Cours d'Audit Informatique ISC-GOMA 2024

Janvier Twizere SINDAMBIWE

RÉPUBLIQUE DÉMOCRATIQUE DU CONGO

ENSEIGNEMENT SUPÉRIEUR ET UNIVERSITAIRE

Institut Supérieur de Commerce

www.iscgoma.net

Notes de cours d'Audit Informatique

Destinées aux étudiants de ***L2 Conception des SI et Réseaux Informatiques***

Collection et mise à jour de **Janvier SINDAMBIWE,**

Msc in Internet Systems

Juin 2024

CHAP. I. GENERALITES SUR L'AUDIT

1.1. Introduction

Audit (terme issu de l'anglais provenant d'une locution latine proche des notions de contrôle, vérification, expertise, évaluation, etc.) vient du verbe latin « **audire** » qui signifie « **écouter** ». Les Romains employaient ce terme pour désigner un contrôle au nom de l'empereur sur la gestion des provinces. Il fut introduit par les Anglo-Saxons au début du XIII^{ème} siècle pour la gestion. ***L'audit est l'examen d'une situation, d'un système d'informations, d'une organisation pour porter un jugement***. C'est la comparaison entre ce qui est observé et ce que cela devrait être, selon un système de références.

L'audit est perçu comme un outil d'amélioration continue, car il permet de faire le point sur l'existant afin d'en dégager les points faibles ou non conformes (suivant un référentiel d'audit). Ce constat, nécessairement formalisé sous forme de rapport écrit, permet de mener les actions nécessaires pour corriger les écarts et dysfonctionnements relevés.

1.1.1. Audit interne vs Audit externe

a) Audit interne

Les audits internes, appelés parfois « audit de première partie » sont réalisés par, ou au nom de, l'organisme lui-même pour des raisons internes et peuvent constituer la base d'une auto-déclaration de conformité. Ils peuvent être opérationnels ou stratégiques suivant l'approche retenue.

b) Audit externe

Les audits externes comprennent ce que l'on appelle généralement les «audits de seconde ou de tierce partie ».

Les audits de seconde partie sont réalisés pour des parties, telles que les actionnaires ou des clients, ayant un intérêt direct dans l'organisme, ou par d'autres personnes en leur nom.

Les audits de tierce partie sont nécessairement réalisés par des organismes externes indépendants. De tels organismes, généralement accrédités (COBIT : Control Objectives for Information and related Technology, Norme Française NF ISO/CEI 17021), fournissent l'enregistrement ou la certification de conformité à des exigences comme celles de l'ISO 9001 ou 14001 ou NF ISO/CEI 27001 relative aux systèmes de management de la sécurité de l'information.

Lorsque les systèmes de gestion de la qualité et environnemental sont audités simultanément, on parle d'**audit commun.** Lorsque le système de management de la

Qualité, de l'Environnement et de la SST (Santé et sécurité au travail) est intégré, on parle d'audit intégré QSE.

1.1.2. Audit d'un SI VS Audit informatique

a) Audit d'un SI

Il est indispensable pour toute organisation qui décide de changements au sein de son système d'information ou de s'assurer de son fonctionnement optimal. Comme toute démarche qualité, il nécessite une méthodologie rigoureuse et une communication idéale au sein de l'équipe.

b) Audit informatique

En anglais *Information Technology audit* ou *IT audit,* l'audit informatique a pour objectif de s'assurer que les activités informatiques d'une entreprise ou d'une administration se déroulent conformément aux règles et aux usages professionnels, appelés de manière traditionnelle les bonnes pratiques. On va pour cela s'intéresser aux différents processus informatiques comme la fonction informatique, les études informatiques, les projets informatiques, l'exploitation, la sécurité informatique,...

L'audit informatique consiste à évaluer le niveau de maturité de l'informatique de l'entreprise.

On peut vouloir aller plus loin et s'intéresser à l'évaluation des systèmes d'information et non plus seulement à l'informatique. C'est le domaine de l'audit des applications. Ainsi dans le cas d'une application comptable on va s'attacher à vérifier l'intégrité des données comptables, la disponibilité de l'application, s'assurer qu'elle répond aux besoins des comptables et que le système comptable s'interface efficacement avec les autres systèmes de gestion de l'entreprise.

1.2. Besoins et missions d'audit informatique

a) Besoins et nécessité 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'affaires et le retour des investissements (RI) avec les divers coûts et les risques encourus.

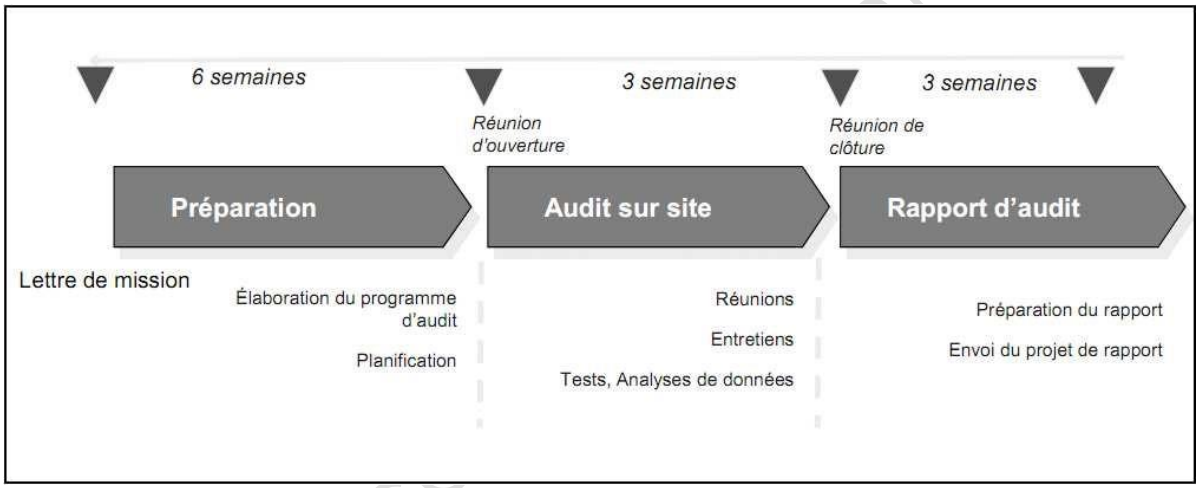
b) Missions d'audit informatique

La notion de contrôle est au cœur de la démarche d'audit informatique. L'objectif est de mettre en place des dispositifs de contrôle efficaces et performants permettant de maîtriser efficacement l'activité informatique. Le contrôle interne, un processus mis en œuvre à l'initiative des dirigeants de l'entreprise, est destiné à fournir une assurance raisonnable quant à la réalisation des trois objectifs suivants :

1. la conformité aux lois et aux règlements,
2. la fiabilité des informations financières,
3. la réalisation et l'optimisation des opérations.

Il est évident que l'audit informatique s'intéresse surtout au troisième objectif.

Voici les phases de réalisation d'une mission d'audit informatique :



Ce cycle de mission s'étale sur une durée de plusieurs mois qui ne convient pas aux projets courts. La solution appliquée pour ce type de projet consiste à effectuer un audit de processus dont les recommandations pourront être appliquées sur le développement suivant.

-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. À 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 (une ou deux fois par an) ;
- Mission spécifique demandée par la direction ;

- Mission due à des événements nouveaux non prévisibles dans l'entreprise.

1. ENQUÊTE PRÉLIMINAIRE

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 d'audit informatique est composée de 7 personnes. Elle est organisée en 3 branches :

- sécurité et infrastructure ;
- applications informatiques ;
- processus et projets informatiques.

L'équipe est structurée 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-dite 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,
- Étudier 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.

Remarque : La phase préliminaire constitue la phase du diagnostic

2. *PHASE DE VÉRIFICATION*

La phase de vérification a pour but de confirmer les points forts et les 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* : ayant pour objectif d'apporter les preuves pour confronter les éléments recensés et déchiffrer le dégât réel.

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, l'édition et la transmission du rapport. Les principales étapes sont :

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

Résumé

De préférence, l'audit est conduit par des équipes n'ayant pas de responsabilité directe dans les secteurs à inspecter (voir audit) et, de préférence, en coopération avec le personnel de ces secteurs. Il appartient à une démarche globale d'amélioration de la qualité ; c'est par la volonté de tous les partenaires qu'il intervient.

