CESAG Centre Africain d'études Supérieures en Gestion

Institut Supérieur de Comptabilité, de Banque et de Finance (ISCBF)

Master Professionnel en Audit et Contrôle de Gestion (MPACG)

Promotion 4
(2009-2011)

Mémoire de fin d'étude

THEME

CONCEPTION D'UN MANUEL DE PROCEDURES D'EVALUATION DE LA GOUVERNANCE DES SYSTEMES D'INFORMATION AU REGARD DU COBIT : CAS DU CABINET CECA

Présenté par :

Durotimi SINIMBOU

Dirigé par :

M. Sylla DOLELE, CISA, CISM, CISSP

Bureau de la sécurité des systèmes d'informations

Banque Mondiale

Octobre 2011

REMERCIEMENT

Nous remercions :

- Dieu, pour nous avoir accordé la santé et le soutien nécessaire ;
- nos parents pour tout cet amour dont ils me couvrent ;
- monsieur Sylla DOLELE d'avoir accepté d'être notre mentor et toute sa disponibilité à tous les niveaux ;
- monsieur Abou WELE de nous avoir accepté comme stagiaire dans le cabinet CECA ;
- tout le personnel du cabinet CECA pour leur accueil chaleureux ;
- M. Le Directeur Général du Centre Africain d'Etudes Supérieures en Gestion(CESAG) pour l'accueil dans cette Institution et le cadre propice aux études ;
- tous les enseignants de Master Professionnel en Audit et Contrôle de Gestion pour la formation reçue ;
- l'ISCBF pour la rigueur dans la formation dont elle est garante.

LISTE DES SIGLES

AFAI : Association française de l'audit et du conseil informatiques

BIA : Business impact analysis

BSC : Balanced Scorecard

CECA : Cabinet d'Expertise Comptable, de Conseils et d'audit

CISA : Certified in Information System Auditors

CISM : Certified in Information System Management

CISSP : Certified in Information System Security

CMMI : Capabily Maturity Modèle Integrate

COBIT : Controle Objectives for Information and related Technology

COSO : Committee of Sponsoring Organizations of the Treadway Commission

DESCAE : Diplôme d'Etudes Supérieures de Commerce et d'Administration des Entreprises

DESS : Diplôme Etudes Supérieures Spécialisées

DSC : Diplôme d'études Supérieures Comptables

FFIEC : Federal Financial Institutions Examination Council

ISACA : Information System Audit and Control Association

ISO : International Organization for Standardization (Organisation internationale de normalisation)

ITGI : Information Technology Governance Institute

OCDE	:	Organisation de Coopération et de Développement Economique
OGC	:	Office of Government Commerce
ONECCA	:	Ordre Nationale des Experts Comptables et Comptables Agréés
OPSI	:	Officier Principale de la Sécurité de l'Information
PCI DSS	:	Payment Card Industry Data Security Standard
PMBOK	:	Project Management Body of Knowledge
PME/PMI	:	Petites et Moyennes Entreprises/Industries
RACI	:	Responsible Accountable Consulted Informed
Risk-IT	:	Information Technologies Risk
ROI	:	Return On investment
SDF	:	Systèmes Financiers Décentralisés
SI	:	Système d'Information
SLA	:	Service Level Agreements
SOX	:	Sarbanes-Oxley
TI	:	Technologie de l'Information
TOGAF	:	The Open Group Architecture Framework
VAL-IT	:	Information Technologie Values

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ANNEXES

TABLE DES MATIERES

INTRODUCTION GENERALE

A travers le temps, que ce soit au sein de la famille, de la communauté, de la nation, de la région etc. l'harmonie, la cohésion, la réussite, le développement pour ne citer que ceux-là, sont le fruit d'une gouvernance. La gouvernance est l'art qui différencie les chefs car, tous se sont distingués à travers le temps surtout dans des confrontations pour prendre le dessus les uns sur les autres. Nous pouvons ainsi citer des chefs de guerre, de nation, d'Etat…

Aujourd'hui, la gouvernance est devenue une nécessité pour les Etats dans la marche vers le développement. Elle est régie par des normes et fait l'objet d'une évaluation par la banque mondiale. Pour l'OCDE (l'Organisation de Coopération et de Développement Economique) une bonne gouvernance publique aide à renforcer la démocratie et les droits humains, favorise la prospérité économique et la cohésion sociale, réduit la pauvreté, améliore la protection de l'environnement et l'utilisation durable des ressources naturelles, et augmente la confiance en l'administration publique et le gouvernement. Ces exigences aux Etats se traduisent par la réglementation de la gouvernance d'entreprise.

La gouvernance d'entreprise selon l'OCDE, implique une série de relations entre la direction de l'entreprise, son conseil d'administration, ses actionnaires et les autres parties prenantes. Elles fournissent également la structure par laquelle sont fixés les objectifs de l'entreprise et les moyens par lesquels ces objectifs sont atteints et la performance surveillée.

La gouvernance peut être perçue comme la gestion, le management, le contrôle, la supervision, la maitrise d'une tâche, d'une activité, d'une procédure, d'un processus, d'une organisation, d'une multinationale, d'une nation, d'un pays, d'un continent et même de la planète. Il va s'en dire que tout ce qui se trouve affecté d'un objectif doit être gouverné. C'est-à-dire dirigé dans le sens de l'atteinte de cet objectif.

L'OCDE dans sa politique de développement des pays, passe par un suivi très particulier des directives aux entreprises, car la croissance des entreprises dans un pays assure son développement. Elle met ainsi l'accent sur la bonne gouvernance du public en passant par les parties prenantes que constituent les organisations.

Gouverner une entreprise, une structure, une société, (etc.), c'est gérer toute information autour; que ce soit des informations directement ou indirectement liées. En effet, l'information est un catalyseur d'action; toute information est porteuse d'action qui impacte positivement ou non (vers l'atteinte de l'objectif visé ou non) l'entreprise.

La démonstration ainsi faite, prouve la place capitale de l'information (voire incontournable et indispensable) dans la maîtrise ou la gestion. Il est alors impossible de gouverner sans information. La possession de l'information change toute chose. C'est ce qui a poussé très tôt les grands stratèges de tous les temps à protéger les informations ou à en fournir de fausses pour atteindre leurs objectifs. C'est l'exemple de Sun Tzu, les américains avec l'invention du codage et du chiffrement, pour ne citer que ces deux là.

Posséder l'information c'est décider, décider c'est agir, agir c'est orienter et orienter c'est gouverner. Ceci, pour résumer tout ce qui précède, voudrait simplement dire, gouverner c'est gouverner l'information. La gouvernance de l'information lui confère certains caractères : l'intégrité, la fiabilité, la disponibilité, la sécurité etc.

Pour assurer ces caractères à l'information, l'information évolue dans un système appelé système d'information. Le système d'information est un ensemble organisé de ressources (matériels, logiciels, personnels, données et procédures) qui permet de regrouper, de classifier, de traiter et de diffuser de l'information sur un environnement donné. Gouverner une organisation c'est en gouverner le système d'information.

Contrairement à la connaissance étendue du système d'information, que le commun des gestionnaires et managers ont, le système d'information n'est pas de l'informatique, bien qu'il puisse être automatisé. Le système d'information est la seconde branche composante du contrôle de gestion, la première plus connue étant le système budgétaire.

La gouvernance du système d'information paraît comme un concept assez nouveau, cela est bien juste, car le système d'information, en son essence, est méconnu. C'est donc ce qui explique le fait de laisser le soin de toute décision en relation aux systèmes d'information (SI) à la direction des SI ou du service informatique. Le COBIT (Control

Objectives for Information and related Technology) et ISACA (Information Systems Auditor and Control Association) annoncent le système d'information comme le support des métiers et de l'affaire de l'entreprise. Ainsi, le système d'information doit s'aligner de façon stratégique aux objectifs d'affaires, et être perçu non comme un consommateur de coût, mais comme produisant de la valeur avec un retour sur investissement calculable et une performance mesurable.

Dans cette optique le COBIT offre un ensemble de bonnes pratiques dans sa gouvernance et les associe à trente-quatre (34) processus qu'il identifie. ISACA quant à lui voit le COBIT comme le référentiel adéquat pour tenir l'évaluation obligatoire des systèmes d'information pour s'assurer de la qualité fiable de l'information.

Face à l'exigence d'ISACA en rapport avec le manque de gouvernance des SI ayant pour causes:

- la méconnaissance de la gouvernance des SI,
- la non détection des défaillances du SI d'entreprise,
- les pertes d'argent, de productivité, d'avantages concurrentiels en n'implémentant pas la gouvernance des SI,
- l'appétit aux risques décidé par le directeur des SI,
- le retard technologique de l'entreprise,
- les problèmes de sécurité des SI,
- les risques d'audit très élevés.

Ces causes induisent respectivement les conséquences suivantes:

- pas de mise en œuvre de bonnes pratiques en matière de gouvernance de systèmes d'information,
- mise en péril de la continuité de l'activité,

- SI non-performant ayant pour corollaire le manque de performance du processus d'affaires ;
- réalisation de risques de criticités très élevées ;
- perte cruciale de parts de marchés ;
- perte d'information d'importance capitale et une accessibilité des informations confidentielles ;
- rejet de l'opinion sur les comptes, les états financiers, l'image fidèle de l'entreprise, pouvant impacter la crédibilité de l'auditeur ou du commissaire aux comptes. Car, « tout système d'information est porteur d'informations financières et de budget, dont il faut suivre l'avancement et les écarts par rapport aux budgets planifiés ».

A cette situation de risques bruts, en tant qu'auditeur, notre mission est d'apporter des dispositifs pouvant tantôt les prévenir, tantôt les réduire, soit les détecter ou encore les corriger.

- mettre en place une gouvernance des systèmes d'information.
- Recruter un expert en gouvernance des SI.
- Exiger le COBIT comme référentiel de bonnes pratiques à la haute direction.
- Former la haute direction à la gouvernance de SI.
- Élaborer un manuel de procédures de l'évaluation de la gouvernance de systèmes d'information conformément au COBIT.

Cette dernière solution paraît moins coûteuse et plus adéquate pour un cabinet dans le cadre de sa mission. Car, c'est ainsi, que le cabinet pourrait obliger la haute direction de l'entreprise à prendre ses responsabilités face à la gouvernance des SI.

Le choix de cette solution produit dans l'esprit de tout lecteur, une série de questions dont la principale est: comment élaborer un manuel de procédures d'évaluation de la gouvernance des SI au regard d'un référentiel?

Ensuite surgissent parmi tant d'autres questions :

- qu'est-ce qu'un référentiel et un manuel de procédures?
- Qu'est-ce que la gouvernance des SI et le COBIT?
- Comment conçoit-on un manuel de procédures?
- Comment mettre en place une gouvernance de systèmes d'information suivant le COBIT?

Le thème de notre recherche pour répondre à ces différentes interrogations, s'intitulera : « CONCEPTION D'UN MANUEL DE PROCEDURES D'EVALUATION DE LA GOUVERNANCE DE SYSTEMES D'INFORMATION ». Il ne portera pas sur l'ensemble du Système d'Information mais seulement sur son aspect gouvernance, c'est-à-dire le rôle de la direction, de la haute direction et du conseil d'administration dans la gouvernance des SI.

L'objectif principal est de faire ressortir l'importance de la gouvernance des systèmes d'information pour l'entreprise d'aujourd'hui.

De façon spécifique, il s'agit de montrer au cabinet CECA l'importance d'une assurance des SI par rapport aux risques d'audit d'une part, et d'autre part, faire connaitre le référentiel COBIT dans son ensemble.

L'intérêt de ce travail est de permettre à tout cabinet et auditeur des SI ou non, d'avoir une assurance raisonnable sur la pratique de l'évaluation de la gouvernance des systèmes d'information.

PREMIERE PARTIE : CADRE THEORIQUE

La revue de littérature vise à appréhender l'ensemble des concepts qui composent et tournent autour du thème. Il a donc pour objectif de permettre une compréhension de ce qu'est le manuel de procédures, la gouvernance, le COBIT, le référentiel. Il permet de constater l'intérêt du choix du thème et de comprendre les interactions entre les différents concepts.

Nous parlerons ainsi du référentiel et du manuel de procédures d'une part, la gouvernance des systèmes d'information et le COBIT d'autre part et enfin la méthodologie de la recherche en chapitre troisième.

Le premier chapitre traitant référentiel et manuel de procédures, apportera des précisions permettant de les comprendre et d'en cerner la nécessité pour une entreprise en général et particulièrement un cabinet. Le chapitre deux nous mène au cœur de la gouvernance des systèmes d'information. On y découvrira la portée de cette dernière dans la gouvernance de l'entreprise sans détour le référentiel de universel qu'est le COBIT. Le COBIT parle des meilleures pratiques de gouvernance de l'information et de l'évaluation celle-ci grâce à ses objectifs de contrôle.

CHAPITRE I: REFERENCIELS ET MANUEL DE PROCEDURES

Aussi bien pour le manager que pour l'auditeur, les référentiels et les manuels de procédures constituent des outils essentiels dans l'exécution de leurs tâches. Pour l'un, ils constituent le guide des pratiques dont la mise en œuvre le libère de toute charge relative à un manque de diligence professionnelle. Pour l'autre, c'est par contre le moyen d'évaluation de la mise en œuvre des bonnes pratiques acceptées par tous et surtout par l'entité à évaluer. « Dès que le référentiel a une diffusion large, on parle de « standard » ; ensuite dans le langage courant on parle de standard *de facto* (standard de fait) » (TENEAU & Al., 2009: 102).

1.1 Référentiel

Le référentiel n'est pas quelque chose de nouveau pour l'esprit humain. Il s'agit là en fait d'un thème ancien et toujours très actuel. Il peut-être donc appréhendé grâce à un champ lexical qui a évolué avec le temps. « Un référentiel se définit dans l'espace grâce à ses axes, par rapport auxquels tout élément se situe selon des coordonnées » (CHALLANDE & LEQUEUX, 2009: 19).

1.1.1 Cadre conceptuel d'un référentiel

Pour cerner ce que c'est qu'un référentiel, passons par des concepts très proches et son étymologie.

Référer signifie « rapporter une chose à une autre » ou « faire rapport », mieux encore en « appeler à ».

Le mot référence est utilisé pour désigner les personnes auprès desquelles on peut prendre des renseignements ou des modèles. Il exprime l'action de se référer ou de renvoyer à une chose universellement acceptée.

Pour résumer Figari (1994 : 44), le référentiel est l'élément sur lequel on se base pour se départager (arbitre). Il peut-être aussi assimilé à une personne ressource dans un domaine spécifique qui prodigue les meilleures solutions du faite de son expérience. Mieux encore un réservoir de meilleures pratiques vers les quelles on se rend pour décanter des situations complexes ou pour les éviter.

Selon TENEAU & Al. (2009: 102) « un référentiel est un ensemble de recommandations qui composent un produit industriel, ou un processus, ou un service. Un référentiel est élaboré au préalable par une organisation réunissant un ensemble d'experts. ».

Au cœur du dispositif de reconnaissance, nous trouvons un texte ou un ensemble de textes fondateurs que nous désignerons par le terme de référentiel. Il peut s'agir de textes normatifs ou législatifs aussi bien que de textes d'origine privée issus du monde industriel. Cet ensemble de documents peut être caractérisé par un nom, une version, une date de création (OTTER, & Al., 2009 : 8).

Le référentiel est l'inventaire d'activités et de compétences nécessaires à l'exercice de ces activités. Les références d'un système d'information intégré dans des bases de données forment ce que l'on appelle « un référentiel » en informatique. (TENEAU & Al., 2009: 102).

Le référentiel est en somme un cadre de référence des normes, des directives et selon le cas des bonnes pratiques dans un secteur ou domaine très spécifique. Il peut à la fois être interne ou externe à l'entreprise. Le référentiel interne à l'entreprise peut être perçu comme son manuel de procédures. Car, il regroupe les bonnes pratiques acquises par expérience dans l'entreprise.

Par contre, le référentiel externe que nous considèrerons comme universel, est le fruit d'un collège de bonnes pratiques acquises dans un domaine précis comme la qualité. Ce dernier est donc plus général et plus étendu, ce qui facilite son adaptation à l'organisation. Ainsi défini, le cadre de référence du domaine des systèmes d'information doit permettre simultanément de garantir une :

- meilleure évaluation de la performance des SI,
- gestion des ressources des SI plus efficace,
- gestion des risques plus pertinente,
- amélioration de la valeur des services de l'entreprise par le biais de ses SI,
- meilleure adéquation des SI à la stratégie de l'entreprise (OTTER, & Al., 2009 : IV).

Compte tenu de la diversité des métiers de l'informatique, de leurs rythmes d'évolution différents, des degrés de maturité entre différents pays, il n'existe pas un cadre unique de référence, mais de multiples outils entre lesquels il peut paraître difficile de faire un choix pertinent, chacun ayant ses propriétés, mais l'ensemble laissant aussi apparaître des lacunes et des redondances. La section suivante fera cas des référentiels les plus connus des SI.

1.1.2 Les référentiels autour du SI

Le domaine des SI regorge un grand nombre de référentiel. Cela est compréhensible d'autant puisque l'information se trouve dans tous les secteurs d'activités. Il en résulte que les bonnes pratiques soient aussi variées et la nécessité de chacun de ces systèmes a ses particularités. Il est de même pour les référentiels de la gouvernance de TI qui sont bien légions. De façon non exhaustive, nous sommes en mesure d'énumérer :

- **Le COSO (Committee of Sponsoring Organizations of the Treadway Commission)** a publié en 1992 un cadre de référence pour le contrôle interne afin d'aider les entreprises à évaluer et à améliorer leur système de contrôle interne. Le

contrôle interne y est décrit comme un processus étant sous la responsabilité d'une instance constituée dans le but d'assurer la réalisation d'objectifs regroupés dans les domaines suivants : efficacité et efficience des opérations, fiabilité des rapports financiers, conformité aux lois et règlements.

- **Le référentiel Balanced Scorecard (BSC)**

Le Balanced Scorecard (BSC), ou tableau de bord prospectif, est une représentation qui permet de clarifier la vision et la stratégie d'une entreprise, et de la traduire en plans d'action. Il donne aussi bien le retour sur le fonctionnement des processus internes que des contraintes externes, permettant d'entrer dans une amélioration permanente de la stratégie et de la performance. Ses auteurs, Robert Kaplan et David Norton, le décrivent comme suit : « Le BSC prend en compte les résultats financiers traditionnels, mais ces résultats n'éclairent que le passé, ce qui convenait à l'ère industrielle, avec des investissements à long terme et une relation client peu présente. Ces éléments financiers sont inadaptés, cependant, pour piloter les entreprises de l'ère de l'information qui doivent construire leur future valeur au travers de l'investissement dans leurs clients, leurs fournisseurs, leurs employés, leurs processus, leur technologie et leur innovation. »

- **Le cadre de référentiel management de la sécurité**

Plusieurs normes, méthodes et référentiels de bonnes pratiques en matière de sécurité des systèmes d'information sont disponibles. Ils constituent des guides méthodologiques ainsi que les moyens de garantir une démarche de sécurité cohérente. L'ISO a entrepris un vaste effort de rationalisation des travaux existants, donnant naissance à la série de normes ISO/IEC 27000. Ce nombre correspond à la réservation d'une série de normes relatives à la sécurité. À ce jour, les normes 27000, 27001, 27002 et 27006 sont publiées. Certaines sont obligatoires pour obtenir une certification, les autres ne sont que de simples guides :

- la norme ISO/IEC 27000 présente le vocabulaire et les définitions du domaine de la sécurité, applicables à chacun des standards ;

- la norme ISO/IEC 27001 décrit la politique du management de la sécurité des systèmes d'information au sein d'une entreprise qui sert de référence à la certification ;
- la norme ISO/IEC 27002 constitue le guide de bonnes pratiques de la sécurité des SI ;
- la norme ISO/IEC 27003 a pour vocation d'être un guide d'implémentation ;
- la norme ISO/IEC 27004 sera un nouveau standard pour le pilotage des indicateurs et des mesures dans le domaine de la sécurité des SI ;
- la norme ISO/IEC 27005 sera un nouveau standard sur le management des risques pour la sécurité des SI ;
- la norme ISO/IEC 27006 résume les exigences applicables aux auditeurs externes dans leur mission de certification sur l'ISO 27001.

– **Le référentiel ITIL : le management des services**

Développé par l'OGC (Office of Government Commerce) **pour le gouvernement britannique, ITIL (Information** Technology Infrastructure Library) se présente comme une série de livres décrivant les bonnes pratiques pour le management des services TI. C'est ce qui lui vaut le nom de « library ». Son approche est davantage orientée sur le « quoi faire » que sur le « comment faire » (KLOSTERBOER, 2011 : 11).

Les principes qui sous-tendent ITIL sont l'orientation client, la prise en compte en amont de tout projet, des exigences de services et l'approche processus. ITIL est devenu un standard de fait, au moins pour le périmètre des centres d'assistance et des opérations.

1. Ceci étant, l'année 2007 a marqué une étape assez décisive, presque un schisme, puisque au moment même où l'ISO se basait sur ITIL V2 pour publier la norme ISO/IEC 20000, on assistait au lancement d'ITIL V3. Cependant, la population des utilisateurs d'ITIL se résume au déploiement fait de la version 2.

1.2 Conception d'un manuel de procédures

La conception d'un manuel de procédures doit être faite pour atteindre les objectifs suivants :

- contribuer à l'atteinte des objectifs de contrôle interne,
- améliorer la qualité des systèmes d'information,
- sauvegarder les actifs de l'entreprise par des procédures de contrôle interne permanent,
- favoriser l'harmonisation des modes d'exécution des tâches en les formalisant,
- favoriser l'assimilation rapide des techniques spécifiques de l'entreprise pour le personnel nouvellement affecté à un poste de travail.

1.2.1 Qu'est-ce qu'une procédure

Selon HENRY & Al., (2001 : 16, 17).

« une procédure est :

- un enchaînement de tâches élémentaires standardisées,
- déclenchées en amont par l'expression quelconque,
- limitées en aval par l'obtention d'un résultat attendu.

Chaque procédure se présente donc comme une suite d'opérations effectuées dans une même séquence de temps, par un nombre limité d'acteurs appartenant à un même sous-ensemble.... Chacune des tâches suppose une série logique d'opérations ou de gestes élémentaires, obéissant à des règles techniques données. Une fiche de procédure contient

donc un ensemble d'instructions permettant de traiter une situation définie par un événement initial et un résultat final ».

Dans l'univers des Systèmes d'Information, la notion de procédure est définie comme le propose ISACA. « Les procédures sont des étapes détaillées, définies et documentées permettant l'implantation des politiques. Elles doivent résulter des politiques mères et doivent mettre en œuvre l'idée (l'intention) de l'énoncé de politique. » (ISACA, 2011 : 113)

Une procédure est une succession imposée de tâches à réaliser. Une procédure répond en général à des impératifs qui ne sont pas discutables par l'opérateur qui les appliquent.

On ne saurait donc définir les procédures sans définir les processus qui les englobent et tâches dont elles sont constituées.

D'après FRECHER & Al. (2003 : 9), un processus est un enchainement d'activités interdépendants qui assurent la production d'une plus-value. Mieux encore, il soutient que l'entreprise peut être scindée en processus.

FRECHER & Al, mettent l'accent sur la valeur qu'apporte l'activité pour laquelle les procédures sont mise en place. Par contre MEIER parle plutôt de la structuration géométrique et logique des ressources des capacités et compétences qui produisent le résultat. Il laisse ainsi ressortir les liens chronologiques et relationnels entre les différentes ressources mais également les capacités et les compétences, pour produire un résultat ou output (MEIER, 2009 :164).

La procédure d'entreprise représente la manière de mettre en œuvre tout ou partie d'un processus métier. Le processus représenterait alors le Quoi?, et la procédure le Qui fait Quoi?, Où? Quand? Comment? Combien? Pourquoi dans la logique du QQOQCCP.
Dans un sondage anodin d'environ 200 livres de gestion ou de management moins de 5 (cinq) ne font mention des mots processus / procédures. Ceci montre combien les processus et procédures sont importants dans le management et la gestion.

1.2.2 Le manuel de procédures

Conformément à l'article 16 du référentiel juridique du Système comptable OHADA « toute entreprise établit une documentation décrivant les procédures et l'organisation comptable. Cette documentation est conservée aussi longtemps qu'est exigée la présentation des états successifs auxquels elle se rapporte ». Il est à cet effet obligatoire qu'une structure dispose de procédures qu'elles soient écrites ou non. Les procédures écrites se retrouvent dans un document dénommé « manuel de procédures ».

HENRY & Al. (2003 : 27) après une étude sur les procédures en entreprise conclut que ces travaux récents prouvent l'efficacité dans un contexte mondialisé de l'utilisation des manuels de procédures. Ceci montre ainsi l'importance des procédures écrites dans un milieu multiculturel. « Les procédures remplissent un rôle similaire à celui du protocole dans les relations diplomatiques. Elles encadrent les interactions des personnes par les procédures les préservant d'éventuelles offenses dans un espace dépourvu de repères partagés ».

De façon synthétique, le manuel des procédures est un document contenant l'ensemble des opérations ou tâches courantes de l'entreprise sous forme d'instructions claires.

Avec une vision d'auditeur, on peut percevoir les procédures non pas comme des garde-fous mais plutôt comme l'élément dont le respect protège l'employé parce qu'ayant mise en œuvre les diligences requises en appliquant les bonnes pratiques.

1.2.3 Concevoir un manuel de procédures dans un projet

Toute conception est faite dans le cadre d'un projet qui part de l'étude de faisabilité à l'acceptation du livrable par son consommateur. C'est ce qui motive la volonté de la conception du manuel de procédure dans un contexte formel qu'est le projet. En définitive, la gestion de la conception du manuel de procédures se fera par projet.

La gestion par projet est, par nature, un domaine dans lequel la rédaction des procédures revêt de l'importance.

On se passera ici des définitions[1] multiples que l'on affecte à la notion de projet ou à la gestion de projet. Nous passerons directement à une démarche projet assez agile qui puisse s'adapter aux différentes phases de la conception d'un manuel de procédures.

1.2.4 Les phases de la conception d'un manuel de procédure

- Le formalisme du manuel

Le formalisme du manuel est l'exigence en termes de présentation. Il devra ainsi composer, autant que possible, une architecture complète et cohérente. « Chaque procédure joue un rôle qui lui est propre. Simultanément, elle est reliée aux autres. Cette cohérence doit être préservée lors des mises à jour » (HENRY & Al., 2003 : 51). Cette présentation doit permettre un accès rapide, désiré et attirant aux informations contenues dans le manuel à travers de catalogues, de sommaires, d'index, de lexiques qui s'adaptent aux utilisateurs. On en débouche au plan type du manuel de procédure proposé par HENRY & Al. :

- généralités [préface de la direction (l'esprit du texte), mode d'emploi du manuel, procédure de mise à jour] ;
- procédures classées [page de synthèse, diagramme de flux, description détaillée des taches] ;
- tables [lexique, listes par processus ou par objets, index, sommaire].

[1] Un projet est «un objectif à réaliser, par des acteurs, dans un contexte précis, dans un délai donné, avec des moyens définis, nécessitant l'utilisation d'outils appropriés.

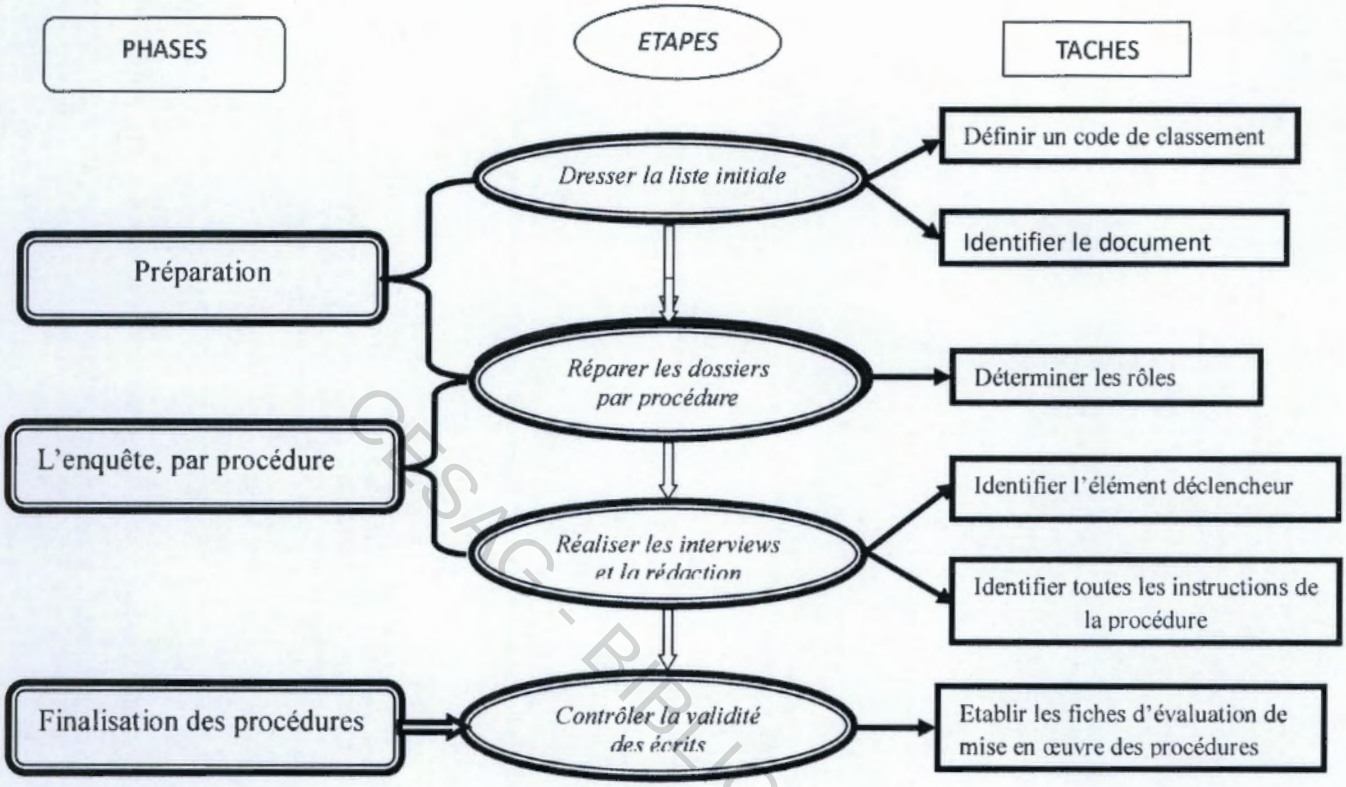
Il précise, entre autres, que pour être opérationnelles les procédures doivent être claires, concrètes, précises et réalistes.

- Le processus de rédaction du manuel de procédures

Tout comme précisé plus haut cela ce fera dans un contexte projet. HENRY & Al. (2003 : 77) le recommandent vivement : « lors de la création d'un nouveau manuel, on a intérêt à en organiser la réalisation sous forme d'un projet, ne serait-ce que pour mieux en garantir la cohérence finale ».

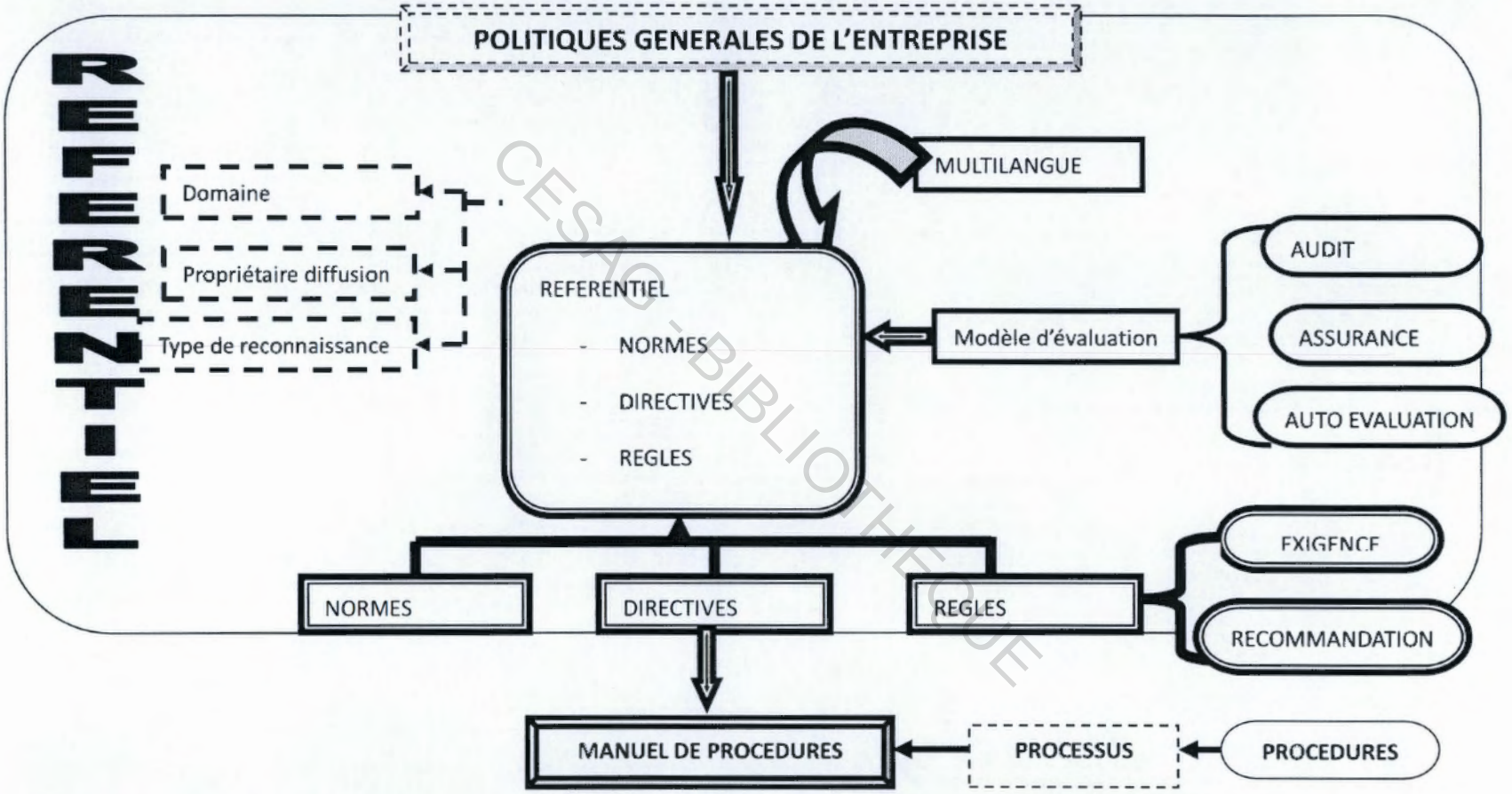
Processus de rédaction en 6 étapes de HENRY & Al. (2003 : 77) avec le deuxième niveau (la rédaction d'une procédure) proposé par BERGER & Al. Nous permettent d'aboutir à cette proposition de démarche d'élaboration.

Figure1 : démarche de rédaction d'une procédure



Source : Nous-même à partir de HENRY & Al. (2001 : 32) et BERGER & Al. (1999 : 67)

Figure2 : lien entre la politique générale de l'entreprise, le référentiel et le manuel de procédures.



Source : nous même à partir de OTTER & Al. (2009 : 7 - 12).

Au départ, la définition du référentiel et du manuel de procédures ne permet pas d'y voir ni la différence, ni le lien. Ce dernier se résume surtout au fait qu'ils contiennent tout deux les bonnes pratiques d'une corporation ou d'un secteur d'activités. La différence majeure en est que le référentiel s'impose au manuel de procédures qui n'est à priori que son reflet avec des touches particulières à l'entreprise en fonction de son organisation.

CHAPITRE II LA GOUVERNANCE DES SYSTEMES D'INFORMATION ET LE REFERENTIEL COBIT

Aujourd'hui, la gouvernance des systèmes d'information s'impose aux organisations en général et en particulier aux entreprises. Et, c'est le COBIT qui s'inscrit comme le garant des bonnes pratiques de cette gouvernance. Pour cette raison nous ne pouvons parler dans ce chapitre de la gouvernance des SI et omettre de mentionner le COBIT.

2.1 Gouvernance des Système d'Information

« L'information est le support formel d'un élément de connaissance humaine susceptible d'être représentée à l'aide de conventions (codages) afin d'être conservée, traitée ou communiquée. » dit DI SCALA (2005: 12)

Au cœur de toute organisation se trouve un élément indispensable à sa gestion, à l'exécution de ses processus, à leurs contrôles, à leurs entrées et sorties. Ceci n'est rien d'autre que l'information. Disposer de l'information avec toutes ses caractéristiques pour sa fiabilité nécessite un système qui le véhicule, le sécurise et le rend disponible. Il s'agit du système d'information (SI).

Vu l'importance que revêt l'information dans l'entreprise, sa gestion est donc primordiale pour sa suivie.

Le système d'information est selon DI SCALA (2005: 767) « dans une entreprise ou une administration, la structure sémantique des données, leur organisation logique et physique, le partage et l'accès à de grandes quantités de données grâce à un système informatique, se nomme un système d'information. ».

Pour GIRAUD & Al., (2005 : 367) le système d'information est l'outil qui rend possible la remontée rapide et la concentration des informations au niveau du siège.

Le système d'information est ici perçu comme un ascenseur unidirectionnel qui ne fait que monter.

« Le système d'information constitue en quelque sorte le signe distinctif de l'organisation qualifiée de « moderne » (par rapport à une organisation qui serait restée « archaïque »). En d'autres termes, à défaut d'un système d'information, point d'organisation. À ce titre, l'organisation est système d'information et le système d'information est organisation, cette double proposition venant constituer en quelque sorte « l'ellipse » qui se trouve à la base d'un modèle informationnel de l'organisation. » (LÖNING & Al., 2008: 206-207).

En considérant ces trois définitions du système d'information, on se rend compte qu'il est le cœur de l'organisation sans lequel la remonté et la mise à disposition de l'information ne seraient possible vers la haute direction pour la prise de décisions d'une part, et utilisable par des agents dans l'exigence de leur travail d'autre part.

Mener c'est maitriser, gérer c'est mener, gouverner c'est gérer. Gouverner c'est prévoir, dit-on, mais c'est tout autant savoir prédire ou supputer l'avenir (BRILMAN & HERARD, 206 : 105).

La gouvernance de l'information à travers les systèmes d'information n'est rien d'autre que la gouvernance d'organisation. Car gouverner c'est utiliser l'information pour décider. La gouvernance de l'information est donc très indispensable voire cruciale pour la croissance, le développement et surtout la survie d'une organisation quelle qu'elle soit.

Nous constatons que c'est à juste titre qu'il est dit: « L'instance de gouvernance de TI est le conseil d'administration, dont les membres sont élus parmi les représentants des chapitres nationaux lors de l'assemblée annuelle. Ceux-ci sont des avocats, des consultants, des gestionnaires et d'anciens hauts fonctionnaires en provenance de plusieurs pays. L'instance de TI s'est également dotée d'un conseil composé de personnalités de haut niveau, dont le but est de soutenir les différents programmes. Ces instances contribuent de manière importante à la mission de TI par le soutien qu'elles donnent à la vision et aux positions officielles de l'organisation dans des forums de

grande visibilité, par leurs apparitions dans les médias et par leur contribution à la recherche sur la corruption (BERNIER, 2006 : 436).

De très grandes structures ont aujourd'hui adopté des systèmes standards de gouvernance de leur information. Cependant, elles n'exercent pas dans la réalité la gouvernance des SI. Pour elles, la direction des systèmes d'information (DSI) suffirait. Erreur monumentale, car des décisions qui relèvent de la haute direction (conseil d'administration) ne peuvent être laissées aux soins de la DSI. Le meilleur exemple entre autres non moins importants est l'appétit aux risques liés à la gouvernance des TI. L'ISACA a donc à juste titre défini les niveaux de responsabilité pour une bonne gouvernance de la sécurité des SI (Annexe 4). Le système d'information est un élément des TI comme l'indique le COBIT : l'Information Technology (IT) : se rapporte tantôt au potentiel global offert par les technologies de l'information (TI), ou à leur utilisation dans l'entreprise sous forme de systèmes d'information (SI).

Ceci implique que la gouvernance des TI inclut celle des SI. On ne saurait donc parler des SI sans faire cas des TI ; car ce serait sortir le SI de son environnement.

2.1.1 La gouvernance de TI

La gouvernance et la gestion des TI font partie intégrante de la gouvernance d'entreprise et constituent des structures de direction de processus qui garantissent que les TI soutiennent et prolongent la stratégie et les objectifs de l'organisation (adapté de l'ISACA, board briefing on IT, 2nd Edition, E.U. 2003).

L'ISACA (Information Systems Audit and Control Association) a développé le COBIT (Objectifs de contrôle pour l'information et les technologies associées) à partir de 1994, en tant que modèle de référence pour l'audit des systèmes d'information. L'ISACA, association internationale d'auditeurs représentée en France depuis 1982 par l'Association française de l'audit et du conseil informatiques (AFAI), a été créée en 1967.

Elle compte aujourd'hui plus de 95 000 membres individuels répartis dans plus de 160 pays qui occupent des postes liés au traitement de l'information, tels que directeurs des systèmes d'information, auditeurs internes et externes, consultants, formateurs ou encore professionnels de la sécurité.

Au début des années 2000, l'ISACA a pris en compte la préoccupation de la Corporate governance portée par le COSO (Committee of Sponsoring Organizations of the Treadway Commission). Le COSO a pour but d'améliorer la qualité des informations financières fournies par les entreprises du secteur privé à travers l'éthique, le contrôle interne et la gouvernance d'entreprise. Cette orientation stratégique s'est traduite en 1998 par la création de l'ITGI (Information Technology Governance Institute), qui pour vocation la conduite de projets de recherche dans le domaine de la gouvernance des systèmes d'information.

En effet, le rôle habituel de la gestion des TI, par conséquent des SI est d'aider les secteurs de production à mener leurs opérations de façon efficace et efficiente. Cependant, aujourd'hui les TI font partie intégrante de chaque facette des opérations d'une organisation. Leur importance continue d'augmenter d'année en année et cette tendance est peu susceptible d'être renversée. Ceci est explicable par l'avancée exponentielle de la technologie.
La gouvernance des TI couvre ainsi, entre autres :

- la gestion des ressources humaines : formation, politique de promotion, répartition et déclaration du temps de travail, évaluation de la performance de l'employé, vacance obligatoire, politique de cessation d'emploi etc. ;
- la pratique et la stratégie d'impartition ;
- la gouvernance dans l'impartition ;
- les fournitures de services ;

- la pratique et stratégie de modélisation ;
- la gestion des modifications ;
- l'amélioration des services et satisfaction de l'utilisateur ;
- la gestion des changements organisationnels ;
- la gestion de la qualité ;
- la pratique de la gestion financière ;
- l'optimisation de la performance ;
- la structure organisationnelle des SI et responsabilités (ISACA, 2011 : 55).

2.1.2 Les domaines de priorité de la gouvernance de TI de l'information

Le COBIT les appelle aussi les cinq (5) axes stratégiques de la gouvernance des systèmes d'information. Ils sont résumés dans le tableau suivant :

Tableau 1 : les cinq axes stratégiques de la gouvernance des SI

L'alignement stratégique	Consiste à s'assurer que les plans informatiques restent alignés sur les plans des métiers, à définir, tenir à jour et valider les propositions de valeur ajoutée de l'informatique, à aligner le fonctionnement de l'informatique sur le fonctionnement de l'entreprise
L'attribution de valeur	Consiste à mettre en œuvre la proposition de valeur ajoutée tout au long de la fourniture du service, à s'assurer que l'informatique apporte bien les bénéfices attendus sur le plan stratégique, à s'attacher à optimiser les coûts et à prouver la valeur intrinsèque des SI
La gestion du risque	Exige une conscience des risques de la part des cadres supérieurs, une vision claire de l'appétence de l'entreprise pour le risque, une bonne connaissance des exigences de conformité, de la transparence à propos des risques significatifs encourus par l'entreprise et l'attribution des responsabilités dans la gestion des risques au sein de l'entreprise.
La gestion des ressources	Consiste à optimiser l'investissement dans les ressources informatiques vitales et à bien les gérer : applications, informations, infrastructures et personnes. Les questions clés concernent l'optimisation des connaissances et de l'infrastructure.
La mesure de la performance	Consiste en un suivi et une surveillance de la mise en œuvre de la stratégie, de l'aboutissement des projets, de l'utilisation des ressources, de la performance des processus et de la fourniture des services, en utilisant par exemple des tableaux de bord équilibrés qui traduisent la stratégie en actions orientées vers le succès d'objectifs mesurables autrement que par la comptabilité conventionnelle.

Source: ITGI (2007 : 56)

2.1.3 La responsabilisation dans la gouvernance des TI selon ISACA

Une gouvernance claire et transparente voudrait que les rôles et responsabilités soient répartis et affectés à leurs titulaires. C'est dans cette optique qu'ISACA après avoir énuméré les meilleures pratiques pour la gouvernance des TI définit clairement les responsabilités et leurs responsables.

2.1.3.1 Rôles et responsabilités de la Haute direction et du conseil d'administration

La gouvernance de la sécurité de l'information nécessite une orientation stratégique et une force d'impulsion. Elle nécessite un engagement, des ressources et l'assignation de responsabilité pour la gestion de la sécurité de l'information, ainsi qu'un moyen pour le conseil d'administration de déterminer que son objectif est atteint. (ISACA, 2011 : 105)

Une gouvernance efficace des SI d'information voudrait une intervention active de la haute direction et du conseil d'administration à travers l'approbation des politiques, une surveillance et des paramètres appropriés ainsi que la production de rapports et l'analyse des tendances. Pour cette raison, il est donc indispensable que les membres du conseil d'administration soient au courant des actifs informationnels et de leur criticité pour les activités d'exploitation (d'affaire). Cette information devrait leur parvenir par la mise en place d'une reddition qui est « Business impact analysis (BIA) » (analyse de l'impact sur les affaires) ajouté à l'évaluation détaillée des risques. Ils pourront décider alors de l'appétit au risque et des coûts d'opportunités.

Cette implication de la haute direction et du conseil d'administration, permet la vue et la réception des décisions relatives à la gouvernance des systèmes d'information par le personnel des échelons inférieurs comme des exigences de la direction qu'ils se doivent de respecter. Pour conforter ces exigences, des pénalités pour non-conformité doivent être déterminées, communiquées, appliquées, du conseil d'administration jusqu'au bas de l'échelle hiérarchique.

2.1.3.1.1 La haute direction

Selon ISACA, « la mise en place d'une gouvernance efficace de la sécurité et la détermination des objectifs de sécurité stratégique de l'organisation sont des tâches complexes et ardues. … Le développement d'une stratégie de sécurité de l'information nécessite son intégration auprès des responsables des procédés administratifs et la coopération de ces derniers. Lorsqu'elle est réussie, on arrive à l'alignement de la sécurité de l'information en appui aux objectifs opérationnels. » (ISACA, 2011 : 105). La prise en compte de ces responsabilités fera ressortir la rentabilité du programme de sécurité de l'information dans l'atteinte de l'objectif visé. Ainsi, un niveau précis et prévisible de certification des procédés administratifs et un niveau d'impact acceptable des évènements défavorables peut s'afficher dans le tableau de bord d'exécution.

2.1.3.1.2 Le comité directeur

Le comité directeur devra gérer les SI conformément au tableau de bord exécutif qui lui est destiné. Le tableau de bord exécutif regroupe les objectifs fixés au comité directeur et les indicateurs de performance permettant d'évaluer le niveau de maturité dans l'atteinte des objectifs fixés.

Le comité directeur est le moyen de rendre présent, réel et viable dans l'entreprise la sécurité qui ne touchait que des aspects d'ordre organisationnels. Ainsi pour s'assurer de la participation de tous les intervenants touchés par les considérations de sécurité, plusieurs organisations utilisent un comité directeur formé de représentants responsables des groupes concernés. (ISACA, 2011 : 105).

Le comité directeur est le canal de communication efficace et fournit une base continue, garantissant l'alignement du programme de sécurité sur les objectifs opérationnels

(alignement stratégique). Pour l'atteindre, il est obligé de réaliser un consensus sur les priorités et les compromis.

Il doit aussi intervenir de façon dynamique dans les processus de modification et de configuration de TI. De la même manière il s'assurera de la réalisation d'une modification des comportements au cours de la gestion du changement.

2.1.3.1.3 L'officier principal de la gestion de la sécurité de l'information

ISACA exige de toute organisation, la possession d'un officier principal de la sécurité de l'information (OPSI), qu'il en porte ou non le titre. Ce peut être le Directeur du personnel Informatique, le Directeur des Technologies, le Directeur Financier, ou dans certain cas le Chef de la Direction, même s'il y a un bureau ou un directeur de la sécurité de l'information en place. La portée et l'ampleur de la sécurité de l'information sont telles que de nos jours que l'autorité requise et les responsabilités qui s'y rattachent en font une des responsabilités de la direction ou de la haute direction. (2011 : 105).

L'office principal de la gestion de la sécurité de l'information peut comprendre entre autre le risque manager et directeur principal de la conformité. Son responsable est chargé du reporting en direction de la haute direction et du conseil d'administration. Ceux-ci s'en serviront pour prendre des décisions d'ordre stratégique comme l'appétit aux risques. Par défaut, la responsabilité légale remontera la hiérarchie et aboutira à la haute direction et au conseil d'administration selon la Sarbanes-Oxley (SOX). L'incapacité à le reconnaître et à mettre en place des structures appropriées de gouvernance peut faire en sorte que la haute direction ne soit pas au courant de cette responsabilité et de la responsabilisation corollaire. Ceci entrainera un manque d'alignement efficace des objectifs.

2.1.3.1.4 Le comité de stratégie des TI

La présence d'un comité de stratégie est perçue comme l'une des meilleures pratiques de l'industrie. Cependant, il doit élargir la portée de son action pour non seulement inclure des conseils sur la stratégie lorsqu'il assiste le conseil d'administration dans ses responsabilités de gouvernance, mais se concentrer également sur la valeur, les risques et la performance des TI. Il s'agit d'un mécanisme pour incorporer la gouvernance des TI à la gouvernance d'entreprise. (ISACA, 2011 : 100).

Le comité de stratégie des TI constitue une aide à la décision en matière des TI pour le conseil d'administration. Tout comme le contrôle de gestion pour la direction, il constitue le pont informationnel, le conseil, et apporte son expertise au conseil d'administration. C'est alors à juste titre qu'ISACA dit (en parlant du comité de stratégie) : « il assiste ce dernier dans la surveillance des questions liées au TI au sein de l'entreprise, en veillant à ce que le conseil dispose de l'information interne et externe dont il a besoin pour prendre efficacement des décisions en matière de gouvernance des TI. » (2011 : 100).

L'analyse et le traitement des questions pertinentes relatives aux technologies de l'information dans l'ensemble de l'organisation se fait en général par son comité de direction. Il doit avoir une compréhension claire de la stratégie des TI et des niveaux de direction. C'est dans ce sens qu'ISACA a publié portant sur l'analyse claire de la stratégie et du niveau de direction résumé dans le tableau ci-après.

Tableau 2: Analyse des responsabilités du comité directeur

Niveau	Comité de stratégie des TI	Comité directeur des TI
Responsabilité	-fournir un aperçu et des conseils : *la pertinence des développements dans les TI dans une perspective administrative ; *l'alignement des TI sur l'orientation de l'entreprise ; *l'atteinte des objectifs stratégiques des TI ; *la disponibilité des ressources, des compétences et des infrastructures en matière de TI pour atteindre les objectifs stratégiques ; *l'optimisation des coûts, y compris le rôle et l'offre de valeur de l'approvisionnement extérieur des TI ; *les risques, le rendement et les aspects concurrentiels des investissements en TI ; *les progrès des principaux projets de TI ; *la contribution des TI à l'entrepris (c'est -à-dire. la remise de la valeur commerciale promise) ; *l'exposition aux risques des TI, y compris les risques de conformité ; *l'endiguement des risques des TI ; *l'orientation de la direction relative aux TI ; *les moteurs et catalyseurs pour les pratiques de gouvernance des TI du conseil d'administration.	-Décide le niveau des dépenses en TI dans l'ensemble et de la manière dont les coûts seront affectés ; -Aligne et approuve l'architecture des TI de l'entreprise ; -Approuve les projets et les budgets, en déterminant les priorités et les jalons ; - Acquiert et affecte les ressources appropriées ; - Veille à ce que les projets respectent continuellement les exigences administratives y compris y compris la réévaluation du dossier administratif ; - surveiller les projets pour la remise de valeur et les résultats attendus, à temps et aussi du budget ; - surveiller les conflits de ressources et de priorités entre les divisions de l'entreprise et les fonctions de TI, ainsi qu'entre les projets ; - fait des recommandations et des demandes de changements aux plans stratégiques (priorités, financement, approches technologiques, ressources, etc.) ; - communique les objectifs stratégiques aux équipes de projet ; - contribue de manière importante aux responsabilités de la direction en matière de gouvernance des TI.
Autorité	- donne des conseils au conseil d'administration et à la direction sur la stratégie des TI ; - est délégué par le conseil d'administration pour fournir	- assiste la direction dans la délivrance de la stratégie des TI ; -supervise la gestion quotidienne de la prestation de

	un apport à la stratégie et préparer son approbation ; - se concentre sur les questions actuelles et futures de stratégie des TI.	services de TI et des projets de TI ; - se concentre sur la mise en œuvre.
Membres	-les membres du conseil d'administration et des spécialistes non-membres.	- cadre parrain ; - cadre administratifs (utilisateurs clés) ; - DPI ; - Conseillers clés tels que requis (TI, vérification, services juridiques, finances).

Source : ISACA (2011 : 102)

2.1.3.1.5 La Direction des Systèmes d'Information

« La direction ou le directeur du système d'information fait pleinement partie intégrante de l'entreprise. Assurer le pilotage d'une DSI, c'est assurer la direction d'une véritable PME/PMI, voire plus, ou beaucoup plus. » (CHALLAND & Al., 2009 : 25).

Dans la présenterons cette direction, nous insisterons sur son importance, son objectif et ses responsabilités. La DSI est au cœur de la gouvernance de l'entreprise, ses exigences de la part de la gouvernance sont très cruciales. C'est pour cette raison qu'elle doit en un premier temps s'assurer de l'alignement sur les directives de la direction générale.

Ainsi, selon CHALLAND & Al., « La Direction Générale de l'entreprise ou le conseil d'administration a émis des directives qui constituent la base du contrat en cours entre le DSI et son entreprise. Les directives ne sont pas forcément toutes explicites, certaines sont implicites. Ci-après les exemples les plus courants de directives.

Directives explicites :

- alléger les coûts de l'informatique, améliorer ses rendements ;
- rendre plus performante et plus rapide la DSI;

- rendre plus agile la DSI;
- rendre sa gestion plus transparente ;
- mieux contrôler et/ou être plus « auditable » ;
- unifier et centraliser les gestions informatiques ;
- assurer une sécurité sans faille globale, car la sécurité totale n'existe pas ;
- améliorer l'image de l'entreprise ;
- faire mieux que la concurrence ;
- réduire le papier, les dépenses d'énergie, paraître « vert » ;
- passer au niveau supérieur international ;
- rester au meilleur niveau technologique.

Directives implicites ou non écrites :

- maintenir la paix sociale chez les informaticiens ;
- changer de fournisseur, ne plus subir le monopole d'un fournisseur attitré ;
- faire mieux que le prédécesseur du DSI ;
- satisfaire les utilisateurs ;
- et bien sûr obéir aux directives et ordres de la direction générale de l'entreprise ».

Toutes ces directives se résument à l'allègement des coûts de l'informatique et améliorer ses rendements. Pour cela elle doit soutenir les corps métiers de l'entreprise. C'est dans le cadre de l'appréciation à sa juste valeur qu'ITIL et VAL-IT ont été réalisés puis publiés par ISACA (l'un pour faciliter la description de ses services et l'autre pour leur attribuer de valeur permettant ainsi le ROI).

Ces directives suscitées peuvent être traduites en buts pour la DSI. On peut alors énumérer :

- la production informatique ; il s'agit d'alléger les coûts de l'existant par son entretien, son ordonnancement et surtout son optimisation ;

- la maintenance des applications ; c'est la capacité de la DSI à identifier le coût réel des besoins divers de maintenance, en distinguant bien la maintenance à chaud (résolution d'incidents ou d'erreurs) incontournable de la maintenance applicative ;
- le développement et l'intégration de nouvelles applications ; il est question de la gestion des projets informatique en tenant compte de l'existant ;
- la gestion de l'informatique : mettre en œuvre et faire vivre des tableaux de bord avec un nombre limité, mais bien choisi, d'indicateurs sur le suivi des grands fondamentaux, définir les contrats de services (service level agreements : SLA), la gestion optimale du temps, une bonne responsabilisation et savoir situer les différents éléments des coûts informatiques ;
- rendre l'informatique plus performante, plus rapide : en exigeant un codage propre[2] qui met en œuvre uniquement les grandes fonctions, penser que les cas les plus compliqués peuvent être traités comme des exceptions à traiter en partie ou en totalité manuellement, envisager des matériels plus performants, penser systématiquement à la parallélisation des traitements (load balancing), rechercher les goulots d'étranglements ;
- rendre l'informatique plus agile ; il s'agit de simplifier les processus de décision, mettre en œuvre des procédures allégées de définition de besoin, avoir un processus de décision rapide pour la prise en compte des incidents, faire des évaluations de risques lors des démarrages de nouvelles phases de projet, réduire et bien structurer les réunions, entretenir de bonnes relations etc. ;
- rendre la gestion plus transparente : la transparence concerne tout ce qui a trait au reporting des activités de leur planification, de leur avancement et aussi de leur qualité ;

2Ce n'est pas sans raison si de nombreux principes de conception de logiciels peuvent se ramener à ce simple avertissement. Les auteurs se tuent à communiquer cette réflexion.
Le mauvais code tente d'en faire trop, ses objectifs sont confus et ambigus. Un code propre est *ciblé*. Chaque fonction, chaque classe, chaque module affiche un seul comportement déterminé, insensible aux détails environnants. (. MARTIN Robert, 2009, Coder proprement, PEARSON, 481.)

- mieux contrôler et/ou être plus « auditable » : « C'est posséder pour l'ensemble des composants et des services du système d'information un système de planification, suivi et contrôle. » ; à cet effet, CHALLAND & Al. (2009 : 36) préconisent de doter l'organisation d'un office de programme (encore appelé plans et contrôle opérationnel) en précisant qu' : « un système auditable et bien contrôlé implique d'avoir construit et fait vivre des tableaux de bord avec des indicateurs ».

Ils concluent en disant : « Tout système d'information est porteur d'informations financières et de budget, dont il faut suivre l'avancement et les écarts par rapport aux budgets planifiés. » (2009 : 37) ;

- unifier et centraliser les gestions informatiques, en évitant les féodalités, communiquer par rapport au système d'information commun actuel et par rapport aux projets communs en cours, bien cerner les particularismes et les variations.
- variations et variantes ; il s'agit des changements notables et réguliers avec les éléments dépendants.

Assurer une sécurité globale ; l'importance de l'information rend délicat ce domaine. C'est à juste titre que CHALLAND & Al. font des remarques et conseils très précis. « **Remarques et conseils au DSI en matière de sécurité**

- Assurer les sauvegardes et copies permettant les reprises en cas d'incident ou de malversation. Ne pas oublier de tester périodiquement les reprises pour éviter de se retrouver « fort dépourvu quand la bise est venue ».
- Ne mettre que le strict nécessaire pour les opérations, ne pas laisser des logiciels plus ou moins utiles, plus ou moins sûrs et qui peuvent devenir des chevaux de Troie dans les serveurs et postes de travail.
- Empêcher les accès physiques inutiles comme la possibilité de copier par clé USB, lecteurs divers, les accès par des ports laissés ouverts sans justification.
- Annoncer périodiquement des exercices de sécurité, les faire et en faire de façon impromptue pour toujours laisser un fond d'incertitude, et même d'insécurité, pour les pirates et indélicats potentiels.

- Construire des défenses efficaces, à commencer par les filtres et pare-feu, ceci accompagné d'une supervision efficace et potentiellement de tous les instants.
- Prévoir le pire mais lors d'exercices avoir toujours un plan de secours en cas d'indisponibilité. On parle dans ce cas de Plan de reprise des activités (PRA) qui vient s'ajouter aux dispositions sur la disponibilité du système d'information, voire de haute disponibilité.
- Nommer un responsable de la sécurité informatique directement rattaché au DSI ; il aura des correspondants sécurité dans les différentes organisations de l'entreprise.
- Faire intervenir une expertise externe pour réaliser un audit de sécurité chaque année ; valider un plan d'actions et le mettre en œuvre dans les meilleurs délais.
- Communiquer à travers les tableaux de bord de la gestion du système d'information, et disposer d'au moins un indicateur pour la sécurité. Un rapport et une information exceptionnelle accompagneront toutes les résolutions d'incidents entraînant, par exemple, des interruptions de service. » (2009 : 39).

- Améliorer l'image de l'entreprise, en participant activement à la communication avec l'extérieur (soigner par exemple les fenêtres externes de l'informatique de l'entreprise).

- Faire mieux que la concurrence ; le benchmarking est l'arme la plus efficace pour y parvenir. A ce sens pour CHALLAND & Al. (2009 : 41) : « Faire mieux que la concurrence signifie d'abord avoir une informatique adaptée, performante et économique ; cela permet d'avoir suffisamment de degrés de liberté pour aider l'entreprise à manœuvrer dans des environnements concurrentiels, ou de crises majeures ».

- Réduire le papier, les dépenses d'énergie, paraître « vert » ; il est question ici de la prise en compte de la responsabilité sociétale.

- Passer au niveau supérieur international, en pensant à un système fédérateur que ce soit par la multitude de langues proposée, des devises, des cultures et règles considérées. Dans ce sens CHALLAND & Al. pensent que : « C'est une illusion de croire qu'un progiciel va régler, d'un seul coup de baguette magique, la convergence des multiples

applications et processus des différentes organisations dans des pays de diverses cultures. » (2009 : 43)

- Rester au meilleur niveau technologique, une veille technologique raisonnable, ou la déléguer à des organismes spécialisés, liés à des groupements d'entreprises, et qui devront obligatoirement avoir pignon sur rue et être objectifs et réalistes.
- Le DSI et la comptabilité informatique, c'est en fait ce qui incarne la gestion transparente précitée. Ses principaux objectifs sont :
  - connaître les différentes consommations pour les divers acteurs utilisateurs des systèmes et ressources du système d'information de l'entreprise ;
  - facturer selon l'utilisation réelle des ressources ;
  - mesurer les écarts entre les différentes consommations planifiées, prévues et réelles.
- Répondre au business modèle de l'entreprise : retour sur les cœurs de métier de l'entreprise, les grands processus et de l'utilité des workflows[3], les objets métier et leurs cycles de vie, retour sur la participation à l'économie de l'entreprise, la contribution du SI dans le juste-à-temps, la diversité et la bonne citoyenneté dans le système d'information pour l'entreprise, la pérennité de l'entreprise et de son SI, l'assurance de la continuité de l'entreprise à travers la capitalisation des savoirs.

2.2 Présentation du COBIT

Comprendre et gérer les opportunités et les risques liés aux systèmes d'information, tel est l'objectif de la gouvernance des technologies de l'information. Elle conditionne au plus haut niveau l'efficacité de la gouvernance de l'entreprise. La gouvernance des

3Un **workflow** est un flux d'informations au sein d'une organisation, comme par exemple la transmission automatique de documents entre des personnes.

Technologies de l'Information (TI) regroupe l'ensemble du système de management (processus, procédures, organisation) permettant de piloter les TI. Cette préoccupation est une déclinaison de la volonté d'assurer une gouvernance d'entreprise (*corporate gouvernance*).

COBIT se positionne à la fois comme un référentiel d'audit et un référentiel de gouvernance. Sur le plan de la gouvernance, il se place d'emblée en alignement avec les métiers et la stratégie de l'entreprise. Au-delà de ces positionnements, COBIT est conçu, développé et amélioré en permanence pour fédérer l'ensemble des référentiels en rapport avec les TI (OTTER Al., 2009 :119)

Il est à constater que les entreprises sacrifient leur argent, leur productivité, leurs avantages concurrentiels en n'implémentant pas efficacement une gouvernance des TI. Les dirigeants ont besoins de meilleurs moyens pour :

- ✓ diriger les TI et en tirer des avantages optimaux;
- ✓ pour mesurer la valeur créée par les TI;
- ✓ pour gérer les risques qui découlent des TI.

Le COBIT est approuvé par tous comme étant un Park d'outils qui assure que les TI fonctionnent efficacement. Il fonctionne comme une voûte planétaire de référentiel, permettant aux langues courantes de communiquer leurs buts, objectifs et d'espérer des résultats pour les parties prenantes. Il est basé sur les référentiels et bonnes pratiques industrielles qu'il intègre :

- ➢ l'alignement stratégique des TI avec les objectifs d'entreprise;
- ➢ le retour sur investissement des services et des nouveaux projets;
- ➢ la gestion des risques;
- ➢ la gestion des ressources;
- ➢ la mesure de la performance.

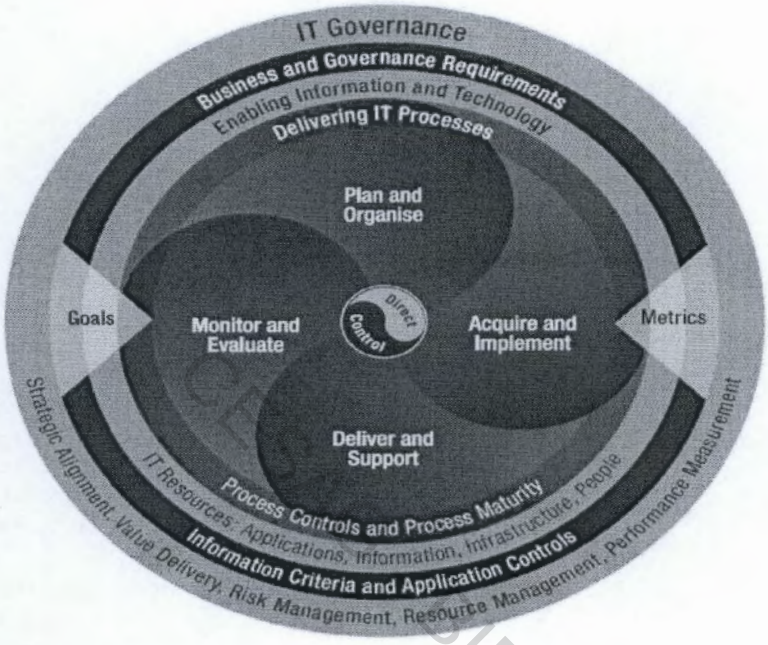
Le COBIT fournit un ensemble de directives pour gouverner les TI au sein de l'entreprise entre autres :

- donner plus d'outils aux TI comme support des objectifs de l'entreprise.
- Plus de transparence et de visibilité sur les coûts relatifs au cycle de vie complet de l'entreprise.
- Plus d'opportunités et d'informations fiables provenant des TI.
- Une haute qualité des services et plus de projets menés à bien.
- Une gestion plus efficace des TI et des risques associés.

Le COBIT permet de répondre aux questions clés des affaires de l'entreprise suivantes : Mes gestionnaires TI font-ils ce qu'il faut? Sommes-nous en train de les faire comme cela se doit ? Les menons-nous à bien ? En profitons-nous?

Le schéma suivant nous donne un une vue globale sur le cadre de référence COBIT.

Figure 3 : Cadre de référence Cobit



Source : ITGI (2007 : 30)

2.3 Le COBIT en détail

COBIT offre un cadre de référence de contrôle structuré des activités informatiques selon trente-quatre (34) processus répartis en quatre domaines :

- le domaine Planifier et Organiser (PO) représente la dimension stratégique de la gouvernance des TI.
- Le domaine Acquérir et Implémenter (AI) rassemble tous les processus qui impactent les ressources, de l'acquisition à l'implémentation : on y trouve aussi bien les projets que la mise en exploitation.
- Le domaine Délivrer et Supporter (DS) est consacré aux services offerts aux clients de la DSI.

- Le domaine Surveiller et Évaluer couvre largement la dimension de contrôle, d'audit et de surveillance de l'ensemble.

La figure 3-1 présente les différents domaines et processus associés.

« Pour chacun des 34 processus, COBIT en décrit le périmètre et l'objet pour ensuite lister et développer :

- **les objectifs de contrôle** destinés aux auditeurs informatiques, qui sont détaillés dans d'autres publications ;
- **un guide de management** inscrit dans une logique de gouvernance des SI ;
- **un modèle de maturité** propre à chaque processus. » (MOSAND& Al., 2009 : 30).

Le COBIT impose des critères de l'information qui sont acceptés à la fois par le manager et l'auditeur. Ce sont : «

- **efficacité** : la mesure par laquelle l'information contribue au résultat des processus métier par rapport aux objectifs fixés ;
- **efficience** : la mesure par laquelle l'information contribue au résultat des processus métier au meilleur coût ;
- **confidentialité** : la mesure par laquelle l'information est protégée des accès non autorisés ;
- **intégrité** : la mesure par laquelle l'information correspond à la réalité de la situation ;
- **disponibilité** : la mesure par laquelle l'information est disponible pour les destinataires en temps voulu ;
- **conformité** : la mesure par laquelle les processus sont en conformité avec les lois, les règlements et les contrats ;
- **fiabilité** : la mesure par laquelle l'information de pilotage est pertinente. »

Le COBIT définit 20 objectifs métiers. Ces objectifs sont tous répartis selon les 4 axes du BSC à savoir : perspective financière, perspective client, perspective interne à la DSI, et perspective future ou anticipation. Ces 20 objectifs métiers renvoient à 28 objectifs informatiques, eux-mêmes liés aux processus COBIT, un même objectif informatique étant associé à un ou plusieurs processus COBIT (voir annexe 6). Ainsi, COBIT offre une

transitivité entre objectifs métier et informatiques, processus et activités. Cette structuration permet d'obtenir une sorte de synthèse de la gouvernance des SI.
Le COBIT décrit chaque processus à travers ses objectifs de contrôle, le guide de management, les activités, les responsabilités et les fonctions dans le COBIT, les objectifs et les indicateurs et le modèle de maturité.

2.3.1 Les objectifs de contrôle

Il s'agit des finalités de mise en œuvre des processus des documents comme le IT Assurance guide : using COBIT, qui déclinent la structure du contrôle à des fins opérationnelles. « Il apparaît clairement que COBIT est un outil opérationnel pour les auditeurs qui y trouveront toute la matière nécessaire pour établir des questionnaires et des grilles d'investigation. » (MOSAND & Al, 2009 : 32).

2.3.2 Le guide du management

Selon MOSAND & Al. (2009 : 32), « la page consacrée au guide de management comprend un descriptif des entrées-sorties du processus, un RACI avec rôles et responsabilités associés aux activités du processus, et enfin, une proposition d'indicateurs de contrôle ».

2.3.3 Les activités

Le COBIT distingue les objectifs de contrôle pour l'auditeur et des activités pour le manager. Cette distinction est bien surprenante dans le sens où la liste des activités reprend certains objectifs de contrôle dans ses intitulés d'une part. Mais il est très intéressant car d'autre part, les activités sont directement extraites de la description des objectifs de contrôle. Tout ceci est fait dans le but de permettre au lecteur du COBIT,

selon qu'il soit auditeur ou manager de se retrouver dans son élément. C'est ainsi que parlant du lecteur MOSAND & Al. (2009 : 32), précise qu'il faut décortiquer chaque objectif de contrôle en tentant d'isoler l'information attachée aux activités, aux instances /organisations, aux fonctions, aux documents / livrables et enfin au contexte pour s'assurer de son adaptabilité.

Pour la mise en œuvre de COBIT, partir des activités est intéressant à condition de ne pas s'y enfermer. Il vaut mieux prendre cette liste comme un « pense-bête » pour donner du corps à une description personnalisée en fonction de l'organisation.

2.3.4 La responsabilité et les fonctions dans le COBIT

Le COBIT distingue au moins 19 fonctions pour la gouvernance des SI. Chacune d'elle peut avoir un ou plusieurs rôles pour chaque activité. Le RACI du COBIT est à titre indicatif et ne saurait être qu'un modèle pour un développement au cas par cas. Exemple de RACI en annexe 1.

2.3.5 Les objectifs et indicateurs

Pour le référentiel COBIT, un processus n'est considéré piloté que quand il existe des indicateurs permettant de s'assurer de l'atteinte des objectifs qui lui sont assignés. Voici un élément qui rassure de la bonne gouvernance car reliant les différents indicateurs de l'activité élémentaire au métier. (MOSAND & Al, 2009 : 33)

2.3.6 Le modèle de maturité

Le modèle de maturité proposé par le COBIT permet d'évaluer la mise en œuvre de chaque processus sur une échelle de 0 à 5. Soit de l'inexistence du processus en passant par son initialisation puis sa reproductibilité vers sa définition pour atteindre sa gestion et en finalité de mise en œuvre son optimisation (Confère annexe 2).

2.3.7 Les documents et publication autour du COBIT

Pour faciliter l'utilisation et la compréhension du COBIT, un certain nombre de documents et de publications ont été faits. Elles sont regroupées dans le schéma en annexe 3

2.4 Gouvernance, sécurisation et contrôle

Les destinations du cobit :

CobiT pour le dialogue entre parties prenantes : le découpage en 34 processus répartis en 4 domaines donne une vision synthétique de la gouvernance TI. En revanche, certains processus peuvent être jugés comme trop globaux, un peu comme des macro-processus. La description détaillée des activités et des objectifs de contrôle donne un niveau de granularité intermédiaire.

CobiT pour le pilotage des systèmes d'information : Dans la mise en œuvre de CobiT, il est conseillé de mener des actions de conduite du changement qui regrouperont les acteurs concernés par un même processus, à l'intérieur comme à l'extérieur de la DSI. Cette démarche a pour effet de préciser à la fois les activités critiques et les

responsabilités associées. Ceci engendre un climat favorable aux bonnes prises de décision visant à accroître l'efficience, optimiser les investissements et éclairer les choix, pour le plus grand bénéfice de l'entreprise.

COBIT pour l'auditeur informatique : le souci d'accompagner au mieux la profession des auditeurs des systèmes d'information (MOSAND & Al., 2009 : 33)

Les limites : ce que COBIT n'est pas

Même si COBIT est à l'origine un référentiel issu du monde du contrôle interne, il n'a pas pour vocation de servir de référentiel de certification selon une approche de conformité à des exigences réglementaires ou contractuelles comme l'ISO 9001, ou d'évaluation de processus comme l'approche CMMI (Capabily Maturity Model Integrate). En revanche, les objectifs de contrôle de COBIT sont largement utilisés pour répondre à des exigences de certification ou de contrôle interne comme SOX, Bâle II.

COBIT ne propose pas de modèle de maturité étagé pour une évaluation de la direction des systèmes d'information. Ainsi, aucun ordre de priorité de mise en œuvre des processus n'est proposé.

COBIT ne propose pas une organisation spécifique liée à la gouvernance des systèmes d'information d'une entreprise comme le proposent les normes de système de management pour la filière qualité.

COBIT ne propose pas non plus un enchaînement des activités propres à modéliser les processus de maîtrise des SI de l'entreprise comme c'est le cas avec ITIL pour la fourniture et le soutien des services.

COBIT ne va pas régler la question de la bonne communication entre la DSI et les parties prenantes.

Enfin, COBIT n'est pas un outil de conduite du changement miraculeux qui diffuserait une culture de la mesure de la performance et de l'amélioration.

En revanche, son déploiement peut aider le management à mener une action de changement simultanément.

2.5 Le COBIT pour l'évaluation (audit/assurance) de la gouvernance des SI

Le référentiel COBIT sert de cadre pour la certification d'une personne physique en matière d'audit, de sécurité ou de gouvernance des systèmes d'information.
COBIT a été et reste le référentiel d'audit de la gouvernance des SI. Son utilisation dans les missions d'audit est quasi immédiate grâce à sa structure de base, aux nombreuses publications qui viennent détailler encore les objectifs de contrôle et aux outils proposés sur le marché pour automatiser les contrôles. Il est mise à jour régulièrement et suffisamment dynamique pour suivre l'évolution technologique (MOSAND & Al., 2009 : 197).

L'audit des SI ou de la gouvernance des SI ne se distingue pas particulièrement des autres audits. En ce sens qu'il se fait dans le cadre d'une mission dont le pic de démarrage est la lettre de mission. La lettre de mission est comparable à un mandat. Elle définit les termes de contrat à savoir la portée de la mission, le périmètre, les responsabilités à attribuer. C'est en suite que l'auditeur doit construire un référentiel d'audit qui établira une transparence totale entre la mission confiée et les investigations à mener.

Le COBIT constitue déjà en soi une base très solide de contrôle auxquelles on peut se référer. Il permet de sélectionner les processus critiques et de les évaluer. Il est parfois nécessaire de le compléter en fonction des spécificités du sujet. « Enfin, COBIT permet à des auditeurs non informaticiens de mener de façon professionnelle des audits informatiques intégrés aux audits généraux.

Les objectifs de contrôle de COBIT constituent une excellente base pour préparer un référentiel d'audit. Il suffit ensuite, au cas par cas, de les étoffer de tests détaillés en fonction de la spécificité du périmètre à auditer (ils sont parfois décrits dans les publications spécialisées publiées par l'ISACA). .» (MOSAND & Al., 2009 : 198).
L'annexe 4 donne une idée du formalisme du référentiel COBIT pour l'audit qui procède par étape et précise des objectifs de contrôle, lesquels sont ensuite détaillés.

La mission d'audit des SI regroupe généralement les trois phases d'audit si bien connues :

- l'étude préliminaire, qui comprend la prise de connaissance de l'entité à contrôler, le dépistage des risques et l'orientation de la mission ;
- la réalisation de l'audit à proprement parler (exécution des travaux de contrôle) ;
- la conclusion de la mission (synthèse, présentation orale et rédaction du rapport).

Les audits traditionnellement ont toujours été classifiés différemment en fonction des critères ou objectifs. Dans le cadre de l'audit des SI les audits peuvent être classées selon : leur profondeur technique, les moyens d'investigation utilisés (intrusion, outillage) ou le périmètre appréhendé.

Somme toute, le COBIT offre à l'auditeur, une classification très solide :

- domaines, processus, objectifs de contrôle ;
- critères d'information (efficacité, efficience, confidentialité, intégrité, disponibilité, conformité et fiabilité) ;
- ressources (applications, infrastructure, information et personnes).

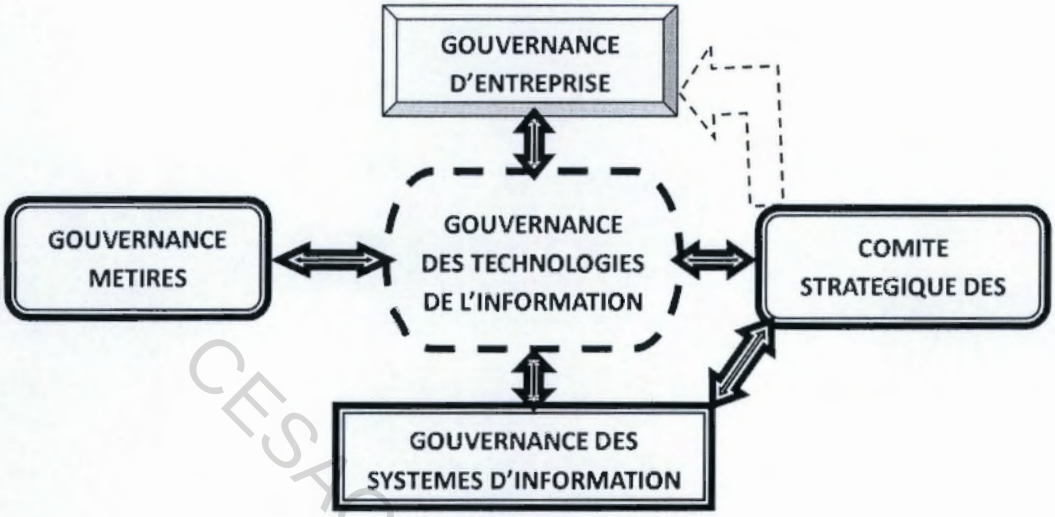
À cette structure se rattache un détail « générique » pour chaque objectif de contrôle, présenté comme suit dans le document *IT Assurance Guide: Using COBIT.*
Cette notion de valeur liée à un objectif de contrôle est tout à fait intéressante puisqu'elle étend le périmètre du contrôle, en incluant non seulement la maîtrise des risques, mais aussi la création de valeur.

Le COBIT étant au niveau de la gouvernance des SI, il phagocyte en totalité ou en partie l'ensemble des référentiels qui traitent de l'information en général et des SI en particulier. Plusieurs institutions et auteurs conviennent que le COBIT est un référentiel fédérateur. Le COBIT lui-même, le guide des certifications des SI, ISACA, ISO, pour ne citer que ceux-là considèrent le COBIT comme un référentiel fédérateur. C'est à ce titre qu'ISACA à produit un certain nombre de mapping entre un certain nombre de référentiel et le COBIT notamment :

- ITIL V3 avec COBIT,
- PCI DSS v2.0 avec COBIT,
- ISO/IEC 20 000 avec COBIT,
- TOGAF avec COBIT,
- SEI's CMM avec COBIT,
- PMBOK avec COBIT,
- ISO/IEC 17799:2005 avec COBIT,
- FFIEC avec COBIT,
- SOX avec COBIT,
- COSO avec COBIT,
- BSC avec COBIT etc.

OTTER & Al. montrent le lien directe entre le COBIT et chacun des référentiels qu'il énonce dans son édition de 2009.

Figure 4: place de la gouvernance des TI et des SI dans une organisation



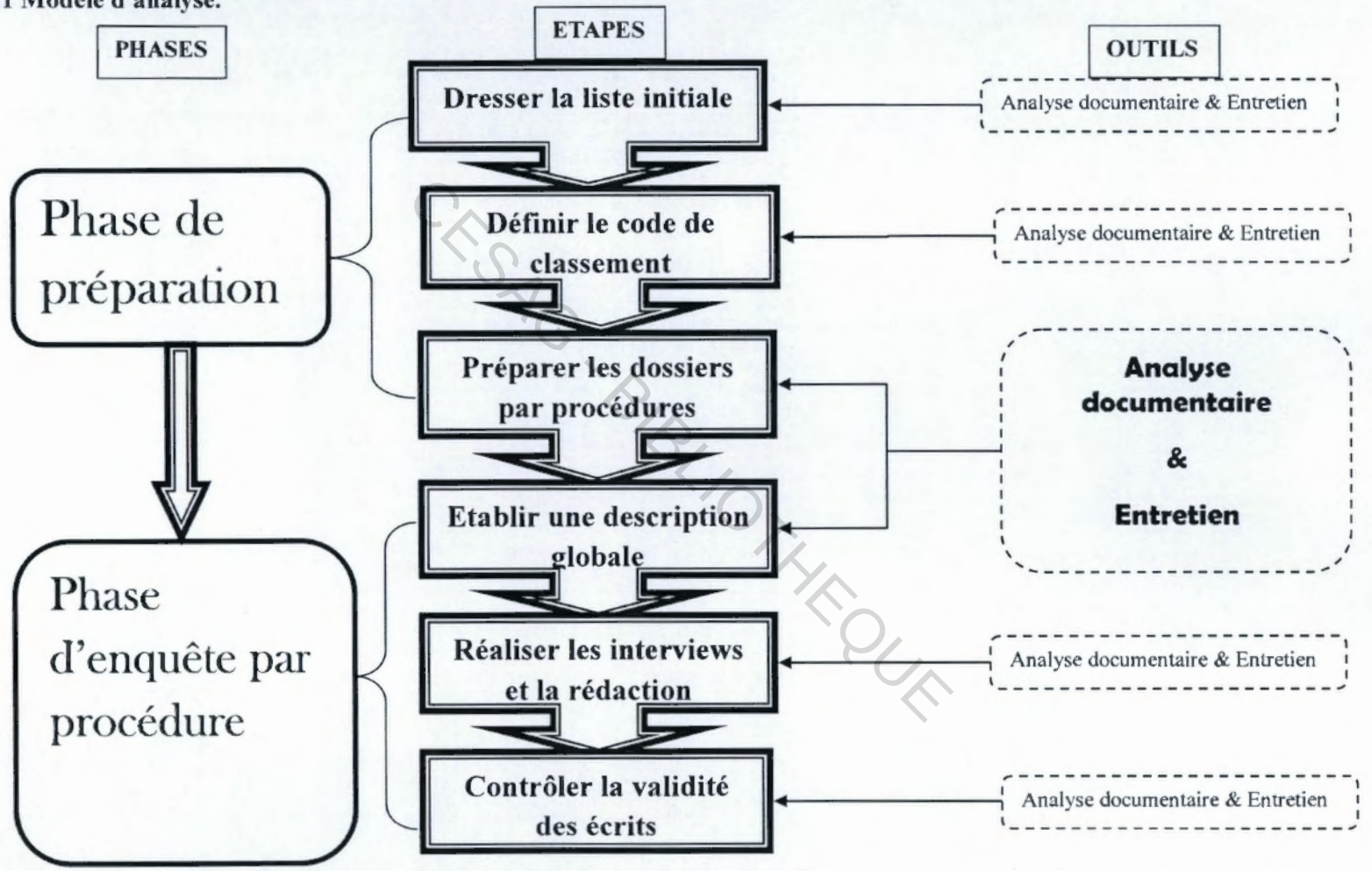
Source : nous-même à partir de MOSAND & Al. (2009 : 3 - 46), OTTER Al. (2009 :119), CHALLAND & Al. (2009 : 5 - 41) et ISACA (2011 : 75 - 102)

Le comité d'élaboration et d'amélioration du COBIT travaille dans une ligne de fédération de toutes les normes sur les SI existantes. C'est dans cette politique que le COBIT dans sa version 5 intègre le Val IT et le Risk-IT pour ne citer que ces deux.

CHAPITRE III : METHODOLOGIE DE LA RECHERCHE

Le chapitre de méthodologie de la recherche à travers le modèle d'analyse et les techniques de collectes de données constitue le plan et la démarche du travail à mener sur le terrain. Il est une vision objective et doit être adapté aux types d'informations et des recherches à mener.

3.1 Modèle d'analyse.



Source : nous-même

3.2 Techniques de collecte de données

Les techniques de collecte de données assorties à notre recherche sont l'analyse documentaire et l'entretien. La conception du manuel de procédures conformément au référentiel, exige une analyse complète du référentiel en question et des autres documents qui en parlent dans l'optique de le critiquer ou de le décrire par explication. C'est aussi une Opération intellectuelle visant à identifier les informations contenues dans un document ou un ensemble de documents et à les exprimer sans interprétation ni critique, sous une forme concise et précise telle qu'un résultat d'indexation, un résumé, un extrait. Le but en est de permettre la mémorisation, le repérage, la diffusion ultérieure des informations ou du document source.

Cependant, ils existent plusieurs techniques de collecte de données. On peut énumérer notamment :

Tableau 3 : tableau comparatif de quelques techniques de collecte de données

Techniques de collecte de données	Caractéristiques	Avantages	Limites
Entretien non structuré (style conversation)	Les questions se présentent dans le contexte immédiat et sont posées naturellement ; il n'y a pas de définition au préalable des questions ou de la formulation des questions.	Rendent les questions plus pertinentes ; les questions correspondent aux individus et aux circonstances. Permettent d'explorer des nouveaux thèmes.	Des informations différentes sont collectées auprès des différentes personnes à l'aide des questions différentes. Moins systématiques et eomplètes. L'organisation et l'analyse des données peuvent être difficiles.
Entretiens semi-structurés (avec guide d'entretien)	Les thèmes couverts sont spécifiés à l'avance mais l'investigateur décide de la séquence et de la formulation des questions pendant l'entretien.	Plus systématiques et complètes mais les entretiens restent encore du style conversation.	Des thèmes importants peuvent être omis par inadvertance. La souplesse de la séquence et de la formulation des questions engendre des réponses différentes à partir des perspectives différentes, diminuant ainsi le caractère

			comparable.
Entretiens ouverts standardisés	La formulation et la séquence exacte des questions sont déterminées à l'avance. Les questions sont formulées de sorte que les réponses soient entièrement ouvertes.	Permettent de mieux comparer les réponses ; données complètes pour chaque participant; facilitent l'organisation et l'analyse des données. Appropriés lorsque le thème de l'étude est relativement bien connu.	Peu de souplesse pour mettre en relation l'entretien avec les individus et les circonstances ; la formulation standard des questions limite le caractère naturel et la pertinence des questions et des réponses.
Listes libres	Demandent aux participants de nommer tous les éléments d'un domaine défini par le participant.	Première étape utile à toute recherche cherchant à définir de nouveaux domaines. Permettent de vérifier la pertinence de nouveaux concepts.	Difficultés possibles pour trouver de termes génériques permettant de démarrer le processus de la liste. Parfois, il n'existe pas assez d'éléments dans les listes.
Echelle de notation	Les participants doivent noter les éléments un par un en fonction d'une échelle déterminée à l'avance pouvant être graphique ou numérique.	Les échelles peuvent être créées pour n'importe quel nombre de concepts ou de caractéristiques. Elles sont faciles à administrer.	Demande des participants alphabétisés ou des éléments visuels. Sensibles aux biais des réponses.
Focus Groups	Techniques d'entretien de groupe semi-structuré qui repose sur la discussion entre participants	Peuvent fournir rapidement une grande quantité d'informations. Méthodes utiles pour identifier et explorer les croyances, les attitudes et les comportements et pour identifier des questions pertinentes pour des entretiens individuels.	N'apporte pas d'informations sur la fréquence ou la distribution des croyances ou des comportements. Sont difficiles à réaliser, demandent des modérateurs compétant. Les participants peuvent s'influencer mutuellement et, par conséquent il faut faire attention en analysant les résultats.
Techniques d'entretien de groupe (non focus groups)	Technique d'entretien plus formelle qui tend à utiliser des groupes naturels préexistants. Parfois, on demande aux membres du groupe de travailler ensemble pour faire une tâche, par exemple une carte communautaire. Le but est d'engager	Permettent de créer le rapport, d'identifier et d'explorer les problèmes et priorités communautaires, de sensibiliser aux problèmes locaux, de faire participer les gens à l'identification des solutions possibles. Amusantes et intéressante	Moins systématiques que les discussions ciblées, par conséquents, les comparaisons entre les groupes sont plus difficiles et demandent une préparation mais peuvent se réaliser avec des modérateurs moins qualifiés. La reconnaissance des problèmes peut mener à des attentes plus

	activement la communauté à l'identification et à l'étude des thèmes.	pour les participants.	élevées. Les chercheurs doivent faire attention à ne pas créer des attentes qui ne pourront pas être satisfaites.
Observations participantes	N'est pas à proprement parler une technique de collecte de données, mais plutôt une approche qui permet aux chercheurs de devenir un membre actif de la culture étudiée. Comprend l'observation non structurée et l'entretien non structuré.	Facilite toutes les autres activités de collecte de données car créé le contact et diminue la réactivité. Aide à formuler des questions pertinentes. Permet de comprendre les processus, les événements et les relations dans leur contexte social.	Peut prendre beaucoup de temps, demande aux chercheurs de très bien parler la langue locale et d'être un bon observateur et rapporteur.
Observation non structurée	L'observateur est « dehors », non participant. Ce qui est observé est défini en termes généraux. Vise à observer le comportement dans un contexte global.	Permet de découvrir les aspects inconnus d'un problème. Permet la découverte de « nouveautés ». Permet de comprendre des comportements dans leur contexte physique et social.	Ne fournit pas de mesures précises du comportement et ne peut donc pas être utilisée pour suivre les changements du comportement.
Observation structurée	Le chercheur est en « dehors », non participant. Observe et fait le compte rendu de manière prédéterminée.	Dégage des données précises et numériques se prêtant à l'analyse statistique et peut être répétée pour suivre le changement de comportement dans le temps.	Le problème devant être étudié doit être bien défini. La formation des observateurs est intense et prend du temps. La structure prédéterminée des observations limite la découverte d'autres comportements pertinents.

Source : nous-même

3.2.1 Analyse documentaire

L'analyse documentaire est le traitement intellectuel du document : il sert à décrire et à caractériser le contenu d'un document. Il s'agit de répondre à la question "De quoi traite ce document ?" en :

1. repérant dans le document les éléments d'information essentiels; ceux pour lesquels ce document pourra être recherché par des lecteurs),
2. les "traduisant", sous une forme concise et précise, en données conventionnelles : mots clés (indexation), code de classement (classification) ou résumé.

Il est nécessaire pour cela :

- d'appréhender le contenu total du document,
- de bien maîtriser le sujet du document ou avoir recours à des dictionnaires, ou à des personnes-ressources (auteur ou spécialiste),
- de recourir à des outils de "cadrage" de la traduction, pour éviter les problèmes inhérents au langage naturel (polysémie, synonymie, mots de la même famille, masculin/féminin, singulier/pluriel,...),
- de se relire et contrôler régulièrement les champs de l'analyse documentaire.

Son objectif est de comprendre l'évolution historique et les résultats d'un projet/d'une organisation en se référant à sa documentation, qu'elle soit présentée sous forme écrite, électronique, photographique ou vidéo. Du point de vue du suivi-évaluation, cette méthode peut fournir des renseignements de référence sur une zone ou un indicateur donné. Elle peut également vous donner une bonne perspective historique des activités mises en œuvre aujourd'hui pour savoir si des changements ont eu lieu ou non, et pourquoi.

Comment procéder:

1. Définissez clairement les questions auxquelles vous souhaitez obtenir des réponses et les renseignements (ou type d'information) qu'il vous faut obtenir à cette fin. Par exemple, "Quels types d'activités génératrices de revenus ont été mises en place?"

2. Énumérez toutes les sources possibles d'information existantes (documentation du projet, registres de l'État, rapports d'organisations ou archives, études universitaires, etc.).

3. Classez par ordre de priorité celles qui sont à même de vous fournir des renseignements utiles le plus rapidement et au moindre coût. C'est là un point important, en particulier lorsque la documentation disponible est volumineuse. Dans de tels cas, n'essayez pas de tout lire - concentrez-vous sur les points principaux.

4. Rassemblez cette documentation et vérifiez en la fiabilité. Notez les renseignements contradictoires. Analysez-les par rapport à la question à laquelle vous tentez d'obtenir une réponse.

5. Recensez les lacunes dans l'information recueillie ou les points sur lesquels des renseignements contradictoires appellent une clarification. Sélectionnez une autre méthode de collecte de l'information, par exemple les questionnaires (méthode 'Questionnaires et enquêtes') ou les interviews (méthode 'Entretiens semi-structurés'), pour combler ces lacunes.

Toutefois, vous serez limité par la disponibilité et l'accessibilité de la documentation, par la manière dont elle est présentée, par sa source (possibilité de subjectivité, etc.), par la façon dont elle a été entreposée et par toutes les questions se rapportant à la qualité qui découlent de ces restrictions. Cette méthode peut permettre d'évaluer le système interne de collecte et de stockage de l'information sur les projets d'une organisation ou d'un ministère.

3.2.2 Les entretiens

Loin d'être un entretien d'embauche, l'entretien dans le cadre de notre travail s'inscrit dans le type narratif. Nous allons ainsi rencontrer des personnes ressources dans les domaines de l'audit des systèmes d'information, management des systèmes d'information, et sécurité des systèmes d'information. Ces interviews nous permettrons d'avoir de l'information très pointue et pertinente sur le processus de gouvernance des SI d'une part, d'autre part la sécurité des SI et enfin sur l'audit des SI. À cet effet, un auditeur des SI titulaire des certifications suivantes sera notre mentor pour ce travail: CISA (Certified in Information System Auditors), CISM (Certified in Information System Management), CISSP (Certified in Information System Security), pour ne citer que ceux-là. Il a pour charge la direction des missions d'audit informatique de la banque mondiale.

Notre tâche sera de regrouper les connaissances théoriques acquises lors de l'analyse documentaire et ceux provenant de plusieurs années d'expériences pratiques.

Les trois chapitres sus étudiés, nous fournissent un cadre de connaissance très large, mais à la fois pointue pour comprendre la sphère de notre thème. Ainsi équipé, nous sommes en mesure de nous avancer vers la rédaction des procédures proprement dites, en passant par une présentation du cabinet qui nous a permis de mettre en pratique notre thème. Cette partie nous a permis en outre, d'appréhender la notion de gouvernance des SI en particulier et plus généralement celle de la gouvernance d'entreprise d'une part. D'autre part, le lien entre un manuel de procédures et un référentiel. Et enfin l'évaluation ou l'audit de la gouvernance des SI.

DEUXIEME PARTIE : CADRE PRATIQUE

Cette partie nous permet de concevoir le manuel d'évaluation de la gouvernance des systèmes d'information. Il articule trois chapitres à savoir la présenter de l'entreprise, les procédures d'évaluation et le diagnostic de la gouvernance des SI. Le cabinet CECA ne pratique pas l'audit des SI et en conséquence ne dispose pas de procédures à cet effet. Nous concevrons directement les procédures d'évaluation de la gouvernance des systèmes d'information et pratiquerons un diagnostic de la gouvernance selon le COBIT dans cette partie.

Le chapitre cinquième met en œuvre les procédures d'évaluation ou d'audit dans un environnement automatisé. Quant au chapitre six, il fait ressortir selon l'approche par les risques les recommandations prodiguées par le COBIT aux DSI et aux auditeurs des SI.

CHAPITRE IV : PRESENTATION DE L'ENTITE ET DE L'EXISTANT

Nous présentons dans ce chapitre l'organisation qui a fait l'objet de notre attention et stimulé pour la rédaction dudit manuel.

Il existe uniquement des ressources humaines compétentes dans d'autres domaines autres que ceux des TI. Il n'existe pas dans le cabinet CECA de manuel de procédure d'évaluation de la gouvernance des SI jusqu'à ce jour. Nous n'avons donc pas à faire une étude de l'existant en termes de procédures d'évaluation de la gouvernance des Technologie de l'Information mais nous passerons directement à la présentation du cabinet CECA.

4.1 Présentation de l'entité

CECA Sarl Expertise comptable, est un cabinet qui se veut être une référence en expertise. Le Cabinet d'Expertise Comptable, de Conseils et d'audit (en abrégé CECA-Sarl) est une société créée le 01 juin 2006 avec un capital social de FCFA 1 000 000. C'est une équipe de jeunes diplômés, qui ont su satisfaire leur clientèle avec les solutions adéquatement fournies. En tant que société à responsabilité limitée, l'associé majoritaire au nom de Monsieur Abou WELE est inscrit au Tableau de l'Ordre Nationale des Experts Comptables et Comptables Agréés du Sénégal (ONECCA) depuis le 25 Novembre 1999 et à partir de 2008, CECA-Sarl figure parmi les Sociétés d'Expertise Comptable.

Cette inscription au tableau de l'ordre donne au cabinet CECA la qualité d'être nommée commissaire aux comptes principale ou suppléant par les structures dont la loi en fait obligation (SA, Sarl (selon le cas), SFD (Système Financier Décentralisé), Coopératives agricoles, Fondations d'unité publique).

Face à la complexité croissante de l'environnement économique, le cabinet s'est assigné les objectifs suivants:

– répondre aux besoins de ces clients en leurs fournissant, en toute indépendance, un travail de grande qualité:

– accompagner les clients dans le renforcement de leurs aptitudes à:

– produire des informations comptables et financières crédibles;

– fiabiliser leur processus de gestion à travers l'élaboration de manuel de procédures administratives, financières et comptables et la confection d'outils ou de supports de gestion;

– générer les bénéfices.

L'expérience pratique acquise par l'Expert comptable associé et le personnel du cabinet dans les domaines variés de la gestion administrative, comptable et financière permet à CECA-Sarl d'intervenir sur une fourchette d'activités particulièrement large.

Ses interventions sont réalisées par la mise en œuvre des techniques les plus avancées acquises à travers de multiples missions d'assistance comptable, d'audits et de conseils effectués par l'Expert Associé et ses collaborateurs au cours des 16 dernières années. Ainsi, CECA fournit à sa clientèle des prestations pouvant être regroupées en quatre (4) domaines principaux:

- audit et certification des comptes;
- assistance comptable;
- assistance et gestion des contentieux fiscaux;
- organisation et conseil.

Les secteurs d'activités économiques couverts par ses prestations sont:

– entreprises et sociétés commerciales;

– systèmes financiers décentralisés (SDF);

– organisation à but non lucratif (associations, ONG, Fondations, Projets ;

– Collectivités locales.

4.2 Étude de l'existant

Le cabinet dispose suffisamment de ressources humaines de très haut niveau. En effet, le personnel de CECA est constitué de professionnels recrutés à des niveaux d'études supérieures en gestion, finance ou audit. Il s'agit des masters professionnels (niveau 1&2), DESS (diplôme d'études supérieures spécialisées), DESCAE (diplôme d'études supérieures de commerce et d'administration des entreprises) et DSC (diplôme d'études supérieures comptable), etc.

Le personnel est recruté suivant des critères bien précis. Le niveau d'étude (diplômes obtenus), compétence, honnêteté et rigueur professionnelle, assiduité, indépendance de jugement, capacité à prendre des initiatives.

En plus des centaines de mission d'audit et de conseils dans les institutions de micro finance, le cabinet a exécuté en 2007 la mission d'élaboration du plan comptable spécifique à la micro finance en Mauritanie en consortium avec le cabinet mauritanien AFACOR confié par le PNUD à la suite d'un appel d'offre international. Cette mission s'est soldée par l'élaboration d'un cadre conceptuel, d'un plan de comptes, un guide d'utilisation des comptes et les modes de présentation des états financiers et des états annexés, annuels et périodiques pour les trois catégories d'IMF (IMF A, B et C. le cabinet a audit plusieurs projets et autres organisations sans but lucratif.

Malgré cette étoffe qualitative de compétence, le cabinet CECA n'est pas en mesure de pratiquer l'évaluation de la gouvernance des SI. Dans un premier temps par un manque de ressources humaines qualifiées à cet effet. Il ne dispose pas non plus de procédures pour lui permettre l'évaluation minimum pour assurer la fiabilité de gouvernance des systèmes d'information de ses clients. De ce fait, ses opinons peuvent être biaisées à causes de failles liés aux technologies de l'information. Nous nous portons à son aide pour lui assurer ce minimum d'évaluation de la gouvernance des TI.

Le manuel proposé à travers les grandes phases d'audit en dehors de l'aspect propre au système d'information est regroupe l'existant non structuré par le cabinet CECA.

Ce manuel qui sera conçu, dans ce mémoire sera également utilisable par des structures tout comme CECA qui souhaite éviter, détecter ou corriger les risques d'audit liés à la non fiabilité des

systèmes d'informations. Dans le chapitre 5, les procédures d'évaluation de la gouvernance des SI sont décrites avec les tâches qui les composent. Le dernier chapitre montre la mise en œuvre d'une gouvernance des systèmes d'information.

Cependant, il est à constater que les grandes lignes ou phases d'audit apparaissent dans la mise en œuvre de l'audit comptable et financier réalisés par le cabinet CECA.

CHAPIITRE V : PROCEDURE D'EVALUATION DE LA GOUVERNANCE DES SI BASE SUR LE COBIT

Nous présenterons les procédures d'évaluation conformément aux différentes phases d'une mission d'audit ou d'assurance. Il est évident que la mission en elle-même ne commence que dès l'instant que la lettre de mission existe et validée.

Pratiquement on peut distinguer quatre (4) phases si nous n'excluons pas celle qui prépare la mission. Les trois (3) phases d'une mission d'audit ou d'évaluation sont la planification, l'exécution et la finalisation. Nous noterons alors trois (3) procédures à savoir, celui de la préparation de la mission, l'exécution et la finalisation.

L'objectif de la conception d'un manuel de procédure d'évaluation de la gouvernance des SI, est de s'assurer que la haute direction s'acquitte de son rôle prépondérant dans la gouvernance des SI. Ce rôle devrait permettre d'atteindre l'alignement stratégique, la mesure de la performance, la gestion du risque, la gestion des ressources, la valorisation des SI.

De façon spécifique, ce manuel de procédures devrait permettre de se rendre compte si la haute direction met en œuvre les diligences qu'il faut afin de maitriser le changement, d'assurer la sécurité et la maintenance des ressources, de suivre les modifications et configurations (normales comme d'urgence), la vue des SI comme soutien métier, de vérifier le niveau de service, de contrôler les contrats avec les tiers, etc.

L'inexistence de procédures d'évaluation de la gouvernance des SI est très frappante malgré le niveau d'avancée technologique atteint. Les entreprises surtout africaines, ont suivi la croissance technologique sans penser à prendre en compte les bonnes pratiques qui les accompagnent.

Nous allons procéder immédiatement à l'élaboration du nouveau manuel de procédures.

CECA Cabinet d'expertise Comptable et d'Audit	MANUEL DE PROCEDURES D'EVALUATION DE LA GOUVERNANCE DES SI
P. Audit des Systèmes d'Information	P – SOMMAIRE
P.1 Préparation de la mission P.1.1 Prise de connaissance globale P.1.2 Orientation et planification P.2 Exécution de la mission P.3 Finalisation de la mission	

Source : nous-même

5.1 La préparation de la mission

Elle regroupe l'ensemble des dispositions et analyses à mettre en œuvre pour s'assurer de l'acceptation de la mission. Pour respecter les trois phases, elle inclut souvent la planification. Dans ce cas, elle se résume : à la prise de connaissance de l'entité à contrôler, au dépistage des risques et à l'orientation de la mission.

La procédure de préparation de la mission se subdivise en deux celle de l'acceptation du mandat, d'orientation et planification. C'est à cette phase que se fait la définition du périmètre d'audit (choix des processus qui s'associeront au processus de gouvernance des systèmes d'information) et de la portée de la mission.

CECA	Procédure	P.1 Préparation de la mission		Mise à jour
	Sous procédures	P.1 Prise de connaissance globale		
	Fonction	Audit / assurance		Folio :
Réf. Tâche	Description	Fait par	Délai	Matérialisé par
P.1.1	Acceptation et continuation de la mission:	Le chef de mission		Simple notification de la mission
	Le commis doit s'assurer de l': -acquérir une compréhension de la mission : il s'agit de pourvoir estimer la portée de la mission en fonction du système d'information en place. - Fournir une indépendance entre les activités qu'il propose à la société et la compétence dans le cadre de la mission: il est question de pouvoir se prononcer sur la compatibilité des prestations à offrir à l'entreprise. - Identifier les risques inhérents à la mission: ceci revient à identifier les risques inhérents liés aux individus, au système et à l'environnement. - Élaborer une lettre de mission signée	Le chef de mission		Lettre de mission

– Acquérir une compréhension de la mission, c'est aussi la compréhension des objectifs et des processus de l'organisation, ce qui inclut l'information et les exigences de traitement, comme la disponibilité, l'intégrité, la sécurité, et les technologies d'affaires, ainsi que la confidentialité des renseignements.

– Fournir une indépendance entre les activités qu'il propose à la société et la compétence dans le cadre de la mission: dans le cadre de l'audit, l'auditeur doit recevoir et évaluer les travaux d'autres experts, tirer ses conclusions sur la fiabilité de leurs résultats et décider de leur utilisation.

– Identifier les risques inhérents à la mission: il s'agit des risques inhérents aux techniques, aux ressources humaines, à l'environnement à exploiter pour la mission et des risques généraux du secteur d'évolution de l'entité.

– élaborer la lettre de mission : elle doit faire mention des sections d'objectif, de responsabilité, du pouvoir, de l'obligation de rendre compte, et surtout la portée. La lettre de mission doit être avalisée au niveau approprié au sein de l'entreprise concernée. La lettre de mission d'audit de la gouvernance des SI comme tout audit contient essentiellement les éléments suivants:

- l'identité des parties ;
- la présentation globale de la mission ;
- la nature et l'étendue des interventions que l'auditeur entend mener conformément aux normes d'exercice professionnel ;
- la façon dont seront portées à la connaissance des organes dirigeants les conclusions issues de ses interventions ;
- les dispositions relatives aux signataires, aux intervenants et au calendrier ;
- la nécessité de l'accès sans restriction à tout document comptable, pièce justificative ou autre information demandée dans le cadre de ses interventions ;
- le rappel des informations et documents que la personne ou l'entité doit lui communiquer ou mettre à sa disposition ;

- le souhait de recevoir une confirmation écrite des organes dirigeants de la personne ou de l'entité pour ce qui concerne les déclarations faites à l'auditeur en lien avec sa mission ;
- le budget d'honoraires et les conditions de facturation;
- des clauses diverses : possibilité de réalisation du contrat, clauses de responsabilité, extension possible de la mission (notamment dans le cadre d'un audit contractuel), exercice du secret professionnel…

CECA	Procédure	Préparation de la mission		Mise à jour
	Sous procédures	Orientation et planification		
	Fonction	Audit / assurance		Folio
Réf. Tâche	Description	Fait par	Délai	Matérialisé par
P.1.2	Orientation et planification			
	obtention d'une lettre de mission signée	Le chef de mission		Lettre de mission signée
	Mobiliser l'équipe d'audit : le choix des membres de l'équipe doit être fait de façon minutieuse en prenant en compte les compétences et les risques inhérents aux individus	Le chef de mission		Constitution d'une équipe compétente
	Connaissance du client et de son environnement; L'auditeur doit prendre connaissance :	Le chef de mission		Connaissance globale de

	– du secteur d'activité de l'entité, de son environnement réglementaire, notamment du référentiel de gouvernance des SI et d'autres facteurs externes tels que les conditions économiques générales ; – des caractéristiques de l'entité qui lui permettent d'appréhender les types de technologies, les informations qu'ils doivent véhiculer à travers le système d'information. Ces caractéristiques incluent notamment la nature de ses activités, la composition de son capital et de son gouvernement d'entreprise, sa politique d'investissement dans le technologie de l'information, son organisation de la gouvernance des TI ; – des objectifs de l'entité et des stratégies des TI mises en œuvre pour les atteindre dans la mesure où ces objectifs pourront avoir des conséquences financières et de ce fait une incidence sur la continuité de l'exploitation;			l'entité à audité
	Cartographie des risques inhérents: il s'agit de faire un regroupement des risques possibles conformément à cet environnement, en les identifiants.	Équipe déléguée (peut être une personne)		Carte de risque
	Évaluation de la structure de contrôle interne: ici c'est la confrontation des risques et des dispositifs de	Équipe désignée		Élaboration des tests de

	contrôles prévus.			corroboration
	Évaluation du risque de fraude: c'est l'identification et la valorisation du risque de commission d'actes illégales.	Équipe désignée		Prévision des investigations
	Concepts d'importance relative pour l'audit des SI : l'évaluation du risque en termes d'importance significative est d'autant plus importante qu'il est difficile de définir dans un contexte technologique très mouvant. Il faut ainsi trouver des éléments pertinents qui permettent d'évaluer le risque encouru. C'est à cet effet que l'ISACA a fait concevoir et publié le Val-IT.	Le chef de mission en collaboration avec des spécialistes métiers		Seuil de signification et niveau d'acceptation
	concevoir l'approche d'audit ou stratégie d'audit: l'approche imposée par le COBIT est celle par les risques mais basée sur chacun des 34 processus COBIT.	Le chef de mission		
	Constitution et briefing des équipes: ici il est question de répartir les équipes en fonction des cycles d'audit et en fixant les objectifs.	Le chef de mission		
	Concevoir le programme de travail	Le chef de mission supervise les équipes		Programme de travail

	Faire valider le programme de travail du point de vue des objectifs de contrôle et de leurs portées.	Le chef de mission		Programme de travail validé par l'audité
	Préparation des documents de travail (workpapers) : les tests de conformité et tests de corroboration.	Les équipes		Document de travail

L'orientation et la planification de la mission se fait à travers les différentes étapes qui suivent :

➢ Obtention d'une lettre de mission signée: la réception de la lettre de mission favorable, lance le démarrage de la mission à savoir la phase de planification.

➢ Mobiliser l'équipe d'audit : il s'agit de l'équipe qui fera la planification et coordonnée par le chef de mission ou le chargé de la planification.

➢ Connaissance du client et de son environnement : c'est la revue analytique qui permet de déterminer les contenus stipulés tels que les politiques, les normes, les directives requises, les procédures et la structure organisationnelle. On l'appelle aussi, prise de connaissance de l'entité et du contrôle interne. La prise de connaissance de l'entité par l'auditeur sera plus ou moins approfondie selon la mission qui lui est dévolue (audit, examen limité, opération contractuellement définie) et le niveau du risque estimé.

La prise de connaissance permet à l'entité de mieux comprendre les événements pouvant avoir une incidence significative sur les comptes, et de tenir compte de ces éléments dans la planification de sa mission. La prise de connaissance permettra à l'auditeur d'orienter sa mission et d'appréhender les domaines et systèmes significatifs.

➢ Cartographie des risques inhérents : elle nous aidera dans la conception du plan d'audit et aussi à démarrer l'approche par les risques préconisée par ISACA. La cartographie touchera entre autres : les risques produits, les risques financier, les risques de gouvernance, les risques liés à la performance passée, les risques d'éthique et d'intégrité, les risques de comptabilité et de contrôle, les risques de continuité d'exploitation, les risques problèmes d'audit, les risques technologique etc.

➢ Évaluation de la structure de contrôle interne: procéder à l'évaluation du contrôle interne grâce aux travaux d'experts antérieurs et la cartographie des risques pour identifier les faiblesses et les forces du contrôle interne.

➢ Évaluation du risque de fraude : c'est le niveau de visibilité de la vulnérabilité qui pourrait pousser à la fraude.

➢ La matrice de confort d'audit permet de confronter les forces et faiblesses du contrôle interne d'après la norme ISA 320.

➢ Concepts d'importance relative pour l'audit des SI : il s'agit ici de considérer l'importance relative (seuil de signification), la tolérance aux risques d'audit tout en déterminant la nature, la durée et la portée des procédures d'audit. De ce fait on devra tenir compte des faiblesses, l'absence de mesures de contrôle puisse provoquer un manque appréciable dans le système d'information. L'auditeur doit prendre en compte l'effet cumulatif de déficiences mineures du contrôle ou de faiblesses et d'une absence de contrôle pouvant se traduire en déficience importante ou en faiblesse matérielle du système d'information.

➢ l'approche d'audit : toute mission doit être conduite suivant une approche. Celle retenue par le COBIT et ISACA est l'approche par les risques. Elle sert dans la conception du programme de travail. Le COBIT et ISACA proposent pour cette approche une cartographie des risques pour chaque sous processus et des objectifs de contrôle qui les maitrisent.

➢ Constitution et briefing des équipes: elle doit être faite de telle sorte qu'elle puisse battre en qualification et en compétence les équipes d'experts précédant. Cette équipe doit être repartie sur les tâches de la mission.

➢ Le programme de travail définit la nature et l'étendue des diligences estimées nécessaires, au cours de l'exercice, à la mise en œuvre du plan de mission, compte tenu des prescriptions légales et des normes d'exercice professionnel ; il indique le nombre d'heures de travail affectées à l'accomplissement de ces diligences et les honoraires correspondants.

Il a pour but de :

- fixer le contenu des interventions ;
- négocier les tâches entre collaborateurs et fixer le temps pour chacun d'eux ;
- coordonner le planning de la mission et le plan de charge du cabinet ;
- répartir les interventions dans le temps de manière à respecter les délais.

L'élaboration du programme de travail comprend :

- une première étape de « planification générale » des interventions à venir. Cette étape permet de définir la mission dans ses grandes lignes et doit aboutir à l'élaboration de quatre supports distincts :
  - la fiche d'orientation générale des travaux ;
  - l'échéancier ;
  - la fiche de planification générale ;
  - le (ou les) planning(s).
- plusieurs étapes d'établissement des programmes correspondant à chacune des phases techniques d'exécution de la mission, essentiellement :
  - programme d'appréciation du contrôle interne ;
  - programme d'observations physiques ;
  - programme de confirmations directes ;
  - programme de contrôle des documents ;
  - programme de contrôle des comptes ;
  - etc.

➢ Faire valider le programme de travail du point de vue des objectifs de contrôle et de leurs portées : la validation du programme de travail est le contrat qui prouve que l'entreprise est d'accord avec les objectifs retenus et les portées de la mission. Il marque en principe le début de l'exécution de la mission.

➢ Préparation des documents de travail (workpapers) : ils permettent l'établissement préalable des tests (conformité et corroborations)

5.2 Exécution de la mission

L'exécution de la mission se passe sur le terrain, soit au sein de l'entreprise. Elle commence par une appréciation du contrôle interne et ensuite l'assurance. C'est au cours de cette étape que se réalisent toutes les tâches planifiées. Elle aboutit à des constats qui donneront lieu à des analyses puis l'émission d'opinions.

CECA	Procédure	Exécution de la mission		Mise à jour
	Sous procédures	Appréciation du contrôle interne		
	Fonction	Audit / assurance		Folio
Réf. Tâche	Description	Fait par	Délai	Matérialisé par
	Recensement des dispositifs pour résorber les risques: c'est l'étape préalable au diagnostic du contrôle interne.	Équipe déléguée		Carte des dispositifs de contrôle existants
	Diagnostic du contrôle interne: il permet de vérifier l'existence réelle et la mise en œuvre des dispositifs grâce aux tests de conformité prévus.	Équipes déléguées		Identification des forces et faiblesses du système
	Confirmation et précision de la portée des tests de corroboration après les tests de conformité.	Le chef de mission et les équipes déléguées		Amélioration des tests de corroboration
	Tests de corroboration : on prévoit les tests de corroboration en fonction de la portée validée. Ici on exploite les documents nécessaires à ces tests (documents préalablement indiqués dans la phase de planification sauf cas de force majeur pour des investigations).	Équipes déléguées		Mise en œuvre des tests de corroboration.

	Analyse des résultats des tests: sur chaque feuille de travail on se prononce sur les résultats obtenus	Équipes déléguées		Workpapers parafé et numéroté
	Mise en commun des documents de travail: elle se fait lors de la synthèse des activités de contrôles.	Toutes les équipes et superviser par le chef de mission		Constitution du document d'audit

Procédures d'exécution (suite)

CECA	Procédure	Exécution de la mission		Mise à jour
	Sous procédures			
	Fonction	Audit / assurance		Folio
Réf. Tâche	Description	Fait par	Délai	Matérialisé par
	Réunion d'ouverture: elle se tient au sein de l'entité à auditer. Elle a pour rôle de préciser aux audités le but et les objectifs de la mission. La réussite facilite l'exécution de la mission.	Le chef de mission		L'exécution des travaux sur le terrain
	Concertation de l'équipe pour démarrer le travail. Elle sert à faire les derniers réglages au niveau des équipes et de s'assurer de l'indépendance des membres de l'équipe par rapport aux audités.	Chefs d'équipes		Répartition des tâches au sein des équipes

	Tests de conformité : on procède aux tests de vérification de la mise en œuvre des bonnes pratiques en termes de gouvernance des SI préconisés par le COBIT.	Équipes déléguées		Résultat des tests de conformité sur leur workpaper
	Tests de corroborations: après les tests de conformité, on va approfondir avec des tests de corroboration les points forts apparents présentant des risques de criticités élevés.	Équipes déléguées		Résultat des tests de corroboration sur leur workpaper
	Analyse des résultats et opinion: sur chaque feuille de travail on se prononce sur les résultats obtenus après analyse.	Les exécutants de tests		Expression d'opinion sur les workpapers
	Recoupement des workpapers : cette séance voit la mise en commun des travaux par équipe et leur validation.	Les équipes		Document de travail par équipe
	Investigation si nécessaire: après la validation on procède aux investigations pour les niveaux même les tests de corroboration non pas été fructueuses et présentant toujours des risques très significatifs.	Équipes compétentes déléguées		Résultat des investigations
	Supervision du travail d'audit par les chefs d'équipes puis au dernier niveau le chef de mission.	Le chef de mission et les chefs d'équipes		Validation des travaux
	Les irrégularités et actes illégaux: les activités irrégulières et actes illégaux sont très fréquente	Équipes déléguées		Informer l'autorité publique

	en TI. Ce peut être entre autre le piratage, utilisation frauduleuse de licence, Hacking, les attaques réseaux.			compétente

L'exécution de la mission, qu'elle soit une mission d'audit ou d'assurance, se décompose en étapes successives.

– Concertation de l'équipe pour démarrer le travail :

– Tests de conformité : pendant ces tests, le chargé des tests doit s'assurer d'avoir des éléments probants pertinents, suffisants et fiables pour atteindre les objectifs de l'audit.

– Tests de corroboration : contrairement aux tests de conformité où les éléments probants, pertinents et fiables sont percevables et souvent confirmés par les questionnaires, ceux des tests de corroborations sont issus d'une vérification dans la mise en œuvre pratique. L'acceptation est alors un peu plus difficile car l'audité ayant prétendu avoir mise œuvre les dispositifs qu'il faut. Il devrait donc être en mesure de sortir une preuve valable et irréfutable.

– Analyse des résultats et opinion : sur chaque feuille de travail, doivent figurer les analyses et conclusions de l'auditeur.

– Recoupement des workpapers : c'est la mise en commun de façon ordonnée et claire des workpapers et les preuves qui les accompagnent pour former le document d'audit qui doit être concerné.

– Investigation si nécessaire : après les tests de corroboration, des investigations peuvent s'avérer nécessaires, il faut alors faire part à la haute direction pour avoir l'accord de le faire si les compétences sont disponibles, sinon demander que l'investigation soit faite par un expert que nous aurons l'obligation de superviser.

– Supervision du travail d'audit : la supervision du travail s'opère tout au long de l'exécution. Le chef de mission doit superviser le personnel participant à l'audit pour fournir

l'assurance raisonnable que les objectifs de l'audit sont atteints et que les normes d'audit professionnelles applicables sont respectées.

– Les irrégularités et actes illégaux : pendant la planification et lors de l'exécution des travaux visant à réduire les risques d'audit au minimum, l'auditeur des SI doit prendre en compte la possibilité d'irrégularités et d'actes illégaux.

5.3 Finalisation de la mission

La finalisation de la mission est la conclusion de cette dernière. Elle commence par l'élaboration du rapport provisoire puis la validation des constats et enfin le rapport définitif.

Selon le contrat, il peut inclure le suivi des recommandations, mais pas leur mise en œuvre, car ISACA l'interdit formellement.

CECA	Procédure	Finalisation de la mission		Mise à jour
	Sous procédures			
	Fonction	Audit / assurance		Folio
Réf. Tâche	Description	Fait par	Délai	Matérialisé par
	Rapport provisoire: il peut être considéré comme le procès-verbal de la mission.	Chef de mission		Pré-rapport
	Validation des constats avec les audité: comme tout procès-verbal il doit-être validé avant publication. Cette étape est confirmation de l'opinion émise par l'auditeur et une infirmation pour les constats justifiés par des exceptions.	L'exécutant de l'interview		
	Réunion de clôture	Chef de mission		
	Transmission du Rapport définitif	Chef de mission		Rapport définitif
	Suivi des recommandations	Chef de mission		

- Rapport provisoire : Le COBIT et ISACA disent que l'auditeur doit se conformer aux normes d'assurance et d'audit des TI lorsqu'il fait un rapport sur les contrôles des systèmes d'information d'une organisation et sur les objectifs de contrôles associés. Ainsi, l'auditeur des SI doit fournir un rapport sous une forme adéquate. Le rapport doit préciser l'organisation, les destinataires du document et les éventuelles restrictions à diffusion. Le rapport doit indiquer la portée, les objectifs, la période couverte, la nature, et l'ampleur de l'audit réalisé.

Il doit indiquer les conclusions, les recommandations de l'audit, ainsi que les éventuelles limitations de portée, réserves ou qualification jugées opportunes par l'auditeur des SI. Il doit collecter les éléments probants suffisants et pertinents pour corroborer les résultats rapportés.

Lors de son édition, le rapport de l'auditeur doit être daté, signé et distribué conformément aux termes de la lettre de mission.

– Validation des constats avec les audités : c'est une étape très importante au cours de la finalisation dont sa négligence pourrait être "eriminelle"(préjudiciable) pour l'auditeur. Car, il peut de ce fait perdre sa crédibilité sachant que c'est une profession dont l'éthique et la déontologie priment sur tout. En effet, les constats non validées peuvent être source de conflits pouvant mettre l'auditeur en mauvaise posture s'ils sont justifiables par des exceptions.

– Réunion de clôture: elle couvre la présentation du rapport final et met fin à la mission sur terrain de l'auditeur. Elle permet à l'auditeur de s'exprimer sur l'ensemble sans trop s'écarter du contenu de son rapport.

– Rapport définitif : il est identique au rapport provisoire, juste au détail près des constats non validés par l'audité et valablement justifiés (par exemple par des exceptions). Il reconduit donc les mêmes termes et les conditions préalables. Il met fin à la mission, à moins que la lettre de mission ne prévoie des clauses de suivi des recommandations.

– Suivi des recommandations: le but de l'activité de suivi est d'orienter les auditeurs des SI chargés de faire un suivi des recommandations et commentaires sur l'audit exprimés dans les rapports.

Loin d'être le parfait modèle d'évaluation de la gouvernance des SI, ce manuel permet d'avoir une assurance raisonnable sur la fiabilité de la gouvernance des systèmes d'information. Il fait ainsi ressortir les différentes tâches à mettre en œuvre au cours d'une mission d'audit ou d'assurance. C'est à cet effet, que le chapitre suivant vient en complément apporter un diagnostic appuyé des meilleures pratiques à mettre en œuvre pour la gouvernance des SI et des recommandations dans la démarche d'audit de l'auditeur en termes d'objectifs de contrôle.

CHAPITRE VI : EVALUATION DE LA GOUVERNANCE DES SI ET RECOMMANDATIONS PRECONISES PAR LE COBIT

Le chapitre 6 vise à s'associe au manuel de procédure en lui apportant une touche plus pratique. Il s'agit ici d'un prototype d'évaluation de la gouvernance des SI avec l'approche risque, proposer par le comité COBIT. Il se réparti comme suit :

- l'objectif de contrôle de chaque sous processus ;
- les facteurs de risque généraux liés aux sous processus ;
- les recommandations érigées en bonnes pratiques pour les opérationnels de la gouvernance des SI dans l'entreprise ;
- des recommandations de contrôles issues d'objectifs de contrôle COBIT pour l'auditeur des SI.

C'est le processus quatre (4) du quatrième domaine (Suivre et Évaluer : SE) du COBIT qui prévoit la mise en place d'une gouvernance des SI. Nous présenterons ce processus tel que le COBIT le décrit en son sein par 34 processus.

L'utilisation de l'approche par les risques exige, l'appréhension du processus à travers ses risques et leurs impacts.

Le processus SE4 est décomposé en sept (7) sous processus. Chacun d'eux dispose d'objectif de contrôle, de risques, les bonnes pratiques et les tests à réaliser pour s'assurer la mise en œuvre réelle des bonnes pratiques préconisées par le COBIT.

6.1 Le SE4.1 : Établissement d'un cadre de gouvernance des TI

L'établissement d'un cadre de gouvernance des TI, est le premier sous processus du processus : mise en place d'une gouvernance des systèmes d'information. Il s'agit en faite de réaliser un référentiel de la gouvernance des SI propre à l'entreprise intégrant les bonnes pratiques.

L'objectif de ce sous processus peut se résumer dans les termes qui suivent d'après le COBIT.

Définir, mettre en place et aligner le cadre de gouvernance des TI avec la gouvernance globale de l'entreprise et l'environnement de contrôle. Fonder le cadre d'un processus informatique adapté, le modèle de contrôle et assurer la responsabilisation sans équivoque des bonnes pratiques afin d'éviter une rupture dans le contrôle interne et de surveillance.

6.1.1 Inducteur ou facteur de risques

• Les responsabilités et les responsables établies sont inefficaces pour les processus TI.

• Le portefeuille TI ne soutient pas les objectifs de l'entreprise et les stratégies.

• Les mesures correctives pour maintenir et améliorer l'efficacité TI processus et l'efficacité non identifiés ou mis en œuvre.

• Les contrôles ne fonctionnent pas comme prévu.

6.1.2 Recommandations aux professionnels opérationnels des SI

1. Établir un comité de la stratégie TI pour fournir des orientations politiques de haut niveau et de vérifier la conformité de stratégie.

2. Établir des processus pour définir les priorités d'investissement TI activé, évaluer l'ajustement stratégique des propositions et effectuer des revues de portefeuille d'investissement pour continuer la pertinence stratégique.

3. Établir des structures de gestion appropriées tel qu'un comité de pilotage informatique, du conseil en technologie, commission d'examen de l'architecture informatique et comité d'audit informatique.

6.1.3 Recommandations aux professionnels indépendants des SI

Vérifier si et confirmer que :

- un processus est prévu pour aligner le cadre de gouvernance informatique avec la gouvernance globale de l'entreprise et l'environnement de contrôle.

- Le cadre de gouvernance TI se concentre sur l'alignement stratégique, l'apport de valeur, la gestion des ressources, gestion des risques et la mesure du rendement.

- Il existe un processus pour mesurer et évaluer la prestation des TI stratégies et objectifs, d'agréger la gouvernance des TI à toutes les questions et des mesures correctives dans un référentiel de gestion consolidée ou un mécanisme de suivi.

6.2 Le SE4.2 : Alignement stratégiqne

L'alignement stratégique est ce sous processus qui permet de s'assurer que le système d'information est gouverné. C'est-à-dire que le conseil d'administration et la haute direction interviennent dans la gouvernance des SI. Ainsi, le système d'information ne peut que soutenir les objectