# AUDIT INFORMATIQUE

## *NOTES DE COURS*

**PLAN DU COURS**

# BUT DU COURS

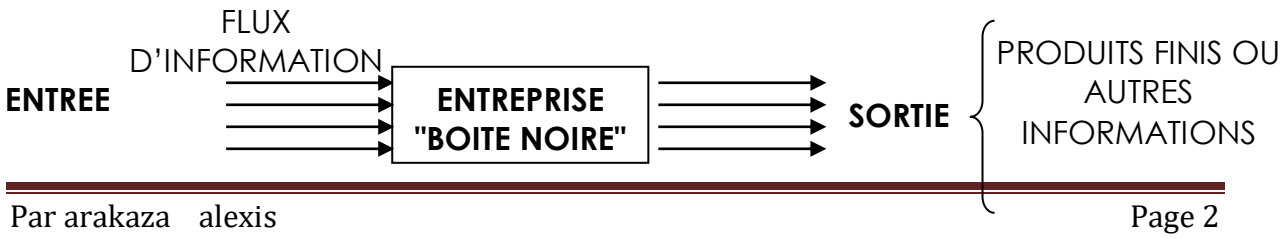
Initier les futurs informaticiens aux techniques et procédures d'audit informatique.

# 0. INTRODUCTION

L'Audit vient du mot latin AUDIRE qui signifie *écouter*, *faire un diagnostic*. Il s'agit donc d'une activité qui diagnostique les *forces* et les *faiblesses* d'un système en référence à des objectifs déclarés ou sous-entendus, qui analyse les raisons de ces lacunes et qui propose un plan d'action afin que le service audité réponde aux besoins et exigences de l'entreprise en terme de qualité de service, de sécurité, d'efficacité, de cohérence,...

L'entreprise peut être considérée comme une ***boîte noire*** avec à l'entrée des flux d'information et à la sortie des produits finis. D'où, la nécessité de coordination et de synchronisation de tous ses éléments.

L'entreprise comme système a besoin d'outils de systèmes d'information et informatiques. Ces outils doivent être fiables. Pour fiabiliser ces moyens, il faut diagnostiquer, vérifier, contrôler et prévenir, trouver les moyens de défaillances, formuler des recommandations. Tous ces problèmes font partis du rôle des auditeurs.



**L'entreprise doit être bien gérée**

- Vérifier
- Diagnostic
- Contrôle
- Recherche les goulots d'étranglements
- Proposer des solutions

## *0.1. BREF HISTORIQUE DE L'AUDIT*

Aucune entreprise ne peut fonctionner sans système d'information de gestion nommé SIG. Aucune ne peut survivre si elle ne possède pas un bon manager ou chef compétent.

Ainsi, MANAGER consiste à trouver l'adéquation entre les ressources humaines, financières, matérielles et les finalités des projets plus les objectifs de son entreprise. Dans ce cas, le SIG est formé par l'ensemble des ressources matérielles, humaines pour traiter les informations et atteindre son objectif. On peut aussi dire qu'un système d'information est un moyen de communication pour une entreprise.

Partant de ce principe, l'historique de l'audit date de 2000 ans AV. JC (code de la comptabilité à Mésopotamie).

A partir du 19ème siècle, il y a eu la naissance des associations comptables pour auditer les entreprises.

Vers les années 1965, la création de l'IFACI : Institut Français des Auditeurs et Consultants Internes.

**Acteurs concernés par l'audit**

1) **Organisateur :** personne intervenant à la demande de la direction et a pour mission de proposer une structure avec la définition précise de rôle et responsabilité de chaque élément de la structure.

2) **Le Responsable de la sécurité :** il a pour mission d'assurer le contrôle et d'inspection des sites afin de détecter les risques éventuels au sein de l'entreprise. Il a aussi pour mission d'assurer la sécurité physique des individus et du patrimoine de l'entreprise.
3) **Contrôleur de gestion:** assistant de la direction qui établit le budget, les prévisions et contrôle les réalisations.
4) **L'auditeur interne :** personne qui intervient suivant un planning ou sur ordre de mission. Il a le rôle de prendre une "**Photo**" à un instant donné. Il apprécie l'état du contrôle interne.
5) **Réviseur comptable :** c'est la personne qui apprécie la validité des documents issus de la comptabilité qui seront rendus publics (le bilan et le compte de résultat).
6) **Consultant :** personne qui subit les lois du marché. Possède une spécialité et une compétence reconnue.

Les directions d'attaches et domaines d'intervention de chaque acteur sont résumés dans le tableau ci-après :

**DIRECTION D'ATTACHE ET DOMAINE D'INTERVENTION DES ACTEURS D'AUDIT**

| ACTEUR | DIRECTION D'ATTACHE | DOMAINE DE COMPETENCE |
|---|---|---|
| ORGANISATEUR | DG, DFC | E |
| RESPONSABLE DE SECURITE | DT | D |
| CONTROLEUR DE GESTION | DG, DFC | F |
| AUDITEUR INTERNE | DG, DFC | B |
| REVISEUR COMPTABLE | INDEPENDANT | A |
| CONSULTANT | INDEPENDANT | C |

A : Contrôleur Comptable

B : Contrôleur Technique, Commercial, Comptable, Sécurité

C : Diagnostic, Avis et Conseil

D : Sécurité physique du système ou des agents

E : Avis et Conseil, Planification d'un projet

F : Contrôleur des résultats de divers services

## *0.2. AUDIT INTERNE ET AUDIT INFORMATIQUE*

L'***audit interne*** est une activité indépendante d'appréciation de contrôle, de l'exécution et de l'efficacité des autres contrôles en vue d'assister la direction.

L'***audit informatique*** est une activité de contrôle du manquement informatique pour apprécier l'utilisation, l'exécution, l'efficacité et l'adéquation des éléments constitutifs du système informatique ou du système d'information avec comme objectif l'orientation de l'entreprise.

## *0.3. BESOIN ET NECESSITE D'AUDIT INFORMATIQUE*

Les raisons qui invitent les dirigeants à effectuer les audits informatiques sont :

- La connaissance de l'impact de changement dû aux introductions de système informatique dans l'environnement du travail ;
- Le besoin de connaître les chiffres d'affaire et le retour des investissements (ROI) avec les divers coûts et les risques encourus.

## *0.4. POSTES DE COUT INFORMATIQUE*

Les coûts informatiques sont catégorisés sur 2 aspects :

- L'entreprise ne possède pas encore les outils informatiques mais envisage l'automatisation ;
- L'entreprise possède un système informatique,

Dans ce cas les charges informatiques sont en dehors de charge du matériel et celles des logiciels. On distingue les charges de premier établissement et les charges répétitives ou périodiques.

**a. Charges de premier établissement**

Ce sont les charges tels que :

- Le coût de l'étude de l'opportunité
- Les dépenses pour la sensibilisation du personnel
- Le coût de conversion (initiation de formation)
- Les frais de réorganisation partielle ou totale
- Le coût ou perte dû(e) à l'interruption des opérations
- Les dépenses de formation du personnel (informaticiens ou utilisateurs)
- Le coût d'analyse conceptuelle
- Le coût de programmation
- Le coût des essais
- Le coût d'établissement de la documentation

**b. Charges périodiques ou répétitives**

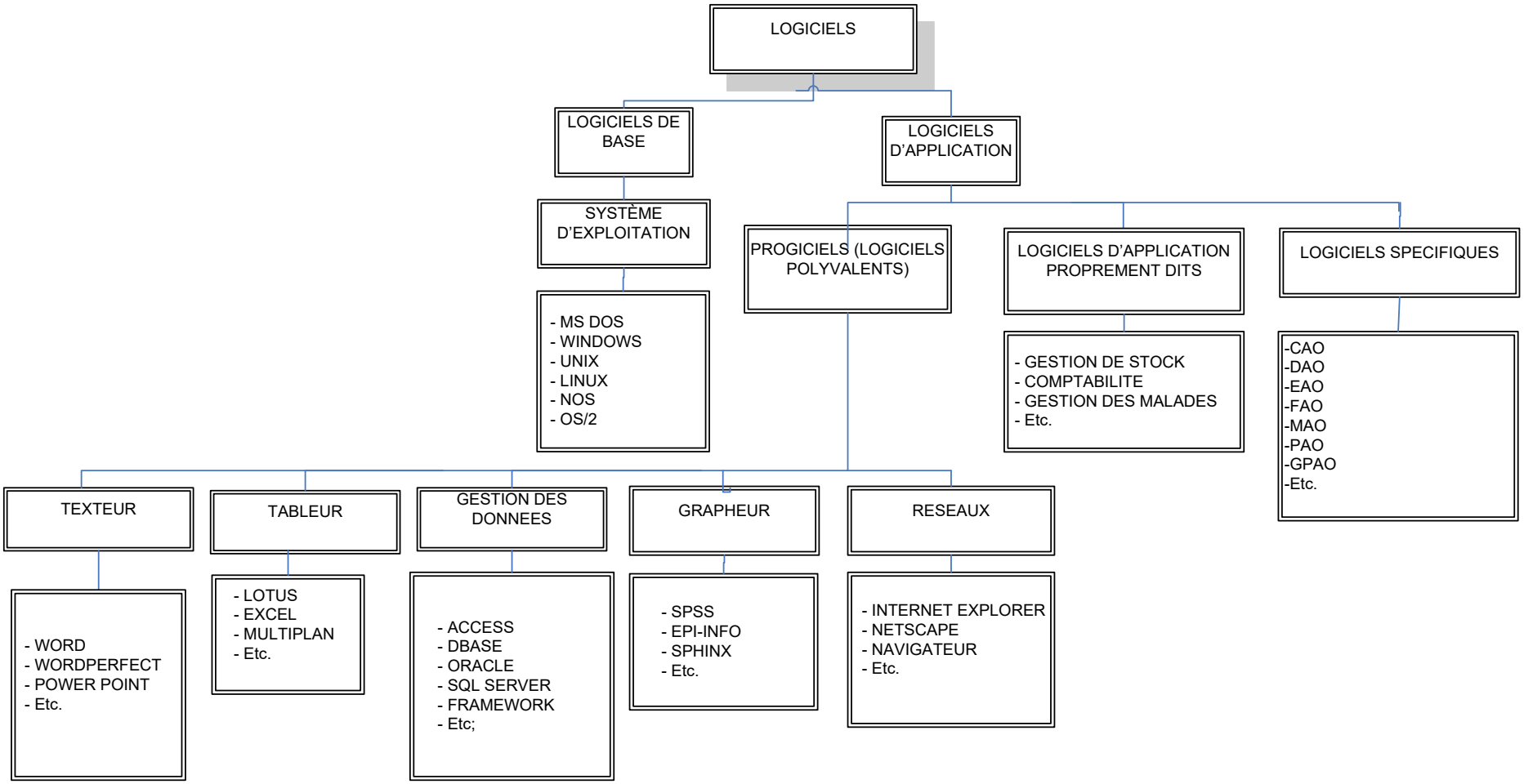
Ce sont des charges qu'on retrouve lors de l'exercice du fonctionnement du système informatique. Ces charges constituent la base du budget informatique.

- Les charges de personnel
- Les charges de matériel (achat, location ou maintenance)
- Les charges locatives de logiciels
- Les charges de fourniture
- Les frais généraux inhérents au système informatique (locaux, climatisation, entretien, assurance).

# CHAP I. CONTEXTE TECHNIQUE POUR LA MISSION D'AUDIT

Les contextes techniques pour les missions d'audit sont liés à l'évolution de la technologie de l'information.

- En ce qui concerne les machines, on est passé aux ordinateurs de la 1ère génération aux ordinateurs de la 4ème ou 5ème génération ;
- En ce qui concerne les logiciels (logiciels de base et logiciels d'application)


LOGICIELS
LOGICIELS DE BASE
LOGICIELS D'APPLICATION
SYSTÈME D'EXPLOITATION
PROGICIELS (LOGICIELS POLYVALENTS)
LOGICIELS D'APPLICATION PROPREMENT DITS
LOGICIELS SPECIFIQUES
- MS DOS
- WINDOWS
- UNIX
- LINUX
- NOS
- OS/2
- GESTION DE STOCK
- COMPTABILITE
- GESTION DES MALADES
- Etc.
-CAO
-DAO
-EAO
-FAO
-MAO
-PAO
-GPAO
-Etc.
TEXTEUR
TABLEUR
GESTION DES DONNEES
GRAPHEUR
RESEAUX
- WORD
- WORDPERFECT
- POWER POINT
- Etc.
- LOTUS
- EXCEL
- MULTIPLAN
- Etc.
- ACCESS
- DBASE
- ORACLE
- SQL SERVER
- FRAMEWORK
- Etc;
- SPSS
- EPI-INFO
- SPHINX
- Etc.
- INTERNET EXPLORER
- NETSCAPE
- NAVIGATEUR
- Etc.

## *I.1. L'EVOLUTION DES DIFFERENTS SYSTEMES*

- En ce qui concerne le type d'architecture des systèmes informatiques

***Exemple :*** Architecture client-serveur

- En ce qui concerne les langages de programmation et les outils du développement ; un des contextes de l'audit informatique c'est les méthodes des systèmes d'information basés sur les 3 cycles :
- Cycle de vie
- Cycle de décision
- Cycle d'abstraction

Tous ces problèmes font que la nécessité d'audit devient de plus en plus présente.

## *I.2. TYPOLOGIE D'AUDIT INFORMATIQUE*

Selon le degré de finalité d'importance, des difficultés, on distingue 3 types d'audit informatique :

1° L'audit de diagnostic

2° L'audit de régularité

3° L'audit d'efficacité

**A). L'audit de diagnostic**

L'audit de diagnostic permet à l'auditeur à porter un jugement sur des objectifs ou nouveaux projets de l'entreprise. Voir même de la politique générale de l'entreprise (sur le schéma directeur).

**B) L'audit de régularité (audit de conformité)**

Cet audit a pour but la vérification de telle ou telle procédure, les problèmes de cohérence des données c'est-à-dire les données intégrées dans les ordinateurs sont réelles ou cohérentes.

**C) L'audit d'efficacité**

C'est l'audit qui consiste à analyser les méthodes d'analyse, de conception et de développement.

Selon la distinction par degré de difficultés croissant on distingue :

- L'audit en milieu informatique

- L'audit de sécurité d'une façon globale
- L'audit informatique système

**Remarque :** Certains auteurs distinguent 2 types d'audit :

- L'audit informatique fonctionnel
- L'audit informatique opérationnel

## *I.3. L'AUDIT INFORMATIQUE FONCTIONNEL*

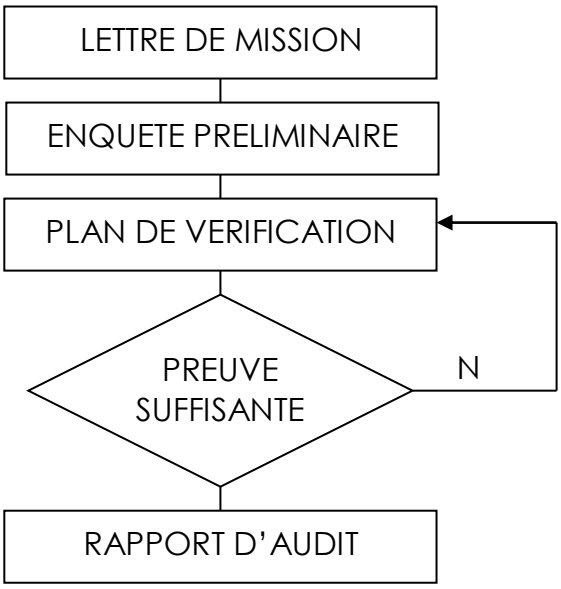
L'audit informatique fonctionnel comporte 4 audits suivants :

