 S'assurer par la revue et l'examen de la documentation de l'existence de programmes d'éducation couvrant des sujets appropriés.
	1.5.2 Les moyens d'éducation sont-ils communiqués au personnel qui utilise, développe ou maintient les ressources informatiques du domaine ?	1.5.2 Obtenir la preuve de communication au personnel concerné des moyens d'éducation relatifs à la sécurité.
	1.5.3 Les utilisateurs sont-ils correctement formés sur l'utilisation des équipements (Procédure de connexion, utilisation des logiciels, etc.) ?	1.5.3 Vérifier sur la base d'un sondage que le personnel a été formé avant tout accès aux ressources informatiques et / ou examiné la documentation appropriée.
	1.6 Rapport des incidents de sécurité	**1.6 Rapport des incidents de sécurité**
	1.6.1 Existe-t-il des procédures de réponse aux incidents de sécurité informatique et des dysfonctionnements des logiciels ?	1.6.1 Vérifier l'existence des procédures de réponse en obtenant et en passant en revue une copie de ces procédures.
	1.6.2 Les procédures définissent-elles ce qui constitue un incident de sécurité informatique, à qui ces incidents doivent être reportés et le traitement	1.6.2 S'assurer que ces procédures définissent les incidents de sécurité informatique, précisent à qui ces incidents doivent être

Domaine	Questions d'audits	Procédure d'audit
	d'incident qu'il faut appliquer ?	remontés et contiennent le traitement d'incident qu'il faut adopter.
	1.6.3 Le personnel a-t-il été formé sur l'importance de la procédure ?	1.6.3 Vérifier par des interviews si le personnel a bien été formé sur l'importance de la procédure et / ou obtenir et examiner la documentation (notes, mails, etc.) destinée au personnel pour les informer sur la procédure.
	1.7 Processus disciplinaire	**1.7 Processus disciplinaire**
	1.7.1 Existe-t-il un processus disciplinaire formel contre le personnel qui sciemment viole la politique ou les procédures de la sécurité informatique ?	1.7.1 S'assurer de l'existence du processus disciplinaire en obtenant et en passant en revue la documentation relative à ce processus et / ou en interviewant le personnel concerné par ce processus.
	1.8 Contrôle de changement opérationnel	**1.8 Contrôle opérationnel**
	1.8.1 Existe-t-il des procédures de contrôle des changements des équipements et des systèmes informatiques ?	1.8.1 Vérifier l'existence des procédures en obtenant et en passant en revue une copie de ces procédures.
	1.9 Contrôle des virus .	**1.9 Contrôle des Virus**
	1.9.1 Existe-t-il des procédures pour prévenir la diffusion des virus ?	1.9.1 Vérifier l'existence des procédures en obtenant et en passant en revue une copie de ces procédures.
	1.9.2 Existe-t-il des procédures formelles qui exigent l'utilisation des logiciels sous licence et l'interdiction d'utilisation des logiciels non autorisés ?	1.9.2 S'assurer en examinant les procédures qu'elles exigent bien l'utilisation des logiciels sous licence et l'interdiction d'utilisation des logiciels non autorisés.
	1.9.3 Le logiciel de détection des virus est-il déployé pour vérifier les médias ou parcourir les postes de travail ?	1.9.3 Vérifier par sondage que le logiciel de détection des virus est déployé pour vérifier et parcourir les postes de travail.
	1.9.4 Le logiciel de détection des virus est-il régulièrement mis à jour ?	1.9.4 Vérifier sur la base d'un sondage (PC & serveurs) que le logiciel de détection des virus a été régulièrement mis à jour.

Domaine	Questions d'audits	Procédure d'audit
	1.9.5 Les disquettes sont-elles toutes vérifiées avant utilisation ?	1.9.5 Vérifier que les procédures imposent l'obligation de vérifier toutes les disquettes avant toute utilisation et s'assurer du respect de ces procédures en inspectant quelques PC.
	1.9.6 Existe-t-il des procédures de continuité d'exploitation ou alternatives en cas d'attaque par des virus ?	1.9.6 Vérifier l'existence des ces procédures en obtenant et en passant en revue une copie de ces procédures.
	1.10 Procédures d'auto-contrôle	**1.10 Procédures d'auto-contrôle**
	1.10.1 Existe-t-il des revues et des évaluations des mécanismes mises en place pour l'identification des déficiences ou des non-conformités avec les normes de sécurités adoptées ?	1.10.5 S'assurer que les revues et les évaluations des mécanismes sont appliquées en obtenant et en passant en revue la politique correspondante / Les procédures et / ou en observant les mécanismes mis en place.
	1.10.2 Est-ce que toutes les ressources informatiques sont incluses dans le processus de la revue informatique ?	1.10.2 Vérifier si toutes les ressources informatiques sont incluses dans le processus de la revue informatique.
	1.11 Documentation des événements de sécurité	**1.11 Documentation des événements de sécurité**
	1.11.1 Les procédures de consignation des événements d'accès aux ressources informatiques sont-elles établies conformément aux recommandations des directives de la sécurité informatique ?	1.11.1 Obtenir les procédures de consignation et les directives de la sécurité de la plate-forme correspondantes. Examiner ces procédures pour s'assurer qu'elles ont été établies conformément aux recommandations.
	1.11.2 Les enregistrements des événements sont-ils conservés pendant une période donnée ?	1.11.2 Demander la durée de la période de conservation des données. Vérifier sur la base d'un sondage que cette période est respectée.
	1.12 Détection d'intrusion	**1.12 Détection d'intrusion**
	1.12.1 Les mécanismes et les procédures de détection d'intrusion	1.12.1 Vérifier l'existence des procédures en obtenant une copie de ces procédures. Déterminer par des

Domaine	Questions d'audits	Procédure d'audit
	sont-ils mis en œuvre ?	interviews quels sont les mécanismes mis en place. Vérifier sur la base d'un sondage que les mécanismes de détection des intrusions ont été bien installés sur les PC, serveurs, etc.
	1.12.2 Toutes les ressources informatiques (matériels, logiciels) sont-elles incluses dans les mécanismes de détection des intrusions ?	1.12.2 Prévoir par sondage les ressources informatiques et s'assurer qu'elles sont incluses dans les mécanismes de détection des intrusions.
	1.12 Processus d'autorisation d'installation des équipements informatiques	**1.12. Processus d'autorisation d'installation des équipeme informatiques**
	1.13.1 Existe-t-il des procédures formelles d'autorisation pour toutes les connexions au réseau de la société ?	1.13.1 Vérifier l'existence du processus d'autorisation en obtenant et en passant en revue la documentation relative à ce processus et / ou en interviewant le personnel concerné par ce processus.
	1.13.2 Existe-t-il des procédures formelles d'autorisation pour s'assurer que tous les outils de connexion au domaine sont techniquement approuvés ?	1.13.2 Vérifier par sondage que les outils de connexion sont approuvés sur le plan technique.
	Sécurité physique des équipements	**Sécurité physique des équipem**
	2.1 Plates-formes et équipements de communication relatifs aux données sécurisées	**2.1 Plates-formes et équipem de communication relatifs aux données sécurisées**
Sécurité logique	2.1.1 Les plates-formes informatiques et les équipements de communication du domaine sont-ils placés dans des zones sécurisées ?	2.1.1 Vérifier sur la base d'un sondage que les plates-formes informatiques et les équipements de communication du domaine sont placés dans des zones sécurisées.
	2.1.2 Des barrières physiques adéquates sont-elles mises en place pour empêcher les entrées non-autorisées ?	2.1.2 Vérifier sur la base d'un sondage que les barrières physiques permettent d'empêcher les entrées non-autorisées.
	2.1.3 En cas de non utilisation, les zones sécurisées sont-elles fermées et	2.1.3 Inspecter quelques domaines et s'assurer qu'ils ont été bien fermés pendant les périodes où ils

Domaine	Questions d'audits	Procédure d'audit
	périodiquement vérifiées ?	ne sont pas utilisés.
	2.2 Contrôle des entrées physiques	**2.2 Contrôle des entrées phys**
	2.2.1 Les domaines sécurisés sont-ils protégés par des contrôles des entrées ?	2.2.1 S'assurer sur la base d'un sondage que les domaines sécurisés sont bien protégés par des contrôles des entrées.
	2.2.2 Les visiteurs sont-ils surveillés pendant leur visite dans les secteurs sécurisés ?	2.2.2 Vérifier sur la base d'un sondage que les visiteurs des domaines sécurisés sont surveillés pendant leur visite.
	2.2.3 Le personnel est-il tenu de porter une identification visible dans les domaines sécurisés ?	2.2.3 Vérifier si les documents (procédures) exigent que le personnel porte une identification visible dans les domaines sécurisés. S'assurer du respect de cette procédure en effectuant des visites dans quelques secteurs.
	2.2.4 Les droits d'accès sont-ils récupérés immédiatement du personnel qui quitte la société ?	2.2.4 S'assurer sur la base d'un sondage que les droits d'accès du personnel ayant quitté la société ont été annulés en obtenant la liste de tous les droits d'accès aux systèmes, sites et bâtiments.
	3.1 Protection des postes de travail contre les accès non-autorisés	**3.1 Protection des postes de t ravail contre les accès non-autoris**
	3.1.3 Les ordinateurs personnels et les ordinateurs de bureau sont-ils protégés par des clefs (mot de passe) en cas de non-utilisation ?	3.1.1 Vérifier sur la base d'un sondage que les PC sont protégés par des mots de passe en cas de non-utilisation. .
	Sécurité du réseau	**Sécurité du réseau**
Sécurité Physique	3.2 **Normes de sécurité de la Plate-forme**	**3.2 Normes de sécurité de la Plate-forme**
	3.2.1 La société a-t-elle adoptée des standards de sécurité des Plates-formes réseaux pour chaque type de Plate-forme utilisée dans le domaine ?	3.2.1 Vérifier l'adoption des standards en obtenant et en passant en revue les documents relatifs à ces standards.
		3.3 Configuration des plates-fo

Domaine	Questions d'audits	Procédure d'audit
	3.3 Configuration des plates-formes	
	3.3.1 Les plates-formes informatiques du domaine sont-elles configurées conformément aux standards de la version actuelle de la plate-forme de sécurité ?	3.3.1 Sélectionner un échantillon de plates-formes et s'assurer que les standards ont été configurés sur toutes les plates-formes.
	3.3.2 Des vérifications mensuelles de la plate-forme informatique sont-elles effectuées pour s'assurer de sa conformité permanente aux standards ?	3.3.2 S'assurer que des vérifications mensuelles ont été effectuées sur les plates-formes informatiques.
	3.3.3 Les déviations aux standards ont-elles été approuvées.	3.3.3 Obtenir et revoir les approbations desdites déviations.
	Contrôle du périmètre du réseau	**Contrôle du périmètre du résea**
	3.4 Documentation de la politique du contrôle d'accès	**3.4 Documentation de la politi du contrôle d'accès**
	3.4.1 Les contrôles d'accès aux équipements informatiques sont-ils définis et documentés ?	3.4.1 S'assurer que les directives du management ont été documentées en obtenant et en examinant la documentation correspondante.
	3.4.2 Les contrôles d'accès sont-ils en conformité avec la politique d'accès du domaine?	3.4.2 Examiner les directives du management et vérifier si elles sont conformes à la politique d'accès au domaine.
	4.1 Normes de sécurité du réseau	**4.1 Normes de sécurité du rés**
	4.1.1 La société a-t-elle adopté des standards de sécurité du réseau pour le contrôle d'accès aux plates-formes informatiques ?	4.1.1 Vérifier que les standards ont été adoptés en obtenant et en passant en revue la documentation correspondante et / ou interviewant le personnel concerné.
	4.2 Maintien du périmètre externe claire et défini (ouverture sur l'environnement externe)	**4.2 Maintien du périmètre ext claire et défini (ouverture su l'environnement externe)**
	4.2.1 Existe-t-il une sécurité externe claire du périmètre des systèmes informatiques ?	4.2.1 S'assurer de l'existence d'une sécurité externe claire du périmètre en obtenant et en passant en revue la documentation correspondante.

Domaine	Questions d'audits	Procédure d'audit
Sécurité réseau	4.2.2 Les connexions au réseau sont-elles installées conformément à la version actuelle des standards de la sécurité du réseau ?	4.2.2 Sélectionner un échantillon de réseau. S'assurer que les standards ont été installés dans toutes les connexions au réseau en inspectant la configuration actuelle de quelques ordinateurs.
	4.2.3 Les déviations par rapport aux standards ont –elles été approuvées ?	4.2.3 Obtenir et passer en revue les approbations des déviations en question.
	4.2.4 Les périmètres de sécurités externes sont-ils régulièrement vérifiés contres des connexions par des modems non-autorisés ?	4.2.4 Vérifier en obtenant des justificatifs ou en interviewant le personnel que les périmètres de sécurités externes sont régulièrement vérifiés contres des connexions par des modems non-autorisés.
Sécurité tiers	**Gestion des connexions par des tiers** **5.1 Accords formels de sécurité informatiques avec les tiers**	**Gestion des connexions par des** **5.1 Accords formels de sécurité informatiques avec les tie**
	5.1.1 Les connexions directes par des tiers sont-elles couvertes par contrats formels de sécurité informatique ?	5.1.1 Vérifier sur la base d'un sondage que les connexions directes effectuées par des tiers sont couvertes par des contrats de sécurité informatique en examinant une copie de ces contrats.
	5.1.2 Existe-t-il un audit pour s'assurer du respect des termes du contrat relatif à la sécurité informatique ?	5.1.2 S'assurer de l'existence d'un audit en interviewant le personnel et / ou en obtenant les documents justificatifs.
	5.1.3 Les accès au domaine par des tiers sont-ils autorisés par la direction générale ?	5.1.3 Vérifier sur la base d'un sondage que les accès au domaine sont autorisés par la direction générale.
	5.1.4 Le personnel des tiers a-t-il signé un accord de confidentialité ?	5.1.4 Vérifier que le personnel des tiers a bien signé un accord de confidentialité.

ANNEXE 5

Exemple d’un programme d’audit de la sécuri
spécifique à l’ERP JD Edwards (Version World sou
AS/400)

Aspects généraux

- Déterminer l'approche de gestion de la sécurité au sein de JDE. Existe-t-il un administrateur de la sécurité JDE ?
- Revoir la procédure de maintenance du carnet d'adresse JDE (Address Book)
- Déterminer si le journal d'audit log du carnet d'adresse est activé, imprimé et revu.
- Revoir la procédure de maintenance des ICA « Instructions de Comptabilisation automatique » de JDE
- S'assurer de l'utilisation des 19 rapports d'intégrité standards de JDE et revoir les procédures de revue des dits rapports et des actions correctives qui en découlent.
- Revoir la procédure de maintenance des procédures du plan comptable JDE.

1. MODULES JDE

- Revoir les constantes systèmes de chaque module et notamment : GL, AP et ARE.
- S'assurer au niveau du module comptabilité fournisseur de l'activation du contrôle "Payee control". Cette fonctionnalité de JDE permet entre autres, de s'assurer de la bonne séparation des tâches entre la saisie et la validation des conditions de paiement d'un fournisseur.

2. SECURITE

- Accéder au menu G94 et imprimer tous les utilisateurs
- A partir de cette liste :

Accès Rapide (Fasth Path)

  - Identifier les utilisateurs ayant accès à la fonctionnalité JDE "Accès rapide" (cette fonctionnalité permet d'accéder à un programme de JDE si on connaît son code transaction).
  - Déterminer la politique d'autorisation appliquée par la société pour accéder à la fonctionnalité "accès rapide".
  - Déterminer si les utilisateurs sont réellement autorisés à accéder à la fonctionnalité "accès rapide".

Navigation (Menu Travel)

- Identifier les utilisateurs ayant accès à la fonctionnalité «navigation ».
- Déterminer la politique appliquée pour donner l'accès à la fonctionnalité "Navigation".
- Déterminer si les utilisateurs sont réellement autorisés à accéder à la fonctionnalité(navigation).

Ligne de commande AS/400 (Command Entry)

- Identifier les utilisateurs ayant accès à la fonctionnalité "Ligne de commande".
- Déterminer la politique d'autorisation appliquée par la société pour accéder à la fonctionnalité "ligne de commande".
- Déterminer si les utilisateurs sont réellement autorisés à accéder à la fonctionnalité "ligne de commande".

Touches de fonction (Function Key)

- Identifier les utilisateurs ayant "Y" au niveau de la colonne «sécurité des touches de fonction » ;
- Déterminer la politique d'autorisation appliquée par la société pour accéder à la fonctionnalité " sécurité des touches de fonction " ;
- Si le client a des personnes compétentes dans la rédaction de Query AS/400, exécuter une requête sur le fichier F96/2 en vue d'extraire tous les utilisateurs ayant accès aux touches F6, F8 (recherche par mot clé) et F18 (options de traitement).

Profiles utilisateurs

- Déterminer s'il existe des profiles utilisateurs JDE n'ayant pas de profil correspondant au niveau AS/400. En cas d'existence de ce type de profil, le message ci-après sera indiqué par JDE "** IBM Profile not found **".

Sécurité “Action Code”

A partir du menu G94, sélectionner l’option “Action Code Security ». Appuyer ensuite sur la touche F21 pour afficher la liste des options de traitements possibles :

- Rapport de la liste par utilisateurs de la sécurité « Action Code » (XJDE0001)
- Rapport de la liste par programme de la sécurité « Action Code » (XJDE0002)

A partir de ces deux états s’assurer que :

- Le profil *PUBLIC est paramétré à NNN (pas d’accès d’ajout, modification et suppression) pour tous les programmes JDE
- Sélectionner des programmes sensibles et revoir la sécurité action code par utilisateur pour s’assurer qu’elle est conforme à une bonne séparation de tâches.

Approbation des lots de comptabilité (batch Approval/Post security)

A partir du menu G94, sélectionner l’option 7 “Approbation des lots de traitements” (batch Approval / Post) et revoir les éléments suivants :

Options	Paramétrage	suggéré
Lots de comptabilité générale GLGL Batch Security	Y/N	Y
Lots de comptabilité AP	Y/N	Y
Lots de comptabilité AR	Y/N	Y

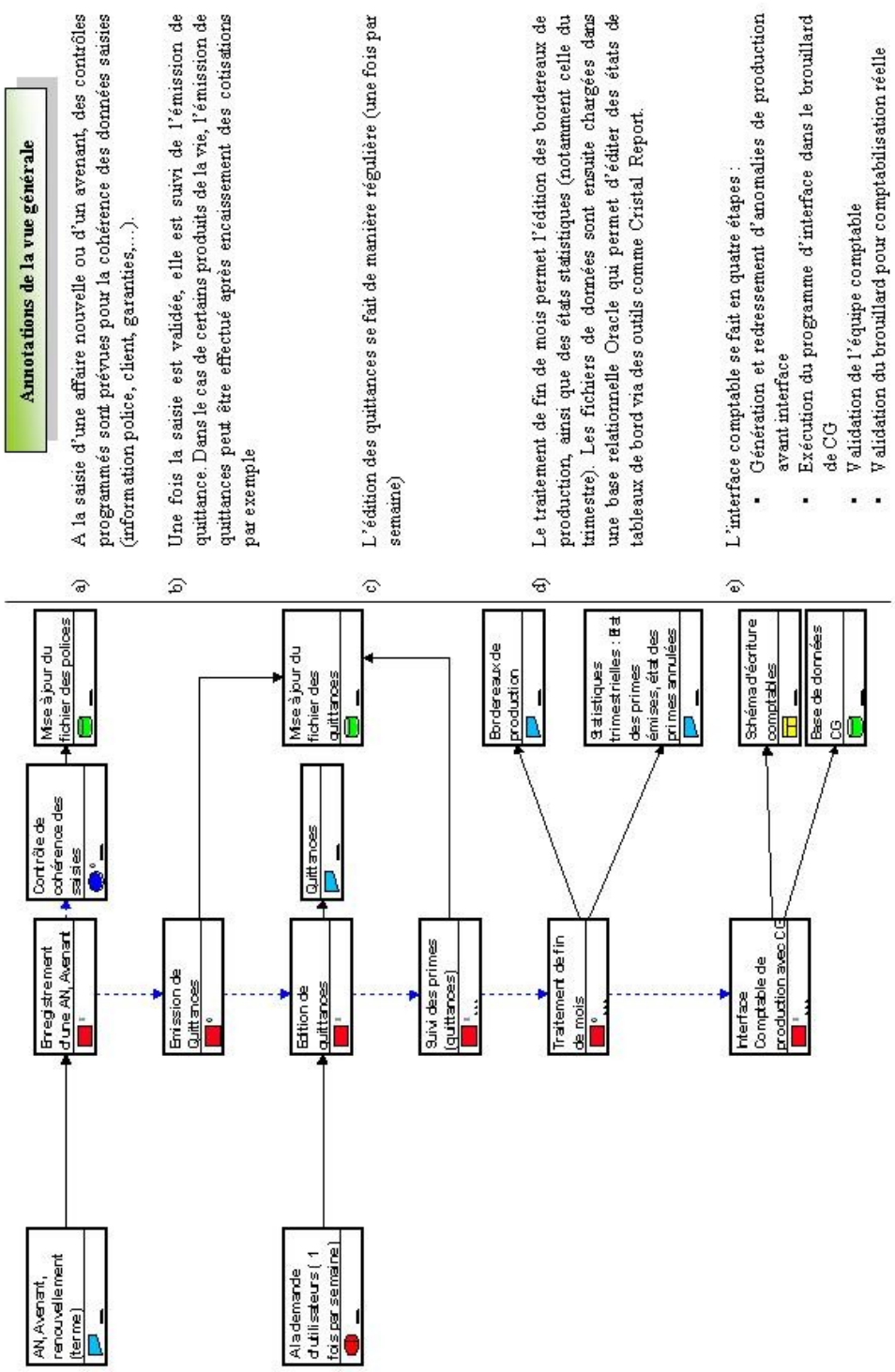
Commandes cachées

Taper ‘36’ au niveau de la saisie dans le menu JDE et voir si le résultat de cette opération permet l’accès à la ligne de commande de l’AS/400.