Quelques conseils pour la rédaction 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.

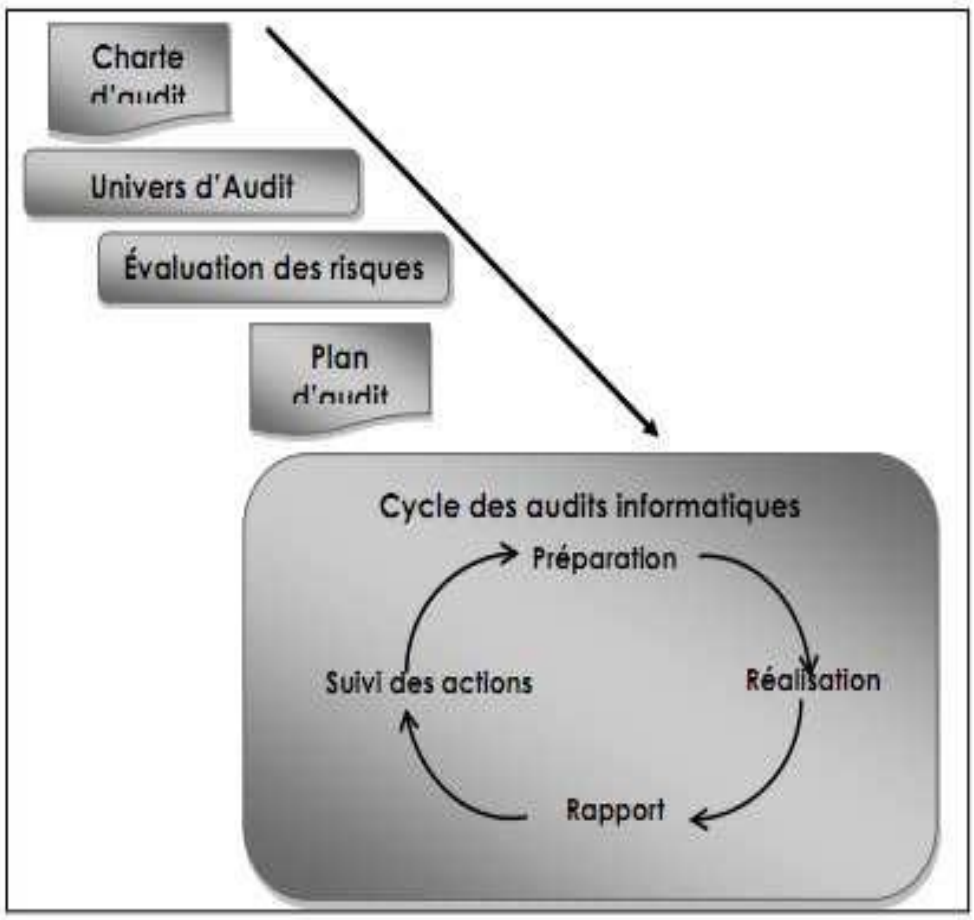
5° Les annexes ne sont pas obligatoires.

6° L'IFACI (Institut Français de l'Audit et du Contrôle Interne) 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.

1.3. Méthodologie d'Audit informatique

C'est la démarche à suivre dans une mission d'audit informatique. Le cycle des missions d'audit peut se présenter comme suit :



- ✓ **La charte d'audit** définit les responsabilités, droits et devoirs des auditeurs et des audités.

- ✓ **L'univers d'audit** est précisé : il s'agit de la liste d'objets auditables : centre de calcul, applications critiques, projets.
- ✓ **Le plan d'audit annuel** s'appuie sur une analyse de risque partagée avec le contrôle interne et avec les DSI (Directions des Systèmes d'Information). Il énumère la liste des projets qui pourraient être audités.
- ✓ **Évaluation des risques :** Elle constitue le programme de travail, précisant les objectifs d'audit, c'est-à-dire en pratique l'ensemble des risques dont on veut tester la couverture : par exemple sur un risque de dérapage de projet on va tester l'application de bonnes pratiques de planification et l'utilisation effective d'une méthodologie.
- ✓ ***Préparation de l'audit :***Une lettre de mission (*Point de départ*), signée au plus haut niveau, est envoyée au futur audité avec copie à l'ensemble de sa hiérarchie. L'analyse de risque est préparée dans la mesure du possible par extraction et analyse de données. Dans le meilleur des cas, on n'aura plus qu'à valider les observations sur site.

La constitution de l'équipe doit permettre de faire face aux difficultés culturelles qui peuvent survenir dans certaines filiales étrangères : dans certains pays, l'accompagnement par du personnel local apporte la crédibilité nécessaire.

- ✓ **Suivi des audits :** L'étape de contrôle post-audit est indispensable. La preuve de la mise en œuvre des recommandations est demandée aux services audités ; on ne se déplace pas sur site, on télécharge les informations utiles. Lorsque les éléments de suivi fournis ne sont pas satisfaisants, une mission de suivi peut être déclenchée, voire un nouvel audit. Le pourcentage de recommandations appliquées est élevé et justifie le niveau de confiance accordé par la direction à l'équipe d'audit interne.

1.4. Démarche d'audit informatique

Une mission d'audit informatique se prépare. La démarche d'audit informatique se définit à partir des préoccupations du demandeur d'audit qui peut être le directeur général, le directeur informatique, le directeur financier,... Il va pour cela mandater l'auditeur pour répondre à une liste de questions précises qui font, plus ou moins implicitement, référence à l'état des bonnes pratiques connues dans ce domaine. Cela se traduit par un document important : la lettre de mission qui précise le mandat à exécuter et qui donne les pouvoirs nécessaires à l'auditeur.

Celui-ci va ensuite s'attacher à relever des faits puis il va mener des entretiens avec les intéressés concernés. Il va ensuite s'efforcer d'évaluer ses observations par rapport à des référentiels largement reconnus. Sur cette base il va proposer des recommandations.

L'auditeur informatique va se servir de référentiels d'audit informatique lui donnant l'état des bonnes pratiques dans ce domaine. Le référentiel de base est COBIT (Control Objectives for Information and Related Technology, en fr : Objectifs de contrôle de l'Information et des Technologies Associées). Mais il va aussi utiliser d'autres référentiels comme : Risk IT, COBIT and Applications
Controls, ISO 27002, CMMi, ITIL, …

Pour mener à bien l'audit informatique il est recommandé de suivre six étapes suivantes :

1. l'établissement de la lettre de mission. Ce document est rédigé et signé par le demandeur d'audit et permet de mandater l'auditeur. Il sert à identifier la liste des questions que se pose le demandeur d'audit. Très souvent l'auditeur participe à sa rédaction.
2. la planification de la mission permet de définir la démarche détaillée qui sera suivie. Elle va se traduire par un plan d'audit ou une proposition commerciale. Ce document est rédigé par l'auditeur et il est soumis à la validation du demandeur d'audit,
3. la collecte des faits, la réalisation de tests, … Dans la plupart des audits c'est une partie importante du travail effectué par les auditeurs. Il est important d'arriver à dégager un certain nombre de faits indiscutables,
4. les entretiens avec les audités permettent de compléter les faits collectés grâce à la prise en compte des informations détenues par les opérationnels. Cependant, souvent ceux-ci font plutôt part de leurs opinions plus que d'apporter les faits recherchés,
5. la rédaction du rapport d'audit est un long travail qui permet de mettre en avant des constatations faites par l'auditeur et les recommandations qu'il propose,
6. la présentation et la discussion du rapport d'audit au demandeur d'audit, au management de l'entreprise ou au management de la fonction informatique.

Il peut arriver qu'à la suite de la mission d'audit il soit demandé à l'auditeur d'établir le plan d'action et éventuellement de mettre en place un suivi des recommandations.

1.5. Référentiels de base

1.5.1. Types

a) Pour l'Audit informatique

Il existe différents référentiels comme :

- **CobiT**: Control Objectives for Information and related Technology. C'est le principal référentiel des auditeurs informatiques, il est l'œuvre de « **Information Systems**

Audit and Control Association ISACA » : une association professionnelle internationale dont l'objectif est d'améliorer la gouvernance des systèmes d'information, notamment par l'amélioration des méthodes d'audit informatique.

- **Val IT** permet d'évaluer la création de valeur par projet ou par portefeuille de projets,
- **Risk IT** a pour but d'améliorer la maîtrise des risques liés à l'informatique. Voir les sites de l'ISACA qui est l'association internationale des auditeurs informatiques et de l'AFAI (Association Française de l'Audit et du conseil Informatique).

Mais on peut aussi utiliser d'autres référentiels comme :

- **ISO 27002** qui est un code de bonnes pratiques en matière de management de la sécurité des systèmes d'information,
- **CMMi** : Capability Maturity Model integration qui est une démarche d'évaluation de la qualité de la gestion de projet informatique,
- **ITIL** qui est un recueil des bonnes pratiques concernant les niveaux et de support des services informatiques.

b) Pour l'audit des sites Web

Il existe des référentiels proposant des grilles d'évaluation pré-établies et reconnues, comme celui d'Opquast par exemple.

Il existe également des outils en ligne permettant de vérifier le respect de standards : accessibilité, résolution d'affichage, référencement**, ...**

En fonction du projet, des objectifs, une grille de critères personnalisée est constituée.

* **RGAA - Référentiel général d'accessibilité**

Le référentiel général d'accessibilité est un référentiel qui définit les modalités techniques d'accessibilité des services de communication publique en ligne de l'État, des collectivités territoriales et des établissements publics qui en dépendent.

Le RGAA intègre les exigences de la loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées.

* **Référentiel ACCESSIWEB**

AccessiWeb est une marque déposée par l'association BrailleNet (membre du W3C) et constitue son pôle « Accessibilité du web ».

Les activités AccessiWeb s'articulent autour de 4 principaux domaines :

- **Référentiels :** production et maintenance de référentiels issus des travaux du W3C/WAI.

- **Formations :** pour les professionnels du Web et pour tout public. Création et animation du plus important réseau français d'experts en accesssibilité (Experts AccessiWeb en Evaluation) : le Groupe de Travail AccessiWeb.
- **Label** : mesure la conformité des sites Web aux standards d'accessibilité de W3C/WAI.
- **Projets de recherche :** participation à des projets européens et porteurs d'initiatives en faveur de l'accessibilité numérique

1.5.2. Présentation du référentiel COBIT

Le référentiel CobiT (Control Objectives for Information & Related Technology), que nous utilisons pour l'audit des systèmes d'information, décompose tout système informatique en 34 processus regroupés en 4 domaines, présentés comme suit:

a) Planification & Organisation

Couvre la stratégie et les tactiques et concerne l'identification des moyens permettant à l'informatique de contribuer le plus efficacement à la réalisation des objectifs commerciaux de l'entreprise.

Définir le plan stratégique informatique	Gérer les investissements	Evaluer les risques
Définir l'architecture des informations	Communiquer les objectifs de la direction	Gérer les projets
Définir la direction technologique	GRH	Gérer la qualité
Organiser le département / service informatique	Assurer le respect des exigences légales	

b) Acquisition & Installation

Concerne la réalisation de la stratégie informatique, l'identification, l'acquisition, le développement et l'installation des solutions informatiques et leur intégration dans les processus commerciaux.

Identifier les solutions automatiques	Acquérir et maintenir l'infrastructure technologique	Installer et certifier les systèmes
Acquérir et maintenir les applications informatiques	Développer et maintenir les procédures	Gérer les changements

c) Livraison & Support

Concerne la livraison des prestations informatiques exigées, ce qui comprend l'exploitation, la sécurité, les plans d'urgence et la formation.

Définir les niveaux de service	Identifier et attribuer les coûts	Gérer les données / applications
Gérer les services de tiers (SLA)	Former les utilisateurs	Assurer la sécurité physique
Gérer les performances et les capacités	Assister les utilisateurs (Help Desk)	Gérer l'exploitation
Assurer la poursuite des traitements	Gérer la configuration	
Assurer la sécurité des systèmes	Gérer les incidents	

d) Monitoring

Il permet au management d'évaluer la qualité et la conformité des processus informatiques aux exigences de contrôle.

Monitoring des processus	Certification par un groupe indépendant
Appréciation du contrôle interne	Audit par un organe indépendant

1.5.3. Certification des auditeurs informatiques

On pourrait imaginer une certification des directions informatiques ou des applications informatiques. Cela n'existe pas. Il existe par contre une certification de la qualité des projets informatiques : CMMI (Capability Maturity Model Integration). En matière de qualité de service fournie par l'exploitation il y a la certification sur la norme ISO 20000 qui est un sous-ensemble d'ITIL (Information Technology Infrastructure Library).

Il existe par contre une procédure de certification des outsourceurs : SAS 70, Statement on Auditing Standards n°70. Cette norme a été créée par l'American Institute of Certified Public Accountants (AICPA) pour éviter à ces organismes de devoir supporter successivement plusieurs audits informatiques sur des sujets voisins. Ce sont des audits réalisés par des tiers et vont s'assurer que les processus mis en œuvre offrent la qualité du service attendue.

En matière d'audit informatique on certifie les auditeurs informatiques. La certification de référence est le CISA (Certified Information Systems Auditor). C'est une certification professionnelle internationale. Elle est organisée par l'ISACA (Information Systems Audit and Control Association) depuis 1978. En France elle est passée depuis 1989. A ce jour dans le Monde 75.000 personnes ont le CISA dont plus de 1.000 en France. L'examen peut être passé deux fois par an : en juin et en décembre, dans 11 langues différentes et dans 200 villes du monde. Il faut répondre à 200 questions à choix multiples en 4 heures portant sur l'audit et l'informatique.

L'examen porte sur 6 domaines :

1. les processus d'audit des systèmes d'information,
2. la gouvernance IT,
3. la gestion du cycle de vie des systèmes et de l'infrastructure,
4. la fourniture et le support des services,
5. la protection des avoirs informatiques,
6. le plan de continuité et le plan de secours informatique.

CHAP.II. DOMAINES D'APPLICATION DE L'AI

La démarche d'audit informatique est générale et s'applique à différents domaines comme la fonction informatique, les études informatiques, les projets informatiques, l'exploitation, la planification de l'informatique, les réseaux et télécommunications, sites Web, la sécurité informatique, l'informatique locale ou l'informatique décentralisée, la qualité de service, l'externalisation, la gestion de parc, les applications opérationnelles… Ci-dessous, une présentation succincte des audits informatiques les plus fréquents.

2.1. Audit de la fonction informatique

Le but de l'audit de la fonction informatique est de répondre aux préoccupations de la direction générale ou de la direction informatique concernant l'organisation de la fonction informatique, son pilotage, son positionnement dans la structure, ses relations avec les utilisateurs, ses méthodes de travail…

Pour effectuer un audit de la fonction informatique, on se base sur les bonnes pratiques connues en matière d'organisation de la fonction informatique. Elles sont nombreuses et bien connues. Parmi celles-ci, on peut citer :

- la clarté des structures et des responsabilités de l'équipe informatique,
- la définition des relations entre la direction générale, les directions fonctionnelles et opérationnelles, et la fonction informatique,
- l'existence de dispositifs de mesures de l'activité et notamment d'un tableau de bord de la fonction informatique,
- le niveau des compétences et des qualifications du personnel de la fonction.

Il existe de nombreuses autres bonnes pratiques concernant la fonction informatique. Pour auditer la fonction on va se baser sur ces bonnes pratiques afin de dégager un certain nombre d'objectifs de contrôle comme par exemple :

- le rôle des directions fonctionnelles et opérationnelles dans le pilotage informatique et notamment l'existence d'un comité de pilotage de l'informatique,
- la mise en œuvre de politiques, de normes et de procédures spécifiques à la fonction,
- la définition des responsabilités respectives de la fonction informatique et des unités utilisatrices concernant les traitements, la maintenance, la sécurité, les investissements, les développements,….
- l'existence de mécanismes permettant de connaître et de suivre les coûts informatiques, soit à l'aide d'une comptabilité analytique, soit, à défaut, grâce à un mécanisme de refacturation,

- le respect des dispositifs de contrôle interne comme une évaluation périodique des risques, la mesure de l'impact de l'informatique sur les performances de l'entreprise…

Ces différents objectifs de contrôle correspondent au processus « Planifier et Organiser » PO 4 de COBIT: "Définir les processus, l'organisation et les relations de travail".

