UNIVERSITE DE KINSHASA

FACULTE DES SCIENCES

MENTION : MATHEMATIQUES, STATISTIQUE & INFORMATIQUE

AUDIT INFORMATIQUE

Support de cours pour Etudiants de L3 LMD, préparé par :

MAPHANA ma NGUMA

Professeur

INTRODUCTION

Comme on le sait, le champ d'application de l'informatique est très vaste et couvre pratiquement tous les domaines d'activité humaine.

Dans tous ces domaines, l'ordinateur qui se trouve au centre du système de traitement automatique des données peut être utilisé:

- *soit comme un outil de gestion courante (paie, facturation, comptabilité, production des statistiques, bureautique, etc.),*
- *soit comme un outil de production (comme dans l'industrie automobile),*
- *soit comme un instrument de contrôle en temps réel de certaines activités ou situations (surveillance à distance de l'évolution de l'état des malades par exemple).*

L'utilité de l'ordinateur dans la vie des organisations n'est donc plus à démontrer.

Toutefois, avec la vulgarisation de plus en plus poussée de l'informatique, peu d'utilisateurs d'ordinateurs accordent encore une attention soutenue aux conditions d'exploitation de cet outil pour en tirer le meilleur avantage. C'est ainsi par exemple que certaines organisations achètent des ordinateurs par « suivisme », pour être à la mode, sans se soucier de l'opportunité de leur acquisition ni de leurs potentialités. Il n'est pas rare en effet de rencontrer aujourd'hui encore des organisations qui disposent d'un important parc d'ordinateurs dont la puissance installée est sous-utilisée ou qui ne sert qu'au

simple traitement de texte, alors que leur acquisition requiert la mobilisation de beaucoup moyens financiers.
Pour éviter de tels écueils, nous pensons qu'un responsable qui souhaiterait tirer profit de l'ordinateur, cet outil par excellence de traitement automatique des données, doit pouvoir procéder de temps en temps, si pas régulièrement, à ***l'audit de son système informatique afin de contrôler les conditions d'exploitation de cet outil, les causes du dysfonctionnement éventuel du système informatique ainsi que le niveau d'exécution des objectifs qui lui ont été assignés. L'objectif ultime de l'activité d'audit est de proposer des recommandations appropriées pour rendre le système informatique plus efficace.***

A cet égard, il est utile que le responsable connaisse les sources potentielles du dysfonctionnement ou de l'inefficacité d'un système informatique, de manière à lui permettre d'agir plus par prévention que par correction. L'auditeur doit aussi en être imprégné pour bien mener sa tâche. Les principales sources de son dysfonctionnement ou de son inefficacité sont :

- *la négligence dans la mise en œuvre du* ***Processus d'Implantation du Système Informatique*** *dans l'organisation ;*
- *l'absence des outils de gestion qui évite au responsable de naviguer à vue, à savoir :*

  - *le* ***Schéma ou Plan Directeur Informatique*** *: l'outil de planification de ses actions et qui permet de répondre à la question* ***Quoi*** *faire ?*
  - *la* ***Politique Informatique****, l'outil règlementant l'acquisition des ressources hardware et software des TIC au sein de l'organisation, le suivi de leur situation et de leur utilisation, leur sécurisation ainsi que leur maintenance ; cet outil permettant ainsi de répondre à la question* ***COMMENT*** *faire ?*

Au regard à ce qui précède, nous avons jugé utile de structurer la partie théorique de ce support de cours en trois chapitres comme suit :

Chapitre 1 : Processus d'implantation d'un système informatique dans une organisation

Chapitre 2 : Principaux outils de suivi et de gestion efficace des activités d'un système informatique
2.1. Le Schéma ou Plan Directeur Informatique
2.2. La Politique Informatique

Chapitre 3 : Audit d'un système informatique

2.1. Les préalables
2.2. Démarche proposée

REMARQUE

Ce support de cours constitue un « guide » ou un « fil conducteur » pour l'apprenant, à un double titre.

- *D'abord, il est structuré et présenté sous forme d'un canevas, sans beaucoup de détails sur le contenu des rubriques renseignées. Les commentaires enrichissants y relatifs seront faits lors des séances théoriques animées par le Professeur.*
- *Ensuite, les contenus des trois chapitres de ce document ne constituent pas des recettes applicables sans discernement. Il s'agit des méthodologies proposées pour bâtir des solutions adaptées à l'organisation concernée et susceptibles de contribuer à l'amélioration de l'efficacité de son système informatique.*

Chapitre I

PROCESSUS D'MPLANTATION D'UN SYSTME INFORMATIQUE DANS UNE ORGANISATION

La mise en place d'un système informatique ne s'improvise pas et doit être conduite de manière réfléchie. On propose dans ce chapitre une procédure avec des étapes logiquement agencées qu'il est recommandé de respecter lors de l'implantation d'un système informatique dans une organisation, si on souhaite que ce dernier joue efficacement son rôle.

1.1. Première étape : ORGANISATION DES ETUDES

1.1.1. Mise en place du Comité informatique

A. Missions

a) définir les termes de référence des études (domaines à informatiser, objectifs à atteindre, délai de réalisation des études)
b) choisir les Experts
c) composer les Groupes de travail
d) allouer les ressources nécessaires pour la réalisation des études
e) contrôler l'état d'avancement des études
f) choisir, parmi les solutions alternatives proposées par les Experts, celle qui paraissent la mieux appropriée eu égard aux objectifs de l'organisation.

B. Composition

- le responsable numéro 1 de l'organisation (exemple : PDG d'une entreprise, Secrétaire Général d'un Ministère, etc…) ou son représentant car la décision prise par ce Comité engage l'organisation
- les responsables fonctionnels concernés par les applications à informatiser, car ils connaissent mieux les problèmes spécifiques des services qu'ils encadrent
- le responsable ou le futur responsable du CTI (c'est le technicien du groupe qui pourra donner un avis autorisé notamment sur la configuration informatique proposé par les Experts) ;
- le responsable financier de l'organisation qui détient les cordons de la bourse.

1.1.2.Choix des Experts

A. Missions

Réaliser les études d'informatisation conformément aux termes de référence définis par le Comité Directeur.

Le contenu de ces études concerne les autres étapes du processus.

B. Composition

- Soit deux ou trois membres du personnel mis full time à disposition de l'opération « études d'informatisation ».
- Soit, en cas de non disponibilité du personnel interne, recours à des Experts externes.

C. Remarques

- le terme « Expert » désigne toute personne qui, par son expérience ou sa pratique ainsi que par ses connaissances théoriques sur un domaine précis, a acquis une grande habileté pour résoudre les problèmes qui se posent dans ce domaine.

- La qualité d'Expert n'est nullement liée à la nationalité d'origine de l'individu, ni à la pigmentation de sa peau.

- Les Experts externes peuvent être pris individuellement ou dans le cadre des Bureaux d'Etudes et de Conseils en informatique au sein desquels ils œuvrent. Dans tous les cas, ils doivent travailler en groupe de deux personnes au moins pour réaliser les études d'informatisation commandées.

- Les Experts externes peuvent être retenus soit de gré à gré, soit à l'issue d'un appel d'offre ouvert ou restreint.

- Profil nécessaire pour être retenu comme Expert pour réaliser des études d'informatisation des systèmes : Ingénieur conseil en informatique. A ce titre, il doit être à même de :

  - analyser correctement le système d'information concerné ;
  - définir la configuration informatique appropriée pour le système étudié ;
  - circonscrire la structure des données et des applications à informatiser.

  En outre, il doit jouir d'une grande expérience dans les domaines renseignés ci-dessus.

1.1.3.Organisation des Groupes de travail

A. Missions

a) décrire l'existant sous la conduite des Experts

b) Exprimer les besoins réels des services concernés par l'informatisation

c) Participer à la définition des solutions aux problèmes rencontrés par les services.

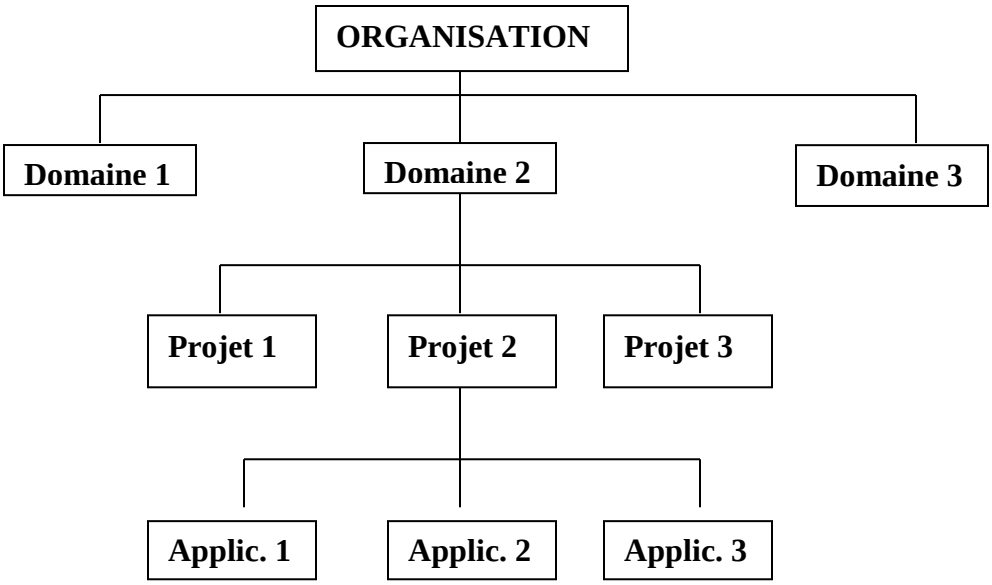
B. <u>Composition</u>

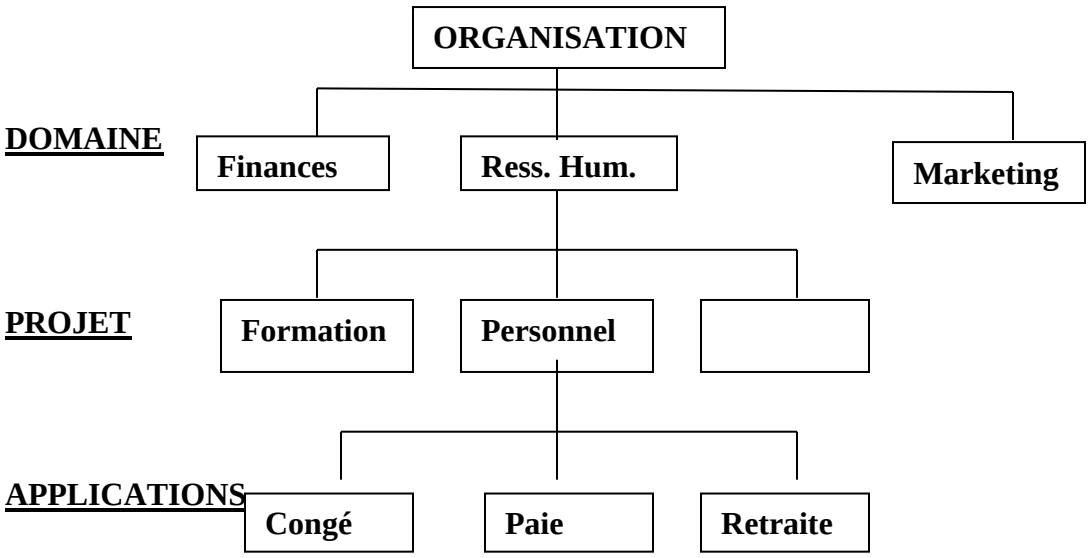
Il peut y avoir autant de Groupes de travail qu'il y a de services à informatiser. Chaque Groupe de travail comprendra 4 à 5 personnes œuvrant au sein d'un service donné.

A ce sujet, il y a lieu de noter que (voir les deux schémas de la page suivante) :

- une organisation peut comprendre plusieurs domaines ;
- un domaine peut regrouper en son sein plusieurs projets ;
- un projet peut comporter plusieurs applications.

Aussi, les groupes de travail peuvent être créés soit au niveau des domaines, soit à celui des projets, soit encore à celui des applications ; cette dernière option devant toutefois être privilégiée.


ORGANISATION
Domaine 1
Domaine 2
Domaine 3
Projet 1
Projet 2
Projet 3
Applic. 1
Applic. 2
Applic. 3


ORGANISATION
DOMAINE
Finances
Ress. Hum.
Marketing
PROJET
Formation
Personnel
APPLICATIONS
Congé
Paie
Retraite

1.2. Deuxième étape : ETUDE PREALABLE ET ANALYSE GENERALE DES BESOINS

1.2.1. Objectifs

- Faire une analyse critique du système d'information en place afin de mettre en évidence les principaux problèmes d'organisation et de gestion qui s'y posent ;

- Formuler la solution globale (tout en la justifiant) pour résoudre les problèmes identifiés et satisfaire au mieux les besoins recensés.

- Faire l'inventaire des besoins insuffisamment satisfaits ainsi que les nouveaux besoins à satisfaire ;

En fait, les deux premiers objectifs correspondent à l'étude préalable à l'issue de laquelle on doit répondre à la question de savoir s'il est opportun ou non de recourir à la solution informatique pour résoudre les problèmes identifiés et satisfaire au mieux les besoins recensés.

1.2.2. Etude préalable

A. Analyse de l'existant

L'analyse de l'existant porte notamment sur les points suivants :

a) la présentation de l'organisation à travers ses missions et ses activités

L'étude d'un système doit toujours débuter par le rappel des missions qui lui sont assignées ainsi que des tâches qu'il est appelé à exercer dans le cadre de ces missions.

La connaissance approfondie des missions et des activités de l'organisation permet d'avoir une idée sur les besoins de gestion des flux d'information et de choisir en conséquence les moyens humains et matériels appropriés dont elle doit disposer, en l'occurrence les moyens informatiques, pour pouvoir les satisfaire au mieux.

b) la structure organique et les relations entre services

L'étude de l'organigramme permet de comprendre les procédures administratives utilisées, la raison d'être de certains documents, les relations entre services et même entre personnes.

Ici, il y a lieu d'approfondir l'étude des services et des postes directement concernés par l'informatisation. On pourra notamment déceler les postes surchargés et qui constituent des goulots d'étranglement dans le système, les principaux défauts de l'organisation en place, les aptitudes et insuffisances des agents qui occupent les postes étudiés.

c) Les documents et fichiers utilisés

L'étude des documents et des fichiers existants permet souvent de détecter certaines causes de dysfonctionnement de la gestion administrative de l'organisation imputables aux documents et fichiers tenus manuellement.

Pour ce qui est des documents, l'étude doit pouvoir préciser notamment :

- le relevé des documents utilisés ;
- leur regroupement par domaine ;
- leur périodicité ou leur fréquence d'utilisation ;
- le nombre de copies de chaque document émis;
- l'objet de chaque document ;

- la provenance, la destination et le circuit de circulation des documents (on peut ici élaborer le diagramme des flux d'information) ;
- le temps de traitement de chaque document ;
- les documents inexistants, mais jugés indispensables ; etc…

En ce qui concerne les fichiers, qu'ils soient manuels ou informatiques, on peut épingler leur volume, leurs modes d'organisation et d'accès, les supports de stockage, etc …

d) les moyens de traitement utilisés

Il s'agit des moyens humains et matériels en place. Cette étude s'appesantira notamment sur :

- leur nombre,
- leurs caractéristiques et leurs performances,
- leur coût.

e) les applications opérationnelles

Il y a lieu de préciser pour chaque application :

- les besoins satisfaits, totalement ou partiellement,
- le langage de programmation utilisé,
- l'option de traitement utilisé,
- les modalités de stockage, d'organisation et d'accès des fichiers.

f) les performances globales du système en place

L'analyse portera ici sur des données quantitatives, telles que les temps de réponse au terminal, le délai de production des documents, les coûts d'exploitation et de maintenance, mais aussi sur des facteurs intangibles tels que la qualité des résultats obtenus, son degré de satisfaction sous l'angle de l'utilisateur, etc…

B. Critique de l'existant

Le diagnostic fait sur la situation présente doit permettre de dégager ses points forts et ses points faibles. Pour ce qui est de ce dernier aspect, on doit dresser la liste des anomalies constatées et essayer de dégager les causes profondes de ces anomalies.

La critique doit concerner l'ensemble des points traités dans l'analyse de l'existant. A l'issue de cette critique, on doit mettre en évidence :

- les besoins insuffisamment satisfaits par les procédures existantes ;
- les besoins nouveaux à satisfaire.

C. Proposition de la nouvelle solution globale

A la fin de l'étude préalable, les experts doivent répondre à ces deux questions fondamentales :

- est-il opportun d'abandonner les procédures de traitement actuelles ?
- Si oui, quelle solution doit-on envisager ?

A cet égard, trois alternatives sont possibles :

- Soit le maintien du statu quo ; ce qui entraîne l'arrêt des études en cours.
- Soit une solution non informatique, mais avec quelques aménagements notamment la réorganisation des services, des postes de travail et des circuits de circulation des documents.
- Soit une solution informatique.

L'alternative à retenir doit permettre aux utilisateurs de rencontrer leurs souhaits ou objectifs poursuivis, qu'il convient de rappeler ici même en termes généraux. Par exemple :

- Nécessité d'obtenir des statistiques fiable de manière régulière ;
- Nécessité de contrôler les recettes réalisées ;
- Nécessité de réduire le temps d'attente des clients ;
- Nécessité de produire les factures à temps ; etc…

Remarque :
Bien que moins coûteuse à court terme, la solution manuelle comporte cependant un inconvénient majeur : risque de saturation à moyen terme, si le volume d'informations à traiter s'accroît.

La solution informatique quant à elle fait gagner du temps et donne des résultats fiables. Elle peut paraître certes paraître coûteuse à court terme, mais elle s'avère généralement rentable à moyen terme.

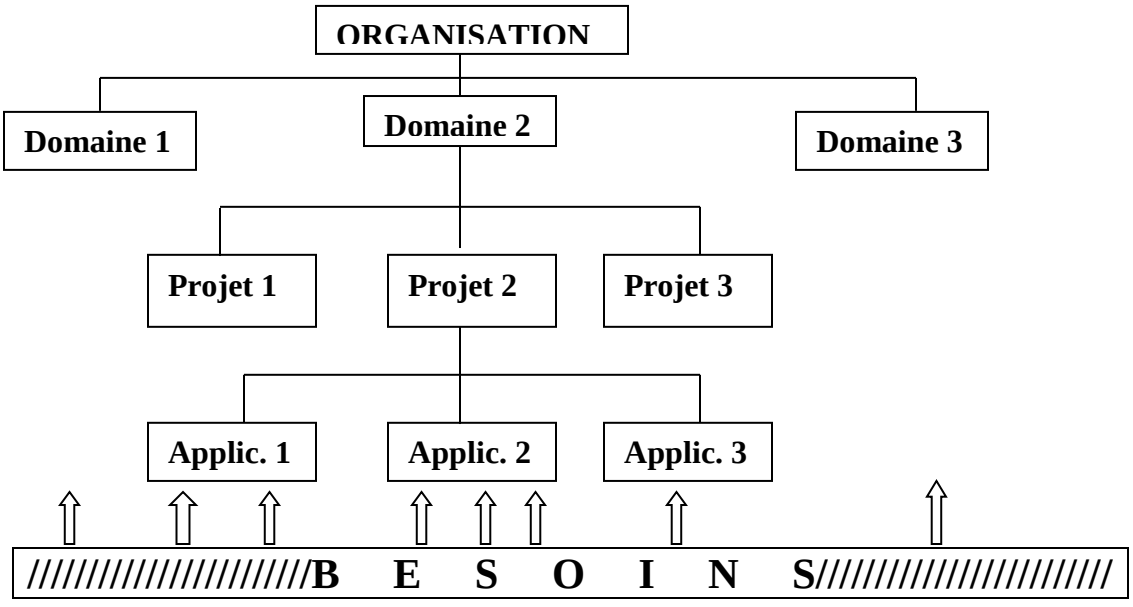
1.2.3. Analyse des besoins

A. Besoins en équipements et matériels de télématique

- Matériels de bureautique et logiciels requis
- Equipements et matériels des réseaux de télématique et logiciels requis

B. Besoins en applications de gestion et outils de développement des programmes et SGBD requis

- Identification des applications de gestion dans une organisation (voir schéma ci-après)



- **Regroupement des applications en Projets et en Domaines**

Avantages de ce regroupement :

- Possibilité de confier leur mise en œuvre à un seul responsable ; ce qui facilite le suivi ;
- Possibilité d'établir des liens dans le cadre d'une BDD ;
- Possibilité de planifier leur mise en œuvre en commençant par les domaines les plus prioritaires
- Possibilité de créer des bases des données communes aux applications relevant d'un même projet ou domaine.

C. Besoins en ressources humaines et en formation

1.3. Troisième étape : ELABORATION DU DOSSIER D'APPEL D'OFFRES POUR L'ACQUISITION DU SYSTEME INFORMATIQUE

Le dossier d'appel d'offres (DAO) comprend quatre éléments ou groupes d'éléments :

- le cahier des charges
- le cahier des prescriptions spéciales aux soumissionnaires
- les formulaires de soumission
- les critères d'évaluation et leurs pondérations respectives

1.3.1. Cahier des charges

Il s'agit d'un document dans lequel le maître d'ouvrage décrit les spécificités d'un travail qu'il compte faire exécuter par une personne physique ou morale, tout en y définissant les conditions techniques, financières ou autres à requises à cet effet de la part cette dernière.

Le cahier des charges doit contenir au moins les éléments suivants :

- une synthèse des besoins à satisfaire par le maître d'ouvrage en matière de traitement automatique de l'information, tels qu'ils résultent de la première étape du processus d'élaboration du SDI ;
- une synthèse des applications et des caractéristiques des fichiers, tel que cela résulte de la deuxième étape du processus d'élaboration du SDI ;
- un cahier des prescriptions techniques décrivant les spécificités du hardware et des performances des systèmes d'exploitation ;
- la définition des clauses contractuelles que devra respecter le soumissionnaire pour être retenu, notamment : la période de garantie, la période de réception provisoire avant la réception définitive, les modalités d'entretien préventif, les délais de livraison, etc…

1.3.2. Cahier des prescriptions spéciales aux soumissionnaires

Il contient un ensemble de prescriptions que les soumissionnaires doivent respecter pour garantir la validité de leurs offres. Elles portent notamment sur :

- la période de validité de l'offre,
- l'adresse du dépôt des réponses à l'appel d'offre,
- les modalités d'expédition des offres,
- le nombre d'exemplaires requis,.

1.3.3. Les critères d'évaluation des offres et leurs pondérations respectives

Pour des raisons d'objectivité et de transparence, il est utile de porter à la connaissance des soumissionnaires les critères à partir desquels leurs offres seront appréciées. Par ailleurs, ces critères seront associés de leurs pondérations respectives, traduisant l'importance intrinsèque que le maître d'œuvre ou d'ouvrage du projet attache à chacun d'eux. Ainsi, chaque soumissionnaire pourrait, à son niveau, se faire une idée sur les chances de succès ou les risques de rejet de son offre.

Ces critères peuvent être quantitatifs (délai de livraison, performances des matériels informatiques, période de garantie, par exemple) ou qualitatifs (engagements sur la formation du personnel informaticien et de réaliser régulièrement l'entretien préventif des équipements proposés, par exemple).

1.3.4. Les formulaires de soumission

Le maître d'œuvre ou d'ouvrage peut se retrouver, dans le cas d'un appel d'offres ouvert, devant plusieurs offres à analyser, parfois volumineuses, présentées dans des formats différents. Ce qui rend fastidieuse leur analyse. D'où l'intérêt de joindre dans le DAO des formulaires standard sur lesquels les candidats devront renseigner les informations pertinentes concernant le système proposé ; chaque formulaire devant se rapporter à un critère d'appréciation donné. Cette approche facilitera à coup sûr le dépouillement des offres reçues.

1.4. Quatrième Etape : DEPOUILLEMENT DES OFFRES RECUES

Le dépouillement est toujours précédé de l'ouverture publique des offres reçues, devant au moins tous les soumissionnaires ou leurs représentants ; question de prouver la bonne foi de l'acheteur qui garantit par là une concurrence loyale entre tous les candidats.

Le dépouillement lui-même est une opération délicate qui est généralement confiée à toute une commission pour garantir une plus grande objectivité.

Pour plus d'objectivité dans la démarche à suivre, la comparaison des offres reçues qui aboutira au choix de la configuration informatique appropriée au regard des spécificités du cahier des charges peut se faire en utilisant une méthode d'analyse multicritère agrégative, étant donné le nombre élevé des points de vue à prendre en compte (méthodes basées sur les moyennes arithmétiques, géométriques ou distances pondérées, méthode AHP, méthodes Electre, etc…).

1.5. Cinquième Etape: PREPARATION DE L'ENVIRONNEMENT D'ACCUEIL

Il s'agit de l'environnement physique et de l'environnement organisationnel.

1.5.1. Sur le plan physique

Il y a lieu de préparer la salle machine pour sécuriser les ordinateurs contre la poussière, l'humidité, l'inondation, l'incendie, la forte chaleur, les coupures intempestives du courant ou les variations incontrôlées de la tension électrique, par exemple.

1.5.2. Sur le plan organisationnel

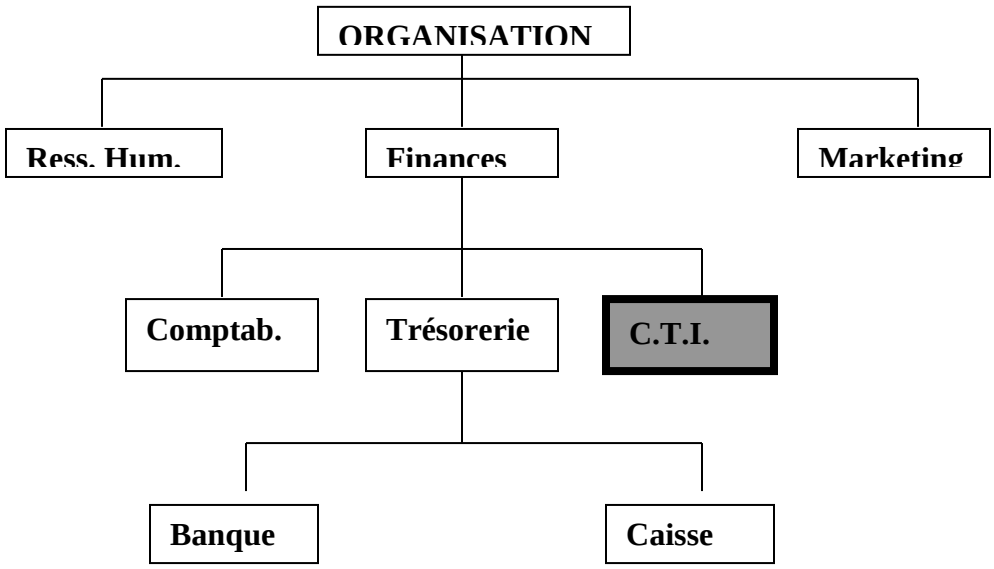
Ici il y a lieu de veiller particulièrement à la forme de dépendance hiérarchique du CTI, à l'élaboration d'un organigramme fonctionnel approprié du CTI et à la définition des attributions spécifiques des postes retenus.

A. Problématique de la dépendance hiérarchique du CTI

L'implantation ou l'introduction d'un système informatique dans une organisation implique souvent la révision des structures en place, notamment pour y intégrer de CTI. Dans ce cadre, il se pose souvent un problème de positionnement du CTI par rapport aux autres entités de la nouvelle structure.

A cet égard, deux alternatives peuvent être envisagées :

1°) *Faire dépendre le CTI d'une des directions fonctionnelles*



Historiquement parlant, c'est la première forme de dépendance hiérarchique à laquelle on a assisté lors de l'introduction de l'informatique dans les entreprises. Le CTI dépendait en effet de la direction (ou du service) dont relèvent les principales applications informatisées. Il s'agissait le plus souvent de la Direction financière, étant donné le caractère stratégique de ses applications pour l'entreprise (comptabilité, gestion de la trésorerie, gestion des fournisseurs, etc…).

Si cette forme de dépendance peut se justifier dans certains cas (comme les fiduciaires), il en va autrement dans d'autres organisations, en particulier les entreprises industrielles et commerciales, pour des raisons ci-après :

- risque de marginalisation d'autres applications, sans doute aussi ou plus importantes que d'autres applications financières. On sait en effet que le champ d'application de l'informatique couvre pratiquement tous les domaines de gestion et de l'activité humaine (gestion financière, du personnel, des stocks, des clients, etc…) ;

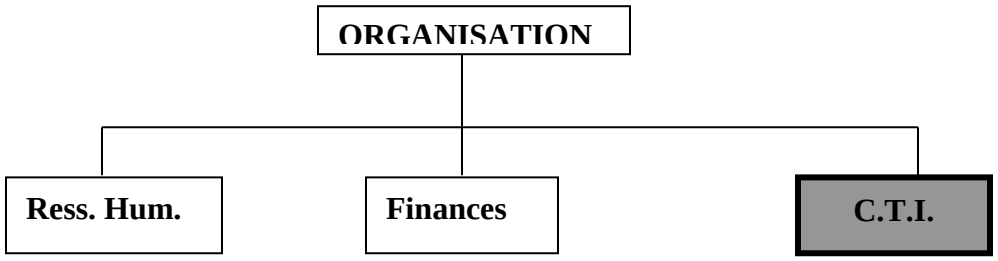
- sentiment de frustration de la part des autres responsables obligés de passer par leur Collègue Directeur financier pour solliciter l'informatisation des applications relevant de leurs secteurs respectifs.

En dépit de ces inconvénients, plusieurs entreprises de la place appliquent toujours cette forme de dépendance hiérarchique pour leurs CTI.

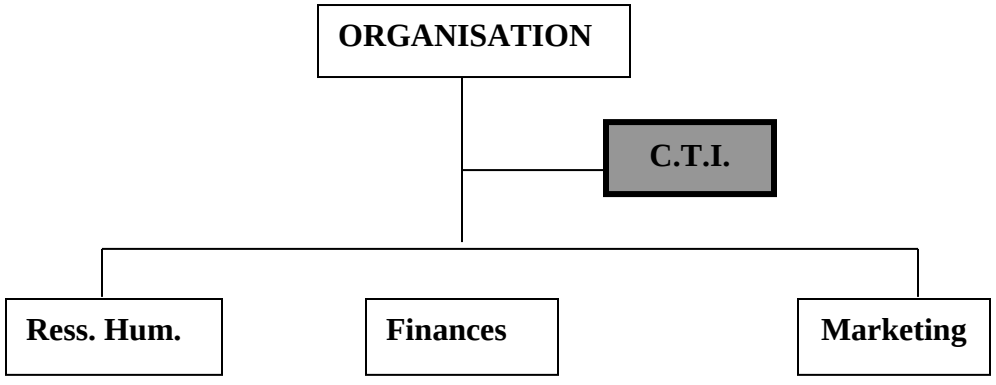
2°) *Faire dépendre le CTI directement du premier responsable de l'organisation*

Deux formules sont envisageables :

- Placer le CTI au même niveau que les Directions fonctionnelles



- Placer le CTI au niveau de l'Etat Major du PDG

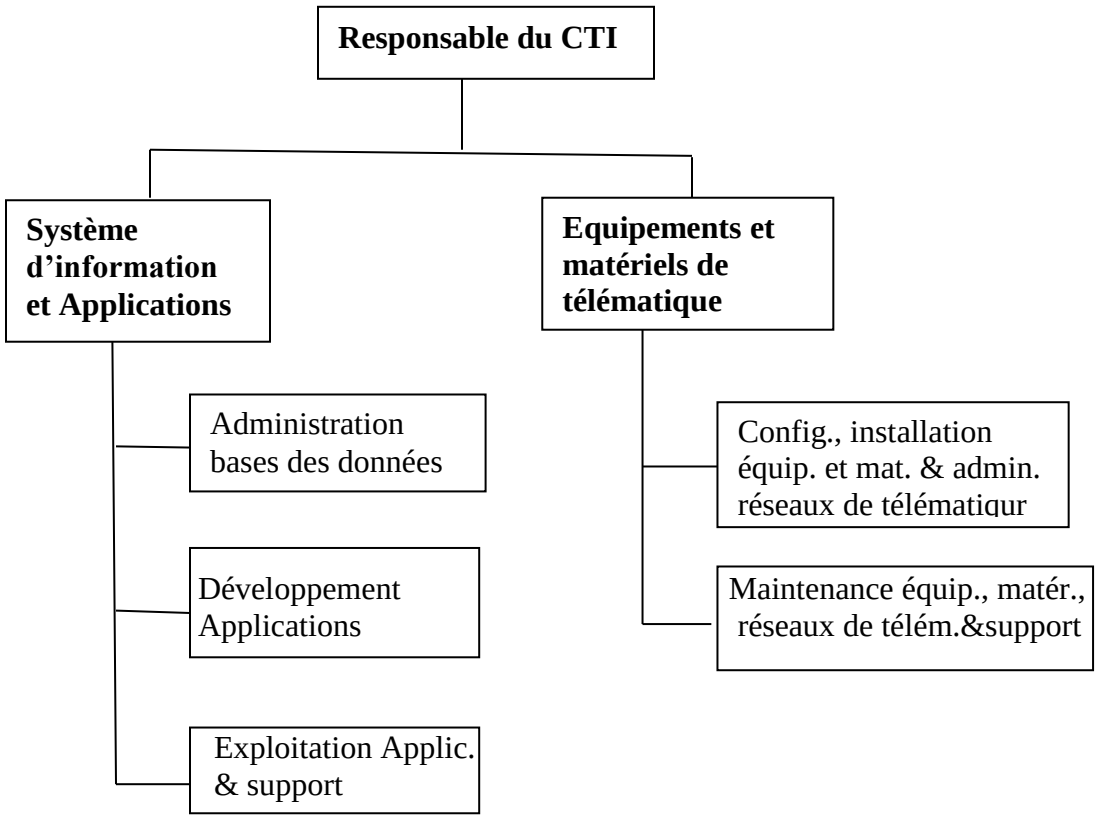


Les deux formules de cette dernière alternative présentent plusieurs avantages :

a) elles valorisent davantage la fonction Informatique dans l'entreprise ;
b) elles annihilent les inconvénients évoqués plus haut, puisque :
   - elles suppriment tout sentiment de frustration de la part des responsables fonctionnels ;
   - elles placent toutes les applications sur un même niveau.
   - elles conviennent mieux dans le cadre d'une informatique décentralisée ou répartie.

B. Macro - structure du CTI

La macro - structure proposée ci-dessous ne peut être considérée comme figée ; elle doit être adaptée à l'organisation en tenant compte de sa taille, de la nature de ses activités, de son implantation géographique et de l'importance du parc informatique acquis.



C. Attributions et spécifications des tâches

Par spécifications des tâches, on désigne les principales exigences ou qualifications requises pour exercer les tâches analysées.

1°) *Responsable du CTI*

- **Attributions**

  - Superviser l'activité du CTI
  - Entretenir les relations avec les partenaires extérieurs, en accord avec ou sous couvert de la hiérarchie. Ces partenaires sont essentiellement : les vendeurs des matériels et logiciels informatiques, les fournisseurs des consommables et services informatiques divers, les clients.
  - Faire rapport à la hiérarchie sur l'activité du CTI.

- **Qualifications requises**

  - Formation académique : niveau de licence ou d'ingénieur au moins ;
  - Formation en informatique : Ingénieur concepteur ou système
  - Expérience exigée.

2°) *Responsable des systèmes d'information et des applications*

- **Attributions**

  - Superviser la conception, le développement et l'exploitation de l'ensemble des applications à informatiser ;
  - Répondre de l'activité de son secteur au Responsable du CTI.

- **Qualifications requises**
  - Formation académique : niveau de licence ou d'ingénieur au moins ;
  - Formation en informatique : Ingénieur concepteur
  - Expérience exigée.

3°) *Responsable des équipements, matériels et réseaux de télématique*

- **Attributions**

  - Superviser les activités de configuration, d'installation, de sécurisation et de maintenance des équipements, matériels et réseaux de télématique ;
  - Administrer les réseaux des télématique ;
  - Répondre de l'activité de son secteur au Responsable du CTI.

- **Qualifications requises**

  - Formation académique : niveau de licence ou d'ingénieur au moins ;
  - Formation en informatique : Ingénieur système
  - Expérience souhaitée.

1.6. Sixième Etape : RECRUTEMENT ET FORMATION DU PERSONNEL

Il s'agit bien sûr du personnel informaticien d'abord. On recrute si l'entreprise n'en dispose pas ; on forme selon les spécificités de la nouvelle configuration informatique acquise dans le cas contraire.

La formation doit aussi intéresser les utilisateurs qui sont obligés d'être à la page.

1.7. Septième Etape : RECEPTION PROVISOIRE ET DEFINITIVE DU NOUVEAU SYSTEME

La période de réception provisoire est celle pendant laquelle l'acquéreur du nouveau système vérifie la conformité du système acquis par rapport aux spécificités du cahier des charges. En cas de discordance, il est autorisé à restituer et l'élément non conforme au vendeur qui est obligé de procéder à son remplacement.

Lorsque plus tard intervient la réception définitive, toute défaillance ne pourra plus être réclamée au vendeur.

Il ne faudra pas confondre la période de réception provisoire de celle de garantie, même si ces deux périodes peuvent coïncider dans le temps. La période de garantie concerne les pannes dont la réparation incombe au vendeur, à moins qu'il ne soit prouvé qu'elles sont imputables à une mauvaise utilisation, par l'acheteur, de l'équipement acquis.

1.8. Huitième Etape : LANCEMENT DU NOUVEAU SYSTEME EN PARALLELE AVEC L'ANCIEN DANS UN PREMIER TEMPS

On n'abandonne jamais les procédures manuelles ou anciennes de traitement de l'information dès l'acquisition du nouveau système informatisé. Un temps d'adaptation est nécessaire pendant lequel les deux systèmes peuvent momentanément cohabiter, notamment dans le but de tester la fiabilité des résultats fournis par le nouveau système.

Chapitre 2

PRINCIPAUX OUTILS DE GESTION EFFICACE D'UN SYSTEME INFORMATIQUE

2.1. LE SCHEMA OU PLAN DIRECTEUR INFORMATIQUE DE L'ORGANISATION

2.1.1. Définition, horizon temporel et utilité

Le Schéma Directeur Informatique (SDI) est un programme d'action à moyen terme contenant l'ensemble des activités à mener pour la mise en œuvre progressive et le développement d'un système d'information informatisé dans une organisation.

Il peut donc être révisé à l'issue de l'horizon temporel défini. Sa durée de validité doit être supérieure à un an, car le SDI a un caractère prospectif, et ne devrait pas, en principe, dépasser 4 ans puisque l'informatique est un secteur d'activité très évolutif.

L'importance du SDI réside dans le fait qu'il constitue un outil de planification qui fixe, pour l'horizon temporel défini et après appréciation de la situation de départ, les objectifs à atteindre, les stratégies à adopter à cet effet, les actions à entreprendre, les moyens matériels, logiciels, humains et financiers requis ainsi que le calendrier de mise en œuvre. Il constitue donc un guide ou une boussole indispensable dont doit se servir tout responsable pour éviter de « naviguer à vue ».

2.1.2.Contenu du SDI

Les éléments constitutifs du SDI peuvent être regroupés en 5 volets.

2.1.2.1. Eléments issus de l'analyse de l'existant

A. Informations à recueillir

Il est question ici de recueillir d'abord le maximum d'informations pertinentes pour appréhender le degré d'inadéquation entre, d'une part, la situation du système informatique en place en termes d'efficacité, et, d'autre part, les besoins de l'organisation. Ces informations portent sur la situation de chaque type des ressources hardware et software, regroupées dans les trois premières composantes du système informatique ci-dessous ainsi que sur la situation des ressources humaines disponibles au niveau de service informatique, s'il existe déjà.

- Concernant les infrastructures de télématique (matériels de bureautique, équipements et matériels de connexion aux réseaux de télématique, dispositifs de protection physique des infrastructures de télématique) :

  - *nombre, état, spécifications techniques et efficacité*.

- Concernant les logiciels-systèmes (systèmes d'exploitation ; progiciels de service : logiciels de bureautique, de protection des données, de monitoring du réseau, etc…) :

  - *efficacité, fonctionnalités, version et période de validité de la licence d'utilisation*.

- Concernant les logiciels d'applications pour utilisateurs :

  - Pour les applications de communication locale *: efficacité ;*

- Pour les applications de gestion : *domaines de gestion informatisés, outils de développement des programmes, fonctionnalités intégrées, SGBD utilisés ;*
- Pour les deux types d'applications : *degré de satisfaction des utilisateurs, niveau de protection des données des utilisateurs contre les virus et les intrus*.

- Concernant la situation des ressources humaines du service informatique :
  - *Effectif, compétences, niveau de formation*.

B. Actions d'informatisation à entreprendre

On identifie ensuite les actions d'informatisation à entreprendre pour combler les insuffisances ou les lacunes mises en évidence et rencontrer ainsi ou satisfaire au mieux les besoins de l'organisation dans ce domaine.

2.1.2.2. Objectifs poursuivis

Ils doivent être formulés en termes de *résultats attendus* si, grâce aux actions à mener, on arrivait à combler les insuffisances ou les lacunes mises en évidence lors de l'analyse de l'existant et à satisfaire ainsi les besoins d'informatisation de l'organisation.

2.1.2.3. Les projets à réaliser et les coûts correspondants

Les actions à mener sont traduites en projets avec leurs durées et coûts respectifs de réalisation.

Pour des raisons de clarté dans la présentation du document, les projets sont regroupés dans les Axes spécifiques, en fonction de certains critères choisis (nature des projets, localisation des projets, etc…). Ce regroupement ne correspondra donc pas nécessairement aux différentes phases de leur réalisation.

2.1.2.4. Les modalités pratiques de mise en œuvre

Les modalités pratiques de mise en œuvre du SDI sont des indications sur :

- Les étapes de réalisation du SDI, dans l'ordre de priorité établie ;
- La durée globale de réalisation du SDI ;
- La procédure du choix des partenaires extérieurs pouvant accompagner le service informatique dans la mise en œuvre du SDI ;
- Les sources de financement des projets.

2.1.2.5. Les annexes

Elles sont constituées des documents de présentation des projets ou cahiers des charges élaborés pour chacun d'eux.

2.2. LA POLITIQUE INFORMATIQUE DE L'ORGANISATION

2.2.1. Généralités sur la politique informatique

2.2.1.1. Définition de la politique informatique

La politique informatique est l'ensemble des procédures, directives, principes ou règles de bonne pratique dont la mise en œuvre, par le Service Informatique, permet une gestion efficace du système informatique au sein d'une organisation.

De manière générale, la gestion peut être définie comme l'art de combiner harmonieusement et d'exploiter rationnellement les ressources matérielles, immatérielles, humaines et financières d'une organisation afin d'atteindre les objectifs qu'elle s'est assignés.

Dans un système informatique, les ressources matérielles et immatérielles forment ce qu'on appelle le parc informatique, et les ressources humaines sont les experts informaticiens du Service Informatique.

2.2.1.2. Parc informatique

A. Définition

Plusieurs définitions ont été données sur la notion de parc informatique d'une organisation. On peut citer quelques-unes :

1°) le parc informatique d'une organisation est un assemblage parfois hétéroclite de matériels et de logiciels accumulés tout au long des années.
2°) le parc informatique d'une organisation est l'ensemble des équipements et logiciels informatiques de cette organisation ;

3°) le parc informatique d'une organisation est l'ensemble des matériels et logiciels informatiques reliés au réseau. Il est géré par un administrateur réseau.

La première définition paraît plus explicite par rapport aux deux autres dans la mesure où elle rend mieux l'idée du parc considéré comme le patrimoine informatique de l'organisation.

B. Composition du parc

Les matériels du parc informatique peuvent être regroupés comme suit :
- matériels de bureautique,
- équipements et matériels de connexion au réseau de télématique et d'interconnexion des sites.

Les logiciels du parc informatique sont tous les programmes ou software utilisés dans différentes applications pour un bon fonctionnement de l'organisation. Il n'existe que deux types de logiciels : les programmes applicatifs et ceux qu'on qualifie de système.

Cependant dans le contexte de la gestion d'un parc informatique, on peut classer les logiciels en trois catégories :
- les programmes destinés aux activités professionnels (ex. bureautique) ;
- les programmes dédiés à l'opérationnalité des machines, comme les systèmes d'exploitation ou les anti-virus ;
- les applicatifs (applications de gestion, etc…).

C. Parc informatique uniforme

L'uniformisation du parc informatique est constatée au niveau des spécifications techniques et des caractéristiques de chaque catégorie des ressources hardware et software. A titre illustratif, tous les services utilisent des imprimantes de même marque et de même type ; tous les ordinateurs fixes et portables sont dotés d'un même type et d'une même version du système d'exploitation.

L'uniformisation des spécifications techniques et caractéristiques par catégorie de ressources hardware et software est recommandée pour des raisons de compatibilité, de facilité de maintenance et même d'acquisition dans la mesure où on pourrait s'adresser directement aux fabricants, avec tous les avantages inhérents à cette formule d'achat (exemples : obtention des remises ou des ristournes, livraison à domicile).

2.2.1.3. Activités relevant de la gestion de ressources du système informatique

Les préoccupations du Service Informatique en matière de gestion du système informatique doivent être focalisées sur la réalisation des activités suivantes en ce qui concerne chaque catégorie de ressources :

A. Concernant les ressources du parc informatique :

Le parc informatique est l'élément clé du bon fonctionnement d'un système d'information : il doit dès lors faire l'objet d'une surveillance de tous les instants. Sa bonne gestion doit intégrer le suivi des matériels et logiciels du patrimoine informatique de l'organisation pour, d'une part, en donner une vue globale de l'état et des coûts d'utilisation et, d'autre part, entreprendre les actions requises afin de garantir l'optimisation du système informatique et la continuité des services.

Les activités à réaliser en rapport les ressources du parc informatique sont :

- *leur acquisition,*
- *le suivi de leur état,*
- *la configuration et l'optimisation du réseau*
- *leur utilisation,*
- *leur sécurité et*
- *leur maintenance*.

B. Concernant les ressources humaines

La politique informatique de l'organisation intègre aussi les règles de gestion des experts informaticiens du Service Informatique. En effet, la mise en œuvre de la Politique Informatique et même son adaptation aux besoins de cette organisation et des évolutions technologiques enregistrées dans le secteur leur incombent. Par ailleurs, ce personnel opère dans un secteur d'activité qui connaît une évolution fulgurante chaque année, chaque mois et même chaque jour. Une attention particulière doit dès lors être portée sur les activités suivantes les concernant :

- *leur embauche et*
- *leur formation professionnelle permanente*,

C. Concernant les ressources financières

L'argent c'est le nerf de la guerre, dit-on. Ceci est aussi vrai dans le domaine de l'informatisation d'une organisation. On a effectivement besoin mobiliser les moyens financiers suffisants et surs pour réaliser le programme d'action élaboré par les actions prévus dans le SDI, mais aussi pour garantir l'application effective de la politique informatique de l'organisation sur de terrain. Celle-ci requiert la mise à disposition des frais réaliser les activités telles que la maintenance des matériels du parc informatique, la formation et le perfectionnement des experts informaticiens du Service Informatique, les formations permanentes des utilisateurs des matériels et logiciels de bureautique, la constitution des stocks de sécurité des matériels du parc informatique et des pièces de rechange nécessaires, etc…

Ici, l'attention du Service Informatique portera principalement sur :

- *Le suivi de la mobilisation des ressources internes ;*
- *La recherche des sources de financement complémentaires.*

Les procédures, directives, principes ou règles de bonne pratique, formant la politique informatique de l'organisation, ont donc pour point de chute les activités référencées ci-dessus.
Le respect, par la Service Informatique, de la politique informatique définie, permettra à ce dernier de réaliser convenablement ces activités pour répondre favorablement aux attentes des utilisateurs du système informatique.

2.2.1.4. Tâches spécifiques en rapport avec chaque activité identifiée

Il est question dans les lignes qui suivent de préciser, pour les différentes activités relevant de la gestion du système informatique, les tâches spécifiques à réaliser et dont la mise en œuvre doit être règlementée pour plus d'efficacité. Il s'agit principalement des tâches spécifiques ci-après :

A. Concernant l'acquisition du parc informatique

- Elaborer les spécifications techniques et caractéristiques des éléments du parc informatique à acquérir ;
- préparer et lancer les appels d'offres ;
- analyser des offres reçues et choisir les fournisseurs.

B. Concernant le suivi de la situation du parc informatique

- Se doter d'un outil de suivi en temps réel de la situation du parc informatique ;
- Faire l'inventaire du parc informatique ;
- Procéder au renouvellement du parc informatique ;
- Constituer les stocks de sécurité des différents matériels ;
- Constituer le répertoire des éléments du parc informatique ;
- Disposer des outils de contrôle de qualité du service rendu par les éléments du parc informatique ;
- Procéder à la répartition ou affectation des éléments du parc informatique par site et par utilisateur.

C. Concernant le suivi de l'utilisation du parc informatique

- Définir les droits d'accès au réseau de télématique de l'organisation ;
- Définir les règles d'éthique pour l'utilisation du réseau de télématique de l'organisation.

D. Concernant la sécurité du parc informatique

- Equiper le local technique de manière à offrir toutes les garanties de sécurité requise pour protéger physiquement les matériels du parc informatique du data center de l'organisation (système d'alimentation électrique, de climatisation, outils de détection et de lutte contre l'incendie, etc…) ;
- Prendre des dispositions pour sécuriser les matériels de bureautique, le réseau et les données stockées contre les virus et toutes sortes d'attaques ou intrusions venant de l'extérieur ;
- Mettre en place des systèmes redondants de connexion Internet ou Intranet, de traitement et de sauvegarde des données stockées afin d'assurer la continuité des services en cas d'incident grave sur les équipements de transmission, de traitement ou de stockage en cours d'utilisation.
- Prendre des mesures pour la mise à jour des versions des systèmes d'exploitation, des anti-virus et d'autres logiciels d'application ou de service utilisés.

E. Concernant la maintenance du parc informatique

- Définir les actions à entreprendre dans le cadre de la maintenance préventive ;
- Constituer des stocks de sécurité des éléments du parc informatique, des pièces de rechange indispensables et des outils de travail des informaticiens en charge de la maintenance des matériels et équipements du parc informatique.

F. Concernant la gestion du personnel informaticien du Service Informatique

- Définir les critères d'embauche des experts informaticiens devant intégrer le Service Informatique ;
- Définir les modules ainsi que le planning de formation professionnelle permanente en faveur des experts informaticiens du Service Informatique en place.

G. Concernant le financement de la mise en œuvre du programme d'action et de la politique informatique

- Voir comment garantir la mise à disposition des ressources financières internes ;
- Définir l'origine des sources de financement complémentaires, en cas de besoin.

2.2.2. Processus d'élaboration de la politique informatique

La démarche pour élaborer la Politique informatique d'une organisation tient donc en plusieurs étapes :

1ère étape : identification des ressources du système informatique à gérer (voir 2.2.1.2.).

2ème étape : identification des activités à réaliser au niveau de chaque ressource (voir 2.2.1.3.).

3ème étape : identification des tâches spécifiques à réaliser au niveau de chaque activité (voir 2.2.1.4.).

4ème étape : définition des modalités de mise en œuvre des tâches spécifiques, c.à.d. en répondant à la question de savoir Comment le faire ? Ces modalités sont coulées sous forme de

procédures, directives, principes, règles et bonnes pratiques à appliquer à cet effet. L'ensemble de ces instructions forme la **Politique informatique** de l'organisation.

2.2.3. Résultats attendus de l'application effective et correcte des directives définies dans la Politique Informatique

L'application effective et correcte des directives définies dans la Politique informatique devrait permettre :

- d'assurer la disponibilité, l'intégrité et l'efficacité des ressources du parc informatique de l'organisation ainsi que la bonne qualité du service rendu par ces ressources aux utilisateurs du système informatique ;
- de parvenir à une meilleure adéquation entre ces atouts et les besoins de l'organisation en matière d'informatisation des services ;
- de garantir, in fine, une mise en œuvre réussie du programme d'actions pour la modernisation des systèmes d'information et de gestion de l'organisation, élaboré par le Service Informatique.

Chapitre 3

LE RISQUE DES SYSTEMES D'INFORMATIONS

1. CONCEPTS DE BASE DE L'AUDIT DES SYSTÈMES D'INFORMATION

INTRODUCTION

1. Définition

Le risque : « Danger, inconvénient plus ou moins probable auquel on est exposé. » (Larousse)

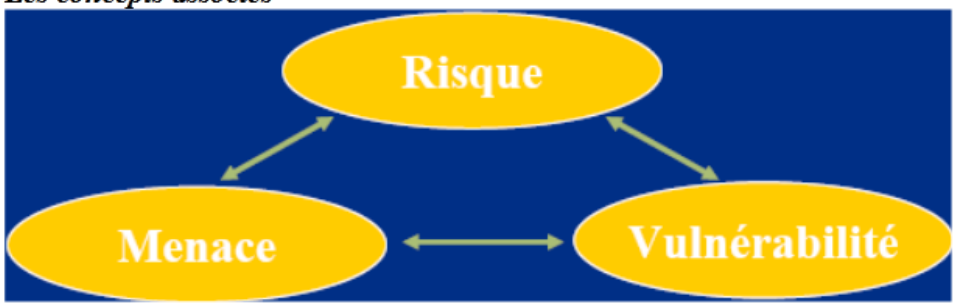
• Les implications directes

- ✓ Risque pour qui ?

Risque en fonction de l'activité (ex : industries, banques, etc.) et de la taille (ex : régionale, nationale, internationale) des entreprises, les risques ne sont pas les mêmes.

- ✓ Importance relative / impact ?
- ✓ Probabilité d'occurrence

Les concepts associés



2. NOTION DE RISQUE

Les organisations visent des objectifs essentiels pour la société.

Par exemple :

- Les banques existent pour permettre aux personnes ayant des idées d'entreprise d'obtenir un accompagnement financier, tout en utilisant les fonds des citoyens qui souhaitent simplement épargner. Elles agissent comme une autorité intermédiaire, favorisant le financement de projets tout en assurant la sécurité et la rentabilité des dépôts des épargnants.
- Les hôpitaux ont pour objectif principal de préserver et d'améliorer la santé des individus en fournissant des soins médicaux adaptés et accessibles ;
- Les universités ont pour mission de transmettre des connaissances et de former les citoyens afin qu'ils puissent assumer les fonctions nécessaires à la bonne marche des pays ;
- Etc.

Pour atteindre ces objectifs, les organisations mettent en place des processus (ensembles d'activités interdépendantes qui transforment) et des fonctions (groupes de tâches similaires regroupées au sein d'une même structure organisationnelle et confiées à des personnes spécifiques).

Cependant, l'atteinte des objectifs fixés par le management d'une organisation peut se heurter à des événements qui compromettent leur réalisation. En effet, lors du déroulement des processus métiers ou dans le fonctionnement des fonctions établies, des événements imprévus peuvent survenir et empêcher l'organisation d'atteindre ses objectifs. Ces événements représentent ce qu'on appelle dans le domaine du contrôle et de l'audit : « le risque ».

De manière simple, le risque peut être défini comme la possibilité qu'un événement empêche une organisation d'atteindre ses objectifs. De manière simple, le risque peut être défini comme la possibilité qu'un événement empêche une organisation d'atteindre ses objectifs. Les risques peuvent être :

- Internes ou externes à l'organisation (ex. : une erreur humaine ou une crise économique) ;
- Prévisibles ou imprévisibles (ex. : une panne programmée ou un incident soudain comme une cyberattaque) ;
- Matériels ou immatériels (ex. : la perte d'un équipement ou l'altération de la réputation de l'organisation).

Dans le cadre de l'audit informatique, qui traite de la prise en charge des processus métiers par des systèmes d'information, le risque informatique se définit comme la possibilité qu'un événement compromette l'intégrité, la confidentialité ou la disponibilité des systèmes d'information. Une telle compromission pouvant avoir pour conséquence de réduire l'efficacité des processus métiers pris en charge par ces outils, impactant ainsi les objectifs opérationnels de l'organisation.

Le risque est une notion clé du métier d'auditeur, car le rôle de l'auditeur consiste à s'assurer que les risques identifiés sont couverts par des contrôles appropriés.

De manière pratique, le risque peut être décomposé en trois grandes composantes :

Risque = Vulnérabilité x Menace x Impact

2.1. Tableau 1 – Les composantes de l'équation du risque

1. Vulnérabilité

Il s'agit des faiblesses ou des insuffisances internes à l'organisation ou à son système qui pourraient être exploitées par une menace. Les vulnérabilités peuvent inclure des lacunes dans les contrôles, des systèmes obsolètes, une formation inadéquate des employés ou une infrastructure insuffisante.

Exemple : Un pare-feu mal configuré ou un système d'information non sécurisé.

2. Menace

Il s'agit de tout événement ou acteur susceptible d'exploiter une vulnérabilité et de provoquer un incident. Les menaces peuvent être internes (erreurs humaines, mauvaise manipulation) ou externes (cyberattaques, catastrophes naturelles, actes de malveillance).

Exemple : Une attaque de ransomware ou une panne d'alimentation électrique.

3. Impact

Cela représente les conséquences possibles si une menace exploite une vulnérabilité. L'impact peut être matériel (perte de données, arrêt de production) ou immatériel (perte de réputation, diminution de la confiance des parties prenantes).

Exemple : Une interruption prolongée des systèmes informatiques pourrait entraîner une perte de revenus ou des sanctions réglementaires.

A. Illustration

Imaginez que vous devez organiser une fête. Les objectifs pour vous pourraient être : veiller au bon déroulement de toutes les activités de réjouissance prévues et assurer le confort et la satisfaction des invités.

Un des risques que vous devez gérer, en tant qu’organisateur, est que celle-ci soit perturbée et s’arrête.

Décomposons ce risque :

- Vulnérabilité : Le lieu de l'événement ne dispose pas de mesures de sécurité suffisantes, telles que des contrôles d'accès à l'entrée ou un plan d'évacuation bien défini ;
- Menace : Un individu malintentionné qui vise à introduire des objets dangereux ou perturber l'événement en créant des troubles ;
- Impact : Blessures aux participants, pertes matérielles, et.

B. Activité pratique

Quel est le risque d'utiliser une carte VISA pour effectuer un paiement en ligne ?

3. NOTION DE CONTROLE

Le contrôle est un mécanisme mis en place pour gérer le risque. Il peut viser une ou plusieurs composantes du risque1 :

- Corriger une vulnérabilité, en renforçant ou en éliminant les faiblesses identifiées dans un système ou un processus ;
- Éliminer une menace détectée, en agissant pour la neutraliser avant qu'elle ne provoque un incident ;
- Réduire l'impact, dans le cas où l'événement ne peut pas être complètement évité.

Dans une organisation, le contrôle est généralement mis en place à trois niveaux :

Niveau 1 : Contrôle au sein des fonctions (première ligne de défense).

- ✓ Ce sont les contrôles effectués par les personnes responsables des processus métiers d'une fonction spécifique de l'organisation ;
- ✓ Ces contrôles sont intégrés aux opérations quotidiennes pour s'assurer que les processus fonctionnent comme prévu ;
- ✓ Dans les organisations où la gestion des risques est critique, une entité spécifique peut être prévue dans l'organigramme pour organiser et coordonner ces contrôles au sein des différentes fonctions (le Département des risques, dans une banque par exemple).

Exemple : Dans une banque, les contrôles de première ligne pour lutter contre le blanchiment d'argent commencent par la vérification des documents d'identité des clients avant d'accepter l'ouverture d'un compte. Ce contrôle est réalisé par l'entité chargée des ouvertures de comptes.

Niveau 2 : Contrôle interne (seconde ligne de défense)

- ✓ Il s'agit des dispositifs mis en place par le Management pour gérer les risques de manière systématique et coordonnée ;
- ✓ Ces contrôles comprennent les politiques, procédures, outils, et mécanismes qui encadrent les opérations de l'organisation ;

- ✓ Ces différents contrôles sont souvent portés par une fonction dédiée, voire deux entités dans certaines organisations, particulièrement lorsque les risques réglementaires nécessitent une attention soutenue.

Exemple : Dans une banque, les contrôles de seconde ligne pour lutter contre le blanchiment d'argent incluent des investigations périodiques sur des opérations dépassant un certain seuil. Ces investigations suivent une procédure définie par le management et sont généralement réalisées par une entité de conformité.

Niveau 3 : Audit interne et externe

- ✓ L'audit interne est une fonction indépendante au sein de l'organisation. Elle est chargée d'évaluer périodiquement l'efficacité des contrôles mis en place. L'objectif est de s'assurer que les dispositifs en place permettent réellement de gérer les risques identifiés.

1 Il est généralement plus facile de réduire les vulnérabilités ou d'atténuer les impacts d'un risque que de contrôler ou d'éliminer complètement les menaces.

- ✓ L'audit externe est également considéré comme un contrôle de niveau 3. Mais contrairement à l'audit interne, il est limité à un périmètre défini dans le cadre d'un mandat. Par ailleurs, il est perçu comme plus indépendant, car réalisé par une entité externe à l'organisation.

Exemple : Dans une banque, l'audit interne peut examiner si les règles KYC (Know Your Customer) ont été correctement appliquées pour tous les comptes ouverts au cours d'une période donnée.

A. Illustration

Reprenons l'exemple de l'organisation d'une fête avec le risque identifié. Quels contrôles, orientés vers le traitement des composantes du risque, pourraient être mis en place ?

Correction

Risque : La fête est perturbée et s'arrête en raison de la combinaison des facteurs ci-dessous :

- ✓ Vulnérabilité : Le lieu de l'événement ne dispose pas de mesures de sécurité suffisantes, comme des contrôles d'accès.

Contrôle à mettre en place :

- Installer des dispositifs de contrôle à l'entrée pour vérifier l'identité des participants (badges, invitations) ;
- Mettre en place un dispositif de surveillance avec des agents de sécurité pour superviser les entrées et sorties, et prévenir les intrusions ;
- Développer un plan d'évacuation détaillé, adapté aux spécificités du lieu, et le communiquer au personnel chargé de la sécurité.

- ✓ Menace : Un individu malintentionné pourrait introduire des objets dangereux ou perturber l'événement en créant des troubles.

Contrôle à mettre en place :

- Organiser un contrôle systématique des sacs et effets personnels à l'entrée, avec des outils tels que des détecteurs de métaux si nécessaire ;
- Positionner des agents de sécurité de manière stratégique dans tout le lieu pour surveiller et intervenir rapidement en cas de comportement suspect ;
- Prévoir une liaison directe avec les autorités locales (police ou gendarmerie) pour une assistance rapide en cas de besoin.

✓ Impact : Les conséquences possibles incluent des blessures aux participants, des pertes matérielles, et une atteinte à la réputation de l'organisateur.

Contrôle à mettre en place :

- Organiser une simulation d'évacuation avant l'événement pour tester les plans d'urgence et s'assurer que toutes les parties prenantes (sécurité, personnel, organisateurs) connaissent leurs rôles respectifs ;
- Prévoir une équipe médicale ou de premiers secours sur place pour réagir rapidement en cas de blessures ou d'incidents médicaux ;

Cet exercice est basé sur une situation courante de la vie. L'accent est avant tout mis sur la manière d'identifier un risque et ses composantes, et d'imaginer les contrôles appropriés à mettre en place. La notion des lignes de défense n'est pas mise en évidence.

- Souscrire une assurance événementielle pour couvrir les dommages matériels et les responsabilités civiles en cas d'incident.

Illustration 2 :

Vous êtes un Consultant en Audit et Conseil informatique. Le management de la banque RAWBANK vous demande de l'aider à rédiger une Politique de gestion des accès dans leur application principale.

Correction ……

4. POSITIONNEMENT DE L'AUDITEUR DES SYSTEMES D'INFORMATION

L'auditeur des systèmes d'information peut se positionner à différents niveaux selon le contexte organisationnel. Les postes les plus fréquents sont les suivants :

A. Auditeur des systèmes d'information au sein de la fonction d'audit interne

Cet auditeur fait partie d'une équipe d'audit interne et intervient dans les missions d'audit prévues dans le cadre du Plan d'audit annuel. Ses responsabilités incluent :

- La réalisation de missions d'audit portant sur des thèmes strictement techniques (comme la sécurité des systèmes, la gestion des accès ou la sauvegarde des données) ;
- L'assistance aux auditeurs classiques pour les aspects de leurs missions nécessitant une expertise informatique (par exemple, l'extraction des données dans des systèmes).

B. Auditeur des systèmes d'information dans un cabinet d'audit externe

Cet auditeur travaille au sein d'un cabinet spécialisé dans la certification des états financiers. Son rôle est généralement d'évaluer les contrôles informatiques ayant un impact significatif sur les états financiers, tels que ceux des systèmes utilisés pour générer les états financiers ou ceux prenant en charge un processus métier se rapportant à une activité dont les contributions financières est importante.

C. Auditeur des systèmes d'information indépendant ou en cabinet spécialisé

Cet auditeur travaille de manière indépendante ou pour un cabinet spécialisé dans des missions spécifiques liées à l'informatique. Ses missions incluent par exemple :

- La réalisation de tests d'intrusion (pentesting) pour identifier les failles de sécurité dans les systèmes informatiques ;
- L'audit de conformité aux normes et réglementations spécifiques, comme ISO 27001 (gestion de la sécurité de l'information) ou RGPD (protection des données) ;
- L'évaluation des stratégies de continuité des activités et des plans de reprise après sinistre (DRP).

Il est essentiel de rappeler que l'auditeur des systèmes d'information intervient dans la troisième ligne de défense, dont le rôle est de s'assurer que les contrôles mis en place par les fonctions opérationnelles (première ligne) et le management (seconde ligne) fonctionnent de manière efficace.

Contrairement aux fonctions de la première et deuxième ligne, l'auditeur n'est pas impliqué dans la mise en place des contrôles.

Lors de ses missions, l'auditeur des systèmes d'information identifie les risques potentiels pour les systèmes d'information et définit des objectifs de contrôle qui permettent de les réduire ou de les gérer. Ensuite, il définit une procédure de test pour s'assurer que ces objectifs de contrôle sont satisfaisants.

D. Activité pratique

La First Bank of DRC a mis en place une Politique de gestion des sauvegardes afin de garantir la sécurité, la disponibilité et l'intégrité des données critiques de l'application de base. Cette procédure est essentielle pour minimiser les impacts liés à la perte en cas de panne ou sinistre.

On y trouve l'extrait suivant :

Sauvegarde incrémentielle

- Description : Une sauvegarde des modifications apportées depuis la dernière sauvegarde (complète ou incrémentielle).
- Fréquence : Quotidienne (tous les jours à 22h00).
- Stockage : Les sauvegardes incrémentielles sont stockées sur un espace cloud sécurisé et sur un disque NAS au siège.

Risque identifié : Les sauvegardes ne sont pas effectuées conformément aux types et fréquences définis par le Management.

Comment procéderez-vous, au cours de l'audit, pour vérifier que ce risque spécifique est géré ?

Chapitre 4

AUDIT INFORMATIQUE

3.1. Les préalables

L'objet de ce chapitre est de rendre les étudiants capables d'apprécier le fonctionnement d'un système informatique dans toutes ses composantes et de formuler des recommandations d'amélioration appropriées en cas de contre-performance constatée.

Pour ce faire, l'auditeur devra s'assurer au préalable auprès des responsables du Service Informatique, de l'existence des outils de gestion efficace de leur système informatique, à savoir : le Schéma Directeur Informatique et la Politique Informatique. Ces documents contiennent en effet les éléments d'appréciation du fonctionnement du système informatique et dont la connaissance, par l'auditeur, constitue un atout de taille pour bien conduire son audit.

L'absence de ces deux outils constitue déjà une lacune importante à relever au niveau des responsables du Service Informatique. Elle devrait même faire l'objet de la première recommandation d'amélioration à charge de ces responsables.

3.2. Définition des objectifs de l'audit

L'audit est l'examen auquel procède un professionnel compétent et indépendant en vue d'exprimer une opinion justifiée sur la régularité et la sincérité et l'image fidèle des états d'une entreprise.

3.3. Démarche proposée

Plusieurs approches peuvent être utilisées à cet effet. Aussi le canevas proposé ici ne peut être considéré comme l'unique possible. Il a toutefois le mérite de permettre à l'auditeur de procéder méthodiquement, en passant en revue chaque composante principale du système informatique audité.

Pour mieux comprendre la logique de l'approche annoncée ci-dessus, il faut se rappeler les trois principes sur lesquels repose la gestion moderne de toute organisation ou de tout système, à savoir :

- L'établissement des prévisions ou fixation des objectifs ;
- Le contrôle des réalisations par rapport aux prévisions ou aux objectifs ;
- L'analyse des écarts constatés.

Ces principes s'appliquent aussi au CTI en tant que système. Aussi, constituent-ils la ligne directrice qui doit guider la démarche tout auditeur désigné pour apprécier son fonctionnement.

De manière concrète, l'audit d'un CTI consiste non seulement à vérifier le respect de ces principes, mais aussi et surtout à aider le responsable à mieux les appliquer. N'oublions pas que l'auditeur n'est pas un OPJ ou un justicier vis-à-vis du responsable, mais doit plutôt se comporter à son égard comme un véritable ingénieur conseil en gestion.

Sa tâche consiste donc à :

1°) analyser les objectifs fixés au CTI dans le cadre du SDI en cours d'exécution, s'il existe. Ce qui implique notamment :

- l'identification de ces objectifs du point de vue des matériels et des logiciels à acquérir ou des programmes d'application à développer, du personnel informaticien à recruter ou former, etc,

- leur classification en fonction de leur échéance de réalisation (objectifs immédiats, proches et lointains) ;

2°) comparer le niveau de réalisation aux objectifs ainsi identifiés et dégager les écarts positifs et négatifs ;

3°) analyser l'adéquation entre objectifs définis dans le SDI et les moyens disponibles, résultant de la mise en œuvre de la Politique Informatique, puis interpréter les écarts obtenus ; ce qui, de manière plus concrète, implique :

- la recherche des causes des contre-performances constatées ou, au contraire, les raisons des succès engrangés, et

- la proposition des remèdes en cas de contre-performance.

Cependant, si les deux premières tâches sont relativement faciles à conduire, il n'en est pas ainsi de la troisième qui est plus complexe et plus délicate et devrait de ce fait mériter plus d'attention. Sa mise en oeuvre requiert en effet une démarche méthodique pour être bien menée. Celle proposée ici, et qui fait l'objet des lignes qui suivent, procède par appréciation de l'importance et de la nature des moyens mis à la disposition du CTI au regard des objectifs qui lui ont été assignés. Ce qui conduira à analyser successivement :

- l'adéquation entre objectifs et moyens matériels,
- l'adéquation entre objectifs et moyens logiciels,
- l'adéquation entre objectifs et moyens financiers,
- l'adéquation entre objectifs et moyens humains,
- l'adéquation entre objectifs et l'organisation en place.

3.3.1. ADEQUATION ENTRE OBJECTIFS ET MOYENS MATERIELS

Quatre points doivent retenir l'attention de l'auditeur.

- ***Performances des ressources hardware***

Il s'agit ici d'apprécier l'adéquation entre la configuration en place et le volume ainsi que la nature du travail à réaliser.

L'analyse des performances doit concerner les principales ressources hardware de l'ordinateur :

- mémoire centrale : capacité
- unité de traitement : vitesse de traitement
- disques : capacité
- imprimantes : type, nombre, vitesse d'impression
- écran : couleur, dimension
- clavier : nombre et disposition de touches

- ***Adéquation entre structure de la configuration informatique en place et modalité de traitement souhaité***

  - Système centralisé ?
  - Système décentralisé ?
  - Système distribué ou réparti ?

- ***Problématique de la fiabilité des équipements***

Un équipement est fiable si la fréquence des pannes ou la probabilité de tomber en panne est faible depuis sa mise en fonctionnement. Dans le cadre de l'audit, l'on doit s'appesantir notamment sur :

- la fréquence des pannes ;
- les éléments les plus défaillants,
- les causes des pannes enregistrées,
- le taux de disponibilité,
- les solutions envisagées en cas de panne prolongée du système d'ordinateur,
- la rapidité d'intervention des techniciens en cas de panne.

- ***Problématiques de la sécurité des équipements***

L'auditeur doit apprécier les mesures de protection des équipements envisagées contre le vol, l'incendie, l'humidité, l'inondation, la poussière, les coupures intempestives du courant, etc…

3.3.2. ADEQUATION ENTRE OBJECTIFS ET MOYENS LOGICIELS

L'auditeur devrait apprécier essentiellement les éléments suivants :

- ***Performances des systèmes d'exploitation***

  - la version utilisée
  - l'adéquation entre modalités de traitement autorisées par le système d'exploitation en place et besoins réels d'exploitation

- ***Performances des progiciels ou packages***

  - Fiabilité des outputs,
  - Conformité des outputs aux besoins d'exploitation,
  - Possibilité d'adaptation des sources aux réalités de l'organisation.

- ***Performances des programmes d'application développées in situ***

  - Fiabilité des outputs,
  - Conformité des outputs aux besoins d'exploitation,
  - Modularité des applications
  - Adéquation entre le langage de programmation utilisé et les besoins d'exploitation
  - Qualité des programmes d'application

- ***Qualité des données et des fichiers***

  - Fiabilité des données saisies,
  - Modes d'organisation et d'accès sur support informatique,
  - Sécurité des données ; appréciation des mesures prises contre les sabotages éventuels, les utilisateurs non autorisés, les altérations possibles des données et des fichiers notamment par les virus, etc …

3.3.3. ADEQUATION ENTRE OBJECTIFS ET MOYENS HUMAINS

Trois points devraient également retenir l'attention de l'auditeur.

- ***Effectif du personnel informaticien***

Il y a-t-il pléthore ou insuffisance du personnel pour chaque catégorie d'informaticiens utilisés (programmeurs, analystes, concepteurs, ingénieurs systèmes) ?

- ***Niveau de formation et l'expérience du personnel informaticien utilisé***

  - adéquation entre qualification du personnel informaticien utilisé et fonctions exercées au sein du CTI (se référer à ce sujet aux aspects développés dans le chapitre 1 au point 1.5.2.C., pages 23 à 24 ci - avant),
  - expérience accumulée par chaque informaticien utilisé.

- ***Aptitudes du personnel informaticien en place***

Le personnel utilisé à différents niveaux est-il performant ?

3.3.4. ADEQUATION ENTRE OBJECTIFS ET MOYENS FINANCIERS

L'auditeur devrait pouvoir vérifier notamment :

- ***L'existence ou non d'un budget spécifique pour le CTI ainsi que les rubriques concernées***

  Ces rubriques sont notamment :

  - formation du personnel informaticien,
  - acquisition des progiciels et équipements informatiques,
  - achat des fournitures ou consommables informatiques,
  - entretien et maintenance des équipements informatiques.

- ***Le niveau d'exécution effective de ce budget, rubrique par rubrique***

Remarque :

Le coût de fonctionnement du CTI doit pouvoir être apprécié non de manière absolue, mais en fonction des services qu'il rend à l'organisation toute entière, c'est-à-dire en terme de rapport **utilité / coût**.

3.3.5. ADEQUATION ENTRE OBJECTIFS ET ORGANISATION EN PLACE

Les aspects organisationnels qui doivent intéresser l'auditeur ont déjà été évoqués au chapitre 1 et portent notamment sur :

- la problématique de la dépendance hiérarchique du CTI, et
- la structure organique du CTI.

Ces aspects ont déjà été abordés au Chapitre 1.