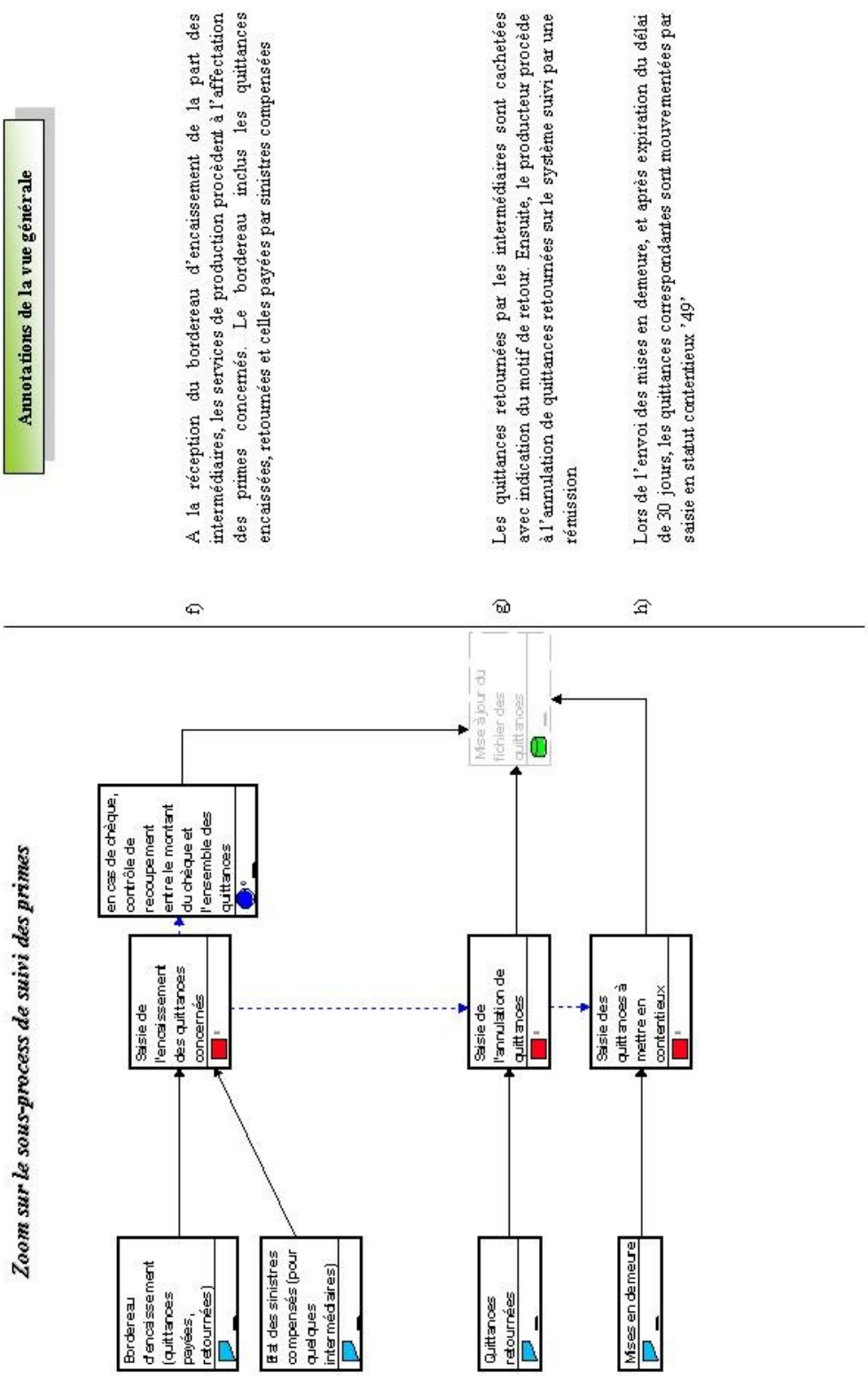
ANNEXE 6

DESCRIPTION DES PROCESS CONTRIBUANT A L'ELABORATION DU DOSSIER FINANCIER ET IDENTIFICATION DES CONTROLES Y AFFERENTS

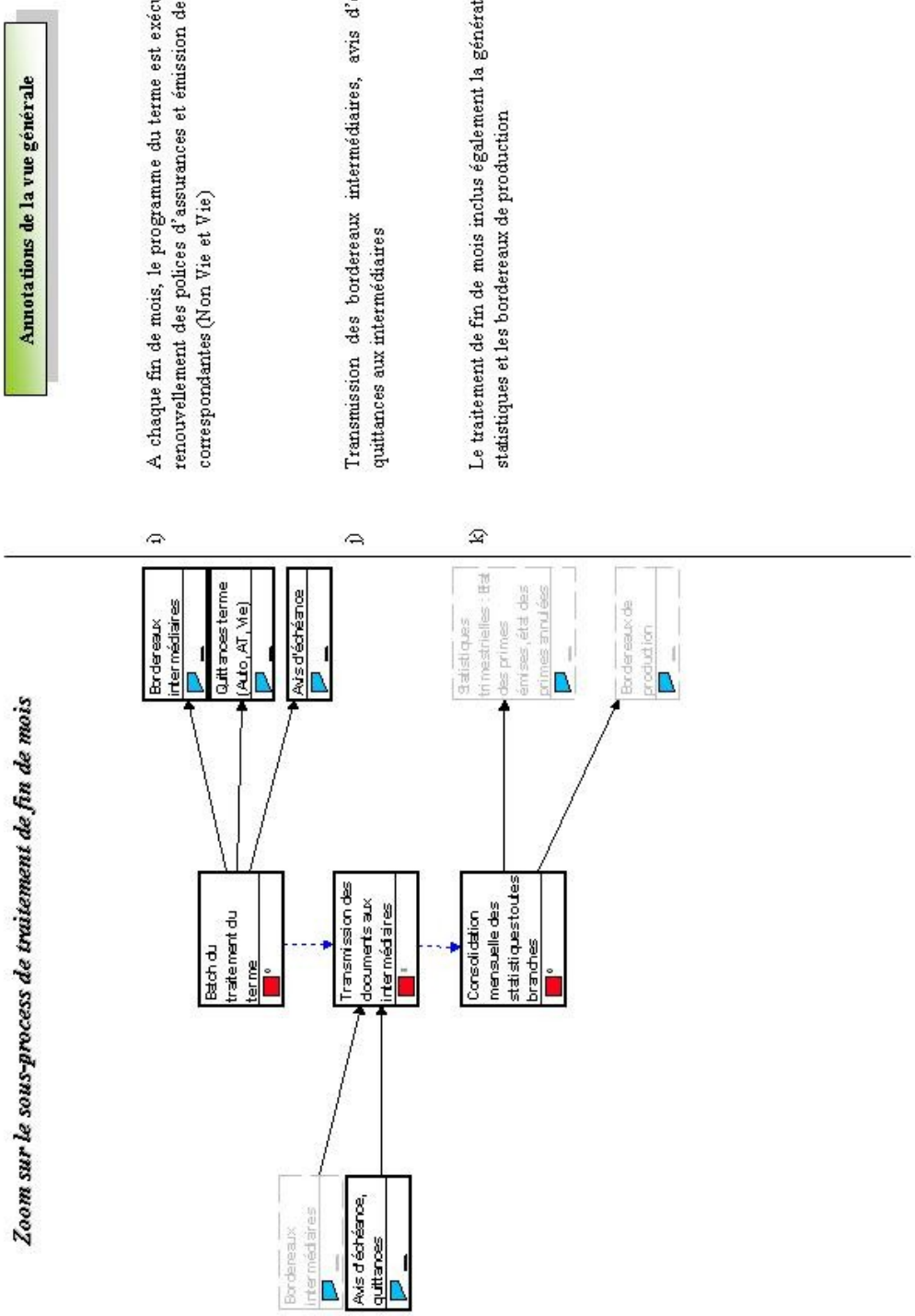
VUE GENERALE DE LA CHAINE DE PRODUCTION (AInfo)



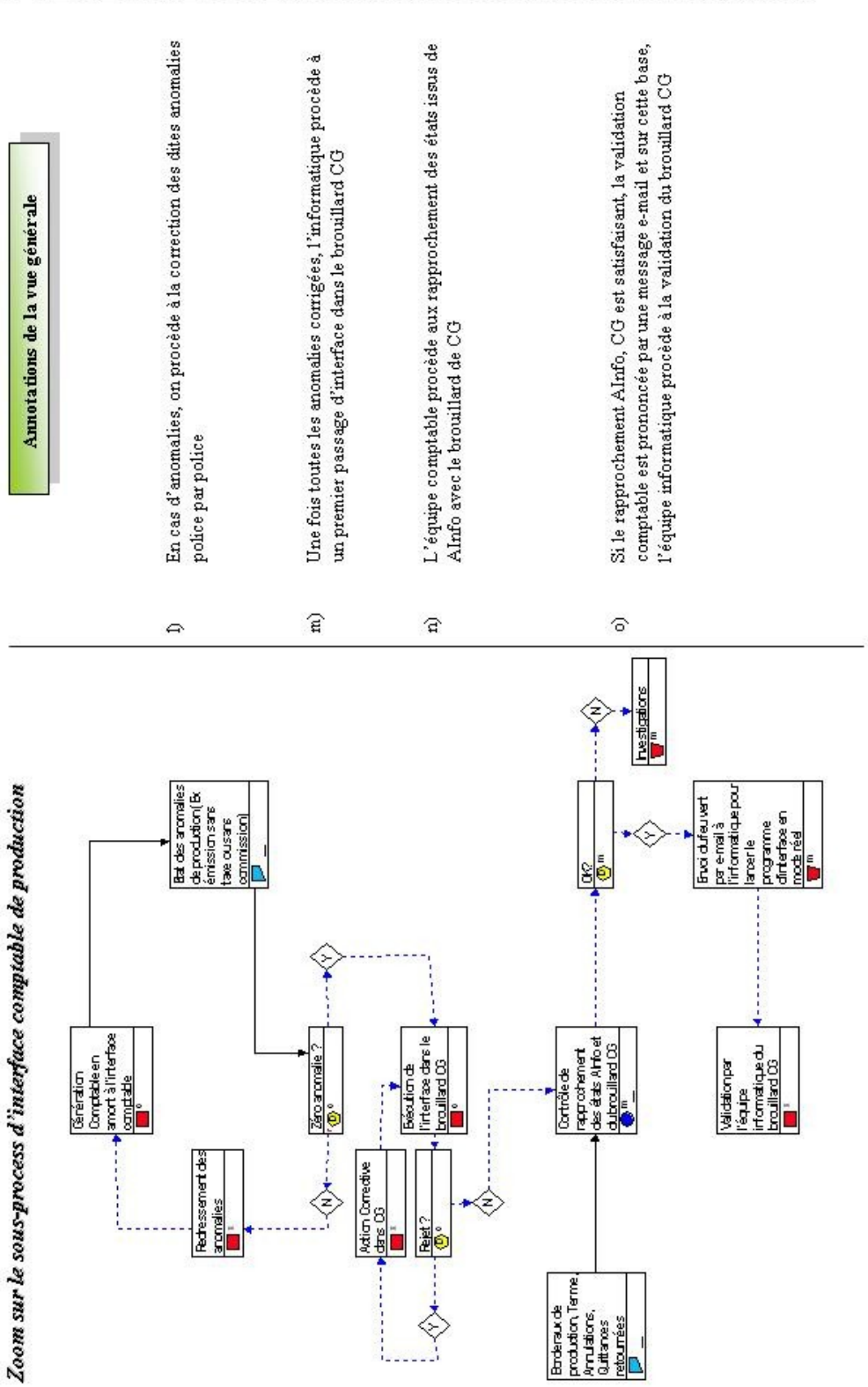
VUE GENERALE DE LA CHAINE DE PRODUCTION (AInfo)



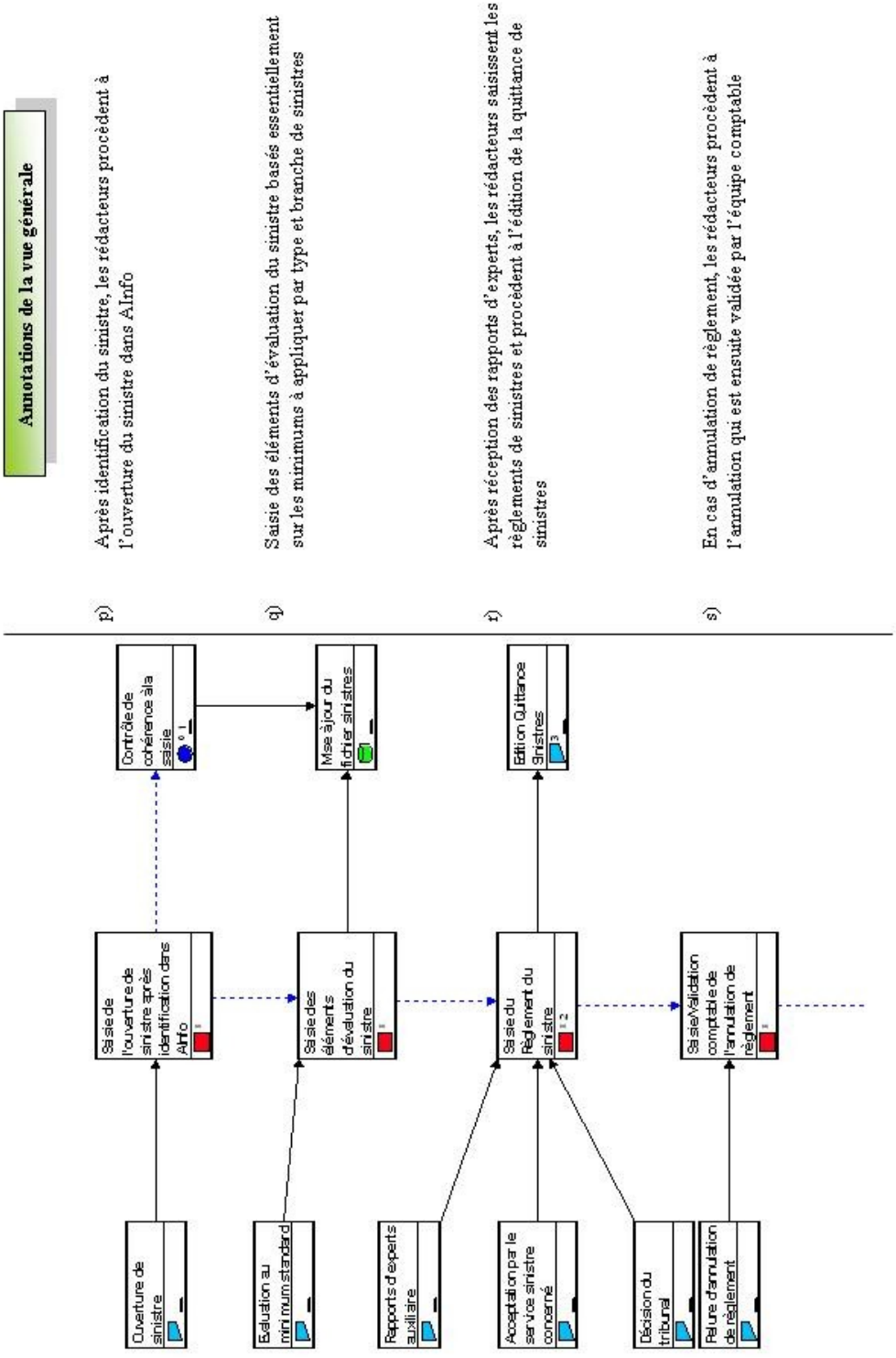
VUE GENERALE DE LA CHAINE DE PRODUCTION (AInfo)



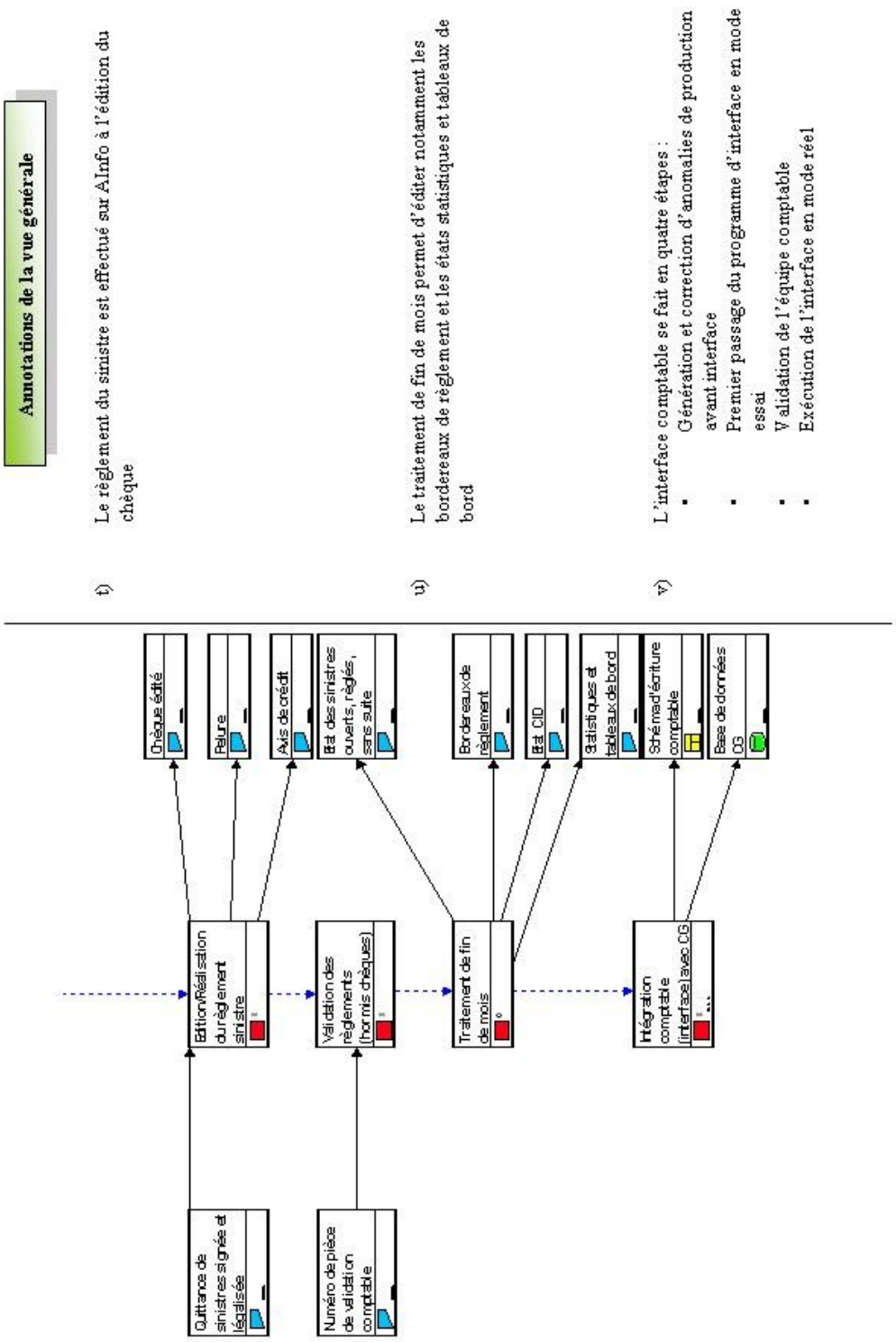
VUE GENERALE DE LA CHAINE DE PRODUCTION (AInfo)



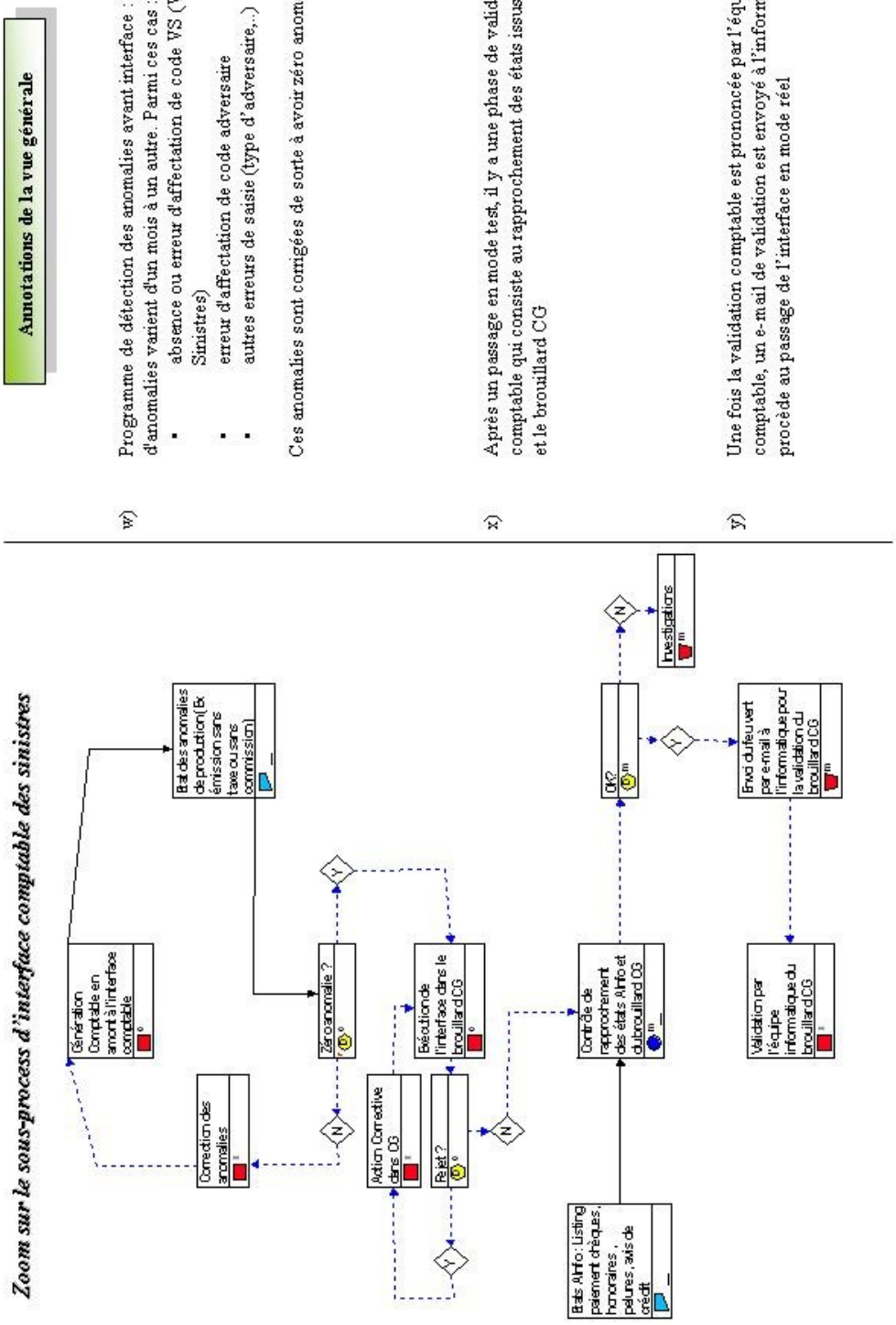
VUE GENERALE DE LA CHAINES DES SINISTRES (AInfo)



