

**AUDIT DES SYSTEMES  
D'INFORMATION AUTOMATISES  
ET OUTILS INFORMATIQUES DE L'AUDITEUR**

**SUPPORT DE COURS**

# SOMMAIRE

| <b>Description</b>  | <b>Page</b> |
|---|-------------|
| Introduction.....   | 3           |
| 1- Les concepts de l'audit informatique.....  | 8           |
| 2- Audit de la politique et des stratégies de mise en place<br>de l'informatique..... | 11          |
| 3- Audit de l'organisation générale et des ressources<br>humaines informatiques.....  | 15          |
| 4- Audit des études.....  | 22          |
| 5- Audit de l'exploitation.....   | 32          |
| 6- Audit des moyens techniques.....   | 55          |
| 7- Audit des applications en exploitation.....  | 66          |
| 8- La conduite d'une mission d'audit informatique .....                               | 80          |
| 9- Les outils de l'auditeur informatique.....   | 89          |

# **INTRODUCTION**

## **LA REVOLUTION TELEMATIQUE**

**Nous vivons actuellement, la quatrième révolution industrielle : l'ère de l'informatique, l'ère de la révolution télématique (informatique + télécommunications).**

L'ordinateur, outil de traitement de l'information, permet à l'homme de développer son pouvoir mental comme le moteur a multiplié sa force physique.

L'informatique a pris une place de première importance dans notre société. Présente au travail, dans les écoles, dans les loisirs et même dans les domiciles, il est indéniable qu'elle fait maintenant partie des habitudes courantes, au même titre que le téléviseur ou l'automobile.

L'informatique s'est développée rapidement, trop rapidement sans doute pour la police qui se prépare fébrilement à faire face à une forme de criminalité nouvelle : **la criminalité informatique**. Une criminalité abstraite car elle est constituée d'éléments inconnus des policiers à savoir : les ordinateurs, les logiciels, le stockage et l'accès à des renseignements. Pour ces raisons, les activités frauduleuses liées à l'informatique sont difficiles à prévenir et à détecter.

Grâce à la jonction de l'informatique, des réseaux de télécommunications et de la télévision, toute une gamme de nouveaux services fait son apparition. On connaît déjà l'édition à distance des journaux dans des imprimeries décentralisées. Les téléconférences, la télétransmission des messages à l'intérieur des organisations, le courrier électronique, se généralisent. Les procédés de télécopie deviennent d'usage courant. Les banques bibliographiques ou documentaires peuvent maintenant être interrogées à distance. Les individus, les entreprises peuvent "commercer" en ligne.

**On ne peut le nier, l'ordinateur a pénétré chacune de nos activités quotidiennes et il demeure évident que l'informatisation fait partie de l'avenir et qu'elle ne pourra qu'influencer davantage notre vie.**

## **L'INFORMATION = LE FACTEUR CAPITAL DU DEVELOPPEMENT ET DE LA SURVIE DE TOUTE ENTREPRISE**

**Au cours de la dernière décennie, l'informatique a décuplé l'habileté de l'homme à utiliser l'information à tel point qu'elle a engendré une révolution du travail intellectuel dont l'impact est considérablement plus grand que celui produit par la révolution industrielle sur le travail manuel.** La révolution industrielle a transformé l'économie de subsistance en économie de consommation, l'organisation artisanale du travail en production à la chaîne, la culture des élites en culture de masse. *La révolution de l'information a non seulement modifié les méthodes de travail, les structures des entreprises mais a également entraîné toute une série de changements structurels dans notre vie et dans nos valeurs.*

**L'information est nécessaire dans tous les domaines de la pensée et de l'action humaine.** En comparant les individus dépourvus d'informations et de connaissance à ceux qui en ont, ces derniers ont de plus grandes possibilités de carrière et sont mieux armés pour prendre des décisions.

**Outre le fait d'être essentielle aux individus qui l'utilisent pour des buts personnels, l'information est aussi nécessaire pour ceux qui prennent les décisions dans les entreprises.** Tous les gestionnaires doivent accomplir certaines tâches ou fonctions de base afin d'atteindre les objectifs fixés. Les objectifs poursuivis diffèrent, mais les aptitudes de base sont les mêmes pour tous. En d'autres mots, tous les gestionnaires doivent savoir planifier, organiser, diriger, recruter et contrôler. Le succès de toute entreprise va dépendre de la capacité des gestionnaires de mener à bien ces diverses fonctions. Ces fonctions seront d'autant mieux réalisées si les dirigeants sont suffisamment informés.

*Pourquoi ?*

Parce que chaque fonction exige une prise de décision et cette prise de décision doit être accompagnée d'une information précise, opportune, complète et pertinente.

**Mettre une information de qualité à la disposition de ceux qui savent l'utiliser facilite la prise de décision ;** les bonnes décisions vont permettre la réussite des activités de gestion ; et une réussite effective en gestion conduit à la réalisation des buts de l'entreprise. **L'information est l'agent de liaison qui maintient l'unité de l'entreprise.**

## **LE SYSTEME D'INFORMATION AUTOMATISE : LE CŒUR DE L'ENTREPRISE**

Les systèmes d'informations traditionnels ont souvent laissé à désirer parce qu'ils devaient posséder les qualités suivantes : peu coûteux, pertinents, opportuns, vraiment intégrés, concis, vraiment disponibles dans une forme variable.

Pour diminuer les difficultés soulevées, par les approches traditionnelles, de nouveaux concepts de systèmes d'information en gestion, orientés vers l'utilisation des ordinateurs, ont été développés. Ces efforts d'améliorations sont dus à un certain nombre de pressions qui ont incité les gestionnaires à s'orienter vers l'utilisation de l'ordinateur. Parmi ces pressions, on peut citer :

### **La capacité de traitement dans plusieurs entreprises a été augmentée par :**

- la croissance en grandeur et non en complexité de l'entreprise ;
- la demande croissante de données par des sources externes ;
- la demande constante des gestionnaires afin d'obtenir davantage d'information. Plus le volume à traiter est grand, plus le traitement par ordinateur se révèle économique en comparaison d'autres traitements ;
- les coûts moins importants de l'informatique.

### **L'information fournie par un système informatisé aura un impact important sur la gestion d'une organisation :**

- en permettant d'identifier rapidement les problèmes et les possibilités ;
- en aidant à l'analyse du problème et au choix de solutions possibles ;
- en influençant le choix le plus approprié.

◆ **LE SYSTEME D'INFORMATION AUTOMATISE :  
EVOLUTION**

| <b>Etapes</b>   | <b>Technologie</b>                    | <b>Acteurs impliqués dans la mise en oeuvre</b>                      |
|---|---------------------------------------|--|
| Centralisation des traitements<br>1950 - 1970         | Mainframe<br>Fichier                  | Informaticien  |
| Décentralisation<br>1970 - 1990                       | PC<br>SGBD                            | Maître d'œuvre<br>Informaticiens                                     |
| Interopérabilité<br>standardisation<br>1990 – 2000    | et Client -serveur<br>ERP<br>Internet | Maître d'ouvrage<br>Maître d'œuvre<br>Utilisateurs<br>Informaticiens |
| Universalité et gestion des<br>connaissances<br>2000- | NTIC                                  | Maître d'ouvrage<br>Maître d'œuvre<br>Utilisateurs<br>Informaticiens |

**LES FACTEURS CLES DE SUCCES ET LES MENACES**

**La disponibilité de l'information est indispensable à la survie de l'entreprise.**

En effet, la perte d'un fichier ou d'une banque de données ou la non disponibilité des équipements informatiques en temps opportun, causée par une erreur de programmation, d'un sabotage ou d'un désastre naturel, peut parfois signifier pour une entreprise, la fin permanente des opérations. Imaginons une entreprise dont le fichier des comptes clients (comptes des recevables) est détruit. Elle serait considérablement affectée par la perte de ces informations et sa survie serait sûrement compromise.

**Par ailleurs, l'importance de l'exactitude de l'information peut parfois être capitale pour une organisation.** Prenons, par exemple, le cas du gestionnaire utilisant l'ordinateur pour manipuler des informations qui l'aideront à orienter une décision stratégique sur son entreprise.

**Toutefois, la prolifération des ordinateurs et des systèmes informatiques ainsi que leur interconnexion (à l'échelle de l'entreprise, de la nature, de la planète), a fait naître une forme de criminalité beaucoup plus sophistiquée,**

plus rentable que toutes les autres connues à ce jour, et dans laquelle on peut évoluer sans danger d'être pris. Les conséquences de cette criminalité dite "informatique", peuvent être désastreuses pour les entreprises.

L'accroissement du nombre de banques de données contenant différentes informations stratégiques pour l'entreprise a multiplié les risques de violation du caractère confidentiel. Il demeure de la responsabilité de l'entreprise de veiller à protéger adéquatement ses informations emmagasinées dans les ordinateurs.

Il faut noter aussi que l'informatique nécessite la mobilisation d'importantes ressources financières.

**L'entreprise doit donc en permanence s'assurer du caractère opérationnel de la sécurité et des performances de son système d'information.**

Elle doit aussi s'assurer qu'en cas de sinistre informatique, elle dispose de mesures palliatives, pour garantir la continuité de sa production (exploitation) informatique.

*Il s'agit donc pour l'entreprise de procéder de manière régulière à l'examen de son système d'information.*

**L'AUDIT INFORMATIQUE EST L'OUTIL PRIVILEGIE POUR LA REALISATION D'UNE TELLE MISSION.**

## **1 – LES CONCEPTS DE L'AUDIT INFORMATIQUE**

L'audit est l'examen d'une situation, d'un système d'informations, d'une organisation pour porter un jugement.

C'est donc la comparaison entre ce qui est observé (un acte de management ou d'exécution) et ce que cela devrait être, selon un système de références.

Il est clair que le jugement ne peut se limiter à une approbation ou à une condamnation, comme c'est souvent le cas, mais il faut préciser aussi ce qu'il aurait fallu faire, et ce qu'il faudra faire pour corriger les défauts constatés.

### **LES DIFFERENTS TYPES D'AUDITS DES SOCIETES**

Une société est créée par un groupement de personnes animé d'un but « la recherche du gain ». Elle a une personnalité juridique distincte des actionnaires ou associés. Sa direction est confiée soit à certains actionnaires, soit à des non-associés. Dans le souci de protéger les actionnaires et aussi des différents partenaires sociaux de la société, la loi sur les sociétés a prévu un certain nombre de contrôles (audits) externes, dits légaux, qui peuvent être :

- soit permanents : commissariats aux comptes ;
- soit occasionnels : expertise judiciaire, commissariat aux apports.

Les dirigeants de l'entreprise, peuvent, en plus du contrôle légal, désigner un professionnel, indépendant, pour procéder à des contrôles, dits audits contractuel.

- Examen de leurs comptes en vue d'exprimer une opinion motivée sur la régularité et la sincérité du bilan et de leurs comptes de résultats.
- examen de leur système d'information, pour apprécier sa fiabilité, sa sécurité et sa pertinence.
- Etc..



## QU'EST CE QUE L'AUDIT INFORMATIQUE ?

Si le concept de l'audit informatique est aujourd'hui largement répandu, ce terme générique recouvre en réalité des objectifs et des méthodes très variés.

Pour le Directeur Général peu féru en la matière, il s'agit souvent d'un moyen de « voir un peu plus clair » dans l'activité d'un des services clés de son entreprise.

Pour le Directeur Informatique, l'audit informatique, apporte, outre un conseil en organisation fourni par des spécialistes extérieurs, le moyen d'accompagner et de justifier la mise en place de nouvelles structures ou de nouvelles méthodes. Le Directeur Financier, quant à lui, y verra plus généralement le moyen d'apprécier la fiabilité des chaînes de traitement dont il est l'utilisateur. Enfin, le Commissaire aux Comptes, indépendant de l'entreprise et dont le rôle est d'en certifier les comptes, s'intéressera en particulier aux moyens d'utiliser l'outil informatique pour établir et conforter son opinion.

Ainsi donc, sous ce même concept se cachent des objectifs totalement différents.

Toutefois, quelque soit son objectif ou son étendue, l'audit informatique concerne les composantes du système informatique d'information de l'entreprise. Celles-ci sont :

- les aspects stratégiques : conception et planification de la mise en œuvre du système d'informations.
- l'environnement et l'organisation générale de la gestion de l'informatique.
- Les activités courantes de gestion de l'informatique.
- les ressources informatiques mises en service.
- les applications informatiques en service.
- la sécurité.

## QUELLE EST DONC LA PLACE DE L'AUDIT INFORMATIQUE ?

Normalement, une place prépondérante, compte tenu de l'importance primordiale du système d'information évoquée ci-avant, en introduction. Cependant, malgré des améliorations très lentes, l'audit informatique est fort peu répandu ; l'informatique étant le dernier métier que l'on songe à auditer, et que l'on n'ose pénétrer.

### Pourquoi ? :

- Les décideurs ont trop souvent rarement conscience des vulnérabilités induites par un système automatisé ;
- L'informatique est vue comme un outil technique neutre et n'est pas conçue comme auditable, alors qu'elle est le support de toutes les activités ;
- Bien que les systèmes soient à la fois de plus en plus intégrés (bases de données) et répartis (réseaux), que les contrôles soient de moins en moins visibles, et les décisions de plus en plus rapides, il est bien rare que l'on songe à identifier le responsable d'une information et celui du contrôle de celle-ci ;
- Le sentiment que l'informatique est trop technique pour pouvoir être audité ;
- L'audit est souvent considéré comme un coût et non comme un moyen efficace de réduire les risques ;
- Enfin, un sentiment répandu est que les informaticiens apprécieraient fort peu d'être audités, s'y ajoutent les problèmes ci-après :

l'évolution rapide des matériels, réseaux, logiciels, systèmes de gestion de bases de données et langages, conduisant à une prolifération anarchique de petits systèmes,

quel profil ?, quelle compétence pour l'auditeur informatique ?

absence de normes, de référentiels, de principes et même de technologies communs.

**Ainsi, la qualité d'un audit informatique dépend - elle trop souvent de la personnalité de l'auditeur .**

## **2 - AUDIT DE LA POLITIQUE ET DES STRATEGIES DE MISE EN PLACE DE L'INFORMATIQUE**

### **2-1 DEFINITION**

La politique et les stratégies de mise en place de l' informatique sont formulées dans les documents suivants :

- Le schéma directeur informatique
- Le plan informatique
- Le plan de sécurité
- Le plan de qualité

#### **Le schéma directeur présente :**

La politique et les objectifs en matière de développement des systèmes informatiques ceci en fonction des objectifs et du métier de l' entreprise  
 L' architecture du système d' information cible  
 L' architecture technologique  
 L' organisation informatique à mettre en place

#### **Le plan informatique présente :**

Les projets de : développements des applications, acquisitions et installation des logiciels de base et des équipements informatiques  
 Le scénario de mise en œuvre des projets informatiques, ainsi que les priorités, les plans d' action et de suivi,  
 L' estimation des coûts  
 La procédure de suivi de l' exécution du schéma directeur.

#### **Le plan de sécurité**

Il formalise la politique de sécurité de l' entreprise, qui doit :

d' une part assurer la reprise du service dans des délais acceptables, donc très courts et donc prévoir des procédures dégradées temporaires et au moins un minimum vital, quelles que soient les circonstances  
 d' autre part, rendre absolument impossible une défaillance permanente et donc prévoir un plan de survie.

Le plan de sécurité présente les risques probables. Ces risques sont :

Accidents  
 Pannes  
 Fraudes et sabotages  
 Destruction  
 Erreurs de conception et de réalisation  
 Erreurs de saisie ou de transmission  
 Etc. ....

**Le plan qualité comprend :**

Les buts ainsi que leur applicabilité  
 Leurs exigences et l'organisation  
 Les méthodes, procédures et contrôles  
 Les règles, normes, standard et conventions  
 Les outils  
 Les démarches de développement et de test  
 Les engagements envers l'utilisateur

## 2-2 OBJECTIFS DE L'AUDIT

**L'audit de la politique et des stratégie a pour objectifs de :**

- S'assurer que la politique d'informatisation, et d'une manière plus générale de mise en place des systèmes d'information, est :
  - clairement définie et formalisée,
  - en adéquation avec le but de l'entreprise, son métier, ses enjeux et ses stratégies de développement.
- S'assurer par ailleurs que :
  - les décideurs et futurs utilisateurs des systèmes ont participé à leur définition et sont solidaires aux actions envisagées,
  - les systèmes définis (application, architecture matériel , etc. ..) sont susceptibles de satisfaire aux besoins à court et moyen terme de l'entreprise et sont en adéquation avec les possibilités offertes par la technologie du moment,

la mise en œuvre des systèmes est correctement planifiée et que les projets et plans d'action élaborés sont cohérents, et maîtrisables.

- Proposer les mesures correctives nécessaires.

## 2-3 TRAVAUX D'AUDIT

Il s'agit d'apprécier, par discussion avec les concernés :

- la formation et l'information des dirigeants en gestion de l'informatique : conception et appréciations sur ce que l'automation peut, et inversement ce qu'elle ne peut pas, apporter dans leurs prises de décision et leur contrôle de gestion ; idées précises de conception, de développement, de contrôle, d'installation et d'exploitation des systèmes.  
A chacun des buts doivent être attachés les avantages escomptés et les conditions de réalisation, ainsi que les contraintes techniques et organisationnelles, et enfin la reconnaissance des inconvénients ;
- l'intérêt apporté à l'informatique et la profondeur de l'étude des opportunités techniques, humaines et économiques, l'implication dans le choix des moyens (type de matériels ,organisation, budgétisation) et des actions (informations reçues ; critères d'appréciation d'un service, de sa productivité et rentabilité ; participation à l'élaboration de la politique, buts et plans ; acceptation des remises en cause de l'existant) ;

L'auditeur procédera ainsi à l'analyse du métier ,de l'environnement, de l'organisation et des flux d'informations de l'entreprise.

Il examinera, par référence à la politique générale, idéalement présentée par un document écrit, si le système sert pertinemment des objectifs précis, bien définis et discutés avec tous les responsables, dans une conception globale et homogène qui n'oublie pas l'existant et a obtenu un consensus.

Il devra aussi examiner l'historique de l'informatique : incidences sur l'organisation, existence et validité des prévisions (de structure juridique, de marché, de politique de produits et bien entendu de l'informatique), pratiques réelles de la direction, difficultés mal résolues, les réticences, voire les rancœurs (qui sont ainsi mises en pleine lumière, même si elles paraissent dissipées). L'aptitude à résoudre les problèmes, à surmonter les difficultés, ne peut être visible que dans une perspective historique.

Il examinera, auprès des techniciens de l'informatique et des utilisateurs si les finalités sont bien communiquées à tous les intéressés et qu'elles ont été comprises, avec des objectifs clairs, des problèmes bien posés, une circulation bien définie des informations, une bonne répartition des tâches et responsabilités.

Il procédera enfin, à l'analyse critique du schéma directeur, des plans informatiques, de sécurité et de qualité, s'ils ont été établis. Il examinera, en particulier, leur adéquation avec les conclusions de ses travaux préliminaires décrits ci-avant.

### **3 – AUDIT DE L'ORGANISATION GENERALE ET DES RESSOURCES HUMAINES INFORMATIQUES**

#### **3-1 DEFINITION**

Le succès de la mise en place du système informatique défini et particulièrement la qualité des applications informatiques installées, dépendent dans une large mesure, de l'efficacité de l'organisation de la gestion de l'informatique.

#### **LES PRINCIPAUX OBJECTIFS DE LA GESTION DE L'INFORMATIQUE SONT LES SUIVANTS :**

- fournir un mécanisme efficace pour traiter tous les besoins informatiques de l'entreprise et les opportunités d'utilisation de l'outil informatique, en tenant compte de ses objectifs généraux et des contraintes ;
- fournir un mécanisme efficace pour planifier, contrôler et coordonner l'investissement et l'exploitation de l'informatique en favorisant la participation de la Direction Générale dans le processus de prise de décision dans le Domaine informatique.

#### **LES PRINCIPALES COMPOSANTES USUELLES DE LA STRUCTURE DE GESTION DE L'INFORMATIQUE SONT LES SUIVANTES :**

- Comité Directeur Informatique ;
- Comité des Projets ;
- Commission Utilisateurs ;
- Département Informatique ;

## **COMITE DIRECTEUR INFORMATIQUE (CDI)**

Ses rôles et ses responsabilités sont les suivants :

- établir, revoir et mettre à jour le Schéma Directeur Informatique,
- allouer les priorités pour les systèmes stratégiques,
- approuver et contrôler l'allocation des ressources pour la réalisation des systèmes stratégiques,
- autoriser et suivre les investissements informatiques principaux,
- approuver les plans annuels du Département Informatique.

## **COMITE DE PROJET (CP)**

Chaque CP contrôlera l'exécution d'un projet stratégique ; ses rôles et ses responsabilités sont les suivants :

- contrôler l'exécution du projet stratégique,
- faire en sorte que le projet soit achevé dans le temps et le budget impartis, contrôle de qualité,
- s'assurer d'une bonne documentation de la gestion du projet,
- autoriser les modifications sur le budget et les délais de développement.

## **COMMISSION UTILISATEURS (CU)**

Les CU présentes dans chacune des Directions de l'entreprise ont pour tâche principale de synthétiser les besoins de la Direction en terme de systèmes informatiques et d'évaluer les avantages liés à chaque système demandé.

Dans le cas où plusieurs systèmes sont demandés, les CU devront assigner à chacun des systèmes une note d'importance et une priorité.

Tous ces éléments seront pris en compte pour la mise à jour du Plan Directeur Informatique.



## **DEPARTEMENT INFORMATIQUE**

*Il a la responsabilité de la gestion courante de l'informatique. Il se compose généralement des structures suivantes :*

- responsable du département,
- service méthodes, études et maintenance,
- service exploitation des applications,
- service support technique (systèmes, réseaux et bases de données, maintenance matériels).

*Ses rôles sont les suivants :*

- centraliser toute activité informatique,
- mettre en œuvre le plan informatique,
- planifier et organiser l'activité informatique,
- gérer tous les projets informatiques,
- définir l'architecture technique de chaque site en application du schéma directeur,
- superviser et réaliser les aménagements des salles informatiques,
- superviser l'approvisionnement en matériels et consommables informatiques,
- gérer la politique de maintenance du matériel,
- définir des règles et politique de gestion du matériel et des consommables,
- gérer la formation du personnel informatique,
- organiser et suivre l'exploitation des applications informatiques,
- superviser et réaliser le support informatique et Bureautique,
- coordonner l'activité informatique.

### 3-2 OBJECTIFS DE L'AUDIT

L'audit de l'organisation générale et des ressources humaines informatiques a pour objectifs de :

- Vérifier que l'organisation générale de l'informatique mise en place ;

Permet : de garantir le succès de la mise en œuvre des futurs systèmes définis, d'assurer la fiabilité et la pérennité des logiciels installés, respecte les règles usuelles du contrôle interne, notamment en matière de séparation des tâches, permet de garantir le respect des orientations définies par la Direction.

- S'assurer aussi, que :

l'entreprise dispose des ressources humaines informatiques adéquates, les coûts de l'informatique sont correctement suivis et maîtrisés.

- Proposer les mesures correctives nécessaires.

### 3-3 TRAVAUX D'AUDIT

#### **REVUE ET EVALUATION DE L'ORGANISATION GENERALE DE LA FONCTION INFORMATIQUE**

##### **1. Les différents organes de gestion de l'informatique sont-elles mises en place et sont-elles opérationnelles ?**

définition et formalisation des missions,  
composition,  
fonctionnement effectif.

##### **2. Positionnement hiérarchique du département informatique ?**

##### **3. Existe-t-il un organigramme écrit du département informatique ?**

Si l'organigramme écrit peut paraître superflu, voire contraignant dans les petites structures, il s'impose dès lors que l'effectif dépasse une dizaine de personnes.

L'auditeur vérifiera bien entendu que l'organigramme qui lui est fourni est à jour, et qu'il couvre l'ensemble des fonctions nécessaires à la bonne marche du service.

Par ailleurs, il s'assurera de l'existence de fiches fonctions, en particulier pour les postes : responsables des méthodes, administrateurs des données, responsable de l'exploitation, etc....

#### **4. La séparation des fonctions est-elle en conformité avec les règles usuelles du contrôle interne ?**

Les principes d'un bon contrôle interne conduisent à ce que soient séparés les fonctions :

- des utilisateurs,
- du personnel de conception et de réalisation des applications (études, développement, maintenance des applications),
- du personnel d'exploitation (mise en exploitation des logiciels produits par le personnel de développement, sauvegardes des données, etc..) et d'administration des données.

#### **5. Les relations entre le département informatique et les services utilisateurs sont-elles satisfaisantes ?**

- qualité du service fourni (disponibilité des ressources matérielles, temps de réponse moyen des transactions, fréquence des incidents par application, délai de réactivité pour satisfaire aux demandes des utilisateurs, etc. ...)

- interface entre le département informatique et les services utilisateurs (existence de la fonction de correspondant informatique)

- prise en considération dans la conception des nouvelles applications des problèmes liés à l'organisation des services utilisateurs et à l'aménagement des procédures administratives.

#### **6. Comment sont choisis les fournisseurs ?**

## REVUE DE LA PLANIFICATION ET DU CONTRÔLE DES ACTIVITES INFORMATIQUES

### 1. La politique, les stratégies et les plans de mise en œuvre des systèmes informatiques sont-ils

définis et formalisés ?  
 suivis ?  
 régulièrement mis à jour ?

### 2. Des organes usuels responsables des principaux choix stratégiques et de suivi de la mise en œuvre des systèmes informatiques sont-ils en place et sont-ils opérationnels ?

### 3. Les activités courantes de l'informatique sont-elles relevées, suivies, contrôlées ?

planification des projets de développement, relevé et suivi des temps d'intervention.  
 rapports d'activités  
 etc..

## SUIVI DES COUTS DE L'INFORMATIQUES

### 1. Examen du budget informatique :

existe – t – il ? comment est-il défini ?  
 contenu du budget,  
 suivi des réalisations et analyse des écarts,  
 justification, approbation des dépassements budgétaires,  
 existence de fonction de contrôle de gestion relatif aux coûts informatiques.

### 2. Les coûts des opérations internes informatiques sont-ils évalués ? refacturés aux services utilisateurs ?

### 3. Examen du mode de financement de l'acquisition des ressources informatiques :

critères du choix du mode de financement (achat, location, crédit-bail),

adéquation avec les conditions du marché du moment, les possibilités financières de l'entreprise, et la durée prévisible d'utilisation du matériel.

## **EVALUATION DES RESSOURCES HUMAINES ET EXAMEN DE L'ENVIRONNEMENT SOCIAL**

**1. Politique de recrutement, de rémunération, de formation continue et de promotion du personnel.**

**2. Adéquation de la qualification du personnel avec les fonctions exercées.**

**3. Motivation du personnel par :**

une rémunération satisfaisante ?

la promotion interne ? la formation continue ?

la participation aux prises de décisions ? les projets réalisés ?

l'image de marque de l'entreprise ?

Etc.

**4. Comment se présente l'environnement social ?**

taux de rotation du personnel informatique,

nombre de licenciements et conditions de licenciements,

mouvements sociaux (grèves, etc. ...).

## **4 – AUDIT DES ETUDES**

### **4-1 DEFINITIONS**

Les études font partie des activités courantes du département informatique. Elles comprennent le développement (conception, réalisation) et la maintenance (mise à jour) des logiciels.

Une bonne organisation d'ensemble de cette activité, l'existence de procédures et de méthodes satisfaisantes constituent une première présomption de la fiabilité et de la pérennité des logiciels développés.

A titre d'exemple, la non-existence de normes de programmation laisse à chaque programmeur la liberté de choix de sa méthode, d'où à terme, une grande difficulté de maintenance des applications et par voie de conséquence, une dégradation progressive de la fiabilité de celles-ci.

### **4-2 OBJECTIFS DE L'AUDIT**

**L'audit des études a pour objectifs de :**

- S'assurer que l'organisation des activités d'études, les méthodes de conception, de développement et de maintenance des applications informatiques, permettent la réalisation de logiciels informatiques performants :

conformes aux besoins de l'entreprise,  
capables d'évaluer facilement,  
intégrés

- S'assurer aussi que :

la documentation produite (documentation technique, manuels utilisateurs) est exhaustive, claire et accessible à des non informaticiens (en ce qui concerne les manuels utilisateurs) et qu'elle répond aux besoins des utilisateurs,

les projets d'études sont correctement évalués, suivis et les coûts afférents évalués.

- Proposer les mesures correctives nécessaires.

#### 4-3 TRAVAUX D'AUDIT

### **REVUE CRITIQUE DE LA METHODOLOGIE DE DEVELOPPEMENT DES APPLICATIONS**

#### **1. Une étude d'opportunité est-elle réalisée préalablement au lancement de la conception d'une nouvelle application ?**

L'étude d'opportunité devra inclure notamment :

la présentation succincte des fonctions à développer,  
 les principales contraintes de mise en œuvre,  
 si nécessaire, une présentation des différentes solutions techniques entre lesquelles il conviendra d'arbitrer,  
 une estimation des volumes à traiter,  
 une estimation des coûts prévisionnels et, le cas échéant, des gains financiers attendus,  
 un échéancier prévisionnel de mise en œuvre.

#### **2. Avant tout développement de logiciels ou toute acquisition de progiciel, les avantages et inconvénients respectifs de l'acquisition du progiciel et de la réalisation du système spécifique sont-ils analysés ?**

#### **3. Est-il rédigé un cahier des charges préalablement au lancement de la réalisation de nouveaux logiciels.**

Si le nombre et le contenu exact des différentes phases d'un projet peut varier en fonction de la taille de l'entreprise et de l'importance des projets, il existe un point de passage obligé dans tout projet : l'accord entre les informaticiens et les utilisateurs sur le contenu de l'application à développer. Cet accord sera impérativement formalisé par un document écrit, que nous appellerons ici cahier des charges, et qui comprendra, en fait, l'ensemble des spécifications fonctionnelles du futur système d'information.

En son absence, il est quasiment certain que les logiciels développés ne correspondront pas aux besoins des utilisateurs. L'économie de quelques jours passés à la rédaction, certes fastidieuse, d'un document de synthèse, apparaîtra alors bien dérisoire au regard des surcoûts et des dépassements de délais qui découleront de cette incompréhension.

Sans que la liste en soit exhaustive, on peut citer au titre des principales spécifications contenues dans le cahier des charges :

- la description des fonctions à développer,
- la description des grilles de saisie et de consultation,
- les traitements à réaliser,
- la liste et le contenu des principaux états édités,
- la liste et contenu des fichiers constitutifs de l'application (à l'exception des fichiers de travail),
- l'estimation des volumes à traiter.

On y trouvera également, selon les cas, les modalités et l'échéancier de mise en œuvre et de démarrage de l'application.

#### **4. Existe-t-il des normes en matière de développement d'applications ?**

Il est bien évidemment indispensable que soit adoptée une méthode en matière de développement d'application. La question de savoir si une méthode reconnue sur le marché est préférable à des normes de "maison" est en revanche plus délicate.

Dans un environnement de grandes entreprises ou d'administrations, le choix d'une méthode largement répandue s'impose incontestablement. Des méthodes comme MERISE, le standard de fait, ou AXIAL (proposé par IBM), présentent l'avantage, par leur diffusion, d'être connues de bons nombre d'informaticiens, et donc de pouvoir être aisément imposées au sein de l'entreprise. Elles présentent en outre l'avantage d'une grande rigueur, nécessaire au développement de projets très importants (très concrètement, nous considérerons comme importants des projets dont le coût global atteint plusieurs centaines de millions de Francs CFA).

Dans des petites ou moyennes entreprise ou bien pour des projets de moindre envergure, les méthodes évoquées ci-dessus présentent généralement l'inconvénient d'une trop grande lourdeur. Il n'est dès lors pas rare de rencontrer dans des entreprises des méthodes "maison". On imposera alors



dans le développement d'un projet le respect de certaines étapes, et la formalisation de documents dont le contenu-type sera prédéfini.

Seront par exemple imposés :

l'étude préalable,  
le cahier des charges,  
l'analyse technique,  
les normes de programmation.

## **5. Existe-t-il des normes en matière de programmation ?**

L'existence de normes de programmation est en principe de nature à améliorer la qualité des logiciels produits, dans la mesure où elles constituent un véritable guide, particulièrement utile pour les programmeurs débutants. Elles conduisent en outre à une meilleure homogénéité de l'ensemble des logiciels de l'entreprise.

Plus précisément nous distinguons :

- **Les normes concernant la structure générale des programmes :**

la programmation structurée ou Warnier

certains langages de développement (langages de quatrième génération, générateurs de programmes) imposent de facto une structure de programmation.

- **Les normes concernant le contenu détaillé des programmes**  
**Citons par exemple :**

les noms de fichiers.  
les noms de zones dans les fichiers,  
les noms des étiquettes dans les programmes,  
etc.

- **Les normes d'ergonomie :**

format des écrans (couleur, caractères, boutons, liste, etc..)  
touches fonctions  
messages

## 6. Des outils de type ~ atelier de génie logiciel dont –ils utilisés ?

Le terme d'~atelier de génie logiciel (AGL) et aujourd'hui utilisé pour désigner des fonctions très diverses dans le développement d'applications. Ses fonctions , couvraient principalement à l'origine la gestion des bibliothèques de logiciels d'études et d'explication et l'automatisation du processus de mise en exploitation.

Ses possibilités sont aujourd'hui beaucoup plus vaste puisqu'elles incluent souvent, outre les fonctions évoquées ci-dessus, l'assistance à la conception des logiciels, la gestion automatisée des spécifications et de la documentation, la génération des logiciels à partir des spécifications, etc. L'auditeur devra, après avoir recensé les méthodes et outils de production d'application, se prononcer sur leurs effets en terme de sécurité et d'efficacité du processus.

## 7. Les principales phases de mise en œuvre d'un projet sont-elles prévues dans le processus de développement des nouvelles applications ?

Sauf exception, certaines phases doivent impérativement être prévues dans le processus de mise en place des nouvelles applications. Les principales d'entre elles sont rappelées ci-après.

- **La formation des utilisateurs**

Une mauvaise formation des utilisateurs aura pour conséquence, soit une utilisation anarchique du système, avec tous les risques que cela implique, soit un désintérêt, voire un rejet, vis-à-vis de celui-ci. Dans les deux cas, l'application est vouée à une phase de démarrage pour le moins agitée.

- **La documentation de l'application**

Une documentation doit comprendre, outre l'analyse :

- les listes de programmes ;
- les dessins d'enregistrements ;
- les schémas de bases de données ;
- les références croisées modules et informations ;
- les références croisées contrôles et informations ;
- les dessins des écrans et états ;
- la documentation utilisateur.

- **La reprise des fichiers**

Le démarrage d'une application nécessite quasiment toujours soit la constitution et la saisie ex-nihilo des fichiers nécessaires à celle-ci, soit ,cas de loin le plus fréquent aujourd'hui (les nouveaux logiciels succédant plus souvent à une ancienne application qu'à un processus manuel), la reprise dans le nouveau système des fichiers issus de l'ancien.

- **L'impact du nouveau système sur l'organisation et les procédures administratives.**

Un nouveau système informatique s'accompagne, dans la grande majorité des cas, d'une réflexion sur l'organisation du travail ainsi que la mise en place des nouvelles procédures.

- **L'implantation physique des matériels**

La réflexion en la matière permet de prévoir notamment :

l'implantation de la ou des unités centrales( dans un système fortement décentralisé, on trouvera une unité centrale par site),

le nombre et la localisation géographique des terminaux, écrans et imprimantes.

- **La validation des logiciels**

Deux méthodes complémentaires conduisent à la validation des logiciels( on parle souvent de « recette ») avant leur mise en exploitation :

les jeux d'essai, qui permettent de simuler des cas réels : après des jeux d'essai conçus et réalisés par les informaticiens, qui permettront de s'assurer que les logiciels sont conformes au cahier des charges, il est indispensable de prévoir des jeux d'essai utilisateurs, qui valideront l'adéquation de l'application aux besoins, et seront en définitive l'ultime contrôle avant le démarrage ;

l'exploitation en double, qui consiste à faire tourner simultanément le nouveau et l'ancien logiciel, afin de comparer les résultats.

- **La sécurité**

Si la sécurité du système d'information est primordiale en phase d'exploitation, une première approche dans certains domaines est souhaitable dès la conception.

Citons par exemple, les réflexions sur :

le moyen de contrôle de la validité des traitements : contrôles d'exploitation, contrôles d'intégrité des bases de données, etc.

le respect par l'application de certains principes de contrôles interne : contrôle hiérarchique, séparation des fonctions, continuité du chemin de révision, etc.

les procédures d'exploitation : reprise en cas d'incident, sauvegardes, site de secours, etc.

## **8. Est-il procédé régulièrement à un suivi de l'avancement et des coûts des projets ?**

Ce suivi a pour objet le contrôle de l'avancement de chacune des tâches élémentaires composant les projets, afin de détecter le plus rapidement possible les risques de dérapage, à la fois en termes de planning et en termes de coûts.

De nombreux progiciels de suivi de projet sont aujourd'hui disponibles, sur grands systèmes ou, plus fréquemment, sur micro-ordinateur. En tout état de cause, un simple tableur peut parfois suffire à un suivi efficace.

Quel que soit l'outil utilisé, l'auditeur s'attachera à vérifier que le responsable du projet dispose des moyens d'anticiper à temps tout dérapage, afin de prendre les mesures nécessaires.

## **9. Les projets font-ils l'objet d'une coordination suffisante ?**

D'une manière générale, le charisme du ou des responsables du projet sont un facteur primordial de la réussite de celui-ci. Pour les projets les plus lourds, la coordination du projet doit être formalisée au travers de réunions périodiques (par exemple hebdomadaires) des principaux responsables.

Nous distinguerons, en fait, pour chaque projet dont l'envergure le justifie :

- la coordination entre les équipes de conception, puis entre les équipes de réalisation,
- la coordination entre les équipes de mise en œuvre,
- la coordination entre les informaticiens et les utilisateurs.

## **EVALUATION DE LA QUALITE DES LOGICIELS PRODUITS**

### **1. Est-il procédé régulièrement à des contrôles de qualité des logiciels produits ?**

Un contrôle par sondage des logiciels produits, qu'il soit réalisé en interne (un membre de l'équipe de développement ou du service informatique étant affecté, à temps partiel, à des tâches de contrôles) ou par des interventions extérieures, permet notamment :

- de contrôler la qualité des logiciels produits,
- de s'assurer de l'homogénéité de ces logiciels.

### **2. Les nouveaux collaborateurs font-ils l'objet d'une attention particulière ?**

Cette attention particulière se traduira de différentes manières :

- **Une formation théorique et pratique**

La formation théorique sera utilement complétée par une formation plus pratique, sous des formes diverses : □ parrainage des nouvelles recrues, passage dans différentes équipes, etc.

- **Un contrôle d'activité renforcé**

Une expérience insuffisante du programmeur est souvent à l'origine de programmes lourds et consommateurs de temps machine. Malheureusement, en l'absence d'un suivi efficace, on ne s'apercevra de ces erreurs de jeunesse que trop tard, une fois que notre programmeur inexpérimenté aura réalisé de nombreux logiciels, qu'il sera impossible de réécrire. Un contrôle

systematique des premiers logiciels écrits par chaque nouveau collaborateur permet de réduire ce risque et de corriger le tir immédiatement.

### **3. La qualité des documents et logiciels produits par les études est-elle satisfaisante ?**

Aussi formalisées soient - elles, les méthodes et normes de développement et de programmation ne peuvent constituer une garantie absolue de la qualité des logiciels, ne serait – ce que parce que l'existence de normes ne garantit pas que celles-ci soient respectées !

L'auditeur aura donc tout intérêt à procéder, par sondage, à un contrôle sur quelques programmes de la qualité et du respect des normes.

## **EXAMEN DE LA DOCUMENTATION**

### **1. La qualité de la documentation produite est-elle satisfaisante ?**

On distingue dans la documentation d'une application informatique :

la documentation d'études, destinée aux équipes de développement et de maintenance,  
la documentation d'exploitation, destinée au personnel de production,  
la documentation destinée aux utilisateurs.

- **La documentation d'études contient notamment :**

la description du contenu des fichiers,  
la description des chaînes de traitements,  
la description détaillée des programmes,  
l'historique des opérations de maintenances.

- **La documentation d'exploitation contient l'ensemble des informations et consignes nécessaires au personnel de production :**

description et organigrammes des chaînes de traitement,  
consignes de préparation,  
description des contrôles de l'exploitation à réaliser lors de chaque traitement,  
consignes de pupitrage.

- **La documentation utilisateurs contient :**

la description générale des applications,  
la description des transactions,  
la description des états édités,  
l'explication des messages d'anomalie.

Outre la qualité et l'exhaustivité de la documentation, l'auditeur s'intéressera à sa souplesse d'utilisation. Ainsi, une documentation gérée sur support magnétique, à l'aide d'un progiciel prévu à cet effet, facilitera grandement les mises à jours et permettra des sauvegardes sur un site extérieur.

D'une manière générale, l'auditeur s'attachera également particulièrement à vérifier que la documentation est à jour. Aussi complète soit-elle, celle-ci devient en effet rapidement inutilisable si les opérations de maintenance ne lui sont pas immédiatement répercutées.

## **EVALUATION DES PROCEDURES DE MAINTENANCE DES APPLICATIONS**

### **Les procédures de maintenance des logiciels sont – elles formalisées ?**

Les demandes de maintenance des logiciels doivent être formalisées et faire l'objet d'une demande écrite de la part des services utilisateurs, visée par le correspondant désigné, et transmise au responsable des études qui, après accord, en assurera le transfert au chef de projet concerné. Les logiciels modifiés sont testés dans l'environnement d'études avant tout transfert en exploitation.

En cas d'urgence, et en particulier si l'opération vise à corriger une anomalie de conception des logiciels, il pourra bien entendu être dérogé à l'exigence d'une demande de maintenance écrite. En tout état de cause, même dans ce cas, le service informatique rédigera une fiche décrivant la modification apportée aux programmes.

Par ailleurs, d'une manière générale, l'ensemble des fiches de maintenance relatives à une application sont archivées dans le dossier de celle-ci.

## **5 - AUDIT DE L'EXPLOITATION**

### **5-1 DEFINITION**

Comme les études, l'exploitation fait partie des activités courantes du département informatique. D'une manière générale elle recouvre toutes les tâches relatives à l'utilisation des applications informatiques et des ressources matériel en service.

Elle comprend, ainsi donc :

- la mise en exploitation des logiciels produits,
- la gestion et l'administration des données opérationnelles de l'entreprise,
- l'exécution des traitements en temps différé,
- la gestion de l'environnement et des matériels d'exploitation (production informatique)
- la gestion des bibliothèques de programmes.

Elle aussi assurer :

- la continuité de l'exploitation en cas d'incident (reprise sur site extérieur),
- la sécurité des données et des dispositifs matériels,
- la gestion de la maintenance des équipements informatiques.

Toutefois , dans les entreprises , étant donné leur complexité et leur charge de travail de plus en plus importantes, les fonctions suivantes sont de plus en plus exclues de l'exploitation :

- administration des données(en fait administration des bases de données)
- gestion des réseaux
- gestion de la sécurité
- gestion de la maintenance des équipements.



## 5-2 OBJECTIFS DE L'AUDIT

L'audit de l'exploitation à pour objectifs de :

- **Apprécier la qualité de la production informatique et de l'appui apporté aux utilisateurs dans leurs travaux informatiques courants :**

disponibilité des moyens informatiques, des traitements et des données (déploiement des moyens informatiques),  
exécution adéquate des traitements,  
formation des utilisateurs à l'exploitation des applications,  
assistance aux utilisateurs en cas d'incident,  
Utilisation efficiente de la Bureautique,  
Etc.

- **Vérifier que les procédures d'exploitation mises en place permettent :**

de garantir la sécurité et l'intégrité des données,  
d'assurer la continuité de l'exploitation( sauvegarde des données,  
restauration et reprise en cas d'incident)

- **Apprécier la qualité de la gestion des moyens techniques**

Acquisition et installation des équipements  
Aménagement physique des locaux  
Maintenance préventive et curative du matériel  
Support technique système et réseaux

## 5-3 TRAVAUX D'AUDIT

### EXAMEN DES PROCEDURES DE MISE EN EXPLOITATION

**Les procédures de mise en exploitation des logiciels sont-elles satisfaisantes ?**

Les principaux objectifs d'un bon contrôle interne dans ce domaine, sont les suivants :

- **La procédure de mise en exploitation doit garantir une bonne séparation entre les fonctions d'étude et les fonctions d'exploitation.**

Concrètement, le personnel d'étude ne doit pas avoir accès aux bibliothèques de programmes d'exploitation, pas plus qu'aux fichiers d'exploitation. Cet objectif vise d'ailleurs beaucoup plus à prévenir les risques d'erreurs de manipulation que les risques d'opérations frauduleuses de la part du personnel d'études.

- **La procédure d'exploitation doit à tout moment garantir que l'on dispose dans les bibliothèques des programmes sources correspondants aux programmes objets en exploitation.**

Le programme □ source est le programme écrit par l'informaticien dans un langage évolué, compréhensible par l'homme ; le programme □ objet est le langage compilé, c'est à dire transformé en code binaire directement exécutable par la machine. Le langage objet étant quasiment illisible par l'homme.

Sont conservés en machine :

d'une part le programme source, dans une bibliothèque de programmes sources, qui sera modifié, puis recompilé, en cas de maintenance de l'application,

d'autre part le programme objet prêt à être exécuté, dans une bibliothèque des programmes objets ; en réalité, et plus précisément, certains programmes objets doivent être assemblés les uns aux autres avant exécution : il s'agit de la phase d'édition de liens (linkedit) qui transforme les modules objets en modules exécutables (load-modules).

En l'absence des programmes sources, ou bien en présence de programmes sources non cohérents avec les programmes objets exécutés, la maintenance de l'application sera à très court terme impossible.

- **La procédure de mise en exploitation doit permettre de conserver l'historique des transferts de logiciels dans l'environnement d'exploitation.**

Cet historique permettra notamment :

d'élaborer des statistiques : mises en exploitation par programme, nombre de maintenances par programme et par application, etc.,

d'effectuer ,si nécessaire, des recherches ,en cas d'incident, sur la date des dernières modifications d'un logiciel.

## **EXAMEN DES PROCEDURES DE SAISIE DES DONNEES**

Rappelons tout d'abord que la saisie des données peut être réalisée :

- **en temps différé**, sur des matériels dédiés à la saisie, à partir de bordereaux remplis par les services utilisateurs ; la saisie, dite « de masse » est alors assurée par des « perforatrices - vérificatrices » dans des « ateliers de saisie » spécialisés dans cette fonction ; les ateliers de saisie sont aujourd'hui en voie de disparition, mais se trouvent encore justifiés dans certains cas particuliers.
- **en temps réel**, c'est à dire avec une mise à jour immédiate des fichiers ; la saisie est alors assurée , soit directement par les utilisateurs , soit par des services assurant une saisie de masse « intelligente » Ainsi en matière commerciale, les commandes seront saisies , selon les cas, par les vendeurs eux-mêmes , par leur secrétariat ( par exemple chaque jour après centralisation des commandes de la journée) ou encore par un service d'administration des ventes ; de la même manière ,dans un établissement financier, les opérations seront saisies, soit par les opérateurs eux-mêmes ,soit par un service de saisie et contrôle, au sein d'un « middle office » ou d'un « front office ».

## Les principes d'un bon contrôle interne sont-ils respectés dans les logiciels de saisie des données ?

Les principaux éléments d'un bon contrôle interne des procédures de saisie des données sont :

- lorsque la saisie est réalisée à partir d'un bordereau, l'existence sur le bordereau du visa d'une personne autorisée, contrôlé par le personnel de saisie ;
- la double saisie (uniquement dans le cas de saisie de masse en temps différé) ;
- l'existence de clés de contrôle pour les codes numériques, les erreurs de saisie du code étant alors immédiatement rejetées ;
- le contrôle par totalisation des lots de saisie, qui vérifie que tout document a été saisi une fois et une seule fois, avec des montants exacts ;
- le contrôle d'existence en table ou en fichier des codes saisis ;
- les contrôles de cohérence (exemple : contrôle de cohérence du jour, du mois et de l'année dans la saisie d'une date) ; dans certains cas la saisie de donnée redondantes sera volontairement prévue à la fin de contrôle (exemple : saisie dans une facture du montant Hors Taxe (A) , de la TVA (B) et du montant TTC (C) : le programme de saisie vérifie que  $C=A+B$ ) ;
- l'affichage pour validation dès la saisie de libellé correspondant (uniquement en cas de saisie interactive) au code saisi : exemple : au moment de la saisie d'une facture fournisseur, le nom fournisseur est affiché à partir du code fournisseur saisi ;
- l'édition pour analyse de la liste exhaustive des données saisies et, le cas échéant d'une liste par exception des données les plus sensibles d

D'une manière générale l'auditeur vérifiera que les procédures de saisie garantissent que :

- toute donnée devant être saisie l'a bien été (principe d'exhaustivité),
- n'ont pas été saisies des données qui n'auraient pas dû l'être( principe de réalité) ;

- des données saisies ne comportent pas d'erreurs (principe d'exactitude)

## **EVALUATION DES PROCEDURES ET CHAINES DE TRAITEMENTS EN TEMPS DIFFERE**

### **1. L'exécution des travaux en temps différé fait -t- il l'objet d'une planification ?**

La planification de l'exécution des traitements est un principe de base d'une organisation rationnelle. A défaut, l'ordinateur pourrait se trouver saturé à certaines périodes ( d'où des retards dans la distributions des résultats ), et inactif à d'autres.

Par ailleurs, une planification systématique permet de s'assurer aisément que seuls les traitements planifiés et autorisés ont été exécutés.

Des progiciels d'assistance à la planification et à l'ordonnancement des travaux sont aujourd'hui disponibles sur le marché (principalement, pour les plus complets, sur les grands systèmes) ,grâce auxquels :

- tout traitement exécuté sans planification est soit rejeté, soit, au moins, mis en évidence pour contrôle,
- les contraintes d'enchaînements des travaux sont mises en paramètres, évitant ainsi certaines erreurs liées à des lancements manuels (travail oublié, ou au contraire exécuté en double, travaux exécutés dans une mauvaise séquence..).

Notamment ces progiciels permettent aux préparateurs (ou plus généralement aux responsables d'application) de paramétrer dans la journée l'exécution de travaux qui s'exécutent de nuit, sous le seul contrôle des pupitreurs.

### **2. La fonction de préparation des travaux est-elle assumée de manière satisfaisante ?**

Citons, au titre des principales caractéristiques d'une organisation satisfaisante de la fonction de préparation des travaux :

- **La qualité de la documentation destinée aux responsables de la préparation** : la qualité de la documentation est, bien entendu, la

condition sine qua non de la qualité du travail de préparation par les responsables d'applications ;

- **L'interchangeabilité des responsables d'application** : s'il n'est pas souhaitable que chaque responsable d'application assume tour à tour la responsabilité de la préparation de l'ensemble des chaînes de traitement (ce qui conduira à une trop grande dispersion), il est du moins nécessaire que plusieurs responsables soient capables d'assurer la préparation de chaque chaîne, de manière à ce que les congés, la maladie ou le départ de l'un d'eux ne deviennent pas la source de tous les dangers ;
- **La qualité des JCL** : des JCL d'exploitation performants réduisent fortement les risques d'erreurs d'exploitation en limitant au strict minimum le nombre de paramètres à modifier lors de chaque exploitation.

Les JCL sont généralement modifiés par les responsables d'application au moment de la mise en exploitation d'une nouvelle chaîne de traitement, dans un souci d'optimiser les performances d'exploitation, que n'ont pas toujours les équipes de développement.

Par ailleurs, les outils d'automatisation des exploitations (génération automatique des JCL, gestion des reprises, gestion des générations successives d'un même fichier, gestion des sauvegardes..) participent notablement à la réduction du nombre des paramètres d'exploitation.

### 3. Les chaînes de traitements font-elles systématiquement l'objet de contrôles à posteriori ?

On peut distinguer dans les contrôles sur une chaîne de traitement :

les contrôles sur la cohérence technique de l'exploitation,  
les contrôles sur la cohérence fonctionnelle de l'exploitation

- **Les contrôles sur la cohérence technique.**

Ils portent par exemple sur :

sur les nombres d'enregistrements traités,  
sur le contenu des bases de données,

sur le bon fin des traitements (par l'analyse des messages et d'indicateurs de fin de traitement),  
sur la cohérence des états édités.

Bon nombre de ces contrôles peuvent d'ailleurs être fortement informatisés, soit par la création de □ chiffriers d'automatiques, soit par l'utilisation des progiciels existants sur le marché, en particulier pour le contrôle de la bonne fin des traitements .

- **les contrôles sur la cohérence fonctionnelle de l'exploitation**

S'il est souhaitable, dans l'absolu, que ces contrôles soient pris en charge par le service informatique, la pratique tend depuis plusieurs années à transférer la responsabilité aux services destinataires.

La principale raison en réside dans l'impossibilité devant laquelle se trouvent les services informatiques pour définir et réaliser des contrôles fonctionnels pertinents.

Il n'en reste pas moins que ces contrôles de cohérence fonctionnelle revêtent une importance primordiale.

#### **4. Les modalités de reprises de l'exploitation de la chaîne en cas d'incident sont-elles clairement définies ?**

Le souci majeur dans ce domaine doit être d'éviter que les pupitreurs aient à prendre des initiatives quant au traitement des incidents , dans la mesure où ils ne connaissent pas les chaînes en exploitation et où la définition des modalités de reprise n'est donc pas de leur ressort.

Dans les grands centres de traitements, les systèmes d'exploitation permettent généralement la totale automatisation des procédures de reprises consécutives à la plupart des incidents. Lorsqu'une reprise automatique s'avère impossible, il est préférable, sauf urgence d'abandonner le traitement et d'attendre la décision du responsable de la production de l'application (c'est à dire de différer la décision au lendemain matin pour les chaînes de nuit).

Pour les petits systèmes, une totale automatisation des reprises n'est pas envisageable. Il est prévu pour les situations urgentes, en cas d'absence du responsable d'application, de fournir au pupitreur un manuel d'exploitation décrivant précisément la procédure de reprise à appliquer.

## **CONTROLE DU PILOTAGE DE L'ENVIRONNEMENT DE PRODUCTION**

### **1. Existe -t- il des outils de contrôle et d'assistance destinés aux pupitreurs ?**

Si dans les grands centres, les pupitreurs travaillent systématiquement en équipe, il n'est pas toujours de même dans les petits centres. Dans certains cas, des travaux non urgents sont lancés et exécutés la nuit en l'absence de toute présence humaine (à l'exception si possible des gardiens) : en cas d'incident, les travaux seront alors interrompus et relancés le lendemain.

Par ailleurs, il existe de plus en plus, dans les grands centres, des outils de contrôles et d'assistance au travail des pupitreurs : interdiction de transmettre certaines commandes, réponses automatiques à l'ordinateur, etc.

Cette automatisation permet alors de focaliser l'activité des pupitreurs sur les tâches les plus délicates, en particulier le traitement de certains types d'incidents. Corrélativement, elle s'accompagne, toujours dans les grands centres, d'une centralisation des fonctions de pupitrage, avec la création d'équipes ayant la responsabilité simultanée de plusieurs unités centrales.

## **CONTROLE DE LA QUALITE DE LA PRODUCTION INFORMATIQUE**

### **1. Existe - t- il un suivi de la qualité des prestations fournies ?**

Ce suivi revêt des formes variées :

- disponibilité de la machine et du réseau,
- temps de réponse des applications interactives,
- fréquence des incidents par logiciel,
- fréquence des retards dans la distribution des états, et retard moyen constaté,
- nombre d'opérations de maintenance par application,
- etc..



## 2. Existe-t-il un suivi destiné à optimiser les performances du système informatique ?

Ce suivi revêt lui aussi des formes variées :

- taux de charge de l'unité centrale,
- taux de remplissage des disques,
- fréquence des entrées – sorties,
- suivi des temps de traitement par logiciel d'application ,
- suivi de l'utilisation du réseau,
- etc.

## 3. Le journal de bord (ou des ) ordinateurs est-il systématiquement édité et archivé ?

Rappelons que ce journal de bord (printlog) retrace, sous une forme plus ou moins détaillée (paramétrable) , l'historique des commandes soumises au système d'exploitation et des messages reçus de celui-ci.

Chaque message vient ainsi alimenter un fichier, qui pourra être utilisé à des fins de recherche après tout incident d'exploitation.

L'auditeur vérifiera en particulier :

- que la taille du fichier permet de contenir l'historique des messages sur une période suffisamment longue( de un à quelques jours),
- que le journal de bord fait l'objet de sorties – papier , archivées elles aussi sur une période suffisamment longue( quelques mois).

## **CONTROLE DE LA GESTION DE L'ESPACE DISQUE**

### **1. Le contenu des disques est –il régulièrement analysé pour suppression des fichiers inutiles ?**

Il est indispensable que soient mises en place des procédures permettant de traquer les fichiers inutiles. Citons par exemple :

- le recensement périodique avec les chefs de projet et les responsables de production d'application de tous les fichiers opérationnels,
- l'élimination automatique des fichiers dont le nom ne respecte pas une structure prédéfinie.

Des progiciels de gestion automatisée de l'espace disque permettent en particulier de lutter contre cette prolifération de fichiers inutiles.

### **2. L'implantation des fichiers sur les disques fait–elle l'objet d'une optimisation ?**

En effet, une optimisation de l'implantation des fichiers sur le disque permet :

- de diminuer le temps de certains traitements, qu'ils soient interactifs ou en temps différé,
- d'améliorer la sécurité .

## **CONTROLE DE LA GESTION DES BIBLIOTHEQUES DE PROGRAMMES**

S'assurer que les règles suivantes sont respectées :

- ne conserver dans les bibliothèques que les programmes effectivement utilisés,
- avoir la certitude que sont disponibles dans les bibliothèques tous les programmes objets utilisés,
- fournir aux personnels d'études et de production un maximum de procédures automatisées de gestion des bibliothèques (mises en exploitation, rapatriement d'un programme de l'environnement de production vers l'environnement de test...)

- interdire aux personnes non autorisées l'accès aux bibliothèques.

## EVALUATION DE LA GESTION DES SAUVEGARDES

Le support physique de la sauvegarde n'a aucune incidence particulière sur la politique générale. Les questions ci-après s'appliquent donc indifféremment à des sauvegardes sur bandes et à des sauvegardes sur cartouches.

Si l'objectif final des sauvegardes est aisément compréhensible, les modalités pratiques en sont souvent fort différentes d'un site à l'autre, ne serait-ce que parce que celles-ci sont tributaires de la taille du centre, des volumes d'informations à sauvegarder et des systèmes d'exploitation proposés par le constructeur.

Quelles que soient les procédures appliquées, l'auditeur s'attachera à vérifier qu'elles satisferont aux objectifs fondamentaux d'une bonne politique de sauvegarde, à savoir :

- permettre le redémarrage de chacune des chaînes de traitement en cas d'incident (exemple : redémarrage d'une chaîne interrompue par une panne d'alimentation, ou encore par un incident logiciel) ;
- permettre de pallier un incident sur un support physique (exemple : un incident sur un disque rend celui-ci illisible et impose son remplacement physique, puis le chargement de son contenu à partir d'une sauvegarde) ;
- permettre le redémarrage sur un site extérieur en cas d'indisponibilité ou de destruction totale du site de production ;
- répondre aux obligations légales en matière d'archivage : obligations commerciales, comptables et fiscales.

### **1. L'ensemble des logiciels et fichiers nécessaires au développement et à l'exploitation est-il régulièrement sauvegardé ?**

Doivent impérativement être sauvegardés :

- les logiciels de base,
- les fichiers et logiciels d'application de l'environnement d'exploitation,

- les fichiers et logiciels d'applications de l'environnement d'études.

## 2. Les sauvegardes permettent – elles de traiter dans un délai satisfaisant tous les types d'incident ?

Nous illustrerons cette question par différents exemples de mauvaises politiques de sauvegarde.

- **Les fichiers et bibliothèques sont sauvegardés totalement une fois par mois, et, dans l'intervalle, toutes les modifications sont historisées.**

Cette politique est mauvaise car, pour les fichiers et bibliothèques fréquemment modifiés, la reconstitution de la situation au moment d'un incident (en particulier si celui-ci survient juste avant une sauvegarde totale) sera excessivement longue.

- **Toutes les sauvegardes sont réalisées par support physique et il n'existe aucune sauvegarde sélective des fichiers**

Dans cette hypothèse, en cas d'incident sur une application donnée, la reconstitution d'un ou plusieurs fichiers sera parfois longue, puisqu'elle nécessite le rechargement préalable d'un disque complet

- **Il n'existe que des sauvegardes sélectives de fichiers et de bibliothèques, et aucune sauvegarde totale par support physique.**

Cette fois, c'est en cas de nécessité de reconstitution d'un support physique (après destruction de celui-ci ou après destruction totale de tout le site) que la charge de travail deviendra considérable.

## 3. Si le parc le justifie, existe – t- il, un logiciel de gestion des bandes (ou des cartouches) ?

La gestion du parc de bandes (ou de cartouches) magnétiques ne pose pas de problème particulier dans les petits centres de traitements :

Les bandes sont peu nombreuses, et sont d'ailleurs souvent référencées et rangées directement par nature de sauvegarde. Un tel mode de gestion est tout à fait impensable dans les grands centres, où les supports doivent alors être numérotés, et rangés en ordre séquentiel. Le gestionnaire de la

bandothèque, généralement à l'aide d'un progiciel, établira la correspondance entre la référence numérique des bandes, leur nature et leur lieu de stockage géographique.

Le progiciel assurera en outre :

- la gestion des lieux de stockage, selon un paramétrage initial (par exemple, pour tout fichier, la version V se trouvera sur le site, et sera transférée sur un site extérieur lorsqu'elle deviendra la version V-1, l'ancienne version V-1 étant elle même banalisée) ;
- la banalisation des bandes supportant des fichiers devenus inutiles ;
- le contrôle d'accès aux bandes contenant des fichiers actifs (et l'interdiction de toute modification sur celles-ci).

L'auditeur pourra notamment vérifier par sondage :

- que toute bande référencée dans le progiciel se trouve bien géographiquement au lieu de stockage prévu (et, le cas échéant, que le nom et la version du fichier contenu sur la bande sont bien ceux qui sont référencés) ;
- que toute bande présente physiquement est bien référencée dans le progiciel.

**4. La gestion des sauvegardes répond-elle aux obligations légales en matière d'archivage ?**

**5. Procède-t-on à des sauvegardes au site extérieur ?**

## **EXAMEN DES PROCEDURES DE REPRISE SUR SITE EXTERIEUR (BACK-UP)**

**1. Est-il prévu une procédure permettant un redémarrage sur un site extérieur, dans un délai satisfaisant ?**

Parmi les principales mesures destinées à préparer un éventuel back-up, on peut citer :

- le contrat de back-up auprès d'une société spécialisée,
- la « salle blanche » , salle vide, pré-équipée pour des télécommunications, et prêt à recevoir des matériels de secours en cas de besoins,
- le contrat d'assistance avec des entreprises disposant d'équipements similaires,
- la mise en commun d'un site de secours entre plusieurs entreprises,
- et enfin solution en plein essor, l'existence dans l'entreprise de deux sites éloignés l'un de l'autre, dont chacun est capable d'assumer le back-up de l'autre, moyennant la mise en œuvre de procédures dégradées.

N'oublions pas enfin que, de nos jours, un plan de reprise sérieux impliquera qu'ait été soigneusement envisagé le back-up du réseau de télécommunications.

## **2. Si la reprise sur un site extérieur implique la mise en œuvre de procédures dégradées, celles-ci ont-elles été définies ?**

Il est bien rare que le site de secours permette de « traiter » les applications dans les mêmes conditions que le site initial. Il est donc indispensable de définir les applications et les utilisateurs prioritaires, c'est à dire les procédures de fonctionnement en mode « dégradé ».

## **3. Les procédures de reprise sur site extérieur sont-elles régulièrement testées ?**

Seul le test « grandeur nature » des reprises décèlera les imperfections de la procédure théorique : mémoire centrale insuffisante, fichiers non sauvegardés utilisateurs non connectés, etc.

## **EVALUATION DE LA SECURITE PHYSIQUE DU CENTRE DE TRAITEMENT**

(voir cours consacré à l'audit de la sécurité.)

### **EXAMEN DES CONTRATS D'ASSURANCE**

L'auditeur vérifiera qu'ont été envisagées les couvertures financières des risques liés :

- à la destruction des matériels,
- à la reconstitution des fichiers perdus,
- aux pertes d'exploitation consécutives à l'indisponibilité des matériels,
- aux pertes financières consécutives à des actes malveillants ou frauduleux.

Les contrats d'assurances contre les risques informatiques peuvent être ventilés en :

- des contrats «tous risques informatiques (TRI) qui recouvrent selon les garanties, tout au partie des dommages liés à des événements accidentels,
- des contrats «extension aux risques informatiques » (ERI) qui couvrent, selon les garanties tout ou partie des dommages liés à une utilisation non autorisée des systèmes informatiques (actes frauduleux ou malveillants),
- des contrats de type « globale informatique » qui cumulent les couvertures liées aux deux types de risques précédents.

### **EXAMEN DES PROCEDURES D'ADMINISTRATION DES BASES DE DONNEES**

#### **1. Existe-t-il « un administrateur des données » ?**

L'Administrateur de données a pour rôle la gestion des données de l'entreprise (dans les PME) et pour les applications importantes, la gestion des données des applications.

Il est le garant de la cohérence et de la non-redondance des données gérées par le SGBD.

On distinguera, au moins dans les grands centres, la notion d'administrateur des données, responsable des données de l'entreprise, de celle d'administrateur de base de données, responsable de l'implantation physique des bases, de leur optimisation et de leur cohérence technique (voir ci-après).

## **2. Un « dictionnaire des données » est –il utilisé ?**

Le dictionnaire des données est un progiciel qui facilite la gestion des données par l'administrateur, et leur utilisation par les équipes de développement.

## **3. Procède-t-on à des travaux de recherche d'optimisation de la base de données ?**

Il existe généralement plusieurs manières de structurer une base de données et de gérer l'accès à celle –ci pour répondre à un même besoin. Selon l'optimisation ou non des méthodes d'accès, les performances d'un même programme peuvent varier dans des proportions tout à fait considérables. L'absence totale d'optimisation conduira dans certains cas à des temps de réponses des applications interactives ou à des temps d'exécution des travaux en temps différé tout à fait inacceptables.

L'optimisation des bases de données constitue donc une tâche essentielle de l'administrateur des données, en relation avec les développeurs.

## **4. L'intégralité des bases et la cohérence des données sont-elles contrôlées régulièrement ?**

Doivent être régulièrement contrôlées :

- la cohérence technique des bases de données,
- la cohérence fonctionnelle des données.

- **Cohérence technique**

La technique des bases de données, quelle que soit leur architecture (hiérarchique, en réseau ou relationnelle) implique la présence de pointeurs et d'index, assurant la relation entre les segments (ou entre les tables), et évitant ainsi la redondance des données.



- **Cohérence fonctionnelle**

S'il est possible de contrôler la cohérence des données lors de leur saisie, ce contrôle n'exclut pas une dégradation ultérieure de celle-ci, pour des raisons diverses (erreur dans un programme en temps différé, modification des données non contrôlées, incident machine...).

Il est donc souhaitable que des contraintes d'intégrité et de cohérence des données puissent être incluses dans la définition de la base elle-même, et que le respect de ces contraintes soit régulièrement contrôlé pour l'ensemble des données de la base.

## **DIAGNOSTIC DE LA GESTION DES RESEAUX**

### **1. Existe-t-il une cellule technique de gestion des réseaux ?**

Dans les environnements « grand système », la mise en œuvre d'un réseau nécessite le choix de logiciels cohérents les uns avec les autres, puis leurs implantation et leur paramétrage.

Le choix des réseaux eux-mêmes nécessite des études techniques et économiques.

Cette fonction est généralement dévolue à une cellule technique, rattachée à l'équipe système.

Outre l'existence même de l'équipe réseau, l'auditeur contrôlera son activité :

- justification technique et économique des choix,
- test des nouvelles configurations,
- back-up entre les ingénieurs systèmes, etc...

### **2. Existe-t-il une cellule d'assistance réseau ?**

Contrairement à la cellule technique précédente, celle-ci a essentiellement un rôle d'assistance aux utilisateurs :

- installation de nouveaux postes de travail,
- première assistance téléphonique en cas de problème,
- maintenance, si celle-ci n'est pas confiée à des sociétés spécialisées,
- gestion de certaines tables.

Il s'agit donc véritablement d'une fonction qui doit être disponible à tout moment pour répondre aux besoins des utilisateurs.

### **3. Les accès aux réseaux sont-ils contrôlés ?**

L'existence d'un réseau implique des risques accrus d'accès non autorisés, pour différentes raisons :

- le nombre de terminaux connectés à l'ordinateur central est en augmentation constante, et ceux-ci peuvent se trouver dans des localisations géographiques très éloignées ;
- si, dans la plupart des applications, la liste des terminaux physiquement autorisés à être connectés au système central est limitativement établie, il est de plus en plus fréquent que pour des raisons de souplesse d'utilisation, des terminaux non identifiés physiquement soient autorisés à accéder au réseau : c'est notamment le cas lorsque des procédures de télémaintenance sont mises en place ;
- la gestion des réseaux combine dans la grande majorité des cas l'utilisation de lignes privées (lignes louées) et de réseaux publics (réseau téléphonique commuté, SYTRANPAC, IRIS), où les données qui circulent sont mélangées à celles d'autres entreprises ;
- enfin certaines applications informatiques sont, par nature, destinées à un accès public : consultation des comptes par la clientèle dans les établissements financiers consultation des stocks et saisie des commandes dans des entreprises industrielles ou commerciales.

### **4. Des techniques de sauvegarde et de reprise propres à l'utilisation d'applications en télétraitement ont-elles été prévues ?**

Les techniques de sauvegarde quotidienne des fichiers (généralement lors des traitements de nuit) trouvent une importante limite dans le cas des applications interactives : les fichiers étant mis à jour en permanence, une sauvegarde à la veille au soir implique, en cas d'incident et de nécessité de reprise à partir de la sauvegarde, que soient ressaisis tous les mouvements de la journée.

Cette contrainte est d'ailleurs acceptable dans certains cas, à condition du moins que les utilisateurs prennent leurs dispositions en conséquence. Dans le cas contraire, des techniques spécifiques doivent être mises en œuvre.

La plus fréquente et la plus ancienne consiste en la journalisation (logging) des transactions : chaque mise à jour de fichiers donne lieu à création de mouvement sur un fichier-journal, régulièrement déchargés sur bande ou cartouche : en cas d'incident la réapplication des mouvements du jour sur la sauvegarde à la veille au soir permettra de reconstituer la situation des fichiers au moment de l'incident.

Plus précisément, le contenu du fichier journal pourra varier d'un environnement à un autre : dans certains cas il contiendra les transactions de mise à jour elles-mêmes, dans d'autre il contiendra l'image des enregistrements du fichier modifié avant et après mise à jour.

Une technique plus récente consiste à créer pour les fichiers mis à jour en temps réel des fichiers « image » sur un disque distinct de celui contenant les fichiers originaux, et mis à jour en même temps que ceux-ci , ainsi en cas d'incident sur le disque contenant le fichier original, il sera possible de poursuivre quasi immédiatement l'application à partir du disque image.

Le principal inconvénient de ces techniques, journalisation et disque « image », qui explique d'ailleurs qu'elles ne soient pas utilisées dans certains sites (essentiellement les PME) réside dans leur coût : la création du fichier journal multiplie les opérations d'entrées-sorties (« I/O ») et requiert donc des configurations matérielles plus importantes. La technique des fichiers « image » est encore plus onéreuse, puisqu'elle nécessite une duplication des volumes disques, qui demeurent des supports magnétiques coûteux.

On notera enfin que la technique de la journalisation pourrait s'étendre dans les prochaines années aux traitements en temps différé : c'est déjà le cas, avec certains SGBD relationnel, tel que DB2 d'IBM, qui permet de journaliser les modifications de la base, issue à la fois des traitements en temps réel et des traitements en temps différé.

## **5. Si les applications le nécessitent, est-il prévu des procédures de « back-up » du réseau ?**

Nous avons essentiellement évoqué ci-avant, les procédures de reprise consécutives à une indisponibilité de l'unité centrale. Mais il existe un autre risque propre aux réseaux : l'indisponibilité d'un support de transmission de données. C'est le cas bien connu, par exemple, de la ligne louée indisponible pendant quelques jours car physiquement endommagée.

Si l'importance des logiciels le justifie, il convient donc de prévoir des procédures de nature à pallier ces défaillances. Citons par exemple :

- le doublement d'une ligne spécialisée par un abonnement à SYTRANPAC, prêt à prendre immédiatement le relais pour le transfert des données,
- le développement de logiciels permettant le traitement en local et en mode dégradé de certaines applications, en cas d'impossibilité totale d'assurer la liaison entre les utilisateurs et le site central,
- l'utilisation de liaisons qui intègrent leurs propres solutions de secours.

## **DIAGNOSTIC DE LA GESTION DE L'INFO CENTRE**

La notion d'infocentre, ou d'infoservice, correspond à la mise à disposition des utilisateurs, de langages de programmation de manipulation aisée, essentiellement destinés à des interrogations des bases de données et permettant de décharger d'autant les équipes de développement du service informatique.

### **1. Les outils d'infocentre sont-ils bien adaptés à l'utilisation par des non-informaticiens ?**

Trop souvent, des langages de programmation rapide totalement inadaptés à une utilisation par des non-informaticiens, car trop complexes, sont abusivement appelés langages d'infocentre.

Au mieux, ils sont oubliés de tous, au pire ils engendreront de nombreux résultats erronés.

Le cas échéant, dans les plus grands centres, plusieurs outils seront mis à disposition des utilisateurs :

- des langages simples destinés à des requêtes élémentaires pour la majorité d'entre eux
- de véritables langages de développement rapide pour les plus avertis.

## **2. L'accès aux outils d'infocentre est-il contrôlé ?**

L'accès aux outils d'infocentre doit être limité aux utilisateurs habilités. De plus, seule la consultation des données est le plus souvent autorisée, non leur mise à jour.

## **3. Les outils d'infocentre ne sont-ils pas détournés de leur objectif d'origine au profit du développement d'applications « pirates » ?**

L'assistance fournie par le service informatique pour l'utilisation de l'infocentre doit être l'occasion de s'assurer que celui-ci n'est pas détourné de sa fonction d'origine.

En effet, s'agissant des micro-ordinateurs, le risque lié à une prolifération non maîtrisée d'applications parallèles développées par les utilisateurs eux-mêmes, existe.

## **4. Les charges-machines imputables à l'infocentre sont-elles surveillées ?**

Les outils d'infocentre sont généralement de grands consommateurs de ressources, qu'il s'agisse d'espaces-disque ou de temps-machine.

Il est donc important que soient réalisés des suivis des consommations par application, par utilisateur, par service, afin de déceler d'éventuels abus.

Notons que ce problème devrait disparaître progressivement au cours des prochaines années, grâce à l'utilisation de nouvelles techniques :

- Machines dédiées à l'infocentre
- Utilisation de micro-ordinateurs, les données étant tout d'abord déchargées du site central vers le micro-ordinateur, puis retraitées sur celui-ci à l'aide d'outils appropriés.

## DIAGNOSTIC DE LA FONCTION SYSTEME

1. Dans les grands centres, a-t-on créé un environnement spécifique pour les ingénieurs-système ?

Les ingénieurs-système ont, dans les grands centres de traitement, des pouvoirs très étendus, de par la connaissance qu'ils ont des logiciels de base.

L'objectif de la création d'un environnement spécifique sera de permettre aux hommes-système de tester en toute sérénité les nouvelles versions des logiciels de base.

2. **S'il a été fait le choix de développer certains logiciels de base en interne, ce choix a-t-il été dûment justifié ?**

Certains grands centres informatiques ont fait le choix, en particulier dans les années soixante-dix et au début des années quatre-vingt, de développer en interne certains logiciels de base : système de gestion de fichier, système d'exploitation, moniteur de télétraitement ... Ces choix, qui entraînent parfois des charges de travail considérables, étaient alors justifiés par la nécessité de traiter des volumes d'information très importants avec des performances que n'offraient pas les logiciels de base disponibles sur le marché.

Malheureusement, la maintenance de ces logiciels, généralement écrits en assembleur, s'est avérée au fil du temps de plus en plus complexe, incitant les responsables de ces centres à revenir à des outils standard, devenus entre-temps plus performants. Mais, là encore, la conversion fut souvent longue et délicate, compte tenu de ses conséquences sur les logiciels applicatifs.

D'une manière générale, l'auditeur s'assurera qu'aucun logiciel de base n'est développé dans l'entreprise sans qu'aient été étudiés les progiciels offrant des fonctions similaires. Aujourd'hui, le développement de logiciels spécifiques importants devrait être tout à fait exceptionnel.

On peut d'ailleurs se demander si les mêmes erreurs que par le passé ne sont pas à nouveau commises, lorsqu'on entend parler de grands groupes qui développent, par exemple, leurs propres logiciels de gestion de réseaux locaux.

## **6 AUDIT DES MOYENS TECHNIQUES**

### **6-1 DEFINITION**

Des moyens techniques comprennent les matériels, les locaux, les réseaux et les logiciels de base.

#### **a) Matériels**

- le matériel représente encore une part financière importante d'un système. Son choix est ultérieurement difficile à remettre en cause et son installation assez longue en général, aussi doit-il être étudié soigneusement.
- Il comprend les processeurs, les matériels annexes de saisie et de restitution des informations, les supports physiques des fichiers,

Dans les systèmes temps réel, en particulier industriels, il comprend aussi des éléments beaucoup plus particularisés, interfaces modes série (synchrone ou asynchrone) ou parallèle, des bus avec leurs protocoles, des capteurs passifs avec leurs conditionneurs, des capteurs actifs, des circuits d'adaptation, des amplificateurs (ordinaires, opérationnels, d'isolement, d'instrumentation, de puissance), des convertisseurs analogique-digital et digital-analogique, des actionneurs.

Dans les réseaux, il y a bien entendu des lignes de transmission de débits variables (électriques, hertziennes, radio, optiques) avec leurs protocoles, mais aussi des matériels locaux : routeurs, multiplexeurs (spatiaux ou temporels), concentrateurs, diffuseurs ; et aussi les équipements terminaux de circuits de données, souvent appelés « modems », même s'il n'est pas question de modulation (transmission en mode de base).

#### **b) Locaux**

Ils sont essentiellement constitués par les bâtiments et leurs équipements annexes. Ils abritent les matériels informatiques.

### c) Réseaux

- Un réseau est composé d'une partie matérielle gérée par un ensemble logiciel de gestion des protocoles, qui présente le même genre de contrainte temps réel qu'un système d'exploitation, et de routeurs, serveurs, concentrateurs et multiplexeurs qui sont des circuits électroniques analogues à des ordinateurs spécialisés.
- Un réseau est en fait souvent un ensemble de réseaux, reliés par des passerelles, chacun devant être adapté à des échanges spécifiques d'informations soit de gestion interne, soit entre entreprises, soit industrielles.

### d) Logiciels de base

Le logiciel de base représente une part croissante du coût d'un système, donc il conditionne la bonne utilisation. C'est toujours intrinsèquement un système temps réel, même s'il ne supporte pas d'application qui le soit.

Il a une importance primordiale pour la sécurité des opérations, car il protège les ressources (mémoires, informations transmises), assure les redémarrages, et contrôle les accès. Accessoirement, il permet la comptabilité de l'utilisation des ressources.

Il peut être reparti, et même sans temps absolu (multiprocesseurs, bases de données réparties) et partiellement câblé, malgré son nom.

Le logiciel de base comprend essentiellement le système d'exploitation qui gère les processus, dont les siens, qui sont tous en compétition et en coopération à la fois. Il est fonctionnellement composé des sous-systèmes suivants :

- noyau (qui attribue le processeur) ;
- gestion de la mémoire interne (souvent virtuelle) ;
- gestion des fichiers ou bases ;
- gestion des entrées-sorties ;
- gestion du réseau.



## 6-2 OBJECTIFS DE L'AUDIT

L'audit des moyens techniques a pour objectifs de :

- S'assurer de la performance des équipements :
  - disponibilité, fiabilité, positionnement chronologique tant sur le plan national qu'international
  - dimensionnement
  - état de fonctionnement, niveau d'utilisation et degré de satisfaction des utilisateurs
  - évolutivité, adéquation aux besoins actuels et futurs de l'entreprise.
- Evaluer le caractère fonctionnel et convivial, le niveau de sécurité d'accès et de protection des locaux qui abritent les équipements informatiques.
- S'assurer de la performance des réseaux, de leur fiabilité, de leur sécurité et de leur adéquation à l'environnement informatique.
- Evaluer la qualité des logiciels de base et s'assurer de leur adéquation avec les besoins de l'entreprise, en particulier des objectifs assignés au système d'information qu'ils supportent.

## 6.3. TRAVAUX D'AUDIT

### a) **Audit spécifique des matériels**

#### **1. Le matériel est-il adapté aux applications à traiter et aux logiciels de base tant qualitativement (nature de ceux-ci, que quantitativement (volume et temps de réponse) ?**

Le choix du type de matériel (modes d'exploitation, réseaux, etc...) est une décision de gestion, car elle structure le système d'information.

C'est le plan qui, ayant défini les applications, permet de déterminer le type des matériels (centralisé, distribué, reparté, multipostes, réseaux locaux et publics), et les modes d'exploitation (par lots - pour être ancien, ce mode reste parfaitement adapté dans de nombreux cas, dont souvent le traitement de la paye -, ou interactif).

Un soin particulier doit être consacré à l'examen actuel et prévisionnel des conflits d'utilisation pour un système centralisé, et aux cohérences des informations pour un système réparti.

Les temps de réponse, particulièrement dans les systèmes temps réel bien entendu, mais aussi les réseaux, doivent être étudiés attentivement, en général par simulation ou essais en vraie grandeur. Les goulets d'étranglement sont souvent les accès aux périphériques et aux réseaux.

La définition des volumes dans les applications permet ensuite de déterminer la configuration proprement dite (taille des mémoires, type, nombre et capacités des périphériques, interfaces caractéristiques des liaisons). Les erreurs proviennent presque toujours d'un excès d'optimisme, et d'un manque de souci de l'évolutivité.

La disponibilité du matériel et la rapidité de remise en fonctionnement sont des critères essentiels dans le choix des constructeurs. Il est important de vérifier leurs dires et de les consigner par contrat.

Une maintenance préventive fréquente, des délais d'intervention brefs, des diagnostics faciles, voire automatisés, sont des facteurs positifs de disponibilité.

Les statistiques de temps d'utilisation et d'entretien des enregistrements des pannes, composant par composant, permettent d'estimer leur homogénéité, leur disponibilité, et éventuellement de conclure à des causes permanentes d'inadaptation, comme l'atteinte d'un point d'écroulement à partir d'une certaine charge.

## **2. Qualité de la maintenance du matériel ?**

La maintenance matérielle s'apprécie en fonction des contrats et des relevés d'indisponibilité ; elle est préventive (entretien) et curative (remise en état). L'auditeur doit examiner les modalités d'appel, les délais d'intervention et ceux, qui peuvent être bien plus longs, de remise en état, les durées d'indisponibilité en résultant, l'inclusion de la main d'œuvre, des pièces, et des déplacements.

La télémaintenance vise à une meilleure efficacité, mais demande comme toute connexion des précautions contre les accès indus : la ligne ne doit être établie que sur demande aux moments convenus, il suffit d'un interrupteur manuel, et si possible manœuvré seulement après retrait de tous les fichiers sensibles.

Surtout dans les systèmes temps réels, cette maintenance matérielle n'est pas toujours facile à distinguer de la maintenance logicielle, surtout de celle du logiciel de base. D'où en particulier l'intérêt d'examiner les contrats de maintenance.

Le choix des supports physiques des fichiers demande le même soin que celui des processeurs, car ils conditionnent le délai de l'analyse-programmation, et il ne faut surtout pas compter trop juste : les informations elles-mêmes n'occupent qu'une place réduite devant les logiciels, les tables d'index, les pointeurs, les zones de manœuvre et les zones mortes. De même, le débit de ligne est une notion physique, très supérieure au débit réel.

L'évolutivité des objectifs, en quantité et en nature, implique que le matériel lui-même soit évolutif tout en restant bien adapté et modulaire (nombre de terminaux connectés par exemple). Le danger est d'approcher de la saturation, en volume ou en temps de réponse.

Et, si le premier cas est assez facile à prédire, le second échappe à toute intuition car l'écroulement d'un système est très brutal pour un seuil donné, difficile à déterminer à priori. Il est bon de prévoir non seulement les extensions, mais aussi les rétractions (par exemple en cas de scission d'entreprise).

L'adaptation aux logiciels de base et aux applications n'a pas pour critère l'optimisation, mais la relative indépendance des changements des uns ou des autres : une extension des applications ne doit pas remettre en cause le matériel, ni inversement une extension du matériel modifier profondément les applications.

### **3. Le matériel est-il fiable ? Quelle est la fréquence des pannes ? Et quel est l'impact réel des pannes ?**

Le matériel doit être fiable ; au sens des systémistes, cela signifie que s'il fonctionne, les résultats sont exacts ; c'est pratiquement toujours le cas, et sinon ils sont tellement aberrants que la détection ne pose guère de problème. Pour les ingénieurs, cela veut dire qu'il est disponible, qu'il n'y a pas de défaillance.

L'impact réel des pannes ne peut être véritablement déterminé que si elles sont enregistrées, composant par composant, mesurées par incidence sur le fonctionnement d'ensemble, avec le moment de la défaillance et celui de la remise en état. Ce qui constitue un cahier des indisponibilités.

### **b) Audit spécifique des locaux**

- **Les locaux sont-ils adaptés et évolutifs ?**

Disposition logique des matériels, des stocks de fourniture, des circuits de déplacement et de portage, ergonomie des postes de travail, éclairage (y compris de secours) et insonorisation.

- **Sont-ils suffisamment protégés ?**

accès  
incendie  
etc..

### **c) Audit spécifique des réseaux**

Il couvre les aspects suivants :

- examen des caractéristiques opérationnelles et des propriétés (nombre, nature, connexions, relations statiques et dynamiques) ;
- examen des performances, ou plutôt de l'adaptation (temps de réponse, surtout pour un réseau temps réel ou industriel, débit, taux d'erreur, disponibilité) par collecte de statistiques, insertion éventuelle de compteurs ;
- examen de la sécurité par recensement des menaces potentielles accidentelles ou délibérées (écoute, modification de messages, mascarade), et des parades (authentification, cryptage, certification), ainsi que la gestion des clefs et l'enregistrement des tentatives déjouées. ;

- gestion des tests, pannes, modes dégradés, réparations et reprises composant par composant, puis détermination des goulots d'étranglement, en partant de l'historique.