1. L'audit des moyens
2. L'audit de la production des services informatiques
3. L'audit de la politique informatique
4. L'audit financier

## *I.4. L'AUDIT INFORMATIQUE OPERATIONNEL*

- L'audit des moyens de traitement et des ressources techniques
- L'audit des applications
- L'audit de la circulation des documents
- L'audit de la sécurité générale liée à l'Informatique

# CHAP II. PHASES D'UNE MISSION D'AUDIT




Une mission d'audit informatique peut se décomposer en 3 phases une fois le sujet et les liens au service à éditer sont déterminés. On peut alors commencer les travaux d'audit qui débutent par :

- La phase d'enquête préliminaire
- La phase de vérification
- La phase de restitution (rapport de mission)

➢ **Lettre de mission**

La lettre de mission est adressée par la direction générale au service de l'audit. Cette lettre déclenche le travail de l'équipe de l'audit. C'est le point de départ d'une mission d'audit.

A la réception de la lettre de mission de service informatique on dresse la liste de portefeuille de mission à effectuer.

Ainsi, la lettre de mission peut être appelée «**ordre de mission**»

Dans la pratique, on distingue les types de mission ci-après :

- Mission de type cyclique (2 fois ou une fois par an)
- Mission spécifique demandée par la direction
- Mission due à des événements nouveaux non prévisibles dans l'entreprise

## 1. ENQUETE PRELIMINAIRE

L'enquête préliminaire demeure avec la définition des objectifs et de la lettre de mission. La durée de l'enquête est de 4 à 5 jours environ mais elle peut être prolongée si c'est nécessaire.

***Composition de l'équipe***

L'équipe est composée comme suit :

- Un chef de mission (Superviseur)
- Un auditeur spécialiste en informatique
- Un deuxième auditeur (généraliste) binôme
- Le chef de service d'audit (éventuellement mais non obligatoire)

L'enquête préliminaire se compose de 4 phases :

1° L'analyse du sujet et la définition des objectifs

2° La préparation de la documentation (élaboration des questionnaires)

3° La prise de contact avec les autorités

4° L'enquête préliminaire proprement-dit sur le terrain (2 ou 3 jours)

Le but de cette dernière phase est de :

- Collecter des informations afin de pouvoir dresser un plan du travail
- Etudier la faisabilité par rapport à l'ordre de mission des objectifs préalablement fixés
- Remettre en cause éventuellement les objectifs après discussion avec le service demandé

  Exemple : pour une mission d'audit de traitement des anomalies et limitation des factures erronées chez un opérateur de télécommunication, l'enquête préliminaire devra permettre de :
- Prendre connaissance des fonctions des divers services en jeu
- Etudier l'organigramme de l'organisation et les relations des services
- S'informer sur le fonctionnement du Centre de Traitement Informatique
- S'informer sur le volume des factures émises et le nombre des factures erronées
- Inventorier le délai, la fréquence de traitement
- Répertorier les divers types d'anomalies au niveau de la saisie

- Identifier le problème ressenti par le service informatique ou d'autres services

**Remarque :** La phase préliminaire constitue la phase du diagnostic

## 2. PHASE DE VERIFICATION

La phase de vérification a pour but de confirmer les points forts et aux points faibles constatés ou supposés dans la phase d'enquête préliminaire et déchiffrer éventuellement les pertes et risques encourus. Cette phase se décompose comme suit :

1° L'établissement d'un programme de vérification

2° L'étape de vérification sur le terrain et la recherche des preuves de défaillance

3° Le dépouillement et la compilation des résultats obtenus

4° L'exploitation de résultat

**Remarque :** On peut distinguer 2 types de vérification :

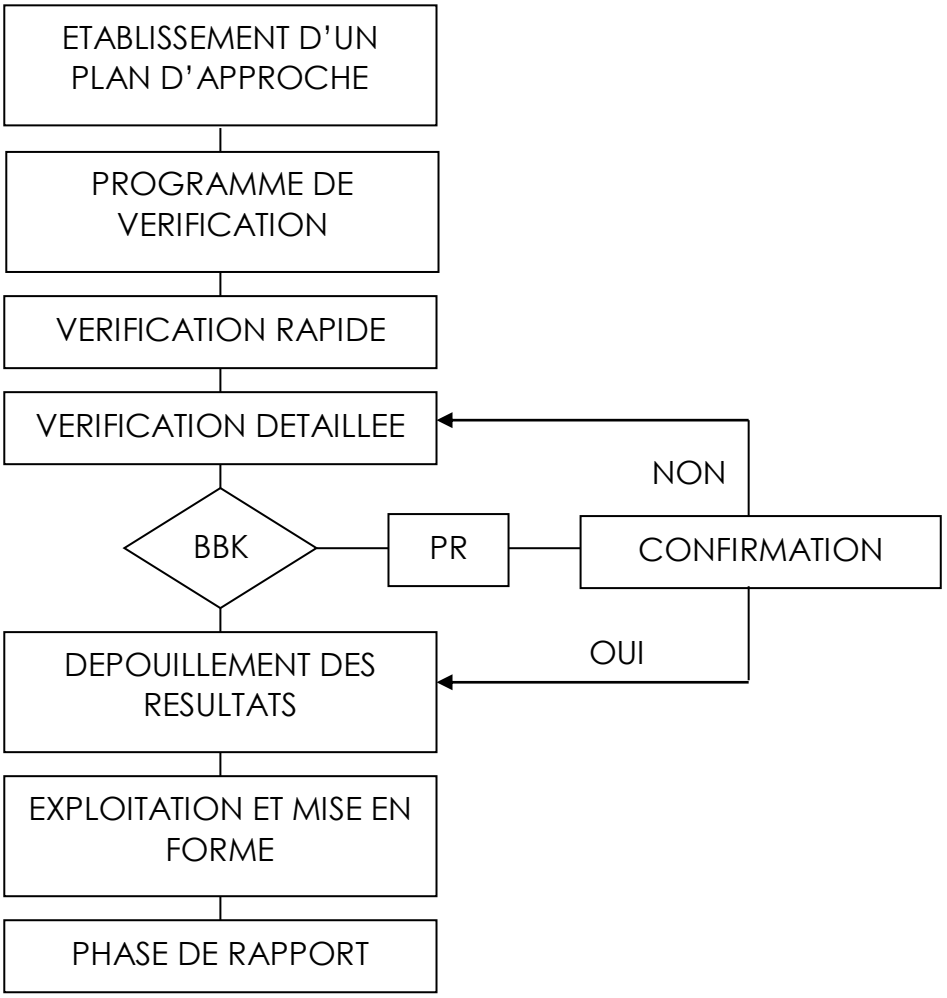
**a) Vérification rapide :** qu'on appelle aussi ***vérification de survol*** (entretien, examen de la documentation, etc.)

L'objectif poursuivi est de permettre aux auditeurs de détecter rapidement les points forts et les points faibles.

**b) Vérification approfondie**

L'objectif est d'apporter les preuves pour confronter les éléments recensés et déchiffrer le dégât réel.

Le schéma général de l'étape de vérification se présente comme suit :




**Remarque :**

BBK : Black Blur Key (Bilan mettant en évidence les points forts et les points faibles)

PR : Point de Reprise

### 3. PHASE DE RESTITUTION DU RAPPORT

C'est la dernière phase d'une mission d'audit appelée ***Phase de restitution du rapport d'audit.***

Elle consiste à la préparation, la rédaction et l'édition d'un rapport.

Les principales étapes sont :

- La rédaction d'un projet de rapport
- La présentation du projet au responsable du service audit
- La rédaction du projet définitif
- La notification et l'envoie du rapport au service intéressé
- L'établissement de fiche de suivi et l'envoie de la lettre de clôture de la mission.

- **QUELQUES CONSEILS POUR LA REDACTION DU RAPPORT FINAL**

1° Le volume et l'épaisseur du rapport sont fonction du terme et de service audité (il n'y a pas de règle fixe)

2° on exige dans ce rapport la clarté et la concision

3° L'organigramme d'un service au sein du rapport est à déconseiller mais il peut se trouver en annexe

4° La description des fonctions n'est pas obligatoire

5° Les annexes ne sont obligatoires

6° L'IFACI (Institut Français des Auditeurs et Consultants Internes) recommande de dresser le tableau des points forts et des points faibles.

**Remarque :** Les techniques et les outils de vérifications sont fonction du problème à résoudre.

# CHAP III. MISSIONS D'AUDIT

Dans la pratique, il existe différents types d'audit, cependant l'expérience à montré que les missions d'audit sont classifiées en 2 catégories :

1° Les missions d'audit demandées par la direction générale

2° Les missions d'audit demandées par la direction technique de l'informatique.

**a. LES MISSIONS D'AUDIT DEMANDEES PAR LA DIRECTION GENERALE**

La grande mission est l'audit de la politique informatique.

L'audit de la politique informatique comprend les missions ci-après :

- L'audit de la politique informatique d'acquisition en vue de l'informatisation
- Audit des projets présents et futurs (audit de processus de développement)
- Audit relatif aux finances de la fonction informatique
- Audit du budget et du suivi
- Audit sur la comptabilité analytique
- Audit sur les prestations internes
- Audit des coûts

## *1. AUDIT DE LA POLITIQUE D'ACQUISITION EN VUE DE L'INFORMATISATION*

Pour effectuer cet audit le document de base est le cahier de charges. Un ***cahier de charges*** est un document contractuel entre le client demandeur d'un service informatique ou d'acquisition des matériels informatiques et ses fournisseurs.

On appelle aussi ***cahier de charges***, le document établi entre l'équipe informatique interne d'une entreprise et une société informatique.

Le cahier de charges comprend les rubriques ci-après :

**a.** Définition générale et contexte du problème :

- Les objectifs

- Les contraintes

**b.** Les documents de base :

- Les divers documents et schémas de circulation
- Les états d'entrée et de sortie pour les applications

**c.** Fonctionnalités du futur système

- Les traitements ou modules de programme
- Des solutions envisagées

**d.** Les directives :

- Les recommandations
- Les prévisions d'extension du système

**e.** Conclusion et engagement

- Rapport des engagements mutuels
- Délai des travaux
- Calendrier des réalisations, etc.

Pour une mission d'audit, le cahier de charges est utilisé pour faciliter par exemple :

- Récolter les informations sur le choix des matériels achetés (leurs caractéristiques notamment le type de processeur, la capacité mémoire centrale, les types des périphériques, les types de réseau installé, etc.)
- Récolter les informations sur les logiciels réalisés ou achetés
- Récolter les informations sur les bases de données mise au point :

Exemple : Base de données répartie, partagée ou orienté-objet

- Récolter les informations sur le coût du matériel
- Récolter les informations sur les applications envisageables ou réalisées
- Récolter les informations sur le type de contrat contractualisé afin d'analyser les devoirs et obligations de chaque partie.

## ➢ METHODES D'ESTIMATION DE CHARGE

### 1. METHODE DE REPARTITION PROFESSIONNELLE

Pour cette méthode on fait une estimation globale de la charge du projet et on répartie cette charge dans le temps. La répartition professionnelle se base sur les étapes ci-après :

| CONCEPTION | 100% | REALISATION |
|---|---|---|

| ETAPE | RATIO |
|---|---|
| ETUDE PREALABLE | 10% du total du projet |
| ETUDE DETAILLEE | 20 à 30% du total du projet |
| ETUDE TECHNIQUE | 5 à 15% de la charge de réalisation |
| REALISATION | Deux fois la charge d'étude détaillée |
| MISE EN ŒUVRE | 30 à 40% de la charge de réalisation |

## 2. METHODE COCOMO (CONSTRUCTIVE COST MODEL)

### B. W BOEHM

Cette méthode repose sur 2 hypothèses:

**1)** Un informaticien chevronné peut facilement donner une évolution de la taille de logiciel à développer

**2)** Un informaticien fait toujours les mêmes efforts pour écrire un nombre donné de lignes de programme quel que soit le langage de programmation utilisé (3ème ou 4ème génération).

A ces 2 hypothèses, BOEHM est arrivé à calculer de coefficient de corrélation entre la taille du logiciel et la charge consommée. L'unité d'œuvre. L'unité d'œuvre utilisée (UNITE DE MESURE) pour ce modèle est l'instruction source (lignes de programme) notée KISL ou KDSI Kilo Octet Instruction Source Ligne (KISL). La méthode permet d'obtenir la charge de réalisation en **M/H** ainsi que ***le délai normal*** recommandé si on ne veut pas prendre des risques supplémentaires. La taille moyenne de l'équipe est donnée par la formule :

1). $Taille \quad Moyenne \quad dela \quad Population = \frac{Charge}{Délai}$

2). $Charge \quad en \quad Mois/H = a(KISL)^b$

3). $Délai \quad normal \quad en \quad Mois = C(Charge \quad en \quad Mois/H)^d$

**KISL :** Nombre de milliers d'instructions sources lignes (le nombre de milliers de lignes de programme source testées).

**KDSI :** Kilo Delivered Source Instructions (Milliers de lignes de codes)

a : Coefficient de la croissance du rendement

b : Coefficient de la décroissance du rendement en fonction de la taille du logiciel.

### b. MISSIONS D'AUDIT DEMANDE PAR LA DIRECTION INFORMATIQUE

Les missions d'audit demandé par les services informatiques sont multiples :

- Audit sur l'utilisation des logiciels
- Audit de qualité de service et de l'informatique horizontale
- Audit de l'utilisation et de l'exploitation de logiciels horizontaux
- Audit d'un grand centre serveur
- Audit des ressources humaines

## *2. AUDIT SUR L'UTILISATION DES LOGICIELS*

**Remarque :** Actuellement beaucoup d'entreprises notamment PME font appel aux logiciels dits horizontaux qui sont utilisables par le PC.

Le problème qui se pose est le piratage de logiciels ou le chargement des paramètres de logiciels. Ces problèmes sont punis par la loi.

En effet, il existe un contrat d'utilisation des logiciels associé au contrat de vente.

Au vue de ces problèmes, le rôle de l'auditeur dans la mission d'audit des logiciels est de :

- Vérifier l'existence d'une documentation complète des produits utilisés ;
- Vérifier l'existence d'un planning de formation des utilisateurs ainsi que le respect de ce planning ;
- Vérifier l'existence de contrat d'utilisation des logiciels ;
- Vérifier que le nombre de produits installés correspond à celui décrit dans les documents.
- Détecter les copies et les logiciels illicitement installés
    - **Les logiciels** sont des produits spécifiques à l'entreprise

- **Les progiciels** sont des produits standards

## *3. AUDIT DE QUALITE DE SERVICE ET DE L'INFORMATIQUE HORIZONTALE*

**Remarque :** La qualité de service informatique ne peut se concevoir sans une surveillance assidue de système et l'existence des relevés d'incidents.