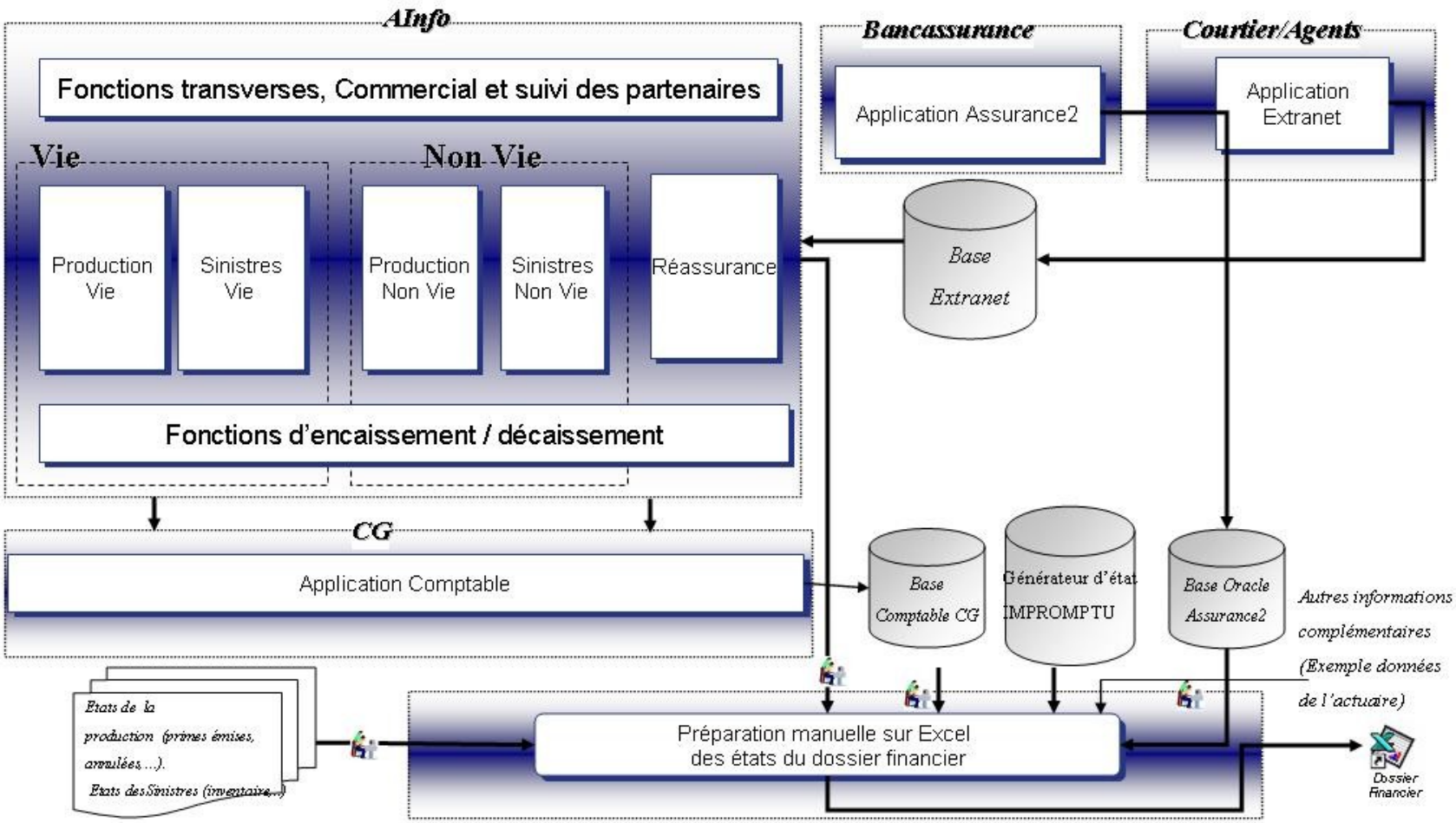
VUE GENERALE DE LA CHAINES DES SINISTRES (AInfo)



VUE GENERALE DE LA CHAINES DES SINISTRES (AInfo)



Cartographie des flux



Liste des états du dossier financier

Réf	Libellé	Départeme	Alimentation
Etat D01	compte Technique - Assurance Vie ;	Comptabilité	Manuelle (Excel)
Etat D02	compte Technique - Assurance Non – Vie ;	Comptabilité	Manuelle (Excel)
Etat D03	détail des primes émises ;	Comptabilité	Manuelle (Excel)
Etat D04	provisions techniques et leur représentation par des éléments d'actif ;	Comptabilité	Manuelle (Excel)
Etat D05	détail des placements ;	Comptabilité	Manuelle (Excel)
Etat D06	détail des primes arriérées ;	Comptabilité	Manuelle (Excel)
Etat D07	primes impayées et leurs provisions à la clôture de l'exercice ;	Dept Recouvrement	Manuelle (Excel)
Etat D08	marge de solvabilité ;	Comptabilité	Manuelle (Excel)
Etat D09	dépouillement du bilan par domaine monétaire ;	Comptabilité	Manuelle (Excel)
Etat D10	primes acquises, sinistres payés et provisions pour sinistres à payer ;	Comptabilité	Manuelle (Excel)
Etat D11	accidents du travail : Primes acquises, sinistres payés et provisions pour sinistres à payer ;	Comptabilité/ Actuariat	Manuelle (Excel)
Etat D12	assurance responsabilité civile des véhicules terrestres à moteur : Primes acquises, sinistres payés et provisions pour sinistres à payer ;	Comptabilité/ Actuariat	Manuelle (Excel)
Etat D13	mouvement des polices au cours de l'exercice (Non Vie) ;	Comptabilité	Manuelle (Excel)
Etat D14	détail de certaines provisions techniques non vie ;	Comptabilité	Manuelle (Excel)
Etat D15	détail des soldes des intermédiaires d'assurances ;	Comptabilité	Manuelle (Excel)
Etat D16	détail des soldes des réassureurs ;	Dept Réassurance	Manuelle (Excel)
Etat D17	détail des résultats de réassurances ;	Dept Réassurance	Manuelle (Excel)
Etat D18	provision pour fluctuation de sinistralité ;	Comptabilité	Manuelle (Excel)
Etat D19	participation des assurés aux bénéfices ;	Comptabilité	Manuelle (Excel)
Etat D20	Statistiques des opérations Vie ;	Comptabilité/ Actuariat	Manuelle (Excel)
Etat D21	dépôts et affectations relatifs à la couverture des provisions techniques ;	Comptabilité	Manuelle (Excel)
Etat D22	situation financière au 30 juin ;	Comptabilité	Manuelle (Excel)
Etat D23	états trimestriels ;	Comptabilité	Manuelle (Excel)
Etat D25	détail de la part des réassureurs dans les primes ;	Comptabilité	Manuelle (Excel)
Etat D26	compte des opérations de réassurance ;	Comptabilité	Manuelle (Excel)
Etat D27	compte technique de la cession légale ;	Comptabilité	Manuelle (Excel)
Etat D28	détail de la part des réassureurs dans les provisions techniques ;	Comptabilité	Manuelle (Excel)
Etat D29	dépôts effectués par les réassureurs ;	Comptabilité	Manuelle (Excel)
Etat R01	récapitulation des primes par nature d'acceptation ;	Comptabilité	Manuelle (Excel)
Etat R02	résultats d'acceptations par catégorie d'assurances ;	Comptabilité	Manuelle (Excel)
Etat R03	résultats d'acceptations par traité ;	Comptabilité	Manuelle (Excel)
Etat D22	comprend le bilan arrêté au 30 juin et le compte de produits et charges du 1er janvier au 30 juin	Comptabilité	Manuelle (Excel)

Etats : D01 et D02.

Acteur : M.

Description :

Le service de la comptabilité prépare trimestriellement des états récap sur Excel de la production à partir des listing informatiques (Listing des primes émises, listing des primes annulées). Ces états donnent des informations ventilées par branche :

- Les primes émises.
- Les primes acquises non émises.
- Les primes à annuler et primes nettes.
- Les primes non acquises.
- Règlement des sinistres

Etapes :

1. Obtenir les états de la production (primes émises, primes à émettre, les annulations, règlement sinistre….).
2. Obtenir les produits techniques d'exploitation de la balance générale (CG).
3. Ventilation des produits techniques d'exploitation selon les clés de répartition calculés au niveau de l'état D24.
4. Obtenir les charges et produits d'exploitation à partir de CG.
5. Ventilation selon les clés de répartition calculés au niveau de l'état D24.
6. Obtenir le bilan de réassurance
7. Saisir les informations sur un tableau excel.