2.2. Audit des études informatiques

L'audit des études informatiques est un sous-ensemble de l'audit de la fonction informatique. Le but de cet audit est de s'assurer que son organisation et sa structure sont efficaces, que son pilotage est adapté, que ses différentes activités sont maîtrisées, que ses relations avec les utilisateurs se déroulent normalement,…

Pour effectuer un audit des études informatiques, on se base sur la connaissance de bonnes pratiques recensées dans ce domaine. Elles sont nombreuses et connues par tous les professionnels. Parmi elles, on peut citer :

- l'organisation de la fonction études en équipes, le choix des personnes et leur formation, leurs responsabilités, …
- la mise en place d'outils et de méthodes adaptés notamment une claire identification des tâches, des plannings, des budgets, des dispositifs de suivi des études, un tableaux de bord,…
- le contrôle des différentes activités qui ne peuvent pas être planifiées comme les petits projets, les projets urgents,…
- la mise sous contrôle de la maintenance des applications opérationnelles,
- le suivi des activités d'études à partir de feuilles de temps.

Il existe de nombreuses autres bonnes pratiques concernant les études informatiques. Pour les auditer on va se baser sur ces bonnes pratiques afin de dégager un certain nombre d'objectifs de contrôle comme par exemple :

- l'évaluation de l'organisation de la fonction d'études informatiques et notamment la manière dont sont planifiées les différentes activités d'études,
- le respect de normes en matière de documentation des applications et notamment la définition des documents à fournir avec les différents livrables prévus,
- le contrôle de la sous-traitance notamment la qualité des contrats, le respect des coûts et des délais, la qualité des livrables, …
- l'évaluation de la qualité des livrables fournis par les différentes activités d'études qui doivent être testables et vérifiables.

Il existe de nombreux autres objectifs de contrôle concernant les études informatiques et ils sont choisis en fonction des préoccupations du demandeur d'audit.

2.3. Audit de l'exploitation

L'audit de l'exploitation a pour but de s'assurer que le ou les différents centres de production informatiques fonctionnent de manière efficace et qu'ils sont correctement gérés. Il est pour cela nécessaire de mettre en œuvre des outils de suivi de la production comme Openview de HP, de Tivoli d'IBM,... Il existe aussi un système Open Source de gestion de la production comme Nagios. Ce sont de véritables systèmes d'information dédiés à l'exploitation. Pour effectuer un audit de l'exploitation, on se base sur la connaissance des bonnes pratiques concernant ce domaine comme par exemple :

- la clarté de l'organisation de la fonction notamment le découpage en équipes, la définition des responsabilités,...
- l'existence d'un système d'information dédié à l'exploitation notamment pour suivre la gestion des incidents, la gestion des ressources, la planification des travaux, les procédures d'exploitation,...
- la mesure de l'efficacité et de la qualité des services fournies par l'exploitation informatique.

Il existe de nombreuses autres bonnes pratiques concernant l'exploitation informatique. Pour effectuer cet audit, on va se baser sur ces bonnes pratiques afin de dégager un certain nombre d'objectifs de contrôle comme :

- la qualité de la planification de la production,
- la gestion des ressources grâce à des outils de mesure de la charge, des simulations, le suivi des performances,...
- l'existence de procédures permettant de faire fonctionner l'exploitation en mode dégradé de façon à faire face à une indisponibilité totale ou partielle du site central ou du réseau,
- la gestion des incidents de façon à les repérer et le cas échéant d'empêcher qu'ils se renouvellent,
- les procédures de sécurité et de continuité de service qui doivent se traduire par un plan de secours,
- la maîtrise des coûts de production grâce à une comptabilité analytique permettant de calculer les coûts complets des produits ou des services fournis.

Ces différents objectifs de contrôle correspondent au processus « Délivrer et Supporter » DS 1, DS 3, DS 6, DS 12 et DS 13 de COBIT : DS 1 "Définir et gérer les niveaux de services", DS 3 "Gérer la performance et la capacité", DS 6 "Identifier et imputer les coûts", DS 12 "Gérer l'environnement physique", DS 13 "Gérer l'exploitation".

2.4. Audit des applications opérationnelles

L'audit d'applications opérationnelles couvre un domaine plus large et s'intéresse au système d'information de l'entreprise. Ce sont des audits du système d'information. Ce peut être l'audit de l'application comptable, de la paie, de la facturation,.... Mais, de plus en plus souvent, on s'intéresse à l'audit d'un processus global de l'entreprise comme les ventes, la production, les achats, la logistique,...

Il est conseillé d'auditer une application de gestion tous les deux ou trois ans de façon à s'assurer qu'elle fonctionne correctement et, le cas échéant pouvoir apporter les améliorations souhaitables à cette application ou à ce processus. L'auditeur va notamment s'assurer du respect et de l'application des règles de contrôle interne. Il va en particulier vérifier que :

- les contrôles en place sont opérationnels et sont suffisants,
- les données saisies, stockées ou produites par les traitements sont de bonnes qualités,
- les traitements sont efficaces et donnent les résultats attendus,
- l'application est correctement documentée,
- les procédures mises en œuvre dans le cadre de l'application sont à jour et adaptées,
- l'exploitation informatique de l'application se fait dans de bonnes conditions,
- la fonction ou le processus couvert par l'application sont efficaces et productifs,
- ...

Le but de l'audit d'une application opérationnelle est de donner au management une assurance raisonnable sur son fonctionnement. Ces contrôles sont, par exemple, réalisés par le Commissaire aux Comptes dans le cadre de sa mission légale d'évaluation des comptes d'une entreprise : est-ce que le logiciel utilisé est sûr, efficace et adapté ?

Pour effectuer l'audit d'une application opérationnelle, on va recourir aux objectifs de contrôle les plus courants :

- le contrôle de la conformité de l'application opérationnelle par rapport à la documentation utilisateur, par rapport au cahier des charges d'origine, par rapport aux besoins actuels des utilisateurs,

- la vérification des dispositifs de contrôle en place. Il doit exister des contrôles suffisants sur les données entrées, les données stockées, les sorties, les traitements,... L'auditeur doit s'assurer qu'ils sont en place et donnent les résultats attendus,
- l'évaluation de la fiabilité des traitements se fait grâce à l'analyse des erreurs ou des anomalies qui surviennent dans le cadre des opérations courantes. Pour aller plus loin l'auditeur peut aussi être amené à constituer des jeux d'essais pour s'assurer de la qualité des traitements. Il est aussi possible d'effectuer des analyses sur le contenu des principales bases de données afin de détecter d'éventuelles anomalies,
- la mesure des performances de l'application pour s'assurer que les temps de réponse sont satisfaisants même en période de forte charge. L'auditeur va aussi s'intéresser au nombre d'opérations effectuées par le personnel dans des conditions normales d'utilisation.

Très souvent on demande à l'auditeur d'évaluer la régularité, la conformité, la productivité, la pérennité de l'application opérationnelle. Ce sont des questions délicates posées par le management à l'auditeur.

2.5. Audit des projets informatiques

2.5.1. Généralités :

a) Définition :

On appelle « **projet** » un ensemble finalisé d'activités et d'actions entreprises dans le but de répondre à un besoin défini, dans des délais fixés et dans la limite d'une enveloppe budgétaire allouée.

Selon AFNOR «Association française de normalisation), un projet est un processus unique qui consiste en un ensemble d'activités coordonnées et maîtrisées, comportant des dates de début et de fin, entrepris dans le but d'atteindre un objectif conforme à des exigences spécifiques, incluant des contraintes de délais, de coûts et de ressources ».

Cette première définition montre bien, qu'un projet est un événement important au sein d'une société puisqu'il implique des contraintes ; non seulement des contraintes de coûts mais également de ressources.

Il est également important de coordonner un projet afin qu'il soit terminé dans les délais et qu'il soit de plus maîtrisé afin d'éviter l'abandon du projet.

D'après AFITEP, un projet est un ensemble d'actions à réaliser avec des ressources données, pour satisfaire un objectif défini, dans le cadre d'une mission précise, et pour la réalisation desquelles on a identifié non seulement un début, mais aussi une fin ».