Les aspects relatifs à la sécurité des réseaux sont présentés plus en détail dans la section consacrée à l'audit de la sécurité.

#### **d) Audit spécifique des logiciels de base.**

Il couvre l'examen des aspects suivants :

##### **1. Adaptabilité ?**

Un logiciel de base est adapté s'il permet une utilisation correcte du matériel, avec les langages et modes d'exploitation choisis, pour supporter les applications.

##### **2. Evolutivité ?**

L'évolutivité impose une certaine transparence pour les applications qui reposent sur lui, étant donné qu'il ne peut y avoir de totale indépendance. Ainsi, un changement d'un de ses composants, éventuellement dicté par une évolution du matériel qu'il gère, ne doit pas entraîner une modification profonde des applications.

##### **3. Homogénéité des composants du logiciel de base ?**

L'homogénéité des composants du logiciel de base signifie qu'ils doivent être adaptés à la configuration du matériel, mais aussi entre eux, avec les langages, avec les utilisateurs, les analystes-programmeurs et les opérateurs. Ce point est souvent décevant, même si le prestataire est unique. Par exemple, entre traducteur de langage, système de gestion de base de données, et comptabilisation des ressources consommées.

##### **4. Fiabilité ?**

La fiabilité du logiciel de base, qui est toujours complexe car elle pose des problèmes de temps réel, est d'autant plus importante qu'elle est impénétrable par l'utilisateur, qui a beaucoup de peine à rectifier les conséquences d'anomalies. Or, elle n'est jamais parfaite, car un système temps réel peut être robuste, mais n'est jamais sans défaut, car quelle que soit leur dénomination, tous les logiciels de base sont des systèmes temps réel.

Particulièrement importantes sont la protection mémoire, celle des fichiers en traitement à distance, et la sauvegarde des informations dans une base de données.

Il est essentiel que le logiciel de base permette d'implanter des points de reprise et de reconstitution précis, efficaces et utilisables. Aucune transaction ne doit être perdue, ni envoyée à un mauvais destinataire, sans avertissement immédiat, ni déformé par la transmission.

## **5. Sécurité et protection ?**

(voir ci-après, audit de la sécurité)

## **6. Documentation**

La documentation est encore plus importante que pour les matériels, ainsi que sa mise à jour.

### **e) Aspects spécifiques à la micro-informatique.**

Les travaux d'audit de la micro-informatique recouvrent l'examen des aspects spécifiques ci-après :

#### **1. L'acquisition et l'utilisation des micro-ordinateurs sont –elles coordonnées ?**

L'auditeur vérifiera donc que soient coordonnés au niveau de la Direction informatique (et non obligatoirement centralisés) :

- le choix des matériels "agréés" dans l'entreprise, en veillant à offrir une diversité de matériels suffisamment étendue,
- le choix des logiciels de Bureautique "agréés": traitement de textes, tableurs, logiciels graphiques, logiciels intégrés, gestionnaires de fichiers, etc.,
- le choix des fournisseurs et la négociation des conditions commerciales,
- les modalités de la maintenance des matériels et des progiciels,

- la définition de la politique en matière d'infocentre, et les modalités des transferts de données entre l'unité centrale et les micro-ordinateurs.

L'absence totale de coordination, que l'on rencontre dans certaines entreprises, est à proscrire car elle conduit rapidement à une situation totalement anarchique. Cette absence de coordination est généralement le résultat d'un abandon de la Direction informatique face à de fortes poussées autonomistes des services en matière de Bureautique, elles-mêmes d'ailleurs souvent la conséquence des fortes réticences qui se manifestaient dans ce domaine au sein des services informatiques il y a quelques années.

## **2. Veille-t-on à ce que la micro-informatique ne devienne pas le support d'un développement anarchique d'applications autonomes et hétérogènes ?**

Si la micro-informatique est aujourd'hui un support fiable et efficace pour traiter l'ensemble des besoins de l'entreprise en matière de Bureautique, son utilisation en tant que support de développement d'applications de gestion, si elle n'est pas proscrire systématiquement, doit du moins être étudiée soigneusement.

Nombre de logiciels de gestion budgétaire, de gestion des immobilisations, de gestion de stock ou de comptabilité générale, développés par des amateurs avec de simples tableurs ou gestionnaires de fichiers, sont de véritables dangers pour les chefs d'entreprise. Ecrits en quelques jours, mis en exploitation sans véritables tests, ces logiciels offrent rarement des contrôles suffisants lors de la saisie des données (qui doit en outre souvent être réalisée en double, compte tenu de l'absence de coordination avec les développements sur grand système).

En revanche, bien maîtrisés, les développements sur micro-ordinateurs, éventuellement complétés par des échanges de données avec les grands systèmes, constituent un précieux moyen pour donner satisfaction aux utilisateurs, tout en déchargeant des services informatiques engorgés.

En définitive, l'auditeur vérifiera :

- que l'utilisation de la micro-informatique à des fins de développement d'applications est connue du service informatique et contrôlée par lui (les logiciels seront si possible développés par le service informatique) ;
- que les applications développées dans ces conditions sont correctement documentées, et présentent les mêmes garanties en matière de sécurité que les applications développées sur grand système :

contrôle des données saisies,  
procédures de sauvegarde et de reprise,  
contrôle d'accès,  
etc.

### **3. L'accès aux traitements applicatifs ou aux données sensibles gérés sur micro-ordinateur est-il contrôlé ?**

Les techniques habituelles de protection d'accès aux fichiers, aux bibliothèques de programmes, et aux applications peuvent trouver à s'appliquer dans un environnement micro-informatique.

Il convient cependant de reconnaître que celles-ci sont encore trop peu répandues, même lorsque des applications "sensibles" sont traitées sur le micro-ordinateur.

Quelle est la proportion de postes de travail sur lesquels les possibilités de contrôle d'accès par mot de passe ont effectivement été utilisées ? La négligence est d'autant plus coupable que, s'il y a quelques années les micro-ordinateurs étaient particulièrement perméables, certains d'entre eux offrent aujourd'hui des possibilités de contrôle d'accès analogues à celles des grands systèmes.

Par ailleurs, et sauf lorsque les micro-ordinateurs sont connectés en réseaux, les meilleures protections demeurent à ce jour les protections physiques : verrouillage par clé ou carte magnétique, ou tout simplement fermeture à clé des bureaux et armoires.

### **4. Des mesures spécifiques sont-elles prises pour limiter les risques de vol des micro-ordinateurs ?**

Dans les grandes entreprises, les risques de vol de matériels doivent demeurer présents à l'esprit. Ce risque est d'autant plus important qu'outre le micro-ordinateur lui-même, certains composants annexes sont susceptibles d'être dérobés : logiciels, cartes d'extension diverses, etc.

Parmi les mesures préventives, on peut citer :

- le contrôle des entrées et sorties de l'entreprise,
- l'identification précise des immobilisations et l'inventaire physique régulier de l'ensemble du parc.



## **5. L'entreprise n'encourt-elle aucune sanction pénale pour l'implantation de logiciels sans licence d'utilisation ?**

Beaucoup de grandes entreprises ont eu jusqu'à ce jour une attitude peu exemplaire dans ce domaine soit par une politique délibérée, soit par manque de contrôle.

Or le non-respect de la réglementation implique pour l'entreprise :

- un risque de sanctions pénales, prévoit les lois relatives à la propriété intellectuelle.
- un risque de détérioration du parc existant, en cas de présence de "virus" dans les logiciels utilisés sans licence.

Des contrôles par sondage de l'absence de logiciels illicites sur les micro-ordinateurs sont donc à prévoir.

## **6. Des programmes de détection de virus sont-ils exécutés régulièrement sur les micro-ordinateurs ?**

Ces logiciels sont susceptibles de détecter la présence de virus sur les micro-ordinateurs, permettant ainsi de les désactiver avant qu'ils n'aient eu le temps de nuire.

## **7 - AUDIT DES APPLICATIONS EN EXPLOITATION**

### **7-1 DEFINITIONS**

**Les applications en exploitation recouvrent les logiciels utilisés dans l'entreprise pour :**

- la planification, le suivi et la gestion des activités courantes ;
- le traitement des données et la diffusion des informations.

Elles se composent :

- d'applications de type scientifique ou industrielle
- d'applications de gestion et d'aide à la décision
- de logiciels bureautiques et de communication

Nous ne traiterons que les modalités de contrôle des applications de gestion.

**Les applications usuelles de gestion informatisées de l'entreprise sont :**

- la comptabilité (générale, auxiliaire, analytique et budgétaire)
- la gestion des achats
- la gestion des stocks
- la gestion des immobilisations
- la gestion des ventes
- la gestion de la production
- la gestion de la trésorerie
- la paye et la gestion des ressources humaines

**Elles comprennent aussi les applications spécifiques au métier de l'entreprise.**

- gestion de la forêt (pour une société forestière),
- gestion de la scolarité (pour un établissement scolaire)
- etc..

## 7-2 OBJECTIFS DE L'AUDIT DES APPLICATIONS INFORMATIQUES EN EXPLOITATION

L'audit des applications a pour objet de se prononcer sur leur qualité. Il s'agit plus particulièrement, d'apprécier :

### **1. La fiabilité du progiciel, et l'utilisation qui en est faite**

On pourrait considérer que, dans le premier cas, c'est la prestation du service informatique qui est contrôlée, alors que dans le deuxième cas, c'est l'activité des utilisateurs qui l'est.

Autrement dit, un logiciel peut être fiable, mais mal utilisé, ou à l'inverse, bien utilisé mais peu fiable.

Imaginons un logiciel comptable, dont la saisie d'écritures s'effectue normalement, mais qui « efface » par erreur les écritures dans les fichiers. Ce logiciel est à l'évidence peu fiable malgré l'utilisation correcte qui en est faite.

A contrario, la plupart des logiciels comptables admettent, afin de corriger des anomalies dans le contenu des fichiers, une procédure de saisie d'écritures déséquilibrées (c'est-à-dire dont le débit n'est pas égal au crédit), cette opération exceptionnelle devant être réservée aux seuls utilisateurs compétents. Utilisée abusivement, cette procédure, quoique répondant à un besoin réel, peut conduire à des situations totalement anarchiques.

Un bon logiciel contient des « garde-fous » contre une mauvaise utilisation, et un bon utilisateur met en place des outils de contrôle de la fiabilité des applications.

Dans l'exemple précédent le service comptable détectera aisément l'inégalité des débits et des crédits, donc l'existence d'écritures effacées, et le logiciel comptable éditera distinctement pour analyser la liste des écritures saisies par la procédure dérogatoire. Encore faut-il que cette liste soit examinée et conservée !

Il n'en reste pas moins que la fiabilité d'une application informatique résulte de la conjonction d'un bon logiciel et d'une utilisation satisfaisante.

## **2. L'adéquation des logiciels développés aux spécifications fonctionnelles et l'adéquation des spécifications fonctionnelles aux objectifs d'un bon contrôle interne.**

Vérifier l'adéquation des logiciels développés aux spécifications fonctionnelles définies dans le cahier des charges, en principe rédigé par les utilisateurs, c'est contrôler que les logiciels développés par le service informatique sont conformes aux besoins exprimés.

Mais cette adéquation n'est pas suffisante pour garantir la qualité de l'application dans son ensemble, puisque les spécifications fonctionnelles peuvent elles mêmes révéler des insuffisances ou des anomalies.

Imaginons par exemple un logiciel de gestion de stock qui fournit chaque mois un état des stocks valorisés en prix moyen pondéré. La nécessité de fournir les éléments d'un contrôle périodique des états édités implique que soit prévue l'édition d'une liste mensuelle comprenant le stock initial et le détail des mouvements du mois valorisés, justifiant ainsi le stock final.

En d'autres termes l'état des mouvements de stock garantit la continuité du chemin de révision, c'est à dire la possibilité de faire le lien entre les informations élémentaires saisies et les données restituées. A contrario, l'absence de cet état interdit toute possibilité de contrôle par les utilisateurs du mode de valorisation des stocks.

L'application ne saurait donc être considérée comme fiable si l'édition de la liste des mouvements de stocks n'a pas été prévue dans le cahier des charges.

Autre exemple, la conception des applications doit permettre de respecter les principes de séparation des fonctions. Ainsi, en matière financière les opérations de comptabilisation et les opérations de trésorerie doivent en principe être gérées par des personnes distinctes. La conception et l'utilisation des logiciels doivent donc permettre de respecter cette séparation, notamment grâce à la mise en œuvre de contrôle d'accès appropriés.

Dernier exemple, un bon contrôle interne implique l'existence de contrôle hiérarchique sur les opérations. Ce principe a pour conséquence informatique la définition :

- soit de procédures de validation des opérations par un supérieur hiérarchique dès leur saisie,

- soit de procédures d'édition d'états de contrôle des opérations saisies (exhaustif ou par exception) pour analyse a posteriori par un supérieur hiérarchique,
  - soit d'une combinaison de ces deux types de procédures.
- Ainsi en matière de gestion commerciale, certaines opérations spécifiques saisies par les vendeurs seront soumises à validation du directeur commercial : remises accordées supérieures à certains seuil, dépassement du crédit maximum autorisé pour un client

### **3. les risques de fraudes et d'erreurs**

Dans la grande majorité des cas, les risques de pertes liées à des erreurs de réalisation ou d'utilisation des logiciels sont infiniment plus importants que les risques de pertes liées à des opérations malveillantes ou frauduleuses. c'est donc naturellement la recherche d'erreur qui sera généralement privilégiée par l'auditeur dans son approche.

Bien entendu, dans certains cas spécifiques (présomption de détournement de fonds) ou dans certains secteurs d'activité (établissements financiers), la recherche d'opérations frauduleuses fera partie des objectifs assignés à l'audit.

Des travaux dédiés à cette recherche seront alors réalisés. Ainsi, dans un établissement financier, on peut envisager l'exécution régulière d'un progiciel spécifique de balayage et d'analyse des mouvements sur les comptes ordinaires, afin de déceler des opérations suspectes, susceptibles de cacher un détournement de fonds.

### **4. la qualité des méthodes de développement des logiciels et la qualité des procédures d'exploitation**

La qualité des procédures de conception et de réalisation des applications constitue une présomption de fiabilité des logiciels et de respect des spécifications fonctionnelles.

Néanmoins de graves anomalies peuvent apparaître dans les fichiers si un logiciel, même parfait, n'est pas exploité de manière satisfaisante. Ainsi, des erreurs d'exploitation, comme l'exécution en double d'un traitement en temps différé ou au contraire sa non-exécution, peuvent altérer les données contenues dans les fichiers.

De mauvaises procédures d'exploitation peuvent également avoir des conséquences nuisibles sur la pérennité des applications. Ainsi en l'absence de sauvegarde sur un site extérieur, des logiciels ou des fichiers d'importance initiale se trouveront –ils perdus et impossibles à reconstituer en cas de sinistre conduisant à la destruction du site informatique.

## **5. La pérennité des logiciels**

Nous venons indirectement d'évoquer cette distinction. Un logiciel peut s'avérer fiable de par la qualité de sa conception, mais non pérenne du fait de mauvaises procédures d'exploitation.

De même, un logiciel fiable à un instant donné, mais mal documenté, verra son espérance de vie notamment réduite. En effet, sa capacité d'évoluer sera très limitée

## **6. La performance des logiciels et leurs niveaux d'intégration**

Il s'agit de :

- La capacité des logiciels à exécuter les traitements prévus dans les délais en tenant compte des ressources disponibles,
- Des interfaces avec les autres logiciels.

## **7-3 TRAVAUX D'AUDIT**

### **1. Interview**

Outre des entretiens avec les responsables du développement et de l'exploitation de l'application, il sera généralement prévu des entretiens avec les principaux utilisateurs concernés.

### **2. Contrôles sur pièce**

Selon les objectifs exacts de la mission, ils concerneront par exemple :

- les documents préalables au développement de l'application (schéma directeur, étude préalable, étude détaillée),
- la documentation d'études,
- la documentation d'exploitation,
- les manuels utilisateurs,
- manuels de procédures,
- les logiciels eux-mêmes.

### **3. Jeux d'essai**

Le jeu d'essai consiste à créer un environnement de test, incluant une copie des logiciels en exploitation et des fichiers spécifiques.

Il est alors possible, dans cet environnement, de contrôler le fonctionnement des logiciels d'une manière approfondie, dans la mesure du moins où les cas de test ont été suffisamment préparés.

Avant d'être une technique d'audit, les jeux d'essai sont d'ailleurs avant tout un moyen pour les utilisateurs d'effectuer la "recette" d'une application préalablement à sa mise en exploitation.

Technique d'une grande efficacité, les jeux d'essai sont pourtant rarement utilisés en matière d'audit. Leur principal inconvénient réside en effet dans la lourdeur de leur mise en œuvre, impliquant souvent des charges de travail prohibitives à la fois pour les informaticiens qui créent la base de test et pour les auditeurs, qui doivent avoir une connaissance parfaite de l'ensemble des fonctionnalités.