Contrôles :

C1. Les états de la production doivent concorder avec la comptabilité générale (CG).

C2. Les totaux des états D01 et D02 doivent concorder avec la comptabilité générale.

Etat : D03

Acteur : M.

Description :
Le service de la comptabilité prépare trimestriellement des états récap sur Excel de la production à partir des listing informatiques (Listing des primes émises, listing des primes annulées). Ces états donnent des informations ventilées par branche :

- **Les primes émises**.
- Les primes acquises non émises.
- Les primes à annuler et primes nettes.
- Les primes non acquises.

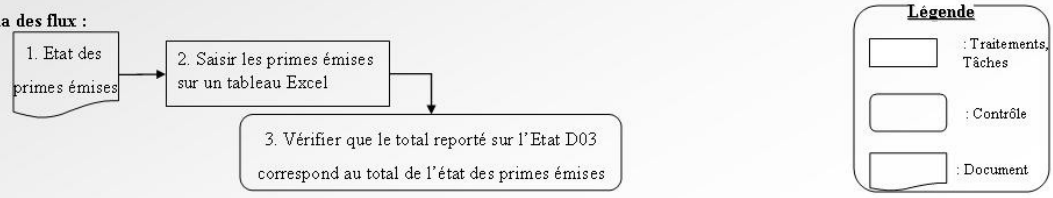
Etapes :

1. Obtenir la version actualisée de l'état des primes émises.
2. Saisir les primes émises sur un tableau Excel

Contrôles :

C3. Vérifier que le total reporté sur l'état D03 correspond au total de l'état des primes émises

Schéma des flux :



Etat : D04

Acteur : M.

Description :
Le service de la comptabilité prépare trimestriellement des états récap sur Excel de la production à partir des listing informatiques (Listing des primes émises, listing des primes annulées). Ces états donnent des informations ventilées par branche :

- Les primes émises et primes non acquises.
- Les primes acquises non émises.
- Les primes à annuler et primes nettes.
- **Les réserves mathématiques**

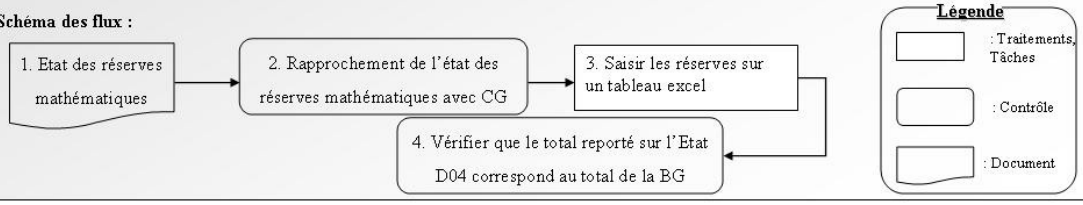
Etapes :

1. Obtenir l'état des réserves techniques préparé par M. sur la base du listing informatique issus de AInfo.
2. Saisir les réserves sur tableau Excel

Contrôles :

C4. Vérifier que l'état des réserves techniques communiqué par M. est cohérent avec CG.
C5. Vérifier que les totaux de l'état D04 sont cohérents avec CG.

Schéma des flux :



Etat : D05, D21 et D22

Acteur : Mme

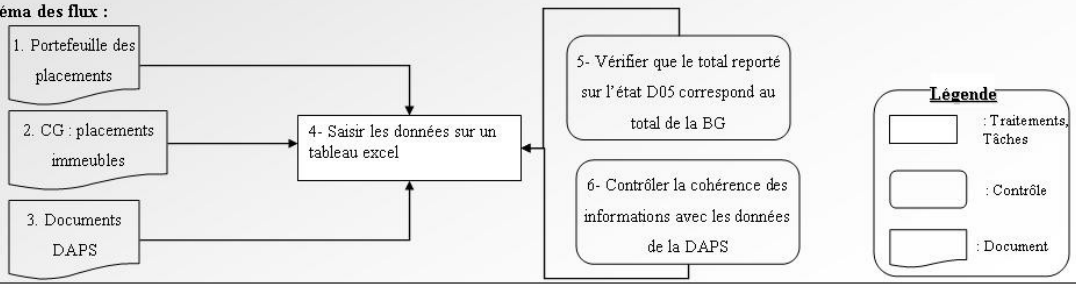
Description :
L'état D05 donne le détail des placements

Etapes :

1. Obtenir le détail des placements financiers (actions, obligations, fonds dédiés et OPCVM) à partir du portefeuille géré par le service trésorerie.
2. Extraire les informations relatives aux placements immeubles de la balance générale (CG).
3. Collecter les informations communiquées par la DAPS (Cours de clôture, valeurs liquidatives…).
4. Saisie des informations sur un tableau Excel.

Contrôles :
C6. Vérifier que le total reporté sur l'état D05 correspond au total de la balance générale (CG).
C7. Vérifier le respect des indications de la DAPS.

Schéma des flux :



Etat : D06

Acteur : M..

Description :

Le service de la comptabilité prépare trimestriellement des états récap sur Excel de la production à partir des listing informatiques (Listing des primes émises, listing des primes annulées). Ces états donnent des informations ventilées par branche :

- **Les primes émises**
- Les primes acquises non émises.
- **Les primes à annuler et primes nettes.**
- Les primes non acquises

Etapes :

1. Primes arriérées : préparé à partir de la balance générale ➔ les soldes du compte 3421 sont reportés sur un tableau Excel.
2. Emissions : élaboré à partir de l'état des primes émises d'une part et de la balance âgée préparée par le service recouvrement moyennant les données issues de AInfo.
3. Annulations : préparé à partir de l'état des primes à annuler.
4. Encaissements : élaboré à partir du détail des encaissements par mois envoyés par le service recouvrement qui utilise les données issues de AInfo.

Contrôles :

C8. Le solde des émissions selon la balance âgée doit correspondre au total de l'état des émissions.

C9. Le solde de l'état D06 (Primes arriérées+ émissions- annulations- encaissements) doit correspondre à la balance générale de clôture.

Etat : D08

Acteur : M.

Description :

Le tableau D08 présente le détail de calcul de la marge de solvabilité.

Etapes :

1. Extraire les informations nécessaires au calcul de la marge de solvabilité du système CG.
2. Saisie des données sur Excel
3. Obtenir les données relatives aux capitaux sous risque de la direction pôle vie et les saisir sur la tableau Excel.

Contrôles :

C10. Vérification des données saisies par rapport au système CG.

C11. Vérification du calcul arithmétique et des formules.

Etat : D09
Acteur : M.
Description : Le tableau D09 présente le dépouillement du bilan par domaine monétaire
Etapes : 1. Obtenir les soldes en devise à partir des relevés bancaires. 2. Obtenir le taux de change à utiliser d'après un communiqué du ministère des finances. 3. Saisir les données sur un tableau excel.
Contrôles : **C12.** Vérifier que le solde de l'état D09 concorde avec la comptabilité générale (CG).

Etat : D10, D11 et D12.
Acteur : Tableau 1: M. Tableau 2: M..
Description : Le tableau D10 présente les primes acquises, les sinistres réglés et les sinistres à payer des branches autres que l'automobile et l'accident de travail. Les tableaux D11 et D12 présentent les mêmes informations pour respectivement la branche AT et la branche Auto
Etapes *P01* : PNA : A partir de l'état de N-1. *P02* : Cumul des primes émises : à partir le l'état de l'exercice précédent. *P03* : - Pour les exercices antérieurs : Etat de N-1 - Pour l'année en cours : à partir de l'état des primes émises. *P04* : PANE : à partir de l'état des primes à émettre *P06* : Primes non acquises : à partir du tableau des PNA : Traitement manuel pour la ventilation des PNA par branche. *Réserves* : AInfo. *Règlements* : AInfo. Pour les chiffres de l'année N-1, la source est l'état envoyé à la DAPS de l'année N-1. Les tableaux triangulaires : Information communiquée par l'actuaire.
Contrôles : **C13.** S'assurer du calcul arithmétique.

Etat : D13

Acteur : M.

Description :

L'état D13 présente les mouvements des polices au cours de l'exercice.

Etapes :

1. Obtenir l'état informatique « MP4 » : « Mouvements- production 4 » : Etat informatique issu de AInfo qui regroupe les polices en cours et les mouvements des polices au cours de l'exercice
2. Reprendre les informations relatives aux exercices antérieurs à partir de l'état D13 de l'exercice précédent.
3. Un traitement manuel est effectué pour regrouper les polices par branche
4. Saisie manuelle des résultats obtenus sur un tableau excel.
5. Pour la branche automobile, les montants des polices sont renseignés à partir de l'état des primes nettes par branche.

Contrôles :

C14. Comparaison des nombres et des montants des polices avec l'exercice précédent

C15. Rapprochement du montant des polices selon l'état informatique avec l'état des primes émises.

Etat : D15

Acteur : M.