Cette seconde définition fait paraître un autre aspect important du terme « projet », elle montre qu'il est essentiel de bien préparer un projet, qu'il est important de faire des plans d'actions au commencement du projet afin que celui-ci aboutisse à ses objectifs.

Un projet a pour but d'analyser l'existant et de lister les impacts que peuvent avoir des modifications sur le système d'information. Ainsi les projets permettent de prévenir des risques et de trouver les solutions adéquates afin de faire les modifications sans impacts lourds pour la société.

Mais bien que des précautions soient prises en amont du projet, durant ce dernier, le chef de projet n'est pas à l'abri d'un changement imprévu. Le chef de projet, devant garantir le bon déroulement du projet, doit s'assurer d'avoir des solutions pour pallier aux éventuels changements inattendus.

b) Acteurs :

- ✓ ***Maître d'ouvrage*** personne physique ou morale propriétaire de l'ouvrage. Il détermine les objectifs, le budget et les délais de réalisation. L'ensemble de documents rédigés par le maître d'ouvrage exprimant les besoins et les contraintes à respecter s'appelle « ***Programme*** ».
- ✓ ***Maître d'œuvre*** personne physique ou morale qui reçoit mission du maître d'ouvrage pour assurer la conception et la réalisation de l'ouvrage. L'ensemble des documents rédigés par le maître d'œuvre définissant la nature des travaux à exécuter par les intervenants individuels concourant au projet global s'appelle « ***Cahier des charges*** ».

c) Méthodes d'estimation des charges

Si vous travaillez en Informatique, vous entendez certainement souvent parler d'estimation des charges ; cette tâche confiée aux chefs de projets, consiste en l'évaluation du coût total du projet informatique en jour*homme. En fait, il existe beaucoup de méthodes théoriques applicables par type de projet. Parmi elles, nous pouvons citer : Méthode de répartition professionnelle, Méthode COCOMO (Constructive Cost Model).

Cependant, ce qui se passe le plus souvent en pratique, c'est que chaque chef de projet (et plus généralement chaque entreprise), apprend de son expérience pour évaluer plus finement les nouveaux projets.

2.5.2. Audit

L'audit du projet informatique est un audit dont le but est de s'assurer qu'il se déroule normalement et que l'enchaînement des opérations se fait de manière logique et efficace de façon qu'on ait de forte chance d'arriver à la fin de la phase de réalisation ou l'implantation

d'un système qui sera performant et opérationnel. Comme on le voit, l'audit d'un projet informatique ne se confond pas avec un audit des études informatiques.

Pour effectuer l'audit d'un projet informatique on se base sur la connaissance des bonnes pratiques connues en ce domaine. Elles sont nombreuses et connues par tous les chefs de projets et de manière plus générale par tous professionnels concernés. Parmi celles-ci on peut citer :

- l'existence d'une méthodologie de conduite des projets,
- la conduite des projets par étapes quel que soit le modèle de gestion de projets : cascade, V, W ou en spirale (processus itératif),
- le respect des étapes et des phases du projet,
- le pilotage du développement/réalisation et notamment les rôles respectifs du chef de projet et du comité de pilotage,
- la conformité du projet aux objectifs généraux de l'entreprise,
- la mise en place d'une note de cadrage, d'un plan de management de projet ou d'un plan d'assurance qualité (PAQ),
- la qualité et la complétude des études amont : étude de faisabilité et analyse fonctionnelle,
- l'importance accordée aux tests, notamment aux tests faits par les utilisateurs.

Il existe de nombreuses autres bonnes pratiques concernant la gestion de projet. Pour effectuer un audit d'un projet informatique on va se baser sur un certain nombre d'objectifs de contrôle comme par exemple :

- la clarté et l'efficacité du processus de développement,
- l'existence de procédures, de méthodes et de standards donnant des instructions claires aux développeurs et aux utilisateurs,
- la vérification de l'application effective de la méthodologie,
- la validation du périmètre fonctionnel doit être faite suffisamment tôt dans le processus de développement,
- la gestion des risques du projet. Une évolution des risques doit être faite aux étapes clés du projet.

Il existe de nombreux autres objectifs de contrôle possibles concernant l'audit de projet informatique qui sont choisis en fonctions des préoccupations et des attentes du demandeur d'audit. Ces différents objectifs correspondent aux processus PO 10, AI 1 et AI 2

de COBIT : PO 10 "Gérer le projet" mais aussi AI 1 "Trouver des solutions informatiques" et AI 2 "Acquérir des applications et en assurer la maintenance".

2.6. Audit de la sécurité informatique

L'audit de la sécurité informatique a pour but de donner au management une assurance raisonnable du niveau de risque de l'entreprise lié à des défauts de sécurité informatique. En effet, l'observation montre que l'informatique représente souvent un niveau élevé pour risque élevé de l'entreprise. On constate actuellement une augmentation de ces risques liée au développement d'Internet. Ils sont liés à la conjonction de quatre notions fondamentales :

1. en permanence il existe des menaces significatives concernant la sécurité informatique de l'entreprise et notamment ses biens immatériels,
2. le facteur de risque est une cause de vulnérabilité due à une faiblesse de l'organisation, des méthodes, des techniques ou du système de contrôle,
3. la manifestation du risque. Tôt ou tard le risque se manifeste. Il peut être physique (incendie, inondation) mais la plupart du temps il est invisible et se traduit notamment par la destruction des données, détournement de trafic, etc.
4. la maîtrise du risque. Il s'agit de mettre en place des mesures permettant de diminuer le niveau des risques notamment en renforçant les contrôles
   d'accès, l'authentification des utilisateurs,...

Pour effectuer un audit de sécurité informatique il est nécessaire de se baser sur quelques objectifs de contrôle. Les plus courants sont :

- repérer les actifs informationnels de l'entreprise. Ce sont des matériels informatiques, des logiciels et des bases de données. Il est pour cela nécessaire d'avoir des procédures de gestion efficaces et adaptées,
- identifier les risques. Il doit exister des dispositifs de gestion adaptés permettant de surveiller les domaines à risque. Cette surveillance doit être assurée par un RSSI, un responsable de la sécurité informatique,
- évaluer les menaces. Le RSSI a la responsabilité de repérer les principaux risques liés aux différents domaines du système d'information. Un document doit recenser les principales menaces,
- mesurer les impacts. Le RRSI doit établir une cartographie des risques associés au système d'information. Il est alors envisageable de construire des scénarios d'agression et d'évaluer les points de vulnérabilité,

- définir les parades. Pour diminuer le niveau des risques il est nécessaire de prévoir les dispositifs comme des contrôles d'accès, le cryptage des données, le plan de secours,...

Il existe de nombreux autres objectifs de contrôle concernant l'audit de la sécurité informatique qui sont choisis en fonction des préoccupations et des attentes du demandeur d'audit.

Ces différents objectifs de contrôle correspondent aux processus de COBIT DS 5 : "Assurer la sécurité des systèmes" et PO 9 "Évaluer et gérer les risques". Il existe un référentiel spécifique à la sécurité informatique : ISO 27002. C'est un code des bonnes pratiques concernant le management de la sécurité des systèmes d'information. Il est complété par la norme ISO 27001 concernant la mise en place d'un Système de Management de la sécurité de l'Information.

2.7. Audit des R.I

Le réseau informatique d'une organisation est certainement un des aspects les plus critiques pour la Direction des Systèmes d'Information (DSI).

En effet, constamment exposé aux risques d'intrusions, le réseau informatique doit être impérativement sécurisé car il est la porte d'entrée à toutes les informations de l'organisation.

L'audit du réseau a pour objectif à la fois d'évaluer le niveau de performance et de disponibilité des infrastructures réseaux, et de déterminer quelles améliorations peuvent être mises en œuvre afin de la renforcer.

La démarche d'audit appliquée par **Acipia** porte à la fois sur les aspects techniques, et sur les aspects humains et organisationnels. Selon les besoins et selon le périmètre à auditer, nous mettons en œuvre les outils et les ressources adaptées afin de collecter les informations nécessaires (entretien, expertise technique, supervision, test de montée en charge, documentation, etc. ...).

