SUPPORT DE COURS DE L'AUDIT DES SYSTEMES D'INFORMATION (INFORMATIQUE)

Raphael Grevisse Yende

SUPPORT DE COURS DE L'AUDIT DES SYSTEMES D'INFORMATION (INFORMATIQUE)

YENDE RAPHAEL Grevisse, Ph.D.

Docteur en Télécoms et Réseaux Inf.

Cours dispensé à l'Institut Supérieur Emmanuel D'Alzon en Première et Deuxième Licence : Réseaux informatiques & CSI.

TABLE DES MATIERES

BIBLIOGRAPHIE

- **Advisory, le conseil durable** (2009), *Efficacité et maitrise du système d'information, PWC,* http://pwc.to/z0SjmD
- **Ahmed Bounfour,** *Capital immatériel, connaissance et performance, Harmattan, 2006 (ISBN 978-2-2960-1128-1) p. 127*
- Cadre de Référence International des Pratiques Professionnelles de l'audit interne, IIAIFACI, 2009.
- **ISACA** publie le cadre de référence de gouvernance COBIT 5 - Isaca.org, 10 avril 2012
- **MOISAND D., GARNIER DE LABAREYRE F.** (2009), *CobiT : pour une meilleure gouvernance des systèmes d'information*, Ed. Paris : Eyrolles, 274 pages.
- **PETIT G., JOLY D. et MICHEL J.** (1985), *Audit et informatique : Guide pour l'audit financier des entreprises informatisées*, Volume 1, Ed. Paris : CLET, 268 pages.
- **SEKKAT O.** (2002), *Le rôle de l'expert-comptable face aux risques de sécurité micro-informatique dans les PME – Proposition d'une démarche d'audit*, mémoire présenté pour l'obtention du diplôme national d'expertcomptable, ISCAE, 200 pages, http://bit.ly/xZFJgX
- **SEMOUD A. et LAYMY A.** (2006), *Système d'information*, Mémoire de Licence en Sciences Economiques, Université Hassan II Mohammedia, http://bit.ly/A6HhvY
- **TOURY A.** (2006), *Proposition d'une méthodologie pour la conduite des missions d'audit informatique*, mémoire présenté pour l'obtention du diplôme national d'expert-comptable, ISCAE, 174 pages, http://bit.ly/xFoxoB
- **TOURY A.** (2006), *Proposition d'une méthodologie pour la conduite des missions d'audit informatique,* mémoire présenté pour l'obtention du diplôme national d'expert-comptable, ISCAE, p. 10, http://bit.ly/xFoxoB

AVERTISSEMENTS

Ce support d' *« AUDIT DES SYSTEMES D'INFORMATION (INFORMATIQUE) » du Docteur YENDE RAPHAEL Grevisse »,* demande avant tout, un certain entendement de l'informatique et des connaissances de base de sécurité des réseaux informatiques et principalement une prédisposition d'analyse inéluctable et cartésienne ; Vu que l'apport de ce cours, met l'accent sur les concepts de l'évaluation des systèmes d'information reposant sur une compréhension technique approfondie de la gestion des matériels informatiques et leurs modes de communication modernes. Le cours d'Audit des systèmes d'information se veut pour objectif primordial de donner aux étudiants ayant participés à ce cours, d'acquérir les fondements de l'audit des systèmes d'information en les initiant aux principaux concepts généraux liés à l'évaluation dans le domaine informatique en présentant les différentes facettes des systèmes d'information.

INTRODUCTION

L'évolution des systèmes d'information a été développée suite au processus de globalisation et d'internationalisation des marchés, cette évolution ne pouvait qu'aider à la croissance des entreprises. Le développement technologique a également marqué l'économie mondiale, et a mis les systèmes d'information au centre des organisations, ceux-ci sont devenu des facteurs stratégiques de la réalisation des performances et de la pérennité. On assistait alors, au positionnement des systèmes d'information au sein d'une fonction réservée spécialement au traitement et au développement des tâches automatisées comme par exemple, la fonction informatique[1].

L'évolution exponentielle de l'environnement interne et externe de l'entreprise requiert de celle-ci une réactivité rapide, en plus d'une claire visibilité sur les actions futures, leurs atouts et leurs enjeux. Alors, le système d'information se trouve confronté à un certain nombre de difficultés de correspondance aux besoins de l'entreprise d'une part, ainsi que d'autres difficultés de certification du point de vue des référentiels et des normes en matière informatique d'autre part. Cette certification de la correspondance, les processus informatiques et les normes relèvent des missions de l'audit informatique. Il représente l'examen officiel de la fonction informatique de l'entreprise en conformité avec les normes et les référentiels d'audit propres au système informatique.

À l'heure où la technologie fait plus que jamais partie des activités et opérations d'une organisation, les auditeurs se heurtent à une difficulté de taille, celle de la meilleure approche pour évaluer, à l'échelle de toute l'organisation, les risques liés aux systèmes d'information et les contrôles y afférents dans le cadre de leurs missions générales d'audit et de conseil. C'est pourquoi les auditeurs doivent prendre en compte l'environnement des systèmes d'information (SI), les applications et productions qui font partie de l'infrastructure, le mode de gestion des applications et opérations et la relation entre ces applications / opérations ainsi que, l'organisation de ces derniers, en recensant les composants de l'infrastructure des systèmes d'information, afin d'obtenir les informations concernant les vulnérabilités et les menaces liés à l'infrastructure[2].

[1] Il s'agit d'une fonction qui a été découverte avec l'invasion des ordinateurs, elle a passé vers une fonction de contrôle, pour être ensuite une fonction de gestion des données. Arrivée à sa maturité, la fonction informatique aujourd'hui utilise un système d'information qui représente une aide à la décision, un système harmonisé avec l'organisation et adapté aux orientations de l'entreprise.

[2] L'évaluation des vulnérabilités au sein des infrastructures SI, qui sont susceptibles d'avoir une influence sur le système de contrôle interne, commence par un inventaire complet du matériel, des logiciels, des réseaux et des données. Ainsi, les systèmes et réseaux connectés à Internet sont exposés à des menaces supplémentaires par rapport à ceux qui ne le sont pas.

Dès lors que l'environnement des SI est bien pris en compte, le responsable de l'audit et l'équipe d'audit peuvent procéder à l'évaluation des risques et établir un plan d'audit. De nombreux facteurs organisationnels entrent en ligne de compte lors de la planification du processus d'audit, tels que le secteur dans lequel travaille l'organisation, son chiffre d'affaires, le type et la complexité de ses processus ou encore la localisation géographique de ses opérations. Deux facteurs ont une incidence directe sur l'évaluation des risques et sur la définition de ce qu'il convient d'auditer au sein de l'environnement du système d'information : les composantes et le rôle de ce dernier. Par exemple :

- Quelles technologies sont employées pour supporter les fonctions opérationnelles?
- L'environnement du SI est-il relativement simple ou complexe ?
- L'environnement du SI est-il centralisé ou décentralisé ?
- Dans quelle mesure les applications sont-elles personnalisées ?
- Les activités de maintenance des SI en général ou bien certaines en particulier sont-elles externalisées ?
- A quel niveau se situe l'évolution annuelle du SI ?

Ces facteurs liés aux SI sont quelques-uns des aspects que les demandeurs de l'audit et l'auditeur en chef doivent prendre en compte pour pouvoir évaluer correctement les risques de l'organisation afin d'établir le plan d'audit adéquat.

De surcroît, il est important que le demandeur de l'audit et l'auditeur en chef recourent à une approche qui détermine précisément la probabilité de survenance des risques et leurs impacts en relation avec l'activité de l'organisation et qui définisse les domaines à risque élevé, moyen et faible, via des analyses quantitatives et qualitatives. De même, ces derniers ne doivent ignorer qu'il y a en permanence des innovations et des évolutions dans le domaine des SI. Malheureusement, ces changements peuvent entraver les efforts des auditeurs visant à identifier et à évaluer l'impact des risques. Pour aider les auditeurs informatiques, les responsables de l'audit interne doivent :

- Mesurer chaque année l'évolution spécifique de la mise en œuvre des technologies de l'information (TI), afin d'identifier celles qui pourraient avoir une incidence sur l'exposition aux risques de l'organisation ;

- Prendre connaissance chaque année des plans à court terme du département informatique, et déterminer quelles peuvent en être les conséquences sur l'évaluation des risques liés aux SI ;

- Commencer chaque audit des SI en actualisant l'évaluation des risques associés ;
- Faire preuve de souplesse vis-à-vis de l'univers d'audit des SI ; surveiller le profil de risque de l'organisation et être prêt à adapter les procédures d'audit à son évolution.

Pour une bonne assimilation de ce type d'audit, sa démarche et son importance au sein d'une structure organisationnelle, il parait convenable de commencer par une section introductive qui va nous permettre la compréhension de l'entité auditée, la fonction informatique. Alors qu'est-ce que la fonction informatique et quelle est son importance ? Ensuite, on passera à la précision de la signification de l'audit informatique, et la présentation de sa méthodologie. Alors, qu'est-ce que l'audit informatique, quelle est sa démarche et quels sont ses outils ? Pour enfin finir avec la présentation des normes et des référentiels auxquels le fonctionnement de la fonction informatique doit correspondre.

YENDE RAPHAEL Grevisse, PhD.

OBJECTIFS DU COURS

L'objectif du cours d'audit des systèmes d'information est de permettre aux participants d'acquérir les fondements de l'audit des systèmes d'information en s'initiant aux principaux concepts généraux liés à l'audit dans le domaine informatique. Et d'une manière spécifique, ce cours vise à :

- Présenter les différentes facettes de l'audit des systèmes d'information en se basant sur la démarche à suivre, le modèle à prendre en considération, ainsi que la catégorie de l'audit à utiliser lors du processus de l'évaluation des systèmes d'information ;
- Appréhender les principaux généraux de l'audit des systèmes d'information, aux moyens des règles, de l'éthique et déontologie et des erreurs à éviter ainsi qu'élucider les éléments de la politique de la sécurité de l'audit informatique ;
- Faire maitriser les normes professionnelles et les référentiels nécessaires à la réalisation de l'audit des systèmes d'information ;
- Fournir les concepts relatifs aux processus de planification et d'organisation de l'élaboration du plan de l'audit des systèmes d'information.

CHAPITRE PREMIER – INTRODUCTION A L'AUDIT DES SYSTEMES D'INFORMATION (INFORMATIQUE)

Le système d'information est d'une grande utilité au sein de l'entreprise, puisqu'il sert d'aide à la décision, il permet en plus d'agir de manière optimale, de faire des prévisions qui vont orienter les stratégies élaborés. En adition il sert à contrôler et superviser les différentes activités de l'entreprise.Avec la complexité de l'environnement de l'entreprise, les dirigeants comptent sur un système d'information ***efficace*** et ***fiable*** pour la création de la valeur et la réalisation d'un avantage comparatif. Le système d'information représente *l'ensemble de moyens, de ressources,d'éléments organisés permettant de collecter, saisir, traiter, stocker et diffuser l'information*[3].L'objectif de la mise en place des systèmes d'information se résume dans leur rôle d'aide à la conception de la stratégie de l'entreprise, ainsi que celui de la supervision de sa réalisation.

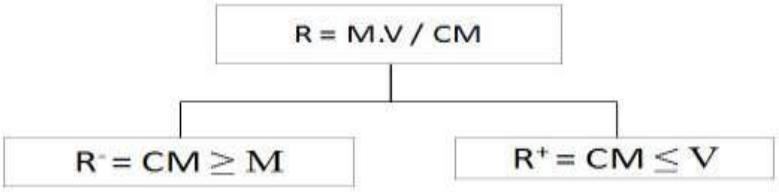
D'ailleurs, la mise en place d'un système d'information permet d'assurer la continuité de l'activité, de se garantir une information fiable et efficace à la gestion, et également se permettre d'effectuer des ajustements au niveau des orientations stratégiques avec grande souplesse.

[3]**TOURY A.** (2006), *Proposition d'une méthodologie pour la conduite des missions d'audit informatique,* mémoire présenté pour l'obtention du diplôme national d'expert-comptable, ISCAE, p. 10, http://bit.ly/xFoxoB

I.1. DEFINTION ET CONTEXTE D'ETUDES

L'audit informatique (*aussi appelé « audit des systèmes d'information ou de l'anglais Information Technology audit »*) consiste à une intervention réalisée par une personne indépendante et extérieure au service audité, qui permet d'analyser tout ou une partie d'une organisation informatique, d'établir un constat des points forts et des points faibles et dégager ainsi les recommandations d'amélioration. Autrement dit, L'audit informatique peut aussi être défini l'évaluation des risques des activités informatiques, dans le but d'apporter une diminution de ceux-ci et d'améliorer la maîtrise des systèmes d'information.

L'audit informatique a pour objectif d'identifier et d'évaluer et déterminer ***les risques*** (*opérationnels, financiers, de réputation…)* associés aux activités informatiques d'une entreprise ou d'une administration.



À cette fin, pour sa mise en place effective, un processus de l'audit des systèmes d'information va se baser sur trois (3) aspects indispensables :

- *le cadre réglementaire du secteur d'activité d'un pays donné (*exemple le ***CRBF 97-02***[4] pour la règlementation des banques françaises) ;
- *les référentiels de bonnes pratiques existants* (*exemple le référentiel* ***CobiT***, **ITIL, VAL IT** …) ;
- les ***benchmarks***[5] à disposition et sur l'expérience professionnelle de l'auditeur impliqué.

[4]Le CRBF est un « règlement n° 97-02 » du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement s'organisant autour des points suivants : les Principes et définitions ; Le système de contrôle des opérations et des procédures internes …

[5] En anglais, un benchmark (français : étalon ou repère) est un point de référence servant à effectuer une mesure les performances d'un système d'information pour le comparer à d'autres … Il peut également signifier une étude s'appuyant sur plusieurs expériences de projets déjà réalisés dans d'autres zones géographiques plus ou moins avancées.

De même, l'audit des systèmes d'information requiert deux grandes caractéristiques pour sa mise en place effective :

- *La première caractéristique* – comporte les évaluations globales d'entités durant lesquelles toutes les activités ayant trait aux systèmes d'informations sont évalués.

- *La seconde caractéristique* – correspond aux évaluations correspondantes aux audits thématiques, ayant pour objectif la revue d'un thème informatique au sein d'une entité (*la gestion de projet, la sécurité logique par exemple*).

L'audit n'est pas à confondre avec l'activité de conseil qui vise, de manière générale, à améliorer le fonctionnement et la performance d'une organisation avec une éventuelle implication dans la mise en œuvre de cette amélioration. Ces deux activités, audit et conseil, ne peuvent être exercées pour une entité donnée par les mêmes acteurs afin de ne pas créer une situation favorable aux conflits d'intérêts. Le processus de l'audit des systèmes d'information représente :

Processus de l'audit informatique

L'audit informatique est une mission, qui ne demande pas de simples auditeurs, puisque ces derniers doivent avoir de fortes connaissances en informatique, car des notions, ainsi que des techniques sont à cerner pour comprendre et savoir gérer un processus d'informatisation.

I.2. MODELES DE L'AUDIT DES SYSTEMES D'INFORMATION

Un « *modèle* » est une base donnée pour servir de référence. En conséquence, il existe 2 modèles d'audit des systèmes d'information : *le modèle de l'audit de besoin* et *le modèle de l'audit de découverte des connaissances*.

I.2.1. LE MODELE DE L'AUDIT DE BESOIN

De part sa définition, un « *besoin* » peut être considéré comme un élément nécessaire à l'existence (autrement dit, c'est un état qui résulte de la privation ou d'un manque du nécessaire). Le modèle de l'audit du besoin est subdivisé en 2 grandes parties : *l'analyse de l'existant* et *la détermination de la cible*.

- *L'analyse de l'existant* – consiste en un examen (appréciation) du terrain au terme duquel l'auditeur informatique formalise la circulation des « documents-types » d'un acteur à l'autre et le traitement que chaque acteur applique à ces documents, à l'aide de *logigrammes* (traitement sur les documents) et la représentation des *graphes relationnels* (circulation des documents) ;

- *La détermination de la cible* – cette seconde partie consiste à référer le mode de circulation des informations et leurs interprétations ; les différentes redondances dans les graphes ; la dispersion des infrastructures ainsi que les point de contrôle et de validation nécessaires, et le découpage en zone en sous-graphes.

N.B : c'est à l'issue de ce modèle, que généralement le processus de l'audit aboutit à une élaboration et approbation d'un projet informatique.

I.2.2. LE MODELE DE L'AUDIT DE DECOUVERTE DES CONNAISSANCES

Le modèle de l'audit de découverte des connaissances consiste à valoriser les données et les connaissances existantes dans l'entreprise. Généralement, ce modèle aboutit au montage d'un système d'information décisionnel (désigne les moyens, les outils et les méthodes qui permettent de collecter, consolider, modéliser et restituer les données matérielles et immatérielles d'une entreprise) mais également être le prélude (précurseur) à un système de gestion de connaissances.

Le modèle de l'audit de découverte des connaissances se pratique de la manière suivante :

- Pas d'objectifs : on ne sait pas ce que l'on va découvrir ;
- Un domaine : on sait sur quels métiers on travaille, donc sur quelles bases de données;
- une équipe intégrée : travaille in situ, trois acteurs dont un expert « métier », un expert « administration informatique » et un fouilleur de données (voir data mining) ;
- Le travail se fait par boucle courte de prototypage ;
- Pour faciliter le brassage des données, on modifie leur format et leur disposition relative. C'est le « pré-processing » qui prend le plus de temps ;
- À l'aide d'algorithmes à apprentissage d'une part, et de visualisations de données d'autre part, le fouilleur met en évidence des liens empiriques entre les données ;
- Les corrélations et liens retenus doivent répondre à trois critères : inconnu de l'utilisateur, explicable a posteriori et utile. La démonstration théorique du phénomène est totalement superflue ;
- Les connaissances détectées sont formalisées (arbres, graphes, tableaux, règles, etc.) puis prototypées logiciellement ;
- La validité des connaissances prototypées est vérifiée grâce à un test statistique (khi deux, kappa, etc.) sur un jeu de données dit « test set », différent du jeu ayant servi à l'analyse (« training set ») ;
- Le test set peut être soit externe au training set, soit recalculé à partir de lui (rééchantillonnage) ;
- Si le test est passé, le modèle est mis en production ;
- On recommence le cycle.

Concrètement, l'empilement des modèles, eux-mêmes parfois complexes (arbres et récursivité) peuvent aboutir à de vrais problèmes d'architecture informatique : *les Parallélisassions des calculs* ; *la Volumétrie des données* ; et *la Charge du réseau, en partie due aux mécanismes de réplication.* D'un autre côté, le résultat de calcul issu d'un empilement de modèles peut aboutir à des résultats particulièrement pertinents et surprenants.

I.3. TYPOLOGIE DE L'AUDIT DES SYSTEMES D'INFORMATION

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 les télécommunications, la sécurité informatique, les achats informatiques, 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 différentstypes d'audits informatiques les plus fréquents :

I.3.1. 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. L'audit de la fonction se base sur ces pratiques dans le but d'identifier un certain nombre d'objectifs de contrôle comme :

- 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, et 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…

I.3.2. AUDIT DES ETUDES 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 des bonnes pratiques recensées dans ce domaine. Elles sont nombreuses et connues par tous les professionnels. Parmi celles-ci 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 tableau 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 l'auditer on va se baser sur ces bonnes pratiques afin de dégager un certain nombre d'objectifs de contrôle comme :

- 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 prévues ;
- 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 fonctions des préoccupations du demandeur d'audit.

I.3.3. AUDIT DE L'EXPLOITATION

L'audit de l'exploitation a pour but de s'assurer que 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 d'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 :

- 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, et 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.

I.3.4. AUDIT DES PROJETS INFORMATIQUES

L'audit des projets informatiques 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 fortes chances d'arriver à la fin de la phase de développement à une application qui sera performante et opérationnelle. Comme on le voit un audit d'un projet informatique ne se confond pas avec un audit des études informatiques. Pour effectuer un 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 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 de management de la qualité ;
- 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 :

- 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 évaluation 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 fonction des préoccupations et des attentes du demandeur d'audit.

I.3.5. AUDIT DES APPLICATIONS OPERATIONNELLES

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 ? Les audits précédents sont des audits informatiques, alors que 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 souhaitable 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 bonne qualité ;
- 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 est efficace et productif,

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.

I.3.6. AUDIT DE LA SECURITE 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 de risque pour 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, l'indisponibilité du service, et le détournement de trafic ;

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 contrôle d'accès, et 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 (*Responsable de la Sécurité des Systèmes d'Information)* ;

- Evaluer 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 RSSI 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 chiffrement des données, le plan de secours,…

Il existe de nombreux autres objectifs[6] de contrôle concernant l'audit de la sécurité informatique qui sont choisis en fonction des préoccupations et des attentes du demandeur d'audit.

[6] Ces différents objectifs de contrôle correspondent aux processus de CobiT DS 5 : « *Assurer la sécurité des systèmes* » et PO 9 « *Evaluer 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.

CHAPITRE DEUXIEME – PRINCIPES GENERAUX DE L'AUDIT DES SYSTEMES D'INFORMATION

Dans le cadre de cours, nous allons définir « ***un principe*** » comme étant un ensemble de règles définissant une manière type d'agir et correspondant le plus souvent à une prise de position morale ou une proposition fondamentale qui sert de base a un raisonnement déterminant un mode d'action. D'une façon générale, l'audit informatique repose sur deux principes essentiels qui suivent logiquement ce qui suit :

1. *Un audit informatique n'a de sens que si sa finalité est définie* : *contrôle fiscal, juridique, expertise judiciaire, vérification de l'application des intentions de la direction, examen de l'efficacité ou de la sécurité d'un système, de la fiabilité d'une application, etc.*

2. *Un audit informatique doit rationnellement être explicite en déduisant les moyens d'investigation jugés nécessaires et suffisants* **:** pratiquement, cela veut dire que l'auditeur doit apprécier dans un but précis une situation concrète observée « *le comment* », l'application du principe et des règles « *le pourquoi* ».

C'est ainsi que l'établissement de ces principes conduira maintenant *aux règles* et a *la déontologie* de l'audit informatique.

II.1. REGLES D'AUDIT DES SYSTEMES D'INFORMATION

Quel que soit le type de l'audit (*interne ou externe, contractuel ou légal, etc.)*, la finalité est toujours de porter un jugement sur le management du système d'information et l'exécution de ses objectifs. Ainsi, les règles de l'audit informatique doivent être établit comme *une comparaison entre ce qui est observé* et *ce que cela devrait être*, selon un système de références :

➔ L'audit informatique doit porter non seulement au jugement, qui ne peut se limiter qu'à une approbation ou plus à une condamnation, qui serait totalement inutile en soi aux audités, mais également préciser ce qu'il aurait fallu faire, et ce qu'il faudra faire pour corriger les défauts constatés.

➔ L'audit informatique doit consister à comparer l'observation d'un ou plusieurs objets, selon un ou plusieurs aspects, à ce qu'ils devraient être, pour porter un jugement et faire des recommandations.

➔ *La tâche de l'auditeur doit être parfaitement définie quant à l'objet et l'aspect de l'audit à mener et elle ne doit pas en déborder* : C'est par exemple, si on demande à l'auditeur de vérifier la sécurité d'une application, et qu'il en est satisfait, il est complètement indifférent de savoir si les résultats en sont exacts ou pas, car c'est une question de fiabilité ; ou qu'ils sont absolument inutiles, car il s'agit d'adaptation.

➔ *L'auditeur ne doit jamais remettre en cause la finalité de son audit en fonction de ce qui est plus simple, ou plus intéressant de faire, selon ses goûts. Il est beaucoup plus facile de formuler cette règle que de l'appliquer* : qui n'a tendance à la transgresser, surtout si des lacunes évidentes mais hors mission se révèlent.

➔ *L'audit informatique doit toujours être faisable* : c'est-à-dire que le travail d'audit peut être assez complexe, et donc il doit obéir aux mêmes règles que le management, et en particulier être découpé en fonctions conduisant L'audit informatique de façon arborescente à un plan avec des étapes significatives de conclusions partielles. Mais le maillon le plus faible de sa démonstration est bien entendu celui qui remet tout en cause. C'est par exemple Si la mission concerne la sécurité d'une application de gestion du personnel, l'auditeur peut éluder avec accord du demandeur d'audit, les questions de plan et de budget ; il lui faudra examiner à fond mais sous le seul aspect de sécurité et dans la mesure où ils concernent cette application, les matériels et logiciels, les ressources humaines, les contrats, les méthodes, et enfin les réalisations et leur exploitation. Cela fait, et puisqu'il a examiné tous les objets concernés selon l'aspect demandé, les conclusions de l'auditeur seront certaines et inébranlables

➔ *Les moyens et actions de l'auditeur doivent être adaptés exclusivement mais exhaustivement au sujet de l'audit* : Cela implique naturellement l'évolutivité (*ouverture de recommandations sur l'avenir, et non des simples objectifs d'audit informatique des constats et d'échecs*), la cohérence et la planification des ressources, bien entendu l'exactitude des conclusions.

➔ *L'audit informatique doit impliquer les méthodes et les programmes sensibles de l'application, les saisies d'informations, les recyclages d'anomalies, et la bibliothèque* : C'est alors seulement l'auditeur pourra affirmer avoir fait une étude exhaustive et trouvé toutes les failles possibles.

➔ *La sécurité de l'audit informatique ne doit s'appliquer qu'aux documents de travail et aux rapports, et non à leur diffusion hors destinataires autorisés* : L'avancement des travaux doit être logique comme une démonstration mathématique, donc arborescente, ainsi pour prouver une telle affirmation, il faut s'assurer de la véracité et de la décomposition des faits. C'est par exemple : Pour prouver qu'une application de gestion du personnel est sûre, et à supposer que le demandeur d'audit, ne soit pas intéressé par un examen de ses finalités, ni des moyens financiers en ce domaine, il faudra examiner les sécurités du matériel et du logiciel de base, y compris les réseaux, utilisés par cette fonction.

II.2. DEONTOLOGIE DE L'AUDIT DES SYSTEMES D'INFORMATION

Par Déontologie de l'audit informatique est l'ensemble des règles et des devoirs qui régissent une profession, le conduit de ceux qui l'exercent, les rapports entre ceux-ci et leurs clients privé ou public. Il s'ensuit que **l'auditeur doit obéir,** de soi-même car en dehors des responsabilités juridiques rien ne l'y oblige, à une *déontologie* certaine. C'est ainsi qu'il doit :

➔ *s'interdire de cumuler **audit et conseil**, sur une même question* : comment auditer quelque chose que l'on a conseillé, ou bien recommander de prendre son conseil? Pourtant il existe des sociétés proposant simultanément conseil, service et audit ; l'intérêt de proposer un audit qui recommandera de prendre un conseil de réalisation, puis le conseil proposant un service, le tout effectué par la même société, laisse à réfléchir sur l'objectivité dans l'intérêt du client.

➔ L'auditeur doit garantir, même implicitement par une simple acceptation d'une tâche, qu'il a, par lui-même ou grâce à une équipe sur laquelle il peut compter, les compétences nécessaires :

➔ L'auditeur doit comprendre qu'il ne s'agit que d'attitudes, presque purement psychologiques: l'auditeur n'a pas besoin du souffle ni des connaissances approfondies pour mener à bien une réalisation, mais il doit être rapide, précis, avec juste les connaissances ponctuelles nécessaires et suffisantes ;

➔ L'auditeur doit s'intéresser au système d'information dans son ensemble, c'est-à-dire il ne doit pas s'atteler aux seuls éléments automatisés, ou au contraire à ceux qui ne le sont pas ;

➔ L'auditeur doit fournir des conclusions motivées, utiles, sur l'objet et l'aspect, ainsi que la période de temps qui a dû être considérée, qui ont été les éléments de sa mission. Ainsi d'autres considérations générales ou non explicitement justifiées doivent être considérées irrecevables, en particulier des termes aussi vagues que « *diagnostic* », ou, pire « *évaluation* ».

➔ L'audit informatique qui suggère une quantification des faits est inacceptables sauf éventuellement dans un contexte précis, et dans le délai imparti et accepté. Le domaine de la tâche d'un auditeur est donc très rigoureusement défini en termes d'objets, d'aspects, et de cadre temporel, et sa démarche est d'une démonstration rigoureuse et exhaustive. Les sujets d'audit doivent être maintenant évidents.

II.3. LES ERREURS DE L'AUDIT DES SYSTEMES D'INFORMATION

Si l'erreur n'était pas humaine, il n'y aurait pas besoin d'auditeur. Elle provient de défaillances dans la représentation de la réalité et la compréhension des observations par :

➔ La faute de connaissance d'interprétation et de représentation ;

➔ La faute concernant les hypothèses déduites (*modèle mental inexact, incomplétude ou ambiguïté)* et induites (*suppositions erronées*) ;

➔ le choix des objectifs (*contradictoires, hors délais, superflus, faute de raisonnement*) ;

➔ le choix des solutions (*saturation mentale, analogie injustifiée, confusion*) ;

➔ l'irréalisation (*erreurs de communication, de procédure, de vérification*).Et en informatique, il ne faut compter sur aucune Indulgence, aucune tolérance, dès lors que la solution est automatisée. Sinon, le principe et ces règles n'auraient pas de raison d'être exposés s'ils ne pouvaient être mis en œuvre.

II.4. LA CERTIFICATION DES AUDITEURS DES SYSTEMES D'INFORMATION

Dans le cadre de ce cours, nous allons définir la « *certification* » comme une procédure d'authentification et de contrôle de la qualité d'un informaticien pour jouir des droits légitimes d'être auditeur informatique (évaluateur des systèmes d'information) par les organismes de normalisation au moyen d'un écrit, oral ou en ligne.

En informatique, il n'existe pas une certification des directions informatiques ou des applications informatiques, par contre une certification de la qualité des projets informatiques comme par exemple *CMMI*. 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. Il existe également une procédure de certification des « *outsourceurs* », comme par exemple le « *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. La norme SAS 70 a été remplacée depuis par la norme ISAE 3402 (*International Standards for Assurance Engagement*) entrée en vigueur le 15 juin 2011. Il s'agit d'une extension de SAS 70 qui définit les standards qu'un auditeur doit suivre pour évaluer les contrôles internes contractuels d'un organisme de service.

Actuellement, En matière d'audit informatique ; il existe deux grandes certification de référence mise au point par ISACA (*Information Systems Audit and Control Association) :*

1. **La certification CISA** (*Certified Information Systems Auditor*) : C'est une certification professionnelle internationale. Elle est organisée par l'ISACA depuis 1978. À ce jour dans le monde 75 000 personnes ont la certification CISA. L'examen peut être passé trois fois par an : en juin, en septembre et en décembre, dans 11 langues différentes et dans 200 villes dans le monde. Il faut répondre de 150 à 200 questions à choix multiples en 4 heures portant sur l'audit et l'informatique. L'examen porte sur 6 domaines :

   - les processus d'audit des systèmes d'information ;
   - la gouvernance IT ;
   - la gestion du cycle de vie des systèmes et de l'infrastructure,

- la fourniture et le support des services ;
- la protection des avoirs informatiques ;
- le plan de continuité et le plan de secours informatique.

2. **La certification CISM** (*Certified Information Security Manager)* : c'est une deuxième certification des auditeurs informatiques de référence depuis 2003. il s'agit d'une certification professionnelle pour les managers en sécurité de l'information délivrée également par l'ISACA. Cette certification est subdivisée en deux grandes catégories :

   - **CRISC** (*Certified in Risk and Information Systems Control*): c'est une certification en risqué et contrôle des systèmes d'information.

   - **CGEIT** (*Certified in the Governance of Entreprise IT*) : c'est une certification en gouvernance des technologies de l'information des entreprises.

Le programme de la certification CISM est composé de 5 domaines de la sécurité de l'information :

- La gouvernance de la sécurité de l'information ;
- La gestion des risques de l'information ;
- L'implémentation d'un programme de sécurité de l'information ;
- La gestion d'un programme de sécurité de l'information ;
- La gestion des incidents de sécurité de l'information.

À ces certifications proposées par l'ISACA, d'autres certifications peuvent s'ajouter à la panoplie de l'auditeur informatique, notamment le *CISSP* sur la sécurité informatique, *la certification ISO27001* lead auditor, *les certifications sur ITIL*, Prince2, CobIT, etc. Enfin, l'obtention du CISA permet de bénéficier d'un module de la certification CIA de l'Institute of Internal Auditors (IIA).

CHAPITRE TROISIEME – SCHEMA CONCEPTUEL DE L'AUDIT DES SYSTEMES D'INFORMATION

Un audit des systèmes d'information ne concerne pas nécessairement la sécurité. En effet, il peut aussi évaluer des aspects stratégiques ou de qualité des systèmes d'information. Par exemple, répondre à la question suivante : Est-ce que les systèmes d'information de l'entreprise répondent efficacement aux besoins des services métiers ? Ce chapitre pourra répondre à la question d'ordre conceptuel tel que la démarche et la planification et les processus d'élaboration de l'audit des systèmes d'information.

III.1. DEMARCHE D'AUDIT DES SYSTEMES D'INFORMATION

Une mission d'audit informatique se prépare. Il convient de déterminer un domaine d'études pour délimiter le champ d'investigation. En ce sens il est conseillé d'effectuer un pré-diagnostic afin de préciser les questions dont l'audit va traiter. Cela se traduit par l'établissement d'une lettre de mission détaillant les principaux points à auditer. Pour mener à bien l'audit informatique il est recommandé de suivre cinq phases suivantes :

III.1.1. LE CADRAGE DE LA MISSION

Les objectifs du cadrage de la mission se présentent comme suit :

- Une délimitation du périmètre d'intervention de l'équipe d'audit informatique. Cela peut être matérialisé par une lettre de mission[7], une note interne, une réunion préalable organisée entre les équipes d'audit financier et d'audit informatique ;
- Une structure d'approche d'audit et organisation des travaux entre les deux équipes ;
- Une définition du planning d'intervention ;
- Une définition des modes de fonctionnement et de communication.

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

[7] 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.

III.1. 2. LA COMPREHENSION DE L'ENVIRONNEMENT INFORMATIQUE

Elle a pour but de comprendre les risques et les contrôles liés aux systèmes informatiques et Elle doit permettre de déterminer comment les systèmes clés contribuent à la production de l'information financière. Elle se fait sur la base de 3 aspects notamment :

1. L'organisation de la fonction informatique : A ce stade, l'auditeur devra saisir les éléments suivants :

- *La stratégie informatique de l'entreprise* : il s'agit bien d'un examen du plan informatique, du comité directeur informatique, des tableaux de bords etc.
- *Le mode de gestion et d'organisation de la fonction informatique* : il s'agit notamment de comprendre dans quelle mesure la structure organisationnelle de la fonction informatique est adaptée aux objectifs de l'entreprise. En outre, il faudrait apprécier si la fonction informatique est sous contrôle du management. A cet effet, il faudrait examiner les aspects suivants : L'organigramme de la fonction informatique (son adéquation par rapport aux objectifs assignés à la fonction, la pertinence du rattachement hiérarchique de la fonction, le respect des principes du contrôle interne) ; La qualité des ressources humaines (compétence, expérience, gestion des ressources, formation) ; Les outils de gestion et de contrôle (tableaux de bord, reporting, contrôles de pilotage) ; Les procédures mises en place(leur formalisation, leur respect des principes de contrôle interne, leur communication au personnel).

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

- *Les caractéristiques des systèmes hardware utilisés* (leur architecture, leur procédure de maintenance, les procédures de leur monitoring) ;
- *Les caractéristiques des systèmes software* (systèmes d'exploitation, systèmes de communication, systèmes de gestion des réseaux, de la base des données et de la sécurité, utilitaires).

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

III.1.3. L'IDENTIFICATION, EVALUATION DES RISQUES ET DES CONTROLES AFFERENTS AUX SYSTEMES

Il y a lieu d'identifier les risques liés aux systèmes informatiques et au contrôle dans un environnement informatisé. Ils concernent aussi bien les risques liés aux contrôles généraux informatiques que ceux liés aux applications. Se focaliser sur les risques ayant un impact direct ou indirect sur la fiabilité des états financiers demeure indispensable. Les risques liés à la fonction informatique sont relatifs à l'organisation de la fonction informatique, au développement et mise en service des applications, à la gestion de l'exploitation et à la gestion de la sécurité. Une fois ces risques recensés, l'auditeur devra évaluer les contrôles mis en place par l'entreprise pour gérer ces risques.

S'en suit, La collecte des faits, et la réalisation des opérations. 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, et les entretiens avec les audités permettent de compléter les faits collectés grâce à la prise en compte des informations détenues par les opérationnels. Cette phase peut être délicate et compliquée. Souvent, les informations collectées auprès des opérationnels ressemblent plus à des opinions qu'à un apport sur les faits recherchés,

III.1.4. LES TESTS DES CONTROLES

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

III.1.5. LA REDACTION DU RAPPORT D'AUDIT ET LES RECOMMANDATIONS

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. 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. Le non-respect de cette démarche peut entrainer une mauvaise réalisation et mise en place d'outils qui ne sont pas conformes aux réels besoins de l'entreprise.

Cette démarche est essentielle pour l'auditeur car il lui apporte des éléments fondamentaux pour le déroulement de sa mission mais celle-ci est encore plus bénéfique pour l'organisation. En effet, les acteurs audités ne sont pas passifs. Ils sont amenés à porter une réflexion sur leurs méthodes de travail et à s'intéresser au travail des autres acteurs de l'entité. Cela conduit à une cohésion d'équipe et à un apprentissage organisationnel. Il s'agit d'un facteur positif car en cas de changement les acteurs seront moins réticents.

III.2. PLANIFICATION ET PROCESSUS D'ELABORATION DE L'AUDIT DES SYSTEMES D'INFORMATION

L'une des principales attributions du responsable de l'audit des systèmes d'information, qui est aussi l'une de ses missions les plus délicates, consiste à élaborer un plan d'audit pour l'organisation. Comme l'explique la Norme 2010 de l'IIA (The Institute of Internal Auditors), « *le responsable de l'audit doit établir une planification fondée sur les risques* » afin de déterminer les priorités d'intervention, qui doivent elles-mêmes se conformer aux stratégies et objectifs de l'organisation. En outre, le responsable de l'audit doit envisager des missions de conseil en fonction de la valeur ajoutée qu'elles pourraient apporter et des progrès qu'elles pourraient induire dans les opérations et les activités de management des risques de l'organisation. Ces activités ont été documentées dans l'étude 2006 du *Common Body of Knowledge* (CBOK, base commune de connaissances) de l'IIA Research Foundation.

Pour élaborer un plan d'audit fondé sur le risque, le responsable de l'audit des systèmes d'information devra d'abord procéder à une évaluation des risques portant sur l'ensemble de l'organisation. L'évaluation adéquate des risques liés aux SI, composante essentielle de l'évaluation globale des risques, constitue un volet essentiel de la gestion des risques. C'est un facteur déterminant pour mettre en place des programmes de missions efficients. « *Pour de nombreuses organisations, l'information et la technologie sur laquelle elle repose représentent leur actif le plus précieux. En outre, étant donné que les entreprises évoluent dans un environnement concurrentiel et en constante mutation, la direction exprime, vis-à-vis des fonctions gérant et mettant en œuvre le SI, un niveau d'exigence croissant à travers : une qualité de service en constante amélioration, des fonctionnalités et une facilité d'utilisation accrues, un raccourcissement des délais, le tout alors que les coûts doivent être comprimés* ».

Quelles que soient la méthodologie retenue et la fréquence des activités de planification de l'audit, le responsable de l'audit et l'équipe d'audit des systèmes d'information devront prendre en compte l'environnement du SI avant de procéder à l'audit. La plupart des activités d'une organisation font appel à la technologie. Qu'il s'agisse de la collecte, du traitement et de la communication d'informations comptables, ou bien de la fabrication, de la vente ou de la diffusion de produits, quasiment toutes les activités d'une organisation reposent, à plus ou moins grande échelle, sur la mise en œuvre de moyens technologiques. Ces derniers ont vu leur rôle évoluer : elle n'est plus seulement un support opérationnel pour les processus de l'organisation, mais fait partie intégrante du contrôle des processus. Le contrôle interne des processus et des activités reposent ainsi de plus en plus sur la technologie, dont les déficiences ou le manque d'intégrité ont un impact important sur l'atteinte des objectifs et la réalisation des opérations de l'entreprise. Toutefois, l'élaboration d'un plan d'audit des SI efficace, fondé sur le risque, est une tâche difficile pour les auditeurs informatiques, surtout lorsqu'ils n'ont pas une connaissance suffisante des SI.

La définition du plan d'audit des systèmes d'information doit respecter un processus systématique si l'on veut être sûr que tous les aspects fondamentaux de l'activité sont bien compris et pris en compte. En conséquence, il est essentiel que le plan s'appuie sur les objectifs, les stratégies et le modèle d'activité de l'organisation. Le tableau ci-dessous décrit la progression logique des flux de travail permettant, au moyen d'une approche du général au particulier (*top-down*), de définir le plan d'audit des SI qui sera utilisé comme guide dans le processus des systèmes d'information.

CONSIDERATION DE L'ACTIVITE	DEFINITION DE L'UNIVERS DES SI	EVALUATION DES RISQUES	FORMALISATION DU PLAN D'AUDIT
• Identifier les stratégies et objectifs de l'organisation ; • Prendre en compte ce qui présente un profil de risque élevé pour l'organisation • Prendre en compte comment l'organisation structure ses opérations • Prendre en compte le modèle de fonctionnement de la Direction des Systèmes d'Information comme support de l'activité de l'entreprise.	•Analyser les fondamentaux de l'activité ; • Identifier les applications importantes qui concourent au traitement des opérations de l'organisation, en tenant compte du rôle des moyens technologiques intervenant dans ce traitement ; • Identifier l'infrastructure critique pour les applications importantes ; • Identifier les grands projets et initiatives ; • Définir des thèmes d'audit réalistes	•Mettre au point des processus d'identification des risques ; • Évaluer les risques spécifiques au SI et classer les thèmes d'audit à partir des facteurs correspondants	• Sélectionner les thèmes d'audit retenus et les grouper en missions d'audit distinctes ; • Définir le cycle d'audit et sa Fréquence ; • Ajouter des missions répondant aux demandes de la direction ou constituant des opportunités pour remplir une mission de conseil ; • Valider le plan avec la direction

III.2.1. PRISE EN COMPTE DE L'ACTIVITE

Il est capital de commencer avec la bonne perspective pour pouvoir définir un plan d'audit efficace. C'est pourquoi, il faut garder à l'esprit que le seul but de la technologie est de constituer un levier pour mieux atteindre les objectifs de l'organisation, sachant que toute défaillance du SI va à l'encontre de ce but et constitue un risque pour l'organisation de ne pas les atteindre. Il est donc important de *commencer par prendre connaissance des objectifs*, *stratégies et modèles d'activité de l'organisation*, ainsi que *la place des moyens technologiques dans son développement*. Pour ce faire, il faut identifier les risques associés aux technologies mises en œuvre, et déterminer comment chacun d'eux peut entraver la réalisation des objectifs de l'organisation. On aboutira ainsi à une évaluation plus significative et plus utile pour la direction générale.

En outre, l'auditeur doit se familiariser avec le modèle d'activité de l'organisation. Chaque organisation ayant une mission distincte et des buts et objectifs qui lui sont propres, le modèle d'activité aide l'auditeur à identifier les produits ou services que propose l'organisation, ainsi que sa base de clientèle, ses chaînes d'approvisionnement, ses processus de fabrication ou de production et ses mécanismes de mise à disposition. C'est ainsi que l'auditeur devra analyser les éléments ci-après :

- **Une organisation unique** - Chaque organisation est différente. Les organisations d'un même secteur n'auront pas toutes le même modèle d'activité, des objectifs et des structures identiques, ni les mêmes environnements et schémas de mise en œuvre du SI. C'est pourquoi, les plans d'audit doivent être conçus spécifiquement pour chaque organisation.

- **L'environnement opérationnel** - Pour se familiariser avec une organisation, les auditeurs doivent d'abord prendre en compte les objectifs et savoir comment les processus sont structurés pour atteindre ses objectifs. Les auditeurs peuvent exploiter diverses ressources internes pour identifier et prendre en compte les buts et objectifs de l'organisation, notamment : les énoncés de la mission, de la vision et des valeurs ; les plans stratégiques ; les plans annuels de prévision de l'activité ; le tableau de bord de performance du management ; les rapports aux actionnaires et annexes ; les documents requis par la réglementation.

- **Facteurs liés à l'environnement des SI** - Pour bien prendre en compte l'environnement opérationnel et les risques qui y sont associés, différents facteurs et techniques d'analyse seront pris en considération. En effet, la complexité de l'environnement de contrôle d'une organisation aura une incidence directe sur son profil de risque global et son système de contrôle interne. Il y a plusieurs facteurs importants à prendre en compte : *Le niveau de centralisation du système et de centralisation géographique (distribution des ressources SI) ; Les technologies déployées ; Le degré de personnalisation ; Le degré de formalisation des politiques et référentiels de l'organisation (gouvernance des SI, par exemple) ; Le degré de réglementation et de conformité ; Le degré et le mode d'externalisation ; Le degré de standardisation des opérations et Le degré de dépendance technologique.*

III.2.2. DEFINITION DE L'UNIVERS DE L'AUDIT DES SYSTEMES D'INFORMATION

Définir ce qu'il convient d'auditer est l'une des tâches les plus importantes de l'audit informatique, étant donné que le programme d'audit des SI aura un impact considérable sur la performance globale du service d'audit. Par conséquent, le but ultime du plan d'audit des SI est d'assurer une couverture adéquate des domaines qui représentent la plus grande exposition au risque et, ceux qui représentent un enjeu majeur pour l'auditeur dans l'apport qu'il constitue en matière de valeur ajoutée à l'organisation.

L'une des premières étapes vers un plan d'audit des SI efficace consiste à définir *l'univers d'audit des SI*, c'est-à-dire un ensemble fini et exhaustif des domaines d'audit, schéma structurel des entités opérationnelles et localisation des activités réalisées par l'organisation, qui représentent les cibles d'audit permettant de donner une assurance appropriée sur le niveau de maîtrise des risques auxquels l'organisation est exposée. Lors de cette première étape, l'identification des domaines d'audit potentiels, au sein de l'univers d'audit, se fait indépendamment du processus d'évaluation des risques. Les auditeurs auront conscience des audits qui peuvent être réalisés avant de réaliser une évaluation et une hiérarchisation des risques aboutissant à un programme d'audit. La définition de l'univers d'audit des SI nécessite une connaissance approfondie des objectifs de l'organisation, du modèle d'activité et des prestations assumées par la Direction des SI. La définition de l'univers des SI se poursuit :

- **Examiner le modèle d'activité -** Pour les organisations, l'atteinte des objectifs repose sur le fonctionnement des diverses directions opérationnelles et fonctionnelles, à travers les processus spécifiques qu'elles ont à gérer afin d'atteindre leurs propres objectifs, en liaison néanmoins avec les autres entités.

- **Rôle des technologies d'appui -** Il peut être simple d'identifier les infrastructures technologiques qui soutiennent le SI lorsque l'on détecte des activités qui reposent sur des applications clés. En revanche, il est bien plus difficile de mettre l'utilisation des moyens technologiques communs, comme le réseau général, une application de messagerie électronique ou son logiciel de chiffrement, en relation avec les objectifs et les risques. Pourtant, ces moyens technologiques communs existent parce que l'organisation en a besoin et une défaillance de ces services et équipements peut empêcher l'organisation d'accomplir sa mission. C'est pourquoi, les moyens technologiques communs clés doivent être identifiés et représentés dans l'univers des domaines auditables, même s'ils ne sont pas directement associés à une application ou à un processus opérationnel.

- **Plans d'activité annuels -** Un autre point est important : il faut tenir compte du plan stratégique de l'organisation. Les plans opérationnels peuvent apporter aux auditeurs des informations sur les changements et projets importants susceptibles de voir le jour dans l'année à venir, qui pourraient nécessiter l'intervention de l'audit et devenir des sujets à intégrer dans l'univers d'audit des SI. Les projets peuvent avoir directement trait aux SI, par exemple la mise en œuvre d'un nouveau système d'ERP, ou porter sur la gestion d'initiatives majeures d'ingénierie ou de construction.

- **Fonctions SI centralisées / décentralisées**- Les auditeurs auront à identifier les fonctions SI administrées au niveau central, qui soutiennent la totalité ou une grande partie de l'organisation. Les fonctions centralisées sont de bons « candidats » aux différents audits réalisés au sein de l'univers d'audit des SI. Il s'agit notamment de la conception et de l'administration de la sécurité du réseau, de l'administration des serveurs, de la gestion des bases de données, des activités de service ou d'assistance et des opérations traitées sur des sites centraux (*mainframe*).

- **Les processus de soutien des SI -** Même si l'organisation comporte une fonction SI décentralisée, elle peut disposer de processus transversaux standardisés. Les organisations qui s'efforcent d'être performantes comprennent l'importance de disposer de processus transversaux standardisés à travers toutes leurs directions opérationnelles, quel que soit leur type d'activité. On peut citer, comme exemples de processus transversaux standardisés, les activités du centre de service (*hotline*), les procédures de gestion des changements, des configurations, des mises en production, des incidents et autres problèmes. Le centre de service est généralement le premier point de contact auprès duquel les clients peuvent formuler une requête ou une demande de résolution de problème lié aux SI. Ce qui déclenche un processus de gestion du cycle de vie de la requête à travers une succession d'événements se rapportant à la gestion des incidents, des problèmes, des changements et des mises à jour.

- **Conformité à la réglementation** - Diverses lois et réglementations à travers la planète, en particulier la loi Sarbanes-Oxley et Bâle II, imposent d'appliquer des contrôles internes et des pratiques de gestion du risque, ainsi que de respecter la confidentialité des données personnelles .Comme indiqué plus haut, certaines de ces réglementations imposent de protéger les informations relatives aux clients en matière de cartes de crédit (par exemple, la GLBA et la PCI DSS) ainsi que les informations médicales personnelles (par exemple l'HIPAA). Même si la plupart de ces règles ne concernent pas directement les contrôles des SI, elles supposent l'existence d'un environnement de SI soumis à un contrôle adéquat. En conséquence, ces points de la réglementation sont susceptibles d'être intégrés dans l'univers d'audit : les auditeurs doivent déterminer si l'organisation a mis en place des processus rigoureux et si elle opère efficacement afin de garantir la conformité.

- **Définir les domaines soumis à l'audit** - La division de l'environnement des SI en plusieurs thèmes d'audit peut être quelque peu influencée par des préférences personnelles ou des considérations relatives aux effectifs. Toutefois, le but ultime est de déterminer comment scinder l'environnement de façon à obtenir les audits les plus efficients et les plus efficaces. La discussion précédente sur la centralisation des fonctions SI et la standardisation des processus de soutien montrait comment les domaines d'audit pouvaient être regroupés au sein de l'univers d'audit afin de définir une approche plus efficiente. Bien que les auditeurs n'aient pas à évaluer les risques à cette étape du processus de planification de l'audit, l'objectif est de disposer d'un plan d'audit centré sur les domaines présentant le risque le plus élevé, dans lesquels les auditeurs peuvent apporter le plus de valeur ajoutée.

- **Les applications -** Le responsable de l'audit interne doit déterminer quel groupe d'audit sera chargé de planifier et de réaliser l'audit des applications. Selon le mode de fonctionnement du service d'audit, les applications peuvent être incluses dans l'univers d'audit des SI, dans celui de l'organisation ou dans les deux. Les services d'audit interne s'accordent, de plus en plus, à dire que les applications doivent être auditées en même temps que les processus qu'elles supportent. On obtient ainsi une assurance sur toute la suite des contrôles, automatisés ou manuels, portant sur les processus examinés, en minimisant les risques de lacunes ou de chevauchements susceptibles d'être rencontrés au cours des travaux d'audit, et éviter autant que possible les confusions quant à ce qui fait partie ou non du champ de la mission.

- **Évaluer les risques** - Une fois l'univers d'audit défini, l'étape suivante de la définition du programme annuel d'audit consiste en une évaluation systématique et uniforme des risques associés à tous les sujets. La section suivante présente des notions fondamentales sur les risques et leur évaluation, qui peuvent aider les responsables de l'audit interne et les auditeurs internes à créer un programme d'audit des SI efficace.

III.2.3. EVALUATION DES RISQUES DE L'AUDIT DES SYSTEMES D'INFORMATION

L'IIA définit le risque comme la « *possibilité que se produise un événement qui aura un impact sur la réalisation des objectifs. Le risque se mesure en termes de conséquences et de probabilité* »[8]. Il est donc absolument crucial que les organisations fassent périodiquement l'inventaire des risques auxquels elles sont exposées et qu'elles entreprennent les actions nécessaires pour maintenir ces risques à un niveau acceptable. Comme indiqué plus haut, le processus d'évaluation des risques ne doit pas être mené avant que le responsable de l'audit et l'équipe d'audit aient bien identifié l'univers d'audit des SI et la place qu'il occupe au sein de l'organisation et au soutient de ses activités.

Il est capital, quel que soit le modèle ou l'approche d'évaluation des risques retenu, que cette évaluation cerne les domaines de l'environnement du SI susceptibles d'entraver fortement la réalisation des objectifs de l'organisation. En d'autres termes, l'évaluation des risques doit intégrer l'infrastructure, les applications et les opérations informatisées et, de façon générale, tous les composants du SI, qui pèsent le plus sur la capacité de l'organisation à veiller à la disponibilité, à la fiabilité, à l'intégrité et à la confidentialité du système et des données. En outre, les auditeurs doivent tenir compte de l'efficacité et de la pertinence des résultats de l'évaluation des risques, lesquels dépendent de la méthode employée et de sa bonne mise en œuvre. En somme, si les données d'entrée utilisées pour évaluer les risques (c'est-à-dire l'univers d'audit des SI et sa relation avec l'univers d'audit de l'organisation) sont déficientes ou utilisées incorrectement, il est vraisemblable que les résultats de l'évaluation en seront, à certains égards, insatisfaisants.

- **Le processus d'évaluation des risques** - Dès lors que le responsable de l'audit interne et l'équipe d'audit ont une bonne connaissance de l'organisation et des technologies qui y sont mises en œuvre, ils peuvent mener une évaluation des risques. Il est crucial d'exécuter ces tâches correctement si l'on veut être sûr que les risques pertinents liés aux SI (c'est-à-dire ceux qui présentent la plus grande probabilité d'occurrence et d'impact sur l'organisation) sont identifiés et évalués avec efficacité, et qu'ont été prises, de façon appropriée, des mesures destinées à les maîtriser. Le résultat du processus d'évaluation des risques sert ensuite au responsable de l'audit interne et à l'équipe d'audit interne pour élaborer un plan d'audit des SI.

[8] Cadre de Référence International des Pratiques Professionnelles de l'audit interne, IIAIFACI, 2009.

- **Identifier et prendre en compte les objectifs de l'entreprise -** L'un des fondements de toute méthode d'évaluation des risques consiste à prendre en compte les objectifs de l'organisation et à déterminer en quoi les SI contribuent à la réalisation de ces objectifs ou les soutiennent. Si les objectifs de l'organisation ne sont pas déjà identifiés, les auditeurs doivent le faire avant de procéder à l'évaluation des risques propres au SI. Les objectifs de l'organisation peuvent être vastes et de nature stratégique (par exemple, devenir un chef de file du secteur) ou plus linéaires et de nature plutôt tactique (par exemple, remplacer les anciennes applications SI par un système d'ERP). En outre, les processus de gestion des risques devront passer par cinq grandes étapes :

  → Il faut identifier et hiérarchiser les risques découlant des stratégies et activités de l'organisation.

  → La direction générale et le Conseil d'administration définissent le niveau de risque acceptable pour l'organisation, y compris le niveau d'acceptation des risques liés aux plans stratégiques de l'organisation.

  → Il convient de concevoir et de mettre en œuvre des actions concourant à la maîtrise des risques, en les réduisant ou les ramenant en tout état de cause dans les limites fixées comme acceptables par la direction générale et le Conseil d'administration.

  → Il convient de mettre en place un dispositif de surveillance continue afin de réévaluer périodiquement les risques, comme l'efficacité des contrôles visant à gérer ces risques.

  → Le Conseil d'administration et la direction générale reçoivent périodiquement des rapports sur les processus de gestion des risques. Les processus de gouvernement d'entreprise en place prévoient également une communication régulière aux partenaires financiers sur l'état d'exposition aux risques, les stratégies et les contrôles mis en œuvre en conséquence.

- **Identifier et prendre en compte la stratégie relative aux SI -** Une fois que le responsable de l'audit interne et les auditeurs sont au courant des objectifs de l'organisation, il leur faut identifier la stratégie générale de l'organisation vis-à-vis des SI, afin de vérifier si elle cadre avec les objectifs identifiés à l'étape précédente. L'organisation peut disposer de divers documents décrivant la relation entre ses objectifs et le plan stratégique des SI, auxquels le responsable de l'audit et les auditeurs ont besoin d'avoir accès, pour en prendre connaissance et en tenir compte dans leurs travaux.

- **L'univers du SI** - Comme indiqué plus haut, les auditeurs commenceront par dresser l'inventaire des composantes de l'environnement informatique afin de déterminer quels domaines du SI verront leurs risques et contrôles examinés. S'il n'existe pas une approche unique idéale pour réaliser cet inventaire, de nombreuses organisations scindent leur univers de SI en trois grandes sous-catégories : infrastructure, production ou exploitation, et applications.

- **Hiérarchiser les risques** - Une fois achevé l'inventaire de l'univers du SI, l'étape suivante consiste à valoriser les risques associés à chacune des sous-catégories (infrastructure, production et applications) : il s'agit de classer ces sous-catégories sur la base de la probabilité d'occurrence des risques qui y sont associés, ainsi que de l'impact que ces derniers pourraient avoir sur l'organisation s'ils se matérialisaient. Autrement dit, les auditeurs détermineront les dysfonctionnements susceptibles d'intervenir pour chaque catégorie et en quoi l'organisation en sera affectée si les contrôles visant à gérer ou à atténuer ces dysfonctionnements ne sont pas appliqués correctement, ou s'ils ne fonctionnent pas efficacement. on peut mesurer le risque et l'impact suivant trois approches :

  → *Estimation directe des probabilités et des pertes attendues, ou application de probabilités à la valeur des actifs afin de déterminer le niveau potentiel de pertes* - Ce processus est le plus ancien, et n'est pas considéré comme une bonne pratique. Si le secteur des assurances le pratique toujours, les auditeurs s'en abstiendront.

  → *Facteurs de risques ou utilisation de facteurs observables ou mesurables afin de valoriser un risque spécifique ou une classe de risques* – Ce processus est à privilégier pour des évaluations globales (macro) de risques, mais il n'est pas particulièrement efficace pour une évaluation élémentaire (micro) de risques, sauf lorsque les caractéristiques des unités objets d'audit sont homogènes sur l'ensemble de l'univers d'audit : une succursale, un site ou une usine, par exemple.

  → *Matrices pondérées ou de classification, ou utilisation de matrices « menaces vs composantes » afin d'évaluer les conséquences et les contrôles* - Cette méthode est préférable pour la plupart des évaluations de risques élémentaires.

- **Principaux cadres de gouvernance des SI** - Jusqu'à présent, ce guide s'est concentré sur les différentes étapes nécessaires pour définir l'univers d'audit des SI et mener une évaluation des risques qui permette de déterminer ce qu'il convient d'auditer et à quelle fréquence. Cette analyse ne s'appuie pas sur un cadre de gouvernance des SI en particulier, comme le COBIT, la norme ISO 27002 ou l'ITIL. Par conséquent, il incombe au responsable de l'audit de déterminer quelles parties de ces référentiels, ou d'autres, répondent le mieux aux besoins de l'organisation.

III.2.4. FORMALISATION DU PLAN DE L'AUDIT DES SYSTEMES D'INFORMATION

La définition de l'univers d'audit des SI et la réalisation d'une évaluation des risques sont les étapes préalables qui permettent de définir ce qu'il faut inclure dans le plan d'audit des SI. Alors que tous les éléments de l'univers d'audit pourraient être examinés périodiquement, lorsque les ressources disponibles sont illimitées, tel n'est pas le cas pour la plupart des fonctions d'audit. Par conséquent, le responsable de l'audit des systèmes d'information doit créer un programme d'audit tenant *compte des contraintes du budget opérationnel de la fonction d'audit* et *les ressources disponibles*. La formalisation du plan de l'audit des systèmes d'information comprend 9 étapes :

- **Contexte du plan d'audit** - Dans l'évaluation des risques, l'objectif est d'appréhender les risques dans un contexte relatif. La cible principale (axe central) en est donc le risque, tandis que les ressources disponibles peuvent constituer un facteur déterminant quant à la réalité du travail effectué. Lors de la définition du programme d'audit, l'objectif est d'examiner les domaines à risque élevé pour définir l'affectation des ressources disponibles. Dans ce cas, les ressources constituent la cible, mais les risques représentent au final le facteur décisif.

- **Demandes des parties prenantes** - Tout au long de l'élaboration du programme d'audit des SI, les auditeurs informatiques devront discuter avec les principales parties prenantes afin de mieux prendre en compte l'activité et les risques de l'organisation. Ces discussions leur permettront de rassembler des informations sur l'organisation, ainsi que sur les éventuelles préoccupations exprimées par ces parties prenantes. C'est aussi l'occasion de prendre connaissance des demandes spécifiques de missions de conseil et d'assurance, adressées à l'audit et appelées ci-après « *demandes des parties prenantes* ».

Les demandes des parties prenantes peuvent émaner du *Conseil d'administration*, du *comité d'audit*, *des cadres dirigeants* ou *des responsables d'exploitation*. Elles doivent être prises en compte au cours de la phase de planification de l'audit, en fonction de la capacité de la mission à améliorer le management global des risques et l'environnement de contrôle de l'organisation. Il se peut que ces demandes soient suffisamment précises pour que l'on puisse déterminer l'allocation des ressources nécessaires, ou que l'allocation des ressources se fonde sur les travaux d'audit précédents. Ces missions peuvent également comporter des enquêtes sur des soupçons de fraude qui peuvent survenir de manière inopinée et des demandes d'examen des activités de prestataires de services.

- **Fréquence des audits** - En fonction des résultats de l'évaluation des risques, tous les domaines ne peuvent pas ou ne devront pas être examinés dans chacun des cycles d'audit. la fréquence des audits est définie sur la base d'une évaluation de la probabilité d'occurrence et de l'impact des risques en regard des objectifs de l'organisation. Les audits étant cycliques, des programmes d'audit pluriannuels sont élaborés et présentés à la direction générale et au comité d'audit, pour examen et validation. On élabore un plan pluriannuel, qui s'étend généralement sur trois à cinq ans, pour spécifier quels audits seront menés et quand, pour veiller à l'étendue adéquate des travaux effectués sur cette période et pour identifier les audits pouvant nécessiter des ressources externes spécialisées, voire des ressources internes supplémentaires. De surcroît, la plupart des organisations établissent un programme sur un an, qui découle du plan pluriannuel. Elles y énoncent les activités d'audit planifiées pour l'année à venir. Outre la fréquence des audits, l'élaboration du programme d'audit prendra en compte d'autres facteurs : *les stratégies de sous-traitance de l'audit interne ; Estimation des ressources disponibles pour l'audit des SI ; L'obligation de se conformer à la réglementation et aux autres dispositions en vigueur ; Les audits externes à synchroniser avec le plan d'audit ; Les initiatives et efforts internes destinés à améliorer la fonction d'audit ; La mise en réserve d'un budget et d'un programme d'audit des SI, permettant de faire raisonnablement face à des situations non prévues.*

- **Principes relatifs au plan d'audit** - Lorsque les auditeurs des systèmes d'information définissent les principes relatifs au plan d'audit, ils doivent prendre en compte les risques et les menaces pour l'élaboration du plan d'audit.

- **Le contenu du programme d'audit des SI -** Le contenu du programme d'audit des SI reflétera directement l'évaluation des risques décrite dans les sections précédentes. Le plan présentera également différents types d'audit des SI, par exemple : *Audits intégrés des processus de l'organisation* ; *Audits des processus SI* (audits de la stratégie et de la gouvernance des SI, pour la gestion des projets, activités, politiques et procédures de développement des logiciels, et sécurité de l'information, gestion des incidents, et gestion des changements) *; Audits des projets de l'organisation et des initiatives portant sur les SI* (notamment les revues du cycle de développement des logiciels) ; *Audits de l'infrastructure technique* (revues de la gestion de la demande, évaluations de la performance, évaluations des bases de données, audits des systèmes d'exploitation, analyses des opérations, etc.) ; *Audit du réseau* (examen de l'architecture du réseau, tests d'intrusion, évaluation des vulnérabilités et de la performance).

- **Intégration du programme d'audit des SI -** L'un des volets essentiels du processus de planification est la définition du degré d'intégration du plan d'audit des SI aux autres activités du service d'audit. Ici, les auditeurs déterminent quelle entité d'audit sera chargée de planifier et de surveiller les audits des applications métier. Cette analyse pourrait être élargie à toutes les composantes des SI.

- **Validation du programme d'audit -** Il n'existe malheureusement pas de test direct permettant de vérifier que le plan d'audit est adéquat et son efficacité potentielle maximale. Les auditeurs devront donc disposer de critères pour évaluer l'efficience de ce plan en regard de ses objectifs. Comme nous l'avons vu précédemment, le plan d'audit inclura les audits fondés sur le risque, les domaines d'audit obligatoires et les demandes de la direction générale relatives à des activités d'assurance et de conseil. L'un des objectifs de la phase de planification étant d'allouer des ressources aux domaines dans lesquels l'audit des systèmes d'information peut créer le plus de valeur ajoutée, comme aux domaines de la sécurité informatique induisant le plus de risques, les auditeurs détermineront la manière dont le programme pourra refléter cet objectif.

- **La nature dynamique du programme d'audit des SI -** La technologie ne cessant d'évoluer, l'organisation se retrouve confrontée à de nouveaux risques, vulnérabilités et menaces. De surcroît, les changements technologiques peuvent amener à définir un nouvel ensemble d'objectifs pour les SI, ce qui débouche sur de nouvelles initiatives, acquisitions ou transformations dans le domaine des SI, ou des changements visant à répondre aux besoins de l'organisation.

Lors de l'élaboration du plan d'audit, il importe donc de prendre en considération le caractère dynamique et évolutif de l'organisation. Plus précisément, les auditeurs devront alors tenir compte du rythme de changement des SI, plus rapide que celui des autres activités, de l'adéquation du calendrier de développement d'un système avec le résultat des audits de ce cycle de développement.

- **Communiquer, obtenir le soutien de la direction et faire approuver le programme d'audit** - Le service d'audit interne présente le programme d'audit à la direction générale et au comité d'audit. D'après la Norme 2020[9], il doit, en particulier, informer ces instances du niveau de ressources requis, de tous les remplacements significatifs susceptibles d'intervenir en cours d'exercice et de l'impact potentiel d'une limitation de ses ressources. Il importe également que le volet SI du programme d'audit ou que le programme d'audit du SI fasse l'objet d'une discussion avec la direction générale et l'organe délibérant, ainsi qu'avec les principaux acteurs impliqués à travers le SI, telles que le DSI, les directeurs de la production et des développements, les cadres de la DSI, les propriétaires d'application et d'autres membres du personnel exerçant des fonctions analogues. La contribution de ces parties prenantes est cruciale pour le succès de la planification de l'audit comme devant permettre aux responsables de l'audit et aux auditeurs de mieux cerner l'environnement de l'organisation, d'identifier les risques et les préoccupations et de sélectionner les domaines d'audit.

  De plus, le dialogue sur le programme d'audit définitif aidera à valider la contribution des parties prenantes tout au long du processus et donnera un premier aperçu des travaux à mener. Les auditeurs discutent du plan d'audit des SI avec les principaux responsables, les gestionnaires et le personnel chargé des SI de façon à obtenir leur soutien. La compréhension, la coordination et le soutien de l'équipe chargée des SI rendront le processus d'audit plus efficace et plus efficient. De plus, la connaissance anticipée du programme facilite un dialogue franc et permanent, qui permet de discuter de l'évolution des risques et de l'environnement opérationnel, à chaque étape de la réalisation du plan d'audit, et de procéder à des ajustements en continu. L'interaction avec les « clients » lors de l'évaluation des risques et avant l'approbation du plan d'audit final est fondamentale pour la qualité globale du plan.

[9] **Norme 2020 – Communication et approbation.** Le responsable de l'audit interne doit soumettre à la direction générale et à l'organe délibérant son programme d'audit et ses besoins, ainsi que tout changement important susceptible d'intervenir en cours d'exercice. Le responsable de l'audit interne doit également signaler l'impact de toute limitation de ses ressources.

CHAPITRE QUATRIEME - LES REFERENTIELS DE L'AUDIT DES SYSTEMES D'INFORMATION

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 est un processus mis en œuvre à l'initiative des dirigeants de l'entreprise et destiné à fournir une assurance raisonnable quant à la réalisation des trois objectifs suivants :

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

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

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 (*comme par exemple, 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. Et c'est sur cette base, qu'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. Il existe différents référentiels comme :

- ***CobiT*** : (*Control Objectives for Information and related Technology*). C'est le principal référentiel des auditeurs informatiques ;
- ***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 ;

NB : Ces trois principaux ci-haut référentiels sont gérés par l'entreprise ***L'ISACA*** (*Information Systems Audit & Control Association*) qui est l'association internationale des auditeurs informatiques, créé en 1967et est représenté en France depuis 1982 par ***l'AFAI*** (***Association Française de l'Audit et du conseil Informatique***), C'est un cadre de contrôle qui fournissent de nombreux supports et vise à aider le mangement à gérer les risques (*la sécurité, la fiabilité et la conformité*) et les investissements. Mais on peut aussi utiliser d'autres référentiels comme :

- ***ISO 27002*** : c'est un code des bonnes pratiques en matière de management de la sécurité des systèmes d'information ;
- ***CMMi*** : (*CapabilityMaturity 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.

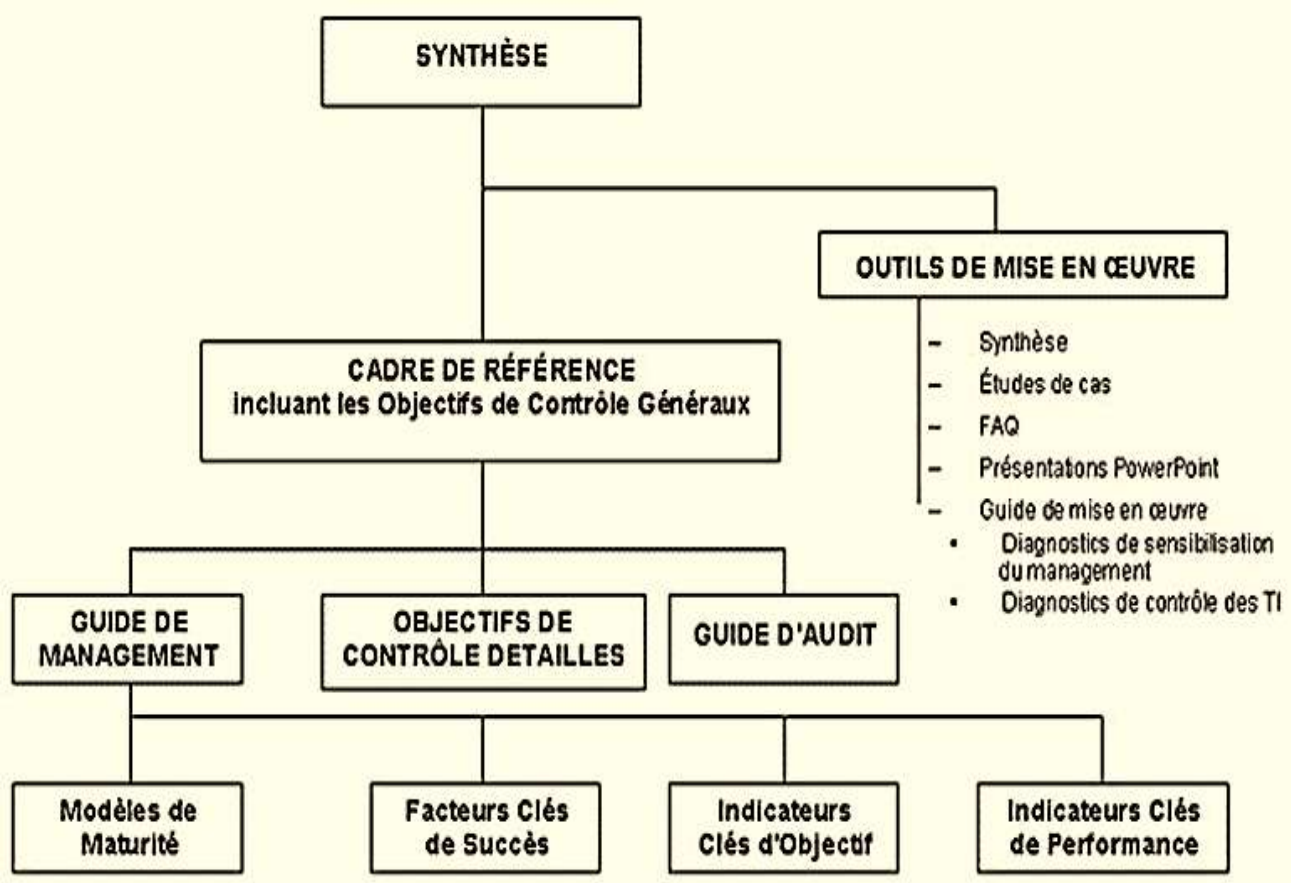
IV.1. LE REFERENTIEL COBIT

Le référentiel COBIT[10] (« *Control Objectives for Information and related Technology* », ou « *objectifs de contrôle de l'information et des technologies associées* ») est référentiel de bonnes pratiquesd'audit informatique et de gouvernance des systèmes d'information d'origine américaine.

En particulier, *le référentiel CobiT* repose sur une approche très fonctionnelle de l'organisation. Sur ce modèle, le Système d'information opère en parallèle de l'organisation réelle et d'une certaine manière, déconnecté de celle-ci - car il se base sur l'agencement nominal des fonctions[11].

[10] Le référentiel COBIT a été développé en 1994 (et publié en 1996) par l'ISACA (Information Systems Audit and Control Association). L'ISACA a été créé en 1967 et est représenté en France depuis 1982 par l'AFAI (Association française de l'audit et du conseil informatiques). C'est un cadre de contrôle qui vise à aider le management à gérer les risques (sécurité, fiabilité, conformité) et les investissements. COBIT a évolué, la version 4 est apparue en France en 2007.

[11] Ahmed Bounfour, Capital immatériel, connaissance et performance, Harmattan, 2006 (ISBN 978-2-2960-1128-1) p. 127



Composants du référentiel CobiT

Il comprend six domaines d'intervention[12]:

- ***Executive summary*** (***Synthèse*** *: Cette partie résume de la méthodologie CobiT*);
- ***Framework*** (***Cadre de Référence*** *: c'est la partie explicative des méthodes, des domaines et des processus*) ;
- ***Control objectives*** (***Objectifs de contrôle détaillés*** *: ces objectifs sont orientés vers le management et les équipes responsables des services informatiques*) ;
- ***Audit guidelines*** (***le guide de l'audit*** *:décèle, analyse et explique les failles d'un système et les risques qui en découlent ainsi que de leur apporter des solutions);*
- ***ImplementationTool Set*** (*les outils de la mise en œuvre du CobiT*) ;
- ***Management Guidelines*** (*le guide du management : Ce guide propose un cadre de 5 degré de pilotage ou « tableau de bord prospectif (**balancedscorecard**) »).*

[12] L'objectif est d'assurer l'adéquation durable entre les technologies, les processus métiers et la stratégie de l'entreprise.

Le référentiel CobiT fournit aux gestionnaires, auditeurs et utilisateurs de TIC (*Technologies de l'information et de la communication*), des indicateurs, des processus et des bonnes pratiques pour les aider à maximiser les avantages issus des techniques informatiques et à l'élaboration de la gouvernance et du contrôle d'une entreprise.

Il les aide autant à comprendre leurs systèmes informatiques et à déterminer le niveau de sécurité et de contrôle qui est nécessaire pour protéger leurs entreprises, et ceci par le biais du développement d'un modèle de gouvernance des systèmes d'information tel que *COBIT*. Ainsi, *le référentiel COBIT* fournit des indicateurs clés d'objectifs, des indicateurs clés de performances et des facteurs clés de succès pour chacun de ses processus. Le référentiel (*modèle*) COBIT se focalise sur ce que l'entreprise a besoin de faire et non sur la façon dont elle doit le faire.

Le référentiel COBIT[13] constitue une structure de relations et de processus (*cadre de référence ou framework)* visant à un pilotage et un contrôle des techniques informatiques par le management de l'entreprise pour atteindre ses objectifs, en utilisant ces techniques comme moyen pour améliorer l'activité et et de répondre aux besoins métiers, besoins consolidés dans le plan stratégique de l'entreprise. Il est basé sur 5 clés principales de la gouvernance et gestion IT :

- Répondre aux besoins des parties prenantes ;
- Couvrir l'entreprise de bout en bout ;
- Appliquer un seul cadre de référence ;
- Séparer la gouvernance et la gestion ;
- Favoriser une approche globale.

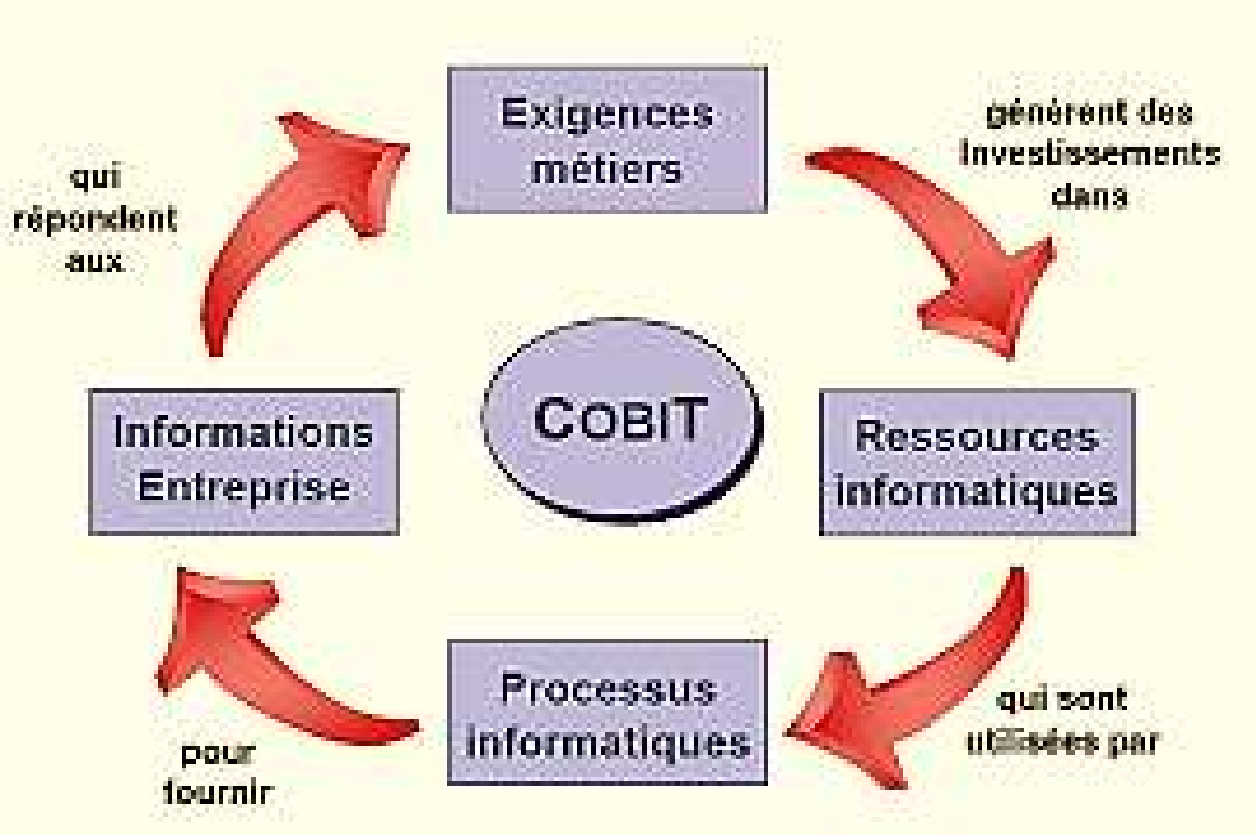
Il existe plusieurs versions du référentiel COBIT, mais dans le cadre de cours, nous n'en citerons que 3 grandes versions notamment :

- Le référentiel CobiT version 4 ;
- Le référentiel CobiT version 5 ;
- Le référentiel CobiT version Quickstart.

[13] L'objectif du référentiel CobiT est d'assurer l'adéquation durable entre les technologies, les processus métiers et la stratégie de l'entreprise.

IV.1.1. LE REFERENTIEL COBIT 4.1

Le référentiel COBIT 4 est une approche orientée processus regroupé en quatre domaines (*planification, construction, exécution et métrologie, par analogie avec la Roue de Deming*), qui constitue 34 processus *(propositions*) distincts qui donnent en tout 215 activités e de « *pratiques de contrôle* » et Un volet « *évaluation des systèmes d'information* ». Le COBIT consiste à décomposer tout système informatique en :



Principes de fonctionnement du référentiel CobiT 4.1.

1. ***La Planification et Organisation*** : dans ce domaine nous cherchons à savoir comment utiliser les techniques informatiques afin que l'entreprise atteigne ses objectifs : (*Définition du plan stratégique informatique, Définition de l'architecture des informations, Définition de la direction technologique, Organisation du service informatique, Gestion des investissements, Communication des objectifs de la direction, Gestion des ressources humaines, Respect des exigences légales, Évaluation des risques, Gestion des projets et Gestion de la qualité*) ;

2. ***La construction (***regroupant ***l'Acquisition et Installation des ressources informatiques)*** : Ici le référentiel COBIT cherche à définir, acquérir et mettre en œuvre des technologies en les alignant avec les processus métiers de l'entreprise : (*Identification des solutions automatiques, Acquisition et maintenance des applications informatiques, Acquisition et maintenance de l'infrastructure technique, Développement et maintien des procédures, Installation et certification des systèmes, Gestion des modifications*) ;

3. ***La Livraison et Support*** : A ce niveau, l'objectif est de garantir l'efficacité et l'efficience des systèmes technologiques en action : (*Définition des niveaux de service, Gestion des services aux tiers, Gestion des performances et des capacités, Garantie de la poursuite des traitements, Garantie de la sécurité des systèmes, Identification et attribution des coûts, Formation des utilisateurs, Assistance des utilisateurs, Gestion de la configuration, Gestion des incidents, Gestion des données et des applications, Sécurité physique du système, et Gestion de l'exploitation*) ;

4. ***Le Monitoring*** : A ce niveau, on vérifie que la solution mise en place est en adéquation avec les besoins de l'entreprise dans une vision stratégique : (*Surveillance des processus, Appréciation du contrôle interne, Certification par un organisme indépendant, et Audit par un organisme indépendan*t).

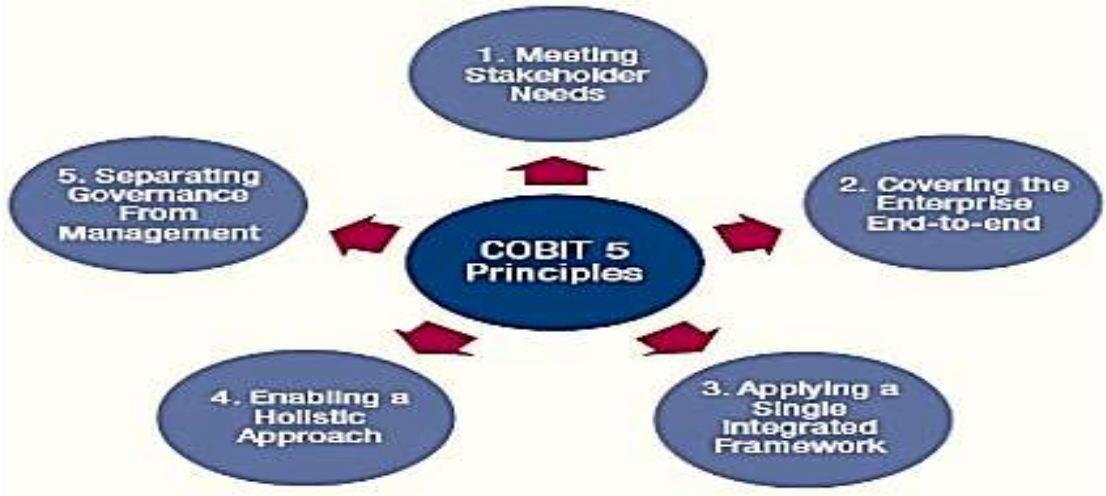
Le référentiel COBIT 4 s'adresse à différents utilisateurs :

- Le management pour lequel il offre un moyen d'aide à la décision ;
- Les utilisateurs directs pour lesquels il permet d'apporter des garanties sur la sécurité et les contrôles des services informatiques ;
- Les auditeurs et les consultants auxquels il propose des moyens d'interventions reconnus internationalement.

IV.1.2. LE REFERENTIEL COBIT 5

La version 5 de COBIT est disponible depuis avril 2012[14]. Le référentiel COBIT 5 est, à ce jour, le seul référentiel qui est orienté business pour la Gouvernance et la Gestion des Systèmes d'Information de l'entreprise. Il représente une évolution majeure du référentiel. Il adapté pour tous les types de modèles business, d'environnements technologiques, toutes les industries, les lieux géographiques et les cultures d'entreprise. Il s'applique à:

- La sécurité de l'information ;
- La gestion des risques ;
- La gouvernance et la gestion du système d'information de l'entreprise ;
- Les activités d'audit ;
- La conformité avec la législation et la réglementation ;
- Les opérations financières ou les rapports sur la responsabilité sociale de l'entreprise.



Principes de fonctionnement du référentiel CobiT 5

Une des principales nouveautés du référentiel COBIT 5 est d'aborder le système d'information, au-delà des processus déjà mis en avant par le référentiel COBIT 4.1, au travers d'autres thématiques complémentaires, dans le cadre d'une approche globale (*ou systémique*). L'ensemble de ces thématiques contribuent de manière interdépendante à la maîtrise de la gouvernance et du management du Système d'Information.

[14]L'ISACA publie le cadre de référence de gouvernance COBIT 5 - Isaca.org, 10 avril 2012

Ce dernier définit 37 processus regroupés en cinq domaines[15] :

1. ***Évaluer, diriger, et surveiller*** : (*Assurer la définition et l'entretien d'un référentiel de gouvernance, Assurer la livraison des bénéfices, Assurer l'optimisation du risque, Assurer l'optimisation des ressources, Assurer aux parties prenantes la transparence*) ;

2. ***Aligner, planifier et organiser*** : (*Gérer le cadre de gestion des TIC, Gérer la stratégie, Gérer l'architecture de l'entreprise, Gérer l'innovation, Gérer le portefeuille, Gérer le budget et les coûts, Gérer les relations humaines, Gérer les relations, Gérer les accords de service, Gérer les fournisseurs, Gérer la qualité, Gérer le risque, Gérer la sécurité*) ;

3. ***Bâtir, acquérir, et implanter*** : (*Gérer les programmes et les projets, Gérer la définition des exigences, Gérer l'identification et la construction des solutions, Gérer la disponibilité et la capacité, Gérer le changement organisationnel, Gérer les changements, Gérer l'acceptation du changement et de la transition, Gérer la connaissance, Gérer les actifs, Gérer la configuration*) ;

4. ***Livrer, servir et soutenir*** : (*Gérer les opérations, Gérer les demandes de services et les incidents, Gérer les problèmes, Gérer la continuité, Gérer les services de sécurité, Gérer les contrôles des processus d'affaires*) ;

5. ***Surveiller, évaluer et mesurer*** : (*Surveiller, évaluer et mesurer la performance et la conformité ; Surveiller, évaluer et mesurer le système de contrôles internes ; Surveiller, évaluer et mesurer la conformité aux exigences externes*).

Des adaptations ont été réalisées sur cette version afin d'assurer une meilleure convergence avec d'autres référentiels tels que : « ***ITIL*** (*Information Technology Infrastruture Library*) et ***CMMI*** (*CapabilityMaturity Model Integration*)». Ainsi le référentiel COBIT 5, encore plus que le référentiel COBIT 4.1, aidera ***les DSI*** (*Directeur des Systèmes d'information*) à mettre en œuvre une démarche d'amélioration globale de la direction des systèmes d'information homogène et coordonnée, qui ne se focalise pas que sur les processus.

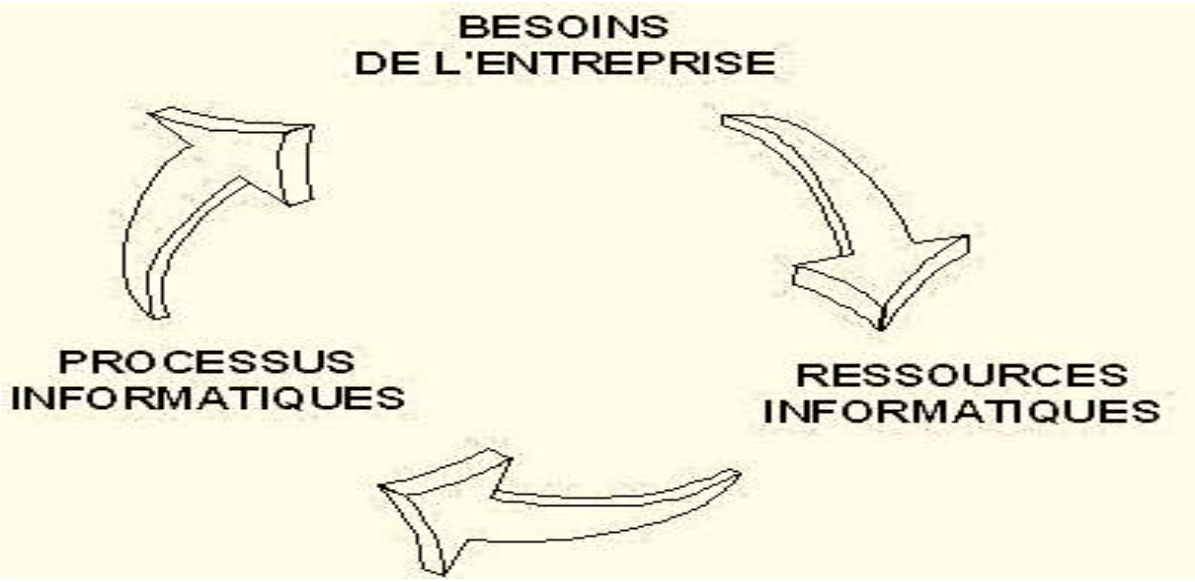
[15]ISACA : « Un référentiel orienté affaires pour la gouvernance et la gestion des TIC de l'entreprise » et « Processus facilitants ».

IV.1.3. LE REFERENTIEL COBIT QUICKSTART

Cette version simplifiée de CobiT s'adresse principalement aux PME[16] pour lesquelles les techniques informatiques ne représentent pas un enjeu stratégique mais simplement un levier dans leur stratégie de croissance. Il se repose sur les hypothèses suivantes :

- l'infrastructure informatique n'est pas complexe ;
- la taille de l'entreprise, le système d'information et l'activité sont bien alignés ;
- les tâches les plus complexes sont externalisées ;
- la tolérance aux risques est relativement élevée ;
- l'éventail des contrôles est peu étendu ;
- la structure de commandement est simple.

Cette version conserve *du référentiel COBIT* 30 processus sur les 34, et 62 objectifs de contrôle sur les 318.



[16] *PME : Petites et Moyennes Entreprises*

Principes de résonnance du référentiel CobiT Quickstart

La mise en œuvre Quickstart comprend six étapes :

- Évaluer le bien-fondé c'est-à-dire déterminer si cette version est adaptée à l'entreprise ;
- Évaluer la situation actuelle à partir de collectes d'informations auprès des personnes clé et de rapports d'audit ;
- Déterminer la cible avec la définition de l'activité, des contraintes légales, et de la dépendance de l'entreprise vis-à-vis de la technologie ;
- Analyser les écarts par l'examen des pratiques de contrôle et des facteurs clés de succès ;
- Définir les projets d'amélioration des processus ;
- Élaborer un programme intégré de mise en place de la gouvernance en tenant compte des besoins immédiats de l'entreprise, des interdépendances entre les projets et des ressources disponibles.

Le référentiel CobiT Quickstart s'intéresser à la direction générale en indiquant ce que l'implantation d'un processus donné va apporter sur les informations (*par exemple sur l'information décisionnelle*) et se base sur les procédés dont :

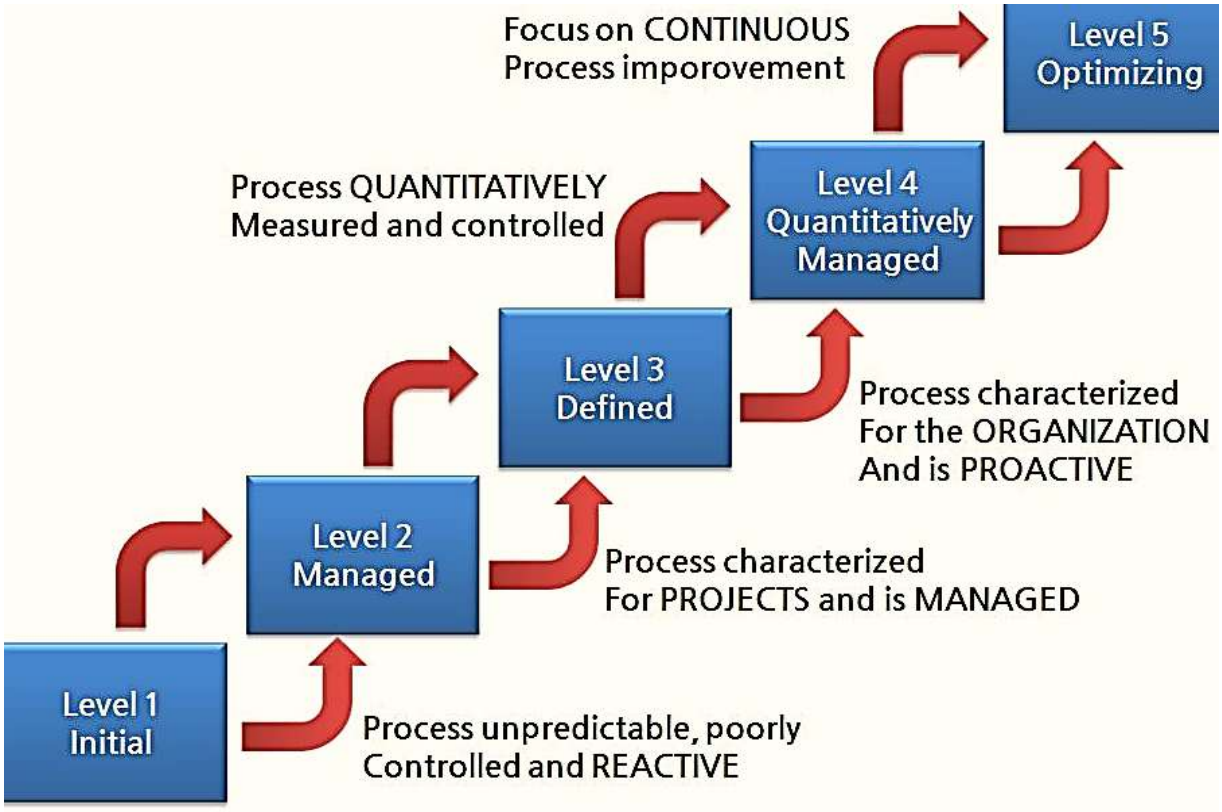
- ***Efficacité*** : qualité et pertinence de l'information, distribution cohérente ;
- ***Efficience*** : rapidité de délivrance ;
- ***Confidentialité*** : protection contre la divulgation ;
- ***Intégrité*** : exactitude de l'information ;
- ***Disponibilité*** : accessibilité à la demande et protection (*sauvegarde*) ;
- ***Conformité*** : respect des règles et lois ;
- ***Fiabilité*** : exactitudes des informations transmises par le management.

Et les différentes ressources telles que :

- ***les compétences*** : le personnel, et collaborateurs (*internes et externes*) ;
- ***les applications*** : ensemble des procédures de traitement ;
- ***l'infrastructure*** : ensemble des installations, Data Center, … ;
- ***les données*** : informations au sens global (*format, structure, ...)* ;
- ***les techniques*** : équipement, logiciels, bases de données, réseaux, …

IV.2. LE REFERENTIEL CMMI

Le référentiel CMMI[17] (*capability maturity model integration*), est un modèle de référence et un ensemble structuré de bonnes pratiques, destiné à appréhender, évaluer et améliorer les activités des entreprises d'ingénierie. *Le référentiel CMMI* définit une échelle de mesure de la maturité à cinq niveaux, ainsi que les indicateurs nécessaires pour évaluer les activités menées par une équipe par rapport à cette échelle (*l'équipe peut être un groupe de travail, un ou plusieurs projets, une société voire une institution d'État*).



Résonnance du référentiel CMMI

[17] Dans les années 1980, le département de la Défense des États-Unis (DoD) a demandé l'élaboration d'un référentiel de critères lui permettant d'évaluer ses fournisseurs de logiciels. Après une lente maturation, le SEI (Software Engineering Institute) de l'université Carnegie-Mellon financé par le DoD a présenté en 1991 le Capability Maturity Model (CMM). Ce modèle de référence ne concerne que les bonnes pratiques du génie logiciel pour appréhender et mesurer la qualité des services rendus par les fournisseurs de logiciels informatiques du département de la Défense des États-Unis (DoD). . Il est maintenant largement employé par les entreprises d'ingénierie informatique, les directeurs des systèmes informatiques et les industriels pour évaluer et améliorer leurs propres développements de produits1. CMMI est une marque déposée par le Software Engineering Institute (Software Engineering Institute'sTrademarks and Service Marks : http://www.sei.cmu.edu/legal/marks/)

1. ***LE NIVAU DE MATURITE 1 « Initial »*** : À ce niveau les solutions ainsi que les projets sont décidés, développés et instaurés par un individu. Les compétences et les ressources propres de cet individu sont la raison du succès ou de l'échec du projet (*par dérision, ce niveau est aussi nommé « héroïque ou chaotique »*). Il n'y a pas de description du niveau de maturité 1 dans le modèle (*pas de surveillance, aucune évaluation de performance et la communication est absente et Les réactions aux incidents se font en mode urgence, sans identification claire des priorités*).

2. ***LE NIVAU DE MATURITE 2 « Managed », (discipline)*** : Une discipline est établie pour chaque projet et se matérialise essentiellement par des plans de projet (*plan de développement, d'assurance qualité, de gestion de configuration…).* Le chef de projet a une forte responsabilité dans le niveau 2 (*il doit définir, documenter, appliquer et maintenir à jour ses plans*). D'un projet à l'autre, il capitalise et améliore ses pratiques de gestion de projet et d'ingénierie.

3. ***LE NIVEAU DE MATURITE 3 « Defined », (ajusté)*** : Ce niveau est caractérisé par une standardisation adéquate des pratiques, une capitalisation centralisée (*en particulier sur les mesures réalisées dans les projets*) et une maîtrise du référentiel interne (*ou Système Qualité*). Il existe des lignes directrices, un plan stratégique et une planification de l'amélioration de processus pour le futur, en ligne avec les objectifs d'affaire de l'organisation. Les employés sont formés et conscients de leurs responsabilités ainsi que de leurs devoirs.

4. ***LE NIVEAU DE MATURITE 4 « Quantitatively managed », (gestion quantitative) :*** Les projets sont pilotés sur la base d'objectifs quantitatifs de qualité produit et processus. La capacité des activités (*ou sous-processus*) critiques est déterminée par l'organisation, ainsi que les modèles de performance et de prévision associés. L'expression de la qualité demandée par le client est prise en compte pour quantifier les objectifs du projet et établir des plans selon la capacité des processus de l'organisation.

5. ***LE NIVEAU 5 « Optimizing », (optimisation***) : Les processus qui sont gérés quantitativement pour le pilotage de projet (*niveau de maturité 4*) sont en amélioration constante afin d'anticiper les évolutions prévues (*besoins clients, nouvelles technologies…).*

Le référentiel CMMI[18] est un cadre générique de processus qui se décline en trois modèles (*appelés « **constellations** »*) :

- ***CMMI-DEV*** pour le développement de systèmes (*logiciel ou autre, modèle publié en août 20063*)
- ***CMMI-ACQ*** pour la maîtrise des activités d'achat (*modèle publié en novembre 20074*)
- ***CMMI-SVC*** pour la fourniture de services (*modèle publié en février 20095*)

La particularité de ces trois modèles de processus est qu'ils ont une partie commune (*le noyau ou core en anglais*) qui représente environ 60 % des pratiques. D'un modèle à l'autre, les différences portent essentiellement sur la catégorie « *Ingénierie* » dont les pratiques varient selon l'activité concernée :

- Les objectifs génériques : le référentiel CMMI fournit cinq objectifs génériques. Ces objectifs génériques (*et les pratiques associées*) s'appliquent à tous les domaines de processus.
- Les pratiques génériques : les pratiques génériques appartiennent aux objectifs génériques. Elles doivent être systématiquement implémentées pour prétendre atteindre un niveau de maturité ou de capacité.
- Les objectifs spécifiques : les objectifs spécifiques sont liés à un domaine de processus.
- Les pratiques spécifiques : elles sont liées à un objectif spécifique, donc à un domaine de processus.
- Les produits d'activité : ce sont tous les éléments générés par un projet (*plan de projet, spécification, cahier de test unitaire, revue par les pairs, etc.)*

[18] Le modèle CMMI est majoritairement utilisé dans des sociétés d'informatique, toutefois les principes de CMMI s'appliquent à n'importe quelle activité d'ingénierie : architecture, mécanique, électronique…

IV.3. LE REFERENTIEL ITIL

Le référentiel ITIL[19] (« *Information Technology Infrastructure Library* » ou « *Bibliothèque pour l'infrastructure des technologies de l'information ») est un ensemble d'ouvrages recensant les bonnes pratiques *(best practices)* du management du système d'information. C'est un référentiel très large qui aborde les sujets suivants :

- Comment organiser un système d'information ?
- Comment améliorer l'efficacité du système d'information ?
- Comment réduire les risques ?
- Comment augmenter la qualité des services informatiques ?

Les recommandations du *référentiel ITIL* positionnent des blocs organisationnels et des flux d'informations. De nombreux logiciels d'exploitation informatique sont conformes à ces recommandations. L'adoption des bonnes pratiques du référentiel ITIL par une entreprise permet d'assurer à ses clients (*internes comme externes*) un service répondant à des normes de qualité préétablies au niveau international. *Le référentiel ITIL* est à la base de la norme BS15000 (*première norme de Gestion de Services Informatiques formelle et internationale)* un label de qualité proche des normes ISO par exemple.

Le référentiel ITIL permet, grâce à une approche par processus clairement définie et contrôlée, d'améliorer la qualité des SI et de l'assistance aux utilisateurs en créant notamment la fonction (*département de l'entreprise*) de Centre de services ou « *Service Desk* » (*extension du « help desk »)* qui centralise et administre l'ensemble de la gestion des systèmes d'informations. Ainsi, *le référentiel ITIL* devient finalement une sorte de « *règlement intérieur* » du département informatique des entreprises qui l'adoptent.

[19] Rédigée à l'origine par des experts de l'Office public britannique du Commerce (OGC), la bibliothèque ITIL a fait intervenir à partir de sa version 3 des experts issus de plusieurs entreprises de services telles qu'Accenture, Ernst & Young, Hewlett-Packard, Deloitte, BearingPoint, le Groupe CGI ou PriceWaterhouseCoopers.Après un développement essentiellement européen jusqu'à la fin des années 1990, ITIL s'est implanté sur le marché nord-américain via des entreprises de conseil en transformation des systèmes d'information. La version 3, en 2007, s'est traduite par une adoption encore plus large notamment en raison de la multiplication des traductions du référentiel. L'OGC a par ailleurs abandonné la propriété d'ITIL à un autre organisme gouvernemental britannique, le Cabinet Office.

Les bénéfices qu'offrent *le référentiel ITIL* aux entreprises qui l'adoptent, sont une meilleure traçabilité de l'ensemble des actions du département informatique. Ce suivi amélioré permet d'optimiser en permanence les processus des services pour atteindre un niveau de qualité maximum de satisfaction des clients. Et Même si *le référentiel ITIL* s'intéresse aux systèmes existants des organisations d'une manière transversale, *le référentiel ITIL* n'a pas été conçu à l'origine pour la gouvernance des systèmes d'information.

Toutefois, selon *la société Metrixware*, dans sa version 3, *le référentiel* ITIL traite de la gouvernance des systèmes d'information. Quoi qu'il en soit, ITIL étant très centré sur le système d'information, son utilisation pour la gouvernance des systèmes d'information posera de toute façon la question de l'alignement stratégique du système d'information sur les processus métier. Le référentiel ITIL décrit comment on s'assure que le « *client* » a accès aux services informatiques appropriés, et comprend :

- Le centre de services (*service desk*)
- La gestion des incidents (*incident management*)
- La gestion des problèmes (*problem management*)
- La gestion des changements (*change management*)
- La gestion des mises en production (*release management*)
- La gestion des configurations (*configuration management*)

NB: il est nécessaire de garder à l'esprit que la liste de référentiels énumérés ci-haut n'est pas exhaustive étant donné qu'on peut dénombrer les référentiels tels :***TOGAF, PMBOK, PRINCE2, COSO, ISO/CEI 20000, ISO/CEI 27001, PCI DSS, Loi Sarbanes-Oxley et Bâle III.***

CHAPITRE CINQUIEME - POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION

Elle procède par :

- la Sécurité de l'information ;
- l'Installation et la gestion de la politique de sécurité des systèmes d'information.

Pour ce faire, la nécessité de l'information et le besoin de la protéger est requise.

V.1. SECURITE DE L'INFORMATION

L'information constitue un des biens ou actifs vitaux du patrimoine de chaque entreprise. Cette information, par le biais des processus business, permet à l'entreprise de réaliser ses tâches, de répondre aux demandes des clients, de comptabiliser ses opérations, etc., bref de fonctionner selon les exigences de ses dirigeants et des autres parties prenantes. En outre, l'entreprise doit se conformer aux lois et aux règlements applicables qui concernent également l'information, par exemple la loi sur la protection des données, les droits d'auteur et le reporting financier.

Aussi, l'entreprise doit-elle protéger son information, de même que les systèmes d'information nécessaires au traitement de cette information, respectivement de ses processus business, dans et autour des activités de base suivantes : Saisie de l'information (input), traitement et enregistrement de l'information, sortie de l'information (output).

V.2. MESURES DE SECURITE, EVALUATION DES RISQUES ET TABLEAU DE BORD

Pour protéger efficacement son information (donc également ses systèmes d'information), l'entreprise doit - en fonction d'une évaluation des risques - mettre en place des mesures de sécurité (des contrôles) de manière à assurer l'intégrité, la confidentialité et la disponibilité de l'information. A ce sujet, la norme ISO, largement reconnue, propose plus de 130 contrôles de sécurité de l'information. Nous avons développé un tableau qui permet à une entreprise d'évaluer ses contrôles et de produire un tableau de bord comme outil efficace de la politique de sécurité informatique, sécurité des systèmes d'information, sécurité de l'information.

V.3. PROCESSUS DE SECURITE DE L'INFORMATION

La mise en place de mesures de sécurité de l'information n'est pas une fin en soi, mais un processus servant à *établir, installer, appliquer, revoir, maintenir et améliorer un SGSI (système de gestion de la sécurité de l'information), ou ISMS (information security management system) de l'entreprise,* selon la norme ISO.

Le processus décrit ci-dessus vise l'amélioration continue et dépend directement des volontés de la direction générale, car il s'inscrit dans le processus général de sécurité de toute l'entreprise et dans le SCI. Selon la Chambre Fiduciaire, le SCI est *"un outil de gestion permettant de garantir de manière appropriée à l'entreprise d'atteindre ses objectifs dans les domaines «Procédures», «Informations», «Protection du patrimoine» et «Conformité (Compliance)». Le SCI englobe toutes les méthodes et mesures organisationnelles appliquées, conformément à un plan, par la direction".* Le COSO propose un concept reconnu pour la mise en place d'un SCI.

V.4. DOMAINE D'APPLICATION (SELON L'ISO)

La présente Norme internationale établit des lignes directrices et des principes généraux pour préparer, mettre en œuvre, entretenir et améliorer la gestion de la sécurité de l'information, sécurité informatique, au sein d'un organisme. Les objectifs esquissés dans la présente Norme internationale fournissent une orientation générale sur les buts acceptés communément dans la gestion de la sécurité de l'information. Les objectifs et mesures décrits dans la présente Norme internationale sont destinés à être mis en oeuvre pour répondre aux exigences identifiées par une évaluation du risque. La présente Norme internationale est prévue comme base commune et ligne directrice pratique pour élaborer les référentiels de sécurité de l'organisation, mettre en œuvre les pratiques efficaces de la gestion de la sécurité, et participer au développement de la confiance dans les activités entre organismes.

V.5. STRUCTURE DE LA NORME (SELON L'ISO)

La présente Norme internationale contient 11 articles relatifs aux mesures de sécurité, qui comprennent un total de 39 catégories de sécurité et un article d'introduction sur l'appréciation et le traitement du risque. Chaque article contient plusieurs catégories de sécurité principales. Les 11 articles (accompagnés du nombre de catégories de sécurité principales incluses dans chaque article) sont les suivants :

1° Politique de sécurité
2° Organisation de la sécurité de l'information
3° Gestion des biens
4° Sécurité liée aux ressources humaines
5° Sécurité physique et environnementale.
6°Gestion opérationnelle et gestion de la communication.
7° Contrôle d'accès.
8° Acquisition, développement et maintenance des systèmes d'information
9° Gestion des incidents liés à la sécurité de l'information.
10° Gestion de la continuité de l'activité.
11° Conformité.

V.6. TABLEAU DE BORD DE LA POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION

Dans le but de permettre à une entreprise d'évaluer sa politique de sécurité des systèmes d'information, sécurité de l'information, nous avons repris dans un tableau Excel 11 articles et n catégories de la norme ISO. L'entreprise peut alors :

- Choisir quels articles et quelles catégories elle veut évaluer, puis
- Evaluer chaque contrôle des catégories choisies en lui donnant une note entre 1 (contrôle inexistant) et 5 (contrôle installé et testé).

Un tableau final établit la moyenne des notes par catégorie et par article. L'entreprise peut s'en servir comme tableau de bord de la politique de sécurité informatique, sécurité des systèmes d'information, sécurité de l'information. L'ensemble fournit un très bon point de départ pour la mise en œuvre d'un système de gestion de la sécurité de l'information (SGSI ou ISMS), selon la norme ISO 27001:2005.

CONCLUSION

La gestion des systèmes d'information fait partie intégrante du management de l'entreprise. C'est l'une des composantes de la gouvernance des SI. De manière globale, la direction générale est la propriétaire du système d'information et doit s'assurer du bon fonctionnement de celui-ci mais aussi de sa pérennité et ce compris de sa bonne évolution et de sa sécurité.

Il paraît évident, à partir de l'ensemble des éléments qu'on a traité tout au long de ce cours, que l'évolution des systèmes informatiques et leur intégration inéluctable, à la gestion entre-autres, a poussé les normes d'audit à s'adapter et à introduire des nouveautés. En effet, parmi ces dernières on trouve l'intégration de nouvelles règles telles que la protection des systèmes informatiques et des réseaux et l'évaluation de nouveaux risques inhérents à ces systèmes mais aussi des risques de vols et de piratage des données.

Toutefois, en République Démocratique du Congo, les normes et référentiels d'audit informatique demeurent inadaptés à un domaine en constante évolution, et ce bien que le législateur congolais s'est forcé à introduire quelques règles en comptabilité et en matière fiscale. Enfin, contrairement au cas de la RDC, les pratiques à l'international ont fait l'objet de plusieurs mises-à-niveau, notamment aux Etats-Unis et en France, afin de suivre l'évolution de l'informatique. Nous espérons que ce présent support pourra aider l'étudiant congolais dans la quête de la maitrise des systèmes d'information dans son environnement quotidien.