Description :

L'état D15 détaille les soldes de C/C des intermédiaires

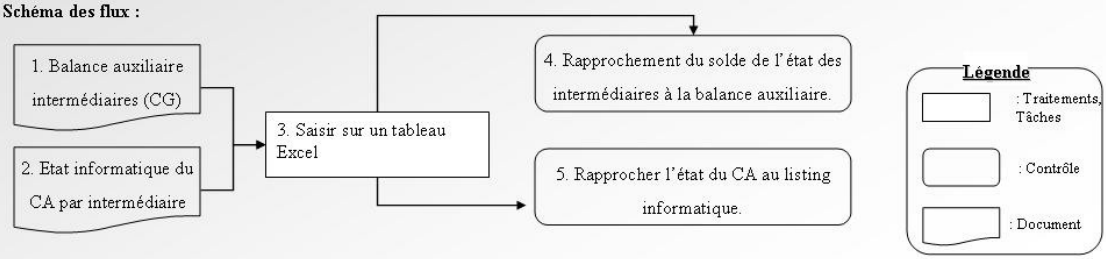
Etapes :

1. Obtenir l'état précédent pour renseigner les soldes des exercices antérieurs.
2. Obtenir l'état informatique du CA par intermédiaire.
3. Saisie des données sur un tableau excel.

Contrôles :

C16. Rapprochement du solde de l'état des intermédiaires à la balance auxiliaire.
C17. Rapprochement du CA total de l'état au CA du listing informatique.
C18. Rapprochement du CA total de l'état au tableau des primes émises par branche.

Schéma des flux :



Etat : D 16 et D17

Acteur : M.

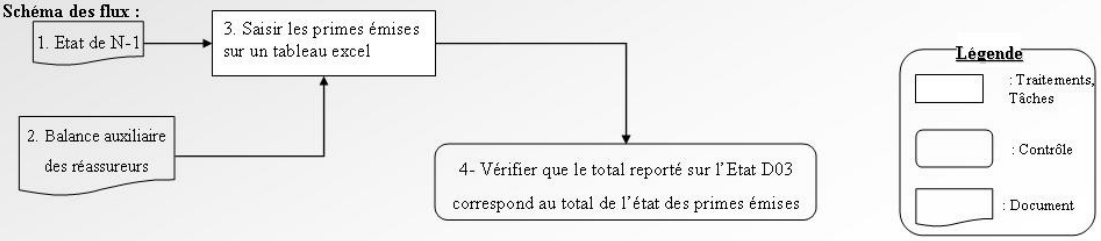
Description :
D16 : Etat des soldes de réassurances
D17 : Etat détaillé des résultats de réassurance

Etapes :

1. Report des solde de N-1 à partir de l'état précédent.
2. Les soldes techniques de réassurance sont renseignés à partir de la balance auxiliaire extra comptable des réassureurs tenue par le service de réassurance.
3. Les mouvements de l'exercice sont renseignés sur la base des avis de débit et de crédit traités initialement par le service comptable et dont une copie est transmise au service de réassurance.

Contrôles :
C19. Contrôle de la concordance des états D16 et D17 avec le suivi des situations des réassureurs du service de réassurance.

Schéma des flux :



Etat : D18

Acteur : M.

Description :
Provision pour fluctuation de sinistralité (RFS)

Etapes :

1. Obtenir les informations nécessaires au calcul de la **Prov.(RFS)** : à partir de CG : Primes, prestations et frais payés, variation des réserves pour SAP.
2. Saisie sur un tableau excel.
3. Calcul du solde technique et du montant à affecter à la réserve de stabilité. (Formule)
4. Obtenir le montant de la réserve de stabilité de N-1 à partir de l'état précédent
5. Calcul de la réserve de stabilité de l'exercice (Formule).
6. Détermination du plafond de la réserve en calculant manuellement la moyenne des primes émises au cours des 3 derniers exercices en assurance « Groupe décès ».

Contrôles :

C20. Vérifications des données saisie sur l'état D18 à partie de CG.

C21. Vérification des formules de calcul.

Etat : D19

Acteurs :
M.

Description :
Calcul de la participation aux bénéfices

Etapes :

1. Tableau 1 : Informations obtenues à partir de la comptabilité : CG
2. Tableau 2 : Détermination de la clé de répartition (QP des réserves techniques moyennes par branche).
3. Détermination du résultat technique, les données dont obtenues de CG, leurs ventilation par branche et par catégorie est obtenu du système AInfo.

Contrôles :

C22. Contrôle des données et des calculs de l'état D19 par le DAF.

C23. Rapprochement entre l'état D19 et l'état D01.

Etat : D23

Acteurs :
M.
M.

Description :
Etat trimestriel des flux

Etapes :

1. Les informations des trimestres précédents sont renseignées à partir de l'état précédent.
2. Obtenir l'état informatique des primes de l'exercice.
3. Traitement manuel pour distinguer les contrats vie et non vie.
4. Saisie des totaux sur un tableau Excel.
5. Obtenir l'état des primes nettes d'annulation et saisie des données sur le tableau Excel.
6. Réception du fichier informatique des primes émises et commissions correspondantes et saisie des données sur le tableau excel. Cet état est édité trimestriellement par le générateur d'états « IMPROMPTU ».
7. Les autres informations sont extraites directement du système AInfo et saisies sur le tableau.

Contrôles :

C24. La somme des primes émises nettes des annulations doit correspondre au CA (Etats de la production).

ANNEXE 7

LEXIQUE FRANÇAIS-ARABE

	FRANÇAIS	عربية
1	COMPTABILITE	محاسبة
2	CAHIER DES CHARGES	دفتر التحملات
3	CHAMP D'APPLICATION	مجال التطبيق
4	E-COMMERCE	التجارة الالكترونية
5	CONFIDENTIALITE DES DONNEES	سرية المعطيات
6	CONNEXION	اتصال
7	COURRIER ELECTRONIQUE	رسالة الكترونية
8	DONNEES NUMERIQUES	معطيات رقمية
9	ECHANGE DE DONNEES INFORMATISEES	تبادل المعطيات المعلوماتية
10	LOGICIEL	برنامج حسوبي (برنامج معلوماتي)
11	MATERIEL INFORMATIQUE	الجهاز المعلوماتي
12	NORMALISATION	تقييس
13	NORME	مقياس
14	NOUVELLES TECHNOLOGIES DE L'INFORMATION	التكنولوجيا
15	RESEAU INTERNET	شبكة الأنترنيت
16	SAUVEGARDE	تحصيل
17	SECURITE	حصانة
18	ACCES	ولوج
19	MODULE	مجال
20	ASPECTS GENERAUX	الهيئات الشمولية
21	PROFIL	التعرفة
22	DOSSIER FINANCIER	ملف مالي
23	COMPAGNIE D'ASSURANCE	شركة التأمين
24	COMMISSAIRE AUX COMPTES	مدقق قانوني للحسابات
25	EXPERT COMPTABLE	خبير حسوبي
26	COMMANDE	طلب اقتناء
27	DOMAINE	مجال
28	FONCTION	وظيفة
29	UTILISATEUR	مستعمل
30	DEVELOPPEMENT	برمجة
31	TEST	اختبار
32	AUDIT	تدقيق

	FRANÇAIS	عربية
33	APPROBATION	موافقة
34	ORGANISATION	هيكلة
35	CYCLE DE VIE	مدار حياتي
36	PROCESSUS	سير
37	PROCEDURE	اجراء
38	APPLICATION INFORMATIQUE	منظمة اعلامية
39	L’INFORMATIQUE	الاعلاميات
40	INTEGRITE DES DONNEES	تكامل البيانات
41	INTRANET	أنترانيت
42	INTEGRITE	سلامة المحتوى والوقوف
43	SYSTEME D’INFORMATION	نظام اعلامي
44	LE CONTROLE INTERNE	المراقبة الداخلية
45	L’AUDIT COMPTABLE ET FINANCIER	تدقيق حسابي و مالي
46	APPLICATION	تطبيقة
47	ADMINISTRATEUR	مدير
48	MIGRATION DES DONNEES	نقل البيانات
49	MOT DE PASSE	آلمة عبور
50	E.R.P	منظومة اعلامية مندمجة
51	BASE DE DONNEES	قاعدة بيانات
52	BASE DOCUMENTAIRE	قاعدة تحصيل الوثائق
53	BUREAUTIQUE	آليات المكتب
54	CIRCUIT INTEGRE	دارة مندمجة
56	CLIENT	زبون
57	DISQUE DUR	قرص صلب
58	DONNEES	بيانات
59	EXTRANET	آلسترانيت
60	INDICATEUR	مؤشر
61	INFORMATION	معلومة
62	INTERFACE	سطح بيني
63	LANGAGE DE PROGRAMMATION	لغة البرمجة
64	MEMOIRE	دآرة
65	MICROPROCESSEUR	معيلج
67	ORDINATEUR	حاسوب

	FRANÇAIS	عربية
68	MODELE	نموذج/طراز
69	SYSTEME D’EXPLOITATION	نظام تشغيل
70	ECHANGE DE DONNEES INFORMATISEES (E.D.I)	تبادل المعطيات والمعلوماتية
71	SECURITE DES TRANSACTIONS	تأمين المعاملات
72	SIGNATURE ELECTRONIQUE	توقيع الكتروني
73	AUTHENTIFICATION	مصادقة/تحديد