Toutefois les principales limites de cette technique sont :

- elle permet de tester les logiciels, mais non le contenu des fichiers en exploitation. Or, nous avons vu que les fichiers peuvent receler des anomalies sans que les logiciels soient eux-mêmes erronés ;
- il est difficilement possible d'être exhaustif dans les cas testés par le jeu d'essai ;
- cette technique permet rarement de déceler des opérations frauduleuses, dans la mesure où celles-ci sont réalisées soit par intervention directe sur les fichiers, soit par une modification temporaire des logiciels, qui n'apparaît plus au moment de la création des logiciels de test.

#### **4. Examen du contrôle de l'environnement informatique pour cette application**

Un des moyens de base pour contrôler une application consiste à contrôler la qualité de l'environnement informatique pour cette application.

Concrètement, seront étudiées, limitativement pour l'application auditée :

- Les procédures de développement et de maintenance : outils, méthodologie, normes, documentation, procédures de mise en exploitation ;
- Les procédures d'exploitation : protection d'accès, sauvegardes, préparation, lancement et contrôle des travaux en temps différé, procédures de reprise, suivi des incidents ;
- Les fonctions techniques : gestion de réseau, support micro-informatique ;
- l'organisation générale du service et du projet.

L'approche, ciblée sur une application, sera d'ailleurs plus précise qu'un contrôle de l'ensemble du site.

Le principal intérêt de cette approche, outre qu'elle peut être réalisée dans le cadre d'un budget limité, réside dans la bonne présomption qu'elle peut donner de la qualité des logiciels. L'absence de méthodologie de développement, la faiblesse de la documentation, l'absence de suivi des incidents, un grand laxisme dans les autorisations d'accès, une politique de sauvegarde mal définie, sont autant de signes inquiétants, dont il est bien rare qu'ils ne se matérialisent pas par de graves carences dans l'application.

Sa principale limite est qu'elle ne fournit que des présomptions, jamais des carences avérées.

#### **5. Examen du contrôle interne de la fonction traitée**

Le contrôle exhaustif d'une application implique à la fois le contrôle des logiciels développés et le contrôle de l'utilisation qui en est faite. Une application ne peut être considérée comme fiable si, en dépit de logiciels de qualité, elle est utilisée en dépit de bon sens.



En outre, l'implication des utilisateurs est d'autant plus importante que des contrôles de cohérence appropriés à leur niveau sont de bien meilleurs garants de la fiabilité des logiciels que la plupart des contrôles techniques internes au service informatique. En dépit d'une idée trop répandue, les utilisateurs sont loin d'être démunis, et ont entre leurs mains les moyens de déceler la grande majorité des défaillances d'un logiciel, que celles-ci trouvent leur origine dans une erreur de programmation ou dans une mauvaise utilisation du système. Encore faut-il pour cela qu'ils n'aient pas renoncé à assumer toute responsabilité au moment de la mise en place des traitements automatisés. Trop souvent en effet, soit par excès de confiance devant un "Dieu informatique" infaillible, soit par négligence (l'informatisation est un excellent prétexte pour ne plus assumer ses propres responsabilités), les utilisateurs ont tendance à ne plus réaliser le minimum de contrôles indispensables à la fiabilité d'ensemble de l'application.

En conséquence, l'auditeur informatique basera une partie importante de ses investigations sur l'utilisation et le contrôle par les utilisateurs des traitements informatiques :

- **la réalisation par les utilisateurs de contrôles de cohérence portant sur les traitements**

Par exemple, en matière de logiciel comptable, des contrôles de cohérence du type :

somme, des écritures saisies = somme des écritures restituées sur les "brouillards de saisie" (listes journalières récapitulatives des écritures saisies) ;  
 somme des écritures listées sur les brouillard du mois = totalisation des écritures sur les journaux comptables du mois ;  
 totalisation des écritures listées sur les journaux comptables du mois = totalisation des écritures du mois sur les grands-livres ;  
 cumul de début de période des écritures sur le grand livre + total des mouvements du mois = cumul de début de période suivante (en débits et en crédits) ;  
 solde des comptes du grand-livre = solde des compte de la balance ;

permettront de déceler la plupart des erreur de conception, d'exploitation et d'utilisation des logiciels comptables. Encore faut-il qu'ils soient mis en œuvre régulièrement et soigneusement.

- **L'existence de contrôles hiérarchiques**

L'existence de contrôles hiérarchiques sur les opérations traitées constituent un élément essentiel de contrôle interne de l'ensemble des cycles de l'entreprise.

Les procédures informatiques permettant la validation ou le contrôle par un supérieur hiérarchique de l'opération, des données saisies, sont nécessaires :

- listes récapitulatives de saisie, détaillées ou par exception, pour contrôle a posteriori ;
- procédure d'autorisation en temps réel de certains mouvements préalablement à leur validation (contrôle a priori).

- **L'existence d'une bonne séparation des fonctions**

D'une manière générale, on distingue dans l'activité d'une entreprise :

- des opérations relatives à la réalisation de l'objet social,
- des opérations relatives à la conservation du patrimoine,
- des opérations relatives au traitement comptable.

Le souci d'une bonne séparation de fonctions conduit à attribuer, pour un même processus de l'entreprise, la responsabilité des travaux relatifs à chacun de ces trois types d'opérations à des personnes distinctes.

Au cas spécifique des systèmes informatisés, le respect de cette séparation de fonctions sera contrôlé par la mise en place de systèmes d'autorisation d'accès aux traitements évoqués ci-après.

- **L'existence de procédures d'autorisation d'accès satisfaisantes**

Une application ne peut être considérée comme fiable si n'importe qui, à l'intérieur ou, pis encore, à l'extérieur de l'entreprise, a la possibilité de se connecter à celle-ci, et d'en consulter ou d'en mettre à jour les données de base.

Au delà des risques d'opérations frauduleuses ou malveillantes que l'on imagine aisément, il en résulte en effet un risque important d'erreurs, commises en toute bonne foi et dont il sera souvent impossible de retrouver l'auteur.

- **La compétence et l'intégrité du personnel**

La compétence et l'intégrité, tant des informaticiens que des utilisateurs, constitue naturellement un élément essentiel de la fiabilité des applications.

- **La continuité du chemin de révision**

La notion de continuité de chemin de révision du système d'information (on parle aussi souvent de piste d'audit, du terme anglo-saxon *audit trail*) correspond à la nécessité de faire le lien entre les données entrées dans ce système et les informations restituées. En d'autres termes, l'application doit fournir les éléments nécessaires à la validation des données issues des chaînes de traitement.

- **L'existence de validations régulières du contenu des fichiers**

Les fichiers gérés par l'application informatisée contiennent certaines données dont le contenu est susceptible de faire l'objet d'une validation. Ainsi, les stocks seront périodiquement contrôlés au cours d'inventaires physiques, et les soldes des comptes de tiers, clients et fournisseurs, seront implicitement validés par l'absence de litiges.

## 7-4 IMPACT DE L'ENVIRONNEMENT EDI

### A - DEFINITIONS

« L'EDI est l'échange entre systèmes informatisés, par voie électronique, de données structurées, organisées en messages normalisés ».

L'EDI (Electronic Data Interchange, en français Echange de Données Informatisé) consiste à échanger directement, selon une structure et un format préalablement définis, des données jusqu'alors transmises par support papier, entre les différentes applications informatiques de partenaires économiques connectés sur un ou plusieurs réseaux.

Cette définition comporte trois éléments : échange - données - électronique. L'échange est la fonction remplie. La donnée est le contenu de la fonction, c'est-à-dire l'information véhiculée. Enfin, l'électronique est le moyen de transmission des données.

En d'autres termes, l'EDI permet la transmission de données entre ordinateurs, selon un format normalisé. Concrètement, cette transmission peut concerner des commandes, des avis de réception, des factures mais aussi des informations financières, des paiements, des balances comptables et bien d'autres messages.

La normalisation en EDI concerne :

- le contenu (normalisation des informations à transmettre)
- le contenant (protocole de télécommunication permettant de transmettre les différents types d'EDI)
- et de façon liée, l'organisation des échanges eux-mêmes, dans un contexte global.

EDIFACT est devenu le langage adopté à l'unanimité par l'ensemble de la communauté internationale (ONU et norme ISO).

**EDIFACT** (Electronic Data Interchange for Administration, Commerce and Transport) / (Échange de Données Informatisé pour l'Administration, le Commerce et le Transport)  
Règles des Nations unies concernant l'échange de données informatisé pour l'administration, le commerce et le transport. Elles se composent d'un ensemble de normes approuvées à l'échelon international, de répertoires et de directives pour l'échange électronique de données structurées, en particulier celles concernant le commerce des biens et services entre systèmes informatiques indépendants.

Les technologies « EDI » vont modifier profondément les structures et les organisations des entreprises. L'expert-comptable doit, dès aujourd'hui, prendre en compte cette évolution qui concernera ses clients et son propre cabinet. Il aura à vérifier des comptabilités intégrant l'EDI, à traiter des volumes d'informations de plus en plus importants, et se verra imposer par ses partenaires des contraintes pour échanger l'information comptable et financière.

En France, l'Ordre des Experts Comptables (OEC) s'est impliqué très vite dans les travaux d'élaboration de normes EDIFACT pour les messages comptables.

L'association EDIFICAS (Echange de Données Informatisé en matière Financière, Informationnelle, Comptable, et d'Audit, Analytique et Sociale) a été créée par l'OEC en collaboration avec les sociétés de services qui œuvrent habituellement avec la profession comptable. Cette association développe des normes pour assurer des échanges de données informatisés dans des conditions de sécurité, d'efficacité, de rapidité qu'autorise l'EDI.

Les buts sont de garantir une pérennité des informations (changement des systèmes) et des gains de temps (compatibilité entre les différents systèmes, suppression des saisies redondantes).

Le rôle d'Edificas est aussi de promouvoir les EDI auprès de la profession comptable et d'assurer la liaison avec d'autres groupes sectoriels (banques, SSII, CGA...).

## **B - CONSEQUENCES SUR L'ORGANISATION DES CABINETS**

Face à la croissance du volume des informations traitées par les entreprises, une réorganisation des tâches va être nécessaire. Le client reçoit dès aujourd'hui un grand nombre d'informations via EDI, qui sont traitées automatiquement, informatiquement et donc collectées, classées et imputées comptablement.

Les missions de tenue de comptabilité sont partiellement prises en charge par l'EDI. Ce transfert des traitements vers l'informatique permet de gagner du temps et de la fiabilité dans le système comptable (évite les erreurs de saisie).

Ce type de fonctionnement va permettre au cabinet de collecter des informations du système informatique du client à distance, pour les traiter et les analyser, ou de pratiquer des circularisations, de faire de la révision... sans aucun déplacement de la part des collaborateurs du cabinet. Cette approche est une nouvelle manière de gérer un dossier client.

En contrepartie de la collecte d'informations du cabinet dans le système du client, le client lui-même pourra consulter une base de données située chez l'expert-comptable. Cette base de données pourra regrouper des informations qualitatives issues du travail et de l'expérience de l'expert-comptable. Ce nouveau service offert par l'expert-comptable apporte une plus-value au client qui pourra consulter des informations financières commentées, des analyses de marges, des données concernant le secteur de l'entreprise ou un marché spécifique, des recommandations sur les procédures...

L'expert-comptable va donc revoir son organisation informatique pour proposer de nouveaux services, et mettre en place des gestions d'accès pour assurer la sécurité de son système. Il devra mettre à jour régulièrement les informations stockées, avoir une politique de stockage des données et des documents (GED).

La réorganisation du cabinet se fera désormais autour du système informatique, ce qui lui permettra de répondre aux contraintes du marché, d'assurer une meilleure productivité et de réduire les coûts de revient de ses missions.

### **C - CONSEQUENCES DES EDI SUR LA MISSION DE L'EXPERT-COMPTABLE**

Dans un audit comptable et financier classique, la présence de l'EDI ne modifie pas les objectifs et les grands axes des méthodes de révision des intervenants, mais le programme doit s'adapter et doit inclure l'étude du dispositif EDI sans pour autant en devenir l'objet principal. Lors de la prise de connaissance, la compréhension du système et des contrôles internes amènera l'auditeur à déterminer les risques spécifiques qu'induisent les systèmes informatiques utilisant l'EDI.

Dans un environnement EDI, il est de plus indispensable de prendre connaissance de l'accord d'échange auquel a adhéré l'entreprise et de son degré d'intégration dans son propre système.

C'est lors de la phase de contrôle des comptes que le travail de l'auditeur change le plus. Lors de l'établissement du programme de vérification des comptes, il faut identifier les comptes qui sont affectés par l'EDI et les justificatifs qui ont disparu. L'auditeur doit disposer de la liste de tous les documents édités ou éditables sur support papier et se former aux outils

d'interrogation des bases de données qui le concernent. Les contrôles qui s'appuient sur l'examen physique des pièces deviennent impossibles. Ils doivent être remplacés par la vérification des messages d'accusé de réception conservés par le système.

Dans un milieu EDI, les contrôles portent plus sur la validité des chaînes de traitements que sur les pièces comptables elles-mêmes. Ainsi, si la fiabilité est démontrée au niveau des traitements automatisés, alors 100 % des informations se trouvent validées !

#### **D- OUTILS A LA DISPOSITION DE L'AUDITEUR**

Il s'agit de :

- jeu d'essais : simulation d'envoi, de traitement et de réception de flux EDI,
- outil d'interrogation et d'extraction de données : interrogation et extraction de données précises, demandées par l'auditeur,
- outil bureautique : interrogation de fichiers dont la taille est compatible avec les capacités d'un micro-ordinateur,
- confirmation : interrogation de partenaires proposés automatiquement par l'ordinateur suivant des paramètres définis par l'auditeur,
- module de certification EDI : module de certification de la qualité d'un produit EDI.

Les deux derniers points sont importants pour s'assurer que le système EDI fonctionne correctement.

Le module de certification EDI est mis en œuvre par des spécialistes. Il permet de vérifier que le système respecte la norme utilisée et que les modalités d'application du contrat d'interchange sont respectées.

Les programmes de confirmation présentent l'avantage d'une réponse directe de partenaires extérieurs à l'entreprise, et de façon automatisée. Cela permet un contrôle régulier des procédures en place et une détection rapide des anomalies de traitement ou de dysfonctionnement des applications. Pour l'auditeur, cette procédure lui enlève la gestion lourde des circularisations effectuées manuellement pour un résultat identique.

## **8 - LA CONDUITE D'UNE MISSION D'AUDIT INFORMATIQUE**

Comme l'audit obéit aux mêmes règles que le management lui-même du système, il doit lui être :

- faisable, c'est-à-dire disposer d'éléments d'information suffisants pour permettre de conclure dans un délai raisonnable ; sinon l'auditeur doit refuser ou interrompre sa mission, en indiquant comme il a été vu que si le système n'est pas compréhensible, il a tous les défauts possible simultanément. L'acceptation d'une mission engage la responsabilité de l'auditeur, car elle implique qu'il certifie implicitement être compétent ;
- correspondre aux besoins des demandeurs et autres intéressés ;
- correctement planifié ;
- adapté particulièrement : la démarche détermine de façon arborescente tous les moyens et actions sans aucune lacune ; la démonstration de ce qu'il prouve est sans faille ;
- compréhensible : les conclusions doivent être exprimées en termes clairs pour les lecteurs.

### **8-1 LA PREPARATION DE LA MISSION**

Il est difficile de définir une norme quant à la durée et aux modalités pratiques exactes de la phase de préparation de la mission. Ainsi, un audit externe aura pour objectif, pour des raisons commerciales, de figer le plus rapidement possible une première proposition d'interventions, quitte à prévoir dans celle-ci une phase d'investigations préalables à l'issue de laquelle les concours de la mission seront précisés.

Un service d'audit interne, affranchi de la contrainte financière liée à l'incertitude quant à l'acceptation ou non d'une proposition, pourra au contraire préférer, selon les cas, une phase d'enquête préliminaire relativement longue, de manière à aboutir à une lettre de mission la plus précise et la complète possible, ou une phase préliminaire extrêmement courte, avec corrélativement une lettre de mission la plus ouverte possible.



Il n'en reste pas moins que certains travaux préparatoires sont indispensables au bon déroulement de la mission. D'une manière générale, il s'agit de l'ensemble des investigations nécessaires à l'élaboration de deux documents préalables au démarrage de la mission elle-même, l'un à usage externe, l'autre à usage interne.

Le document à usage externe sera la proposition d'intervention, dans le cas d'un audit réalisé par une société extérieure, ou la lettre de mission, dans le cas d'un audit interne.

Le document à usage interne constituera le programme de travail des auditeurs.

### 8-1-1 La proposition d'intervention ou la lettre de mission

Ce document matérialise l'accord entre le mandant (souvent la Direction générale de l'entreprise) et son mandataire (audit externe ou audit interne) sur le contenu et les modalités pratiques de la mission. Il légitime en outre l'intervention vis-à-vis des services audités. Il présente les aspects ci-après :

#### **a) les objectifs de la mission**

Les objectifs recherchés dans une mission d'audit informatique pouvaient être très variés : examen du contrôle interne de la fonction informatique, examen de la sécurité physique, audit des protections d'accès, contrôle des méthodes de développement, audit des performances, audit d'une application spécifique

La proposition d'intervention devra donc lever toute ambiguïté en précisant les objectifs visés.

#### **b) Le périmètre de la mission**

La lettre de mission définira clairement les sociétés et établissements, ainsi que les sites concernés par les travaux. Dans le cas d'un audit d'application, ce sont les fonctionnalités auditées qui seront elles-mêmes précisées.

### **c) La période d'intervention**

Seront ici précisées à la fois la durée globale de la mission et ses principales échéances (date de début et de fin des travaux, étapes intermédiaires, date de remise des conclusions...).

### **d) Les contraintes à prévoir pour les services audités**

En particulier, il est souhaitable de préciser dès le début de la mission la disponibilité qui sera demandée aux services audités. La trop grande surcharge de travail induite par un audit est en effet souvent invoqué, à tort ou à raison, par ceux-ci, et est ainsi la source de relations difficiles.

En cas d'utilisation de logiciels d'audit, des contraintes spécifiques sont également à prévoir pour les services audités.

De la même manière, la mise en œuvre de jeux d'essai nécessite le plus souvent un travail préparatoire important.

### **e) Les méthodes de travail employées**

La définition détaillée des méthodes de travail employées est davantage du ressort du programme de travail, document interne, que de la proposition d'intervention. Il est néanmoins le plus souvent souhaitable de préciser, au moins dans les grandes lignes, ces méthodes de travail : utilisation ou non de questionnaires, méthodes basées sur les interviews ou sur l'étude de documents, mise en œuvre de jeux d'essai, utilisation de logiciels...

### **f) La constitution de l'équipe**

La composition de l'équipe, ainsi que le nom du responsable de la mission, seront ici précisés. Dans le cas de missions d'audit externe importantes, il est généralement souhaitable que soit fourni un curriculum vitae très succinct des différents intervenants.

### g) Les documents préparatoires

Afin de faciliter le démarrage de la mission, une liste de documents préparatoires à fournir aux auditeurs sera le cas échéant incluse dans les propositions d'intervention, ou transmise aux services audités préalablement au premier entretien. Ce seront par exemple :

- **Pour un examen du contrôle interne de la fonction informatique**

- l'organigramme du service,
  - la description de la configuration matérielle,
  - une description succincte des logiciels, la liste des progiciels,
  - les principales notes relatives à l'activité informatique dans l'entreprise, et à l'organisation du service,
  - le plan informatique
  - le budget du service informatique,
  - les comptes rendus des dernières réunions du comité informatique.

- **Pour un audit d'application**

- l'organigramme du service et la liste des principaux interlocuteurs à rencontrer (utilisateurs et informaticiens),
  - les documents de présentation de l'application,
  - le cas échéant, la description du contenu de certains fichiers sur lesquels il est envisagé de réaliser des contrôles.

#### 8-1-2 Le programme de travail

Le programme de travail définit précisément les méthodes d'audit retenues et le travail à réaliser par les auditeurs.

Il contient une ventilation des charges de travail à prévoir pour chaque module d'audit.

On trouvera dans l'encadré ci-après un exemple de programme de travail succinct d'une mission d'audit d'application.

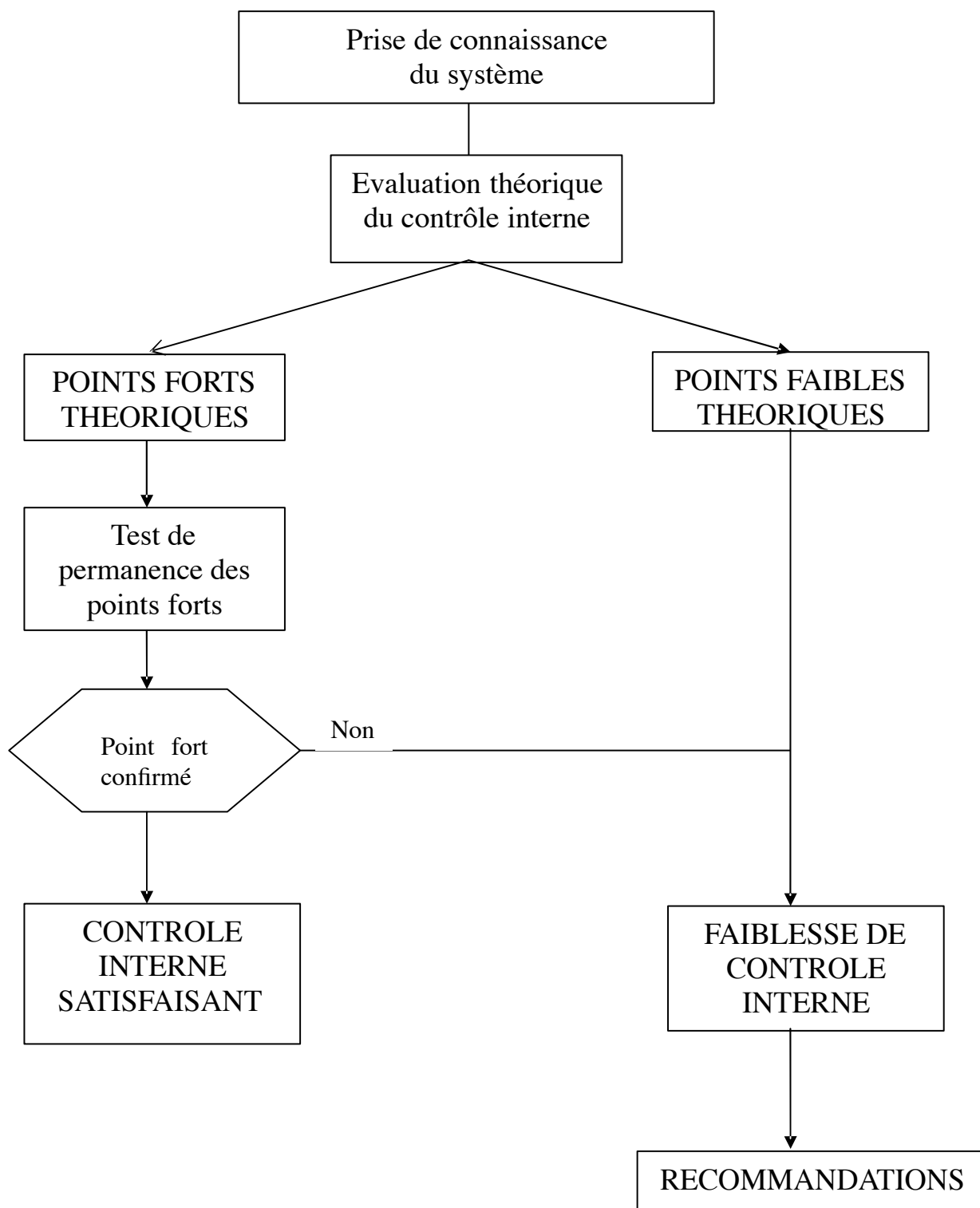
**Programme de travail de la mission d'audit du logiciel de gestion du personnel par le  
Commissaire aux comptes dans un environnement PME (budget 80 heures)**

- |   |           |
|---|-----------|
| - lancement de la mission   | 4 heures  |
| - prise de connaissance de l'application :<br>entretiens avec le chef de projet et avec les principaux utilisateurs,<br>lecture de la documentation disponible        | 16 heures |
| - analyse critique des fonctionnalités de l'application   | 8 heures  |
| - examen du contrôle interne de la fonction informatique<br>pour cette application : procédures de développement et<br>d'exploitation, analyse de la documentation... | 16 heures |
| - développement de logiciels d'audit (fonctionnalités à définir<br>lors de la prise de connaissance de l'application)<br>et analyse des résultats                     | 20 heures |
| - rédaction du rapport et synthèse  | 16 heures |

## 8-2 LES METHODES D'INVESTIGATION

### 8-2-1 La démarche générale d'évaluation du contrôle interne

#### Présentation schématique



Une prise de connaissance et l'analyse des procédures du système évalué permettent de mettre en évidence ses forces et ses faiblesses théoriques. Néanmoins, un point fort théorique n'en devient réellement un que si la procédure décrite est bien celle qui est effectivement appliquée. C'est l'objet des tests de permanence de vérifier cette permanence de l'application de la procédure théorique.

### 8-2-2 L'évaluation du contrôle interne de la fonction informatique

#### **a) L'évaluation des forces et faiblesses théoriques**

L'analyse des procédures, nécessaire à une première évaluation des forces et faiblesses du système, se fera essentiellement au travers :

- d'interviews des responsables du service informatique ainsi que , ainsi que, généralement des principaux services utilisateurs ;
- d'un travail sur pièce à partir de l'ensemble des documents disponibles dans le service : plan informatique, norme interne, organigramme, plan de sécurité...

#### **b) Les tests de permanence**

Une qualité première d'un bon auditeur est de valider systématiquement ses conclusions. Il n'est pas question ici de décrire pour chaque point d'audit les procédures d'évaluation. Celles-ci découlent d'ailleurs d'elles-mêmes dans la plupart des cas.

Voir exemple en annexe

### 8-2-3 Autres travaux

Voir sections précédentes

## 8-3 L'APPRECIATION DU VOLUME D'INTERVENTION

L'appréciation de la charge de travail à prévoir pour réaliser la mission pose le problème de la nécessité d'un compromis entre la recherche d'un coût d'intervention minimum et celle d'investigation le plus complet possible.

Au préalable, il convient de bien comprendre que, si la charge de réalisation d'un application, répond à des besoins définis précisément dans un cahier des charges, est fixe et incompressible, la charge de réalisation d'un audit informatique est fonction d'un programme de travail , et peut donc être modulé, du moins à l'intérieur de certaines limites :

une borne inférieure en deçà de laquelle il est raisonnablement impossible de porter une appréciation motivée ;

une borne supérieure au-delà de laquelle l'apport marginal des investigations complémentaires sur les conclusions de l'audit est trop limité pour présenter un intérêt quelconque.

## 8-4 LA PRESENTATION DES CONCLUSIONS

La fin de la mission d'audit se matérialise généralement par une présentation contradictoire avec les services audités des principales conclusions, suivie de l'émission du rapport. Outre une analyse critique, il est souhaitable que celui-ci contienne une synthèse des recommandations formulées par l'auditeur.

## 8-5 LE SUIVI DES RECOMMANDATIONS

Lorsque des faiblesses graves ont été recensées, il est tout à fait souhaitable que les auditeurs puissent assurer un suivi de la mise en œuvre des recommandations qu'ils ont formulées. Ce suivi pourra notamment être assuré :

soit au travers d'une participation régulière aux principales réunions de synthèse relatives à l'avancement des travaux,

soit au travers de la réalisation de missions légères d'actualisation du rapport.



## **9 - LES OUTILS DE L'AUDITEUR INFORMATIQUE**

L'auditeur informatique peut disposer de deux types d'outils importants dans le cadre de son activité :

- **les méthodes d'analyse des risques informatiques,**
- **les progiciels d'audit .**

### **9.1 LES METHODES D'ANALYSE DES RISQUES INFORMATIQUES**

Il existe sur le marché des différentes méthodes dont l'objectif est de fournir une évaluation globale de sécurité et des risques informatiques au sein d'une entreprise.



La plus célèbre d'entre elles est incontestablement la méthode MARION , élaborée par le CLUSIF ( Club de la sécurité informatique Française), l'APSAIRD ( Assemblée Plénière des Sociétés d'Assurance contre l'incendie et les Risques Divers).

Ces méthodes ont toutes en commun de fournir :

- un questionnaire d'évaluation du risque : chaque question donne lieu à une notation de l'environnement étudié ;
- une présentation conviviale des résultats de l'évaluation, souvent après saisie des réponses au questionnaire sur un micro-ordinateur et traitement des résultats.

**La méthode MARION comporte six étapes :**

- l'analyse des risques a pour objet le recensement des risques encourus et l'évaluation du coût maximum des pertes consécutives à chaque risque recensé ;
- l'expression du risque maximum admissible permet de définir , en accord avec la direction de l'entreprise , le seuil critique au-delà duquel le risque n'est plus admissible ;

- l'analyse de la sécurité existante, basée sur les réponses à un questionnaire d'évaluation, aboutit à une synthèse de risque encouru sous la forme de la célèbre  rosace 
- l'évaluation des contraintes permet de prendre en compte l'existant dans l'analyse des risques et la définition des remèdes : contraintes techniques, humaines ;
- le choix des moyens définit les moyens à mettre en œuvre pour améliorer la sécurité de manière cohérente ;
- la définition du plan de sécurité définit les modalités pratiques selon lesquelles la sécurité sera améliorée.

## 9.2 LES PROGICIELS D'AUDIT

Ils trouvent leur utilité dans la plupart des missions confiées à l'auditeur informatique. Ainsi :

- dans le cadre d'un audit d'application, ils permettent de contrôler le contenu des fichiers et de déceler d'éventuelles anomalies ;
- dans le cadre de l'assistance à la révision comptable, ils permettront de valider les résultats de certains traitements, ou encore de mettre en évidence des informations anormales ou erronées.

Par abus de langage, on désigne souvent sous le terme d'audit informatique le développement de programmes de contrôle dans le cadre d'audit comptable ou audit opérationnel.

En réalité, l'informatique n'est alors qu'un outil mis à disposition de l'auditeur pour mener à bien sa tâche première : l'audit comptable a pour objet de vérifier la régularité et la sincérité des comptes de l'entreprise, l'audit opérationnel de se prononcer sur la fiabilité et l'efficacité d'un cycle de l'entreprise (approvisionnements, ventes, production..).

Compte tenu de la forte automatisation de la plupart des entreprises, leur contrôle passe nécessairement de plus en plus par un contrôle des applications informatisées, ainsi que par l'utilisation d'outils informatiques destinés à réduire la durée de ces contrôles tout en améliorant leur efficacité.

Prenons l'exemple du commissaire au compte auditant les immobilisations. Réalisé manuellement, le contrôle du calcul des dotations est à la fois fastidieux et peu convaincant, compte- tenu de la faible taille de l'échantillon qu'il est raisonnablement possible de valider.

En revanche, l'écriture d'un logiciel, généralement peu complexe, analysant le fichier des immobilisations, permettra de recalculer et de valider la dotation de l'exercice.

Qui plus est, des programmes complémentaires mettront en évidence d'éventuelles anomalies pour analyse :

- liste des immobilisations dont la dotation cumulée depuis l'origine est inférieure au minimum linéaire (les dotations étant alors insuffisantes et les dotations irrégulièrement différées, car non comptabilisées, étant finalement non déductibles fiscalement) ;
- liste des immobilisations dont la date de mise en service diffère notablement de la date d'installation ;
- etc..

Parfois même, l'auditeur développe des programmes pour connaître l'incidence financière de ses remarques. Face à des comptes clients insuffisamment provisionnés, il écrira un programme de recherche des créances anciennes et, si nécessaire, d'évaluation du montant de la provision à constituer.

On le voit, l'informatique est devenue aujourd'hui l'outil indispensable de l'auditeur, sans la maîtrise duquel celui-ci ne pourra accomplir sa mission d'une manière totalement efficace.

De façon générale, cette technique vise à développer des programmes informatiques dont l'objectif est de contrôler la fiabilité des applications auditées.

Des langages de programmation, particulièrement adaptés au développement rapide de requêtes d'analyse des fichiers, ont parfois été abusivement baptisés

des logiciels d'audit. En réalité, certains de ces langages ont d'autres objectifs de base, et ne sont qu'accessoirement utilisés en matière d'audit :

- langages d'infocentre, pour analyse rapide des fichiers par utilisateur,
- langages de développement rapide de programmes d'édition, destinés aux informaticiens pour des sorties d'états peu complexes.

Les objectifs recherchés par la conception et la réalisation des programmes d'audit varient et peuvent être ventilés en deux catégories :

- **Les programmes de sélection pour analyse de certains enregistrements contenus dans les fichiers.**

Les types de sélection sont eux-mêmes variés

Dans certains cas, il s'agit d'un simple échantillonnage : sélection pour contrôle d'une facture sur 1000, sélection des achats les plus significatifs par leur montant...

Parfois encore, ces enregistrements recèlent des informations qui, quoique n'étant pas nécessairement erronées, justifient une recherche complémentaire par leur caractère exceptionnel : éditions des ventes pour lesquelles le pourcentage de remise au client est supérieur à certain seuil, édition des immobilisations acquises antérieurement à une certaine date .

Dans d'autres cas enfin, les sélections correspondent systématiquement à des anomalies, que celles-ci soient issues d'une erreur de programmation ou d'une mauvaise application des procédures : état des stocks négatifs, état des ventes à perte, liste des codes articles figurant dans le fichier de facturation et ne figurant pas dans le fichier des références article.

- **Les programmes de validation d'informations issues de l'application**

L'objectif de l'auditeur ici sera de valider les logiciels eux-mêmes, pour certains traitements importants, généralement en écrivant un programme ayant les mêmes fonctionnalités que celui qui est audité.

Si cette approche peut paraître surprenante, elle permet de déceler des erreurs bien inattendues. Ainsi, la réécriture d'un programme de valorisation de stock aboutira – t – elle à une valeur de 1251000,00 F alors que le programme □ officiel donne un total de 1151 000 francs. En l'occurrence,

le contrôle réalisé aura mis en évidence une insuffisance de capacité d'une zone de travail du programme □ officiel ¶ Cette zone ne comporte que cinq chiffres significatifs , un article dont la valeur totale était de 106 000 francs n'avait été valorisé que pour 6000 francs. Or , en présence d'un fichier très volumineux , représentant une liste de plusieurs dizaines de pages , cette erreur pouvait fort bien passer inaperçu lors d'un contrôle manuel.

Bien entendu , la réécriture pour contrôle de certains programmes ne peut que rester une technique limitée. Sa généralisation conduisant en effet .... à réécrire l'application auditée.

- **La Révision Assistée par Ordinateur**

La Révision Assistée par Ordinateur est un outil informatique d'aide à la révision des comptes, destiné à l'expert-comptable et à leurs collaborateurs. Il permet, après reprise de la balance du client, un suivi du dossier permanent, une analyse des risques, la constitution du dossier annuel, la préparation des feuilles maîtresses, et la passation d'écritures d'opérations diverses.