Le problème de surveillance du système en ce qui concerne la qualité de service concerné :

- La qualité de service rendu par le système pour les utilisateurs en temps réel.
- La qualité de service des interventions des constructeurs des machines ainsi que les indisponibilités détaillées des pannes éventuelles des ordinateurs.

A titre indicatif, on peut illustrer les qualités de services pour l'utilisateur en temps réel, les qualités de services des ordinateurs de service d'intervention par les données ci-après :

| **PRINCIPAUX INDICATE URS** | **VALEUR DE MOIS** | **MOYENNE DES 6 DERNIERS MOIS** |
|---|---|---|
| TAUX D'INDISPONIBILITE | 1,08 | 1,09 |
| TMBF UTILISATEUR (EN HEURES) | 96,4 | 99,3 |
| NOMBRE MOYEN D'ARRET | 1,91 | 1,92 |
| DUREE MOYENNE D'UN ARRET (EN HEURES) | 1,05 | 1,10 |

TMBF : Time Between Failure c'est-à-dire le temps moyen que la machine peut connaître une panne.

**Qualité de service global des ordinateurs**

| PRINCIPAUX INDICATEURS | VALEUR DE MOIS | MOYENNE DES 6 DERNIERS MOIS |
|---|---|---|
| TAUX D'INDISPONIBILITE | 0,12 | 0,13 |
| TMBF | 3,62 | 2,62 |
| NOMBRE MOYEN D'ARRET | 0,27 | 0,38 |
| DUREE MOYENNE D'ARRET | 1,92 | 1,64 |

**TAUX D'INTERVENTION**

Commentaire :

Les tableaux ci-dessus indiquent les différentes qualités de services dans des centres informatiques en tenant compte des critères ci-après :

- Taux d'indisponibilité
- Le nombre moyen d'arrêt
- La durée moyenne d'un arrêt en heure

On suppose que l'utilisateur utilise la machine à 100% en temps réel et que les ordinateurs travaillent aussi à 100%. Parmi ces indicateurs, le TMBF est souvent le plus élevé pour les utilisateurs.

Ceci s'explique par le fait qu'il y a un faible coût d'intervention au niveau de maintenance, entretient et réparation de machine soit 3,62%. D'où l'utilisateur utilise à 96% les machines.

Partant de ces informations, l'audit de la qualité de service concerne pour l'auditeur la vérification :

- De l'adéquation entre l'investissement et le besoin de l'entreprise
- De la formation des utilisateurs vis-à-vis de logiciel utilisé
- De l'existence du contrat de maintenance avec le fournisseur du produit.

La durée maximum d'utilisation d'un ordinateur c'est 2ans

## *4. AUDIT D'UN GRAND CENTRE SERVEUR*

Pour l'Audit d'un grand centre serveur, la lettre de mission est envoyée simultanément à la division informatique et au responsable d'audit. Ces 2 personnes se réunissent pour définir les différentes missions d'audit à effectuer en dressant un planning de mission.

Le nombre total des jours évalués est de 35 jours ouvrables répartis comme suit :

- Phase de pré-audit et de planification 16% de 35 jours
- Phase d'enquête préliminaire 24%
- Phase de vérification rapide 18%
- Phase de vérification pour réalisation de l'audit proprement dit 26%
- Phase de restitution du rapport 16% comprenant la phase de rapport(1) 8% et la phase de rapport(2) 8%.

Les missions d'audit vont consister à:

- Connaître les procédures journalières ou hebdomadaires utilisées
- Exécuter des procédures et connaître la marche à suivre en cas de panne.
- Ajuster les ressources physiques et logiques aux services dégradés
- Connaître les commandes exécutées par le système

Dans ce cas, le rôle de l'auditeur pour l'audit d'un grand centre serveur est de :

- S'assurer de l'existence des documents ainsi que leur bonne tenue
- S'assurer que les plannings sont respectés
- S'assurer qu'il existe des mécanismes de secours en cas de panne
- S'assurer de l'existence de bonne méthode de travail
- S'assurer qu'il existe un contrat de maintenance.

L'auditeur se chargera de relever les points forts et les points faibles du système. L'aspect de la sécurité doit être aussi abordé notamment l'accès aux informations et dans la salle du serveur.

## *5. AUDIT DES RESSOURCES HUMAINES*

L'auditeur des ressources humaines est l'un des plus délicats dans la pratique par ce que il met en lumière l'inadéquation de la personne vis-à-vis de son poste, sa démotivation, son incompétence, etc.

Ainsi, le manque de compétence peut contribuer à une mauvaise connaissance ou utilisation du système et à une mauvaise exploitation d'utilisation de l'informatique.

En effet, dans la plupart des centres informatiques, les problèmes liés aux ressources humaines sont :

- Retard de traitement
- Etat de listing non conforme en sortie
- Etat de listing non conforme aux documents comptables
- Discordance entre les informaticiens et les utilisateurs
- Etc.

Dans ce cas le rôle de l'auditeur est de :

- Vérifier l'existence de l'organigramme clair et précis ainsi que la définition des fonctions pour chaque informaticien ou utilisateur.
- Vérifier l'existence des clauses relatives au non concurrence, la fidélité et la déontologie aux secrets professionnels
- Vérifier l'existence de plan de formation adéquat
- Vérifier l'adéquation des formations demandées vis-à-vis des besoins concernant le système informatique
- Vérifier ou sonder la motivation du personnel
- S'assurer de la compétence des agents
- S'assurer de l'existence d'une politique d'horaire cohérente
- S'assurer que seules les personnes concernées et autorisées sont dans la salle machine

# CHAP IV. PROBLEME DE SECURITE ET AUDIT ASSOCIE

**Remarque :** L'information est une des ressources primordiales et constitue une partie vitale du patrimoine de l'entreprise. Ainsi, le problème de sécurité devient de plus en plus crucial : sécurité pour la protection de patrimoine et des biens de l'entreprise pour la protection contre le vol, le sabotage et l'espionnage industriel.

Du point de vue informatique, la sécurité se base sur les audits ci-après :

- Plan de sécurité de l'entreprise
- Plan de sécurité concernant la protection des matériels et de la salle de stockage des informations
- Sécurité des matériels
- Sécurité de la documentation
- Sécurité de support d'information (les contenants)
- Sécurité dans le domaine des fichiers (les contenus de données et programmes)

## *A. PLAN DE SECURITE CONCERNANT LA PROTECTION DE MATERIEL ET DE LA SALLE DE STOCKAGE*

Ce type d'audit ne concerne que les services possédant les **"MAINFRAMES".** Ainsi, la sécurité consiste aux aspects ci-après :

- Accès de la salle : le lieu de stockage des ordinateurs ne doit pas être un lieu de passage non contrôlé (contrôle par badge, par code). Il faut éviter à tout pris de va-et-vient des personnes étrangères au service.
- Protection de la salle concernant le serveur de l'entreprise (prévoir les mécanismes d'isolations calorifiques et d'aire conditionnel)
- Prévoir le contrat d'assistance et de maintenance
- Veiller à l'alimentation électrique
- Protection contre l'incendie

- Problème de pollution et de poussière

## *B. SECURITE CONCERNANT LES FICHIERS*

Il faut éviter la perte ou la destruction accidentelle des fichiers. Réaliser toujours le Backup ou la duplication des fichiers.

- Garder les différents fichiers stockés dans les mémoires, dans les armoires hermétiquement fermé
- Veiller à la protection des données et de programmes vis-à-vis à des personnes étrangères au service.
- Protéger les postes de saisie des informations

## *C. SECURITE DES MATERIELS*

Pour les matériels, veuillez à la sécurisation du lieu où sont stockés et exploités les matériels ainsi que la documentation technique servant à exploiter les machines (Prévention et création de mot de passe qui ne doivent être connus par le personnel exploitant et par un groupe restreint.

- Contrôler les normes de ventilation
- Etc.

## *D. SECURITE DE LA DOCUMENTATION*

- Eviter l'éparpillement de la documentation notamment la documentation concernant le système d'exploitation
- Garder les documents dans des classeurs ou armoires métalliques
- Limiter la diffusion de certains documents (Problème de confidentialité)

En ce qui concerne la sécurité de support d'informatique :

- Eviter les contacts directs sur la surface magnétique
- Eviter l'exposition au soleil ou auprès de source de la chaleur
- Contrôler la température de la salle de stockage.

L'auditeur prendra soin, vérifiera et soulèvera les non conformités des éléments ci-dessus énumérés. Il en est de même pour les programmes et données.

**Remarque :** Les moyens de détection pour l'auditeur concernant le problème de sécurité sont :

- Contrôler le temps, la taille, la date de création de fichier par exemple
- Demander au constructeur de chaque système le moyen de sécurité maximale
- Sensibiliser les utilisateurs à respecter les mécanismes de procédure de sécurité prévue par l'entreprise ou de service informatique
- Utiliser aussi les normes qui existent en matière de sécurité.

## *E. AUDIT ET SECURITE DANS LE DOMAINE DU RESEAU*

Pour la sécurité dans le domaine du réseau, on recommande toujours l'utilisation de norme de sécurité. En effet, de par sa nature, un réseau informatique permet l'interconnexion de 2 ou plusieurs stations de travail d'où la facilité d'accès ou d'entrée sur un serveur sur un calculateur est réelle. De ce fait, les normes de sécurité peuvent porter sur les aspects ci-après :

- Identification de la ligne pour accéder à tel ou tel réseau
- Restriction d'accès
- Sécurité sur le transfert d'appel
- Prévision de mot de passe
- Prévoir de centre de contrôle de réseau
- Etc.

**Remarque :** Actuellement, le problème de la sécurité des réseaux est lié aux surveillances du réseau soi-même la prévention des pannes et le fonctionnement du réseau. Ainsi, les matériels à surveiller sont :

- Les matériels de transmission
- Les matériels de commutation (Problème d'adressage, table de routage, des passerelles, de pont, etc.)
- Vérifier l'état des équipements
- Vérifier les charges (nombre d'utilisateurs et des programmes)
- Vérifier la comptabilité des protocoles
- Vérifier le bon fonctionnement de signalisation d'erreur
- S'assurer de la cohérence de faille des paquets transmis et reçus

- Etc.

La plupart de ces tâches sont confiées à des sociétés de service (Voir cours de télématique et réseaux).

**2.** iblez un chapitre du cours d'audit informatique et faites un commentaire sur tous les aspects essentiels y afférent.