Ces informations sont ensuite confrontées à l'état de l'art en matière de réseau informatique, et analysées par les ingénieurs afin de connaître les risques réellement encourus et les impacts d'une défaillance sur la production d'une société. Si des dysfonctionnements sont connus et se produisent ponctuellement, ils font l'objet d'une attention particulière.

D'autres démarches peuvent être menées par l'équipe technique selon l'architecture réseau utilisée: Faire une cartographie de l'état du câblage et vérifier la qualité de tous les raccordements pour s'assurer du respect des normes en vigueur ;

- Faire un contrôle qualitatif des connexions ;

- Identifier et classer les flux grâce à des outils spécifiques (sondes) ;
- Vérifier l'utilisation et la performance des liens, des utilisateurs et des applications ;
- Contrôler le temps de réponse des différentes applications ;
- Isoler les problèmes de performances liés aux serveurs et au réseau ;
- Diagnostiquer le profil des connexions et des réponses des serveurs, l'historique du trafic… ;
- Faire un rapport de synthèse du réseau et établir des recommandations d'évolution, d'optimisation des infrastructures réseaux.

A la suite de ces démarches, l'auditeur ou l'équipe technique soumet toujours à ses clients des recommandations en matière de refonte partielle ou totale de leurs architectures, d'optimisation du réseau grâce à des actions augmentant l'efficacité de celui-ci et peut proposer une solution technologique nouvelle si l'état actuel du réseau ne permet plus de répondre aux besoins du client.

2.8. Audit des S.I

2.8.1. Définition :

L'audit des SI a pour objectif de mettre en évidence les dangers liés à l'infrastructure technique ainsi que les risques fonctionnels du SI. Il couvre un périmètre plus large que l'audit informatique car il s'intéresse davantage aux aspects fonctionnels et organisationnels liés au système d'information en plus de l'aspect technique. L'audit des SI s'appuie sur une méthodologie appelée **CobiT (**Control Objectives for Information and related Technology**)** qui constitue le référentiel international de contrôle en matière des systèmes d'information. Celui-ci offre certains standards de contrôle ainsi que de « bonnes pratiques » dans l'appréciation des dangers informatiques. L'audit des systèmes d'information est donc l'acteur de contrôle du management des systèmes d'information.

2.6.2. Renforcer la sécurité informatique de l'entreprise.

La complexité des systèmes d'information, souvent facteurs clés dans la performance des entreprises mais dont dépendent fortement la conduite de l'activité opérationnelle et la fiabilité de l'information financière, rend incontournable leur prise en compte dans une démarche d'analyse des risques de toute entreprise.

A travers une bonne organisation, pour intervenir efficacement sur les problématiques de systèmes d'information, un accompagnement d'une équipe d'expert peut être utile pour :

- identifier les risques liés aux différents systèmes d'information avec la mise en œuvre d'outils d'analyse et de scoring des risques informatiques ;

- mettre en place des contrôles informatisés sur des processus et des zones de risque spécifiques : achats, stocks en-cours de production, facturation,
- immobilisations, fraudes et erreurs, etc. ; formuler des recommandations et des axes d'amélioration pour renforcer la sécurité de systèmes d'information.

Pour répondre aux attentes, une proposition de deux types d'intervention, pouvant être combinés : l'examen des systèmes d'information et l'analyse de données des processus métier et financiers.

a) Examen des systèmes d'information a. Cartographie des applications

En préalable, la mise en place de la cartographie des applications permet de recenser les applications, les interfaces et leurs contrôles afin de mieux comprendre l'environnement informatique et comment s'organisent les processus métier au sein des systèmes d'information.

Conduite généralement sur la base d'un entretien avec le responsable informatique, la cartographie est réalisée en une demi-journée environ, selon la complexité informatique.

Les travaux sont modélisés dans un document présentant la vision synthétique et fonctionnelle du système d'information, le détail de la fonction de chaque application, les interfaces et leurs contrôles associés.

b. Revue des systèmes d'information

L'objectif de la revue des systèmes d'information est d'évaluer le dispositif de contrôle interne des applications et de la fonction informatique. Les domaines étudiés en priorité constituent les axes de vigilance majeurs :

- ❖ sécurité physique de la salle informatique ;
- ❖ procédure de sauvegardes des serveurs et plan de secours en cas de sinistre ;
- ❖ sécurité des accès aux données : réseau et applications ;
- ❖ stratégie et contrôle interne du service informatique ;
- ❖ processus de gestion des évolutions des systèmes d'information.

L'intervention se déroule en moyenne sur une à deux journées en fonction de la complexité des systèmes d'information, la taille du service informatique et la granularité des travaux. Des tests complémentaires et approfondis peuvent notamment être nécessaires pour la conduite et la pertinence de la mission.

Un outil de scoring des risques informatiques est utilisé pour mieux identifier les axes d'amélioration et faciliter la communication des conclusions dans un rapport détaillant l'ensemble des travaux menés.

b) Analyse de données

L'analyse de données est une technique d'audit permettant de détecter des anomalies dans les données d'un processus provoquées par un utilisateur ou par un programme informatique.

La mise en œuvre d'une approche d'analyse par les données est un moyen d'analyse adapté à une grande diversité de systèmes d'information :

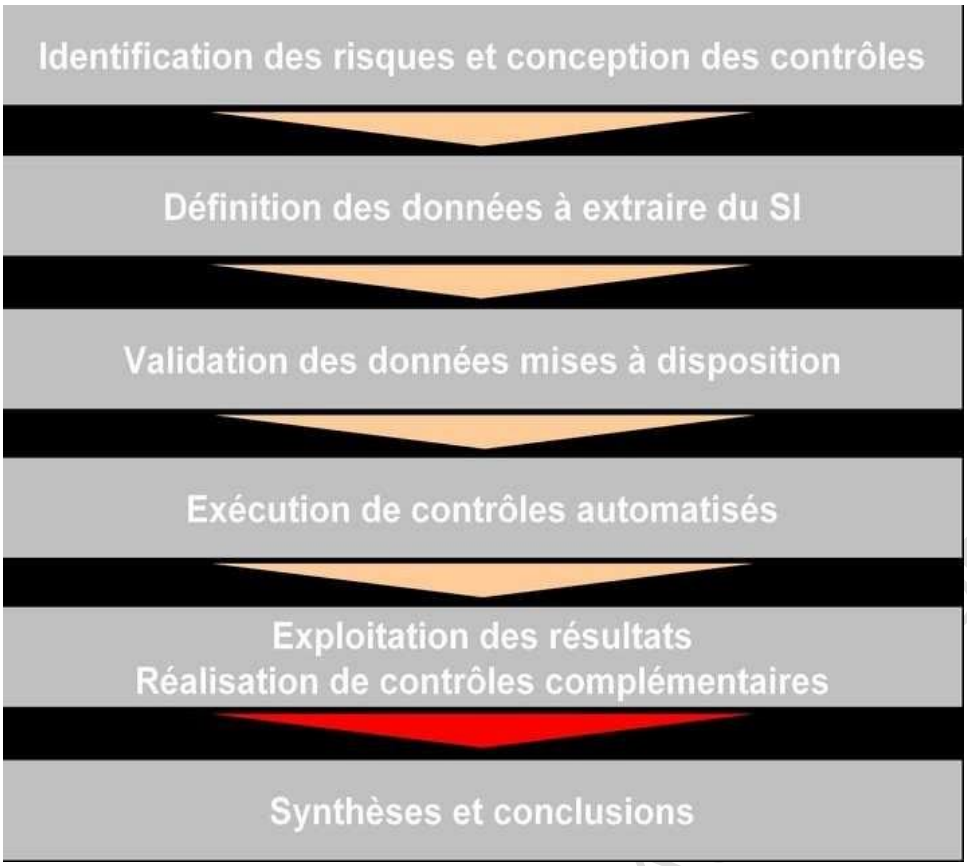
- volumétrie des données ;
- multiplicité des applications et des interfaces ;
- complexité des processus informatisés et des règles de gestion.

Cette approche permet de mieux appréhender les risques des processus en effectuant des tests sur l'exhaustivité de la population étudiée.

La démarche utilise des contrôles standards qu'on adopte au contexte en fonction des contraintes du système d'information, des objectifs de contrôle et des attentes :

- recherche d'erreurs et de fraudes par l'analyse du journal des écritures comptables : identification des schémas d'écritures de fraudes, oubli de déduction de TVA ou TVA déduite à tort, personnes non habilitées à la saisie de certains types d'écritures comptables, etc. ;
- vérification de la fiabilité du processus des stocks : analyse qualitative (stocks négatifs et doublons par exemple), calcul de la rotation des stocks et mise en relation avec la provision pour dépréciation, vérification de l'équation de stock au niveau de chaque article ;
- contrôle de l'exhaustivité des appels de facturation : organismes de logements sociaux, associations, etc.

Le processus de mise en œuvre suit les étapes suivantes :



En préalable, la prise de connaissance de l'environnement applicatif et des interfaces permet de mieux identifier les données à utiliser.

La mise en place d'une analyse de données, dont la durée est variable en fonction de l'étendue des travaux, généralement entre 2 et 4 jours, conduit à la formulation de conclusions dans un rapport détaillant les étapes d'analyse.

CHAP.III. AUDIT DES SITES WEB

3.1. Quid des sites Web ?

3.1.1. Définition

Un site, site web (de l'anglais website, littéralement « site de la toile d'araignée » en français) est un ensemble de pages web et de ressources liées et accessible par une adresse web. Un site web est hébergé sur un serveur web, lui-même accessible via un réseau internet ou intranet. Le site web contient textes et multimédia.

Aujourd'hui, le Web est accessible via le protocole HTTP (HyperText Transfer Protocol) et les URL (Uniform Resource Locator). Les fichiers hébergés sur le site web reposent sur du HTML (HyperText Markup Language) + d'autres langages complémentaires. Le protocole HTTP permet au client (généralement via un navigateur web) d'accéder à des ressources par un URL. HTML et de structurer les données ou lier les ressources entre elles, notamment avec des liens hypertexte.

On parle parfois de "site Internet" au lieu de "site web". On devrait parler de website à destination d'internet, mais par abus de langage, l'expression site internet reste souvent utilisée. Les websites ne sont pas forcément accessibles sur internet. Par exemple, les intranets peuvent contenir un ou plusieurs sites web non accessibles via internet.

Un site web est composé d'un ensemble de documents structurés, nommés *pages web*, stockés (hébergés) sur un ordinateur (serveur) connecté au réseau mondial (internet).

Une page web contient essentiellement du texte, et est souvent enrichie d'images, de sons, de vidéos et de liens vers d'autres pages web.

3.1.2. A quoi sert un site web ?

Le monde évolue. Dans la vie quotidienne, internet est devenu aussi indispensable que la télévision, le téléphone, le réfrigérateur, etc. Lorsque vous arrivez sur un site web, c'est dans un but précis : trouver les réponses à vos questions, partager, communiquer, s'amuser.
L'ère numérique implique l'accès à l'information en direct, répondant au besoin du *tout* et *tout de suite*. Une page web contient des informations, généralement pour informer ou faire connaître.

Dans le cadre d'une utilisation privée, une page web permet par exemple de communiquer et de partager des ressources telles que des photos, des vidéos, des messages, etc. Pour accéder à ces ressources, il suffit d'être connecté sur internet, n'importe où dans le monde.

Les entreprises, quant à elles, auront tendance à vouloir développer leur image et notoriété, et utiliser leur site web comme support de diffusion d'information et de publicité : cela consiste à présenter l'entreprise, son activité et ses produits. C'est le meilleur rapport qualité/prix par excellence pour être visible par l'ensemble de la planète.

L'intérêt d'un site web est de pouvoir être vu par tout le monde. Son potentiel, quel que soit l'usage qu'on en fait, est illimité. Pour votre entreprise, un site web, c'est faire du marketing ciblé à moindre coût, mettre en avant votre image et affirmer votre présence sur le réseau internet. C'est surtout une façon de démontrer votre capacité d'ouverture et d'évolution : les possibilités sont illimitées en termes de différenciation, de marketing et de séduction des visiteurs.

3.2. Audit des sites Web

Pour évaluer sa qualité, nous proposons une méthode pour faire un audit de son site internet en examinant 4 aspects fondamentaux : la technologie, le design , l'ergonomie et le contenu.

3.2.1. Technologie du site Web

- Tous les internautes doivent pouvoir accéder à votre site internet et y naviguer sans obstacle, à toute heure du jour et de la nuit, et – désormais – où qu'ils soient.
- Tester l'accessibilité et la navigation sur différents supports est la première chose à faire lorsque l'on a décidé de faire un audit de son site internet.
- Observez si vous pouvez effectivement aller sur votre site depuis par exemple : un ordinateur; un smartphone; une tablette.

Pour chacun de ces supports, vous devez pouvoir lire les contenus (textes, photos, sons ou vidéos) et passer de page en page sans problème (les boutons sont-ils correctement accessibles ou le clic est-il pris en compte sur une zone qui le dépasse ?).

Une fois cette première vérification effectuée, vous pouvez tester différents navigateurs tels que Firefox, Chrome ou Internet Explorer. Tous n'interprètent pas forcément le code de votre site internet de la même façon et vous pouvez vous retrouver avec des rendus graphiques vraiment différents d'un ordinateur à l'autre.

Enfin, sur cet aspect de la technologie utilisée, vous obtiendrez une bonne idée de l'aspect qu'a votre site chez les différents internautes en demandant à vos contacts d'aller tester votre site internet. Les erreurs qu'ils relèveront en matière d'affichage ou d'utilisabilité vous permettront de voir si les différentes versions des navigateurs réagissent toutes de la même façon avec votre site.

3.2.2. Design du site Web

Même si nous avons tendance à dire à nos clients que le design n'est pas le plus important pour trouver des clients, quand on a décidé de faire un audit de son site internet, il faut tenir compte de cet aspect. En effet, le design de votre site internet transmet l'image de marque de votre entreprise à travers Internet et cela mérite que vous trouviez la nuance qui vous correspond.

Pour cela, faites encore appel à vos proches, amis et famille, en leur demandant de rester constructifs : s'ils répondent "oui c'est beau" ou "non c'est moche" demandez-leur de répondre aux questions subsidiaires "pourquoi aimes-tu ceci ou cela ?" "à quoi cela te fait penser la palette graphique ?", etc … De la même façon, il ne faut pas rentrer dans les détails précis mais essayer d'obtenir une tendance des avis des uns et des autres.

3.2.3. Ergonomie des pages Web

L'ergonomie est l'art de **placer les bons éléments aux bons endroits** et de **faire suivre à vos visiteurs un chemin utilisateur le plus direct possible**. Pour faire un audit de son site internet en matière d'ergonomie, une bonne pratique est d'**ouvrir sa page d'accueil et d'aller naviguer autant que l'on peut** sur les différentes pages du site : il ne doit y avoir aucun cul de sac !

Chacune des pages doit donc **proposer une porte de sortie** : achat d'un produit inscription à une newsletter navigation vers un article de blog formulaire de contact …

Globalement, vous devez vérifier que la navigation proposée à vos

visiteurs est facile et que ces derniers sont à tout moment au courant de l'action que vous voulez qu'ils fassent. C'est ce qu'on appelle le call to action.

3.2.4. Contenu de qualité

Aujourd'hui, sur Internet, la réussite passe par un contenu intéressant pour les visiteurs de votre site internet. Ce contenu peut souvent être "rangé" dans l'une de ces catégories : Utile; informatif; divertissant.

Une première chose consiste à vérifier que l'on dit des choses justes et de façon correcte (orthographe, grammaire, ponctuation, présentation …) !

Si on décide de faire un audit de son site internet un peu plus poussé, la seconde condition que l'on doit valider concerne l'unicité des messages pour chaque page. Le schéma à respecter pour avoir un site clair qui fait bien passer votre vision, votre message et vous permette d'atteindre vos objectifs, doit respecter le fait d'avoir sur chaque page une idée, un message unique !

Lorsque vous aurez vérifié tous ces points et éventuellement optimisé ce qui peut l'être sur ces 4 aspects, vous aurez véritablement à votre disposition un dispositif efficace pour attirer des visiteurs, les convertir en prospects puis les fidéliser.

3.3. Types d'audits des sites Web

3.3.1. Audit de l'ergonomie

La notion d'ergonomie pourrait se résumer au seul fait de proposer un site web qui correspond exactement aux attentes des utilisateurs. Il doit donc être utile et simple d'utilisation.

En effet, il faut avoir un site internet qui répond aux attentes et aux besoins de sa cible, attentes et besoins qui vont varier en fonction des spécificités de chaque profil (âge, niveau d'expérience, habitudes de naviguer sur le web..).

L'ergonomie s'appuie sur deux piliers, desquels découlent les deux étapes de l'audit :

a) *La connaissance des internautes* : Analyse du comportement des utilisateurs et identification de leur mode de fonctionnement ainsi que leurs attentes ;

b) *Le respect de bonnes pratiques* : Analyse de la structure du site, en détaillant son arborescence et le schéma de navigation.

3.3.2. Audit des fonctionnalités

Aujourd'hui un site internet se doit d'être dynamique, actif.. . Le site doit donner envie et inciter les internautes à établir un contact avec le propriétaire du site ! L'internaute doit pouvoir interagir rapidement et facilement ! « Il est dommageable qu'un mauvais fonctionnement technique ou une négligence organisationnelle du créateur du site vienne compromettre ce premier contact ».

Dans cette partie de l'audit il s'agit donc de vérifier que l'ensemble des fonctionnalités présentes sur le site sont fonctionnelles.

Il est conseillé de faire l'inventaire de ces fonctionnalités, les classer en 3 catégories et les analyser pour s'assurer de leur bon fonctionnement :

- ***Les fonctionnalités standards*** : moteur de recherche, formulaire de contact, téléchargement, plan d'accès, impressions des pages, …
- ***Les fonctionnalités e-business*** : conditions générales de vente, options de livraison et délais estimatifs, processus de facturation, mentions obligatoires CNIL, …
- ***Les fonctionnalités collaboratives*** : inscription à la newsletter, commentaires sur articles, affichage des articles liés, flux RSS, partages sur les réseaux sociaux ou via mail…

3.3.3. Audit de la compatibilité de site web

« L'audit de compatibilité permet de tester l'affichage du site sous différentes configurations, mais également de tester le temps nécessaire pour afficher la page web dans son intégralité (disponibilité) »

On va analyser donc dans cet audit l'affichage de notre site sous :

- différentes plateformes : ordinateurs, tablettes tactiles, mobiles
- différents systèmes d'exploitation : Windows, Mac, Android, iOS,
- différents navigateurs : chrome, Firefox, IE, safari..
- différentes résolutions : 1366×768, 1280×800, 1024×7698 (ordinateurs) et 320×480, 480×800 (mobile)…

3.3.4. Audit des contenus

L'audit des contenus consiste à analyser l'ensemble des contenus présentés sur le site.

a) Inventaire de l'existant

Comme à chaque fois il faut commencer par faire l'inventaire de l'existant, Xenu par exemple peut vous aider à trouver toutes les URLs de votre site et à identifier le type de fichier (HTML, IMG..).

Ensuite, il est conseillé de créer un tableau, un fichier Excel par exemple, en répertoriant l'ensemble des contenus pour lesquels vous identifierez un nombre importants d'informations : nom de la page, adresse de la page, type de contenu, responsable, date de la dernière révision, poids, état…

b) Appréciation générale

Chaque page de votre site va devoir être agréable à regarder (lire et parcourir). Les zones de texte doivent apparaitre clairement et se présenter sous forme de blocs. L'ensemble doit être aéré et harmonieux, dit l'auteur..

Les éléments à analyser et à optimiser : les titres des pages, le premier paragraphe, les sous-titres, la longueur des paragraphes, le ton employé, les visuels et les autres médias…

c) Mise en valeur du contenu

Il faut essayer de mettre en avant les principaux contenus et les mettre tous en valeur pour rendre la lecture agréable. On va soigner : la fréquence de mise à jour, les liens transversaux, les liens de proximité, …

d) Qualité du contenu

De la qualité du contenu dépend la qualité du site et la crédibilité de l'entreprise, il faut donc apporter une attention particulière : à l'orthographe et la grammaire, aux références citées, la proportion textes/visuels, la publicité omniprésente et intrusive, …

3.3.5. Audit d'accessibilité

Un site accessible lorsque son accès et sa consultation sont à la portée de tous, y compris les personnes en difficultés, atteintes d'un handicap (physique, auditif, visuel) … Voici quelques critères d'accessibilité :

- Fournir un équivalent textuel pour chaque élément non texte (ALT, légendes, descriptions) ;
- Veiller à ce que les informations avec de la couleur soient lisibles en désactivant les couleurs ;
- Identifier les changements de la langue naturelle du texte d'un document ;
- Organiser les documents afin qu'ils puissent être lus sans feuille de style ;
- Avoir un code conforme W3C.

3.3.6. Audit du référencement et du positionnement du site Web

Il consiste à effectuer un recueil des positions obtenues par un site web sur les différents moteurs de recherche et sur un univers défini de requêtes en lien avec l'activité du site.

Pour chaque mot clé retenu et moteur de recherche, l'audit de référencement relève la page d'apparition du site web et sa position sur cette page.

Dans ses versions les plus avancées et les plus pertinentes, l'audit de référencement peut permettre d'établir un score de visibilité qui consiste à affecter des points pour la présence sur chaque mot clé. Les points sont attribués en fonction du volume de requêtes sur le mot clé, de la place obtenue dans les SERP et de la part de recherche ou part de voie du moteur. L'audit de référencement se fait généralement à l'aide d'un logiciel ou service spécialisé.

L'audit de référencement peut également comprendre une phase d'analyse permettant d'expliquer les causes des éventuelles lacunes rencontrées.

3.3.7. Audit de l'e-réputation

Réaliser un audit d'e-réputation consiste à chercher sur le web tout le contenu produit qui traite d'une marque ou d'une personne.

En gros, on va chercher un peu partout sur la toile les informations nous concernant : sur Google et les autres moteurs de recherche, sur le groupes et forums de discussion, les blogs, les microblogs et surtout les réseaux sociaux ! Les informations vont vite sur la toile, il faut vraiment être au courant de tout pour pouvoir gérer son image.

3.3.8. Audit réglementaire du site

Les sites internet sont régis par un certain nombre de lois et règles que tout propriétaire de site doit respecter pour être en conformité avec la loi. Il faut donc vérifier, ici, la légalité du site.

On apprend comment créer des "Mentions légales" et des "Conditions Générales de vente" conformes à la loi…

3.4. Étapes des travaux

3.4.1. Cerner l'objectif

Avant de réaliser l'audit d'un site internet (en vue de sa refonte, de son amélioration…), il faut commencer par définir les objectifs de celui-ci : vendre, communiquer sur l'image de la marque, apporter un support client… C'est en fonction de ces objectifs que seront définis les critères d'évaluation du site.

3.4.2. Établissement de la Grille d'évaluation

L'audit du site doit être le plus objectif possible. C'est pourquoi on utilise des grilles d'évaluations comportant de nombreux critères répartis par thématiques.

En fonction du site à auditer et des objectifs définis, tous les critères ne seront pas à analyser. En effet, si l'objectif d'amélioration porte sur le manque de visibilité du site, et donc son référencement, les critères portant sur l'ergonomie seront secondaires et inversement.

3.4.3. Tri et analyse des résultats

Une fois la grille complétée, le plus important reste à faire: repérer les points forts et les points faibles du site.

Pour cela, on effectue un tri des résultats en attribuant des notes par catégories de critères, voire par sous-catégories ou par degré d'importance du critère en fonction de l'objectif préalablement défini.

Idéalement, ces résultats seront présentés sous la forme de données mais également représentés sous forme graphique afin de pouvoir communiquer et analyser plus facilement leur portée. Car l'analyse de ces données nous donnera les axes prioritaires du projet.

CONCLUSION

Pour atteindre ses objectifs, toute mission d'audit informatique doit être bien préparée et être effectuée par une équipe des experts certifiés, sur base de bonnes pratiques connues pour chaque domaine à auditer.

A l'issue de toutes les étapes de vérification, le rapport final, contenant obligatoirement les constats et les recommandations, doit être remis à qui de droit. Une fiche de suivi est enfin rédigée pour s'assurer de la mise en pratique desdites recommandations, à défaut de quoi, une descente sur terrain ou une autre mission d'audit est à effectuer.

TABLE DES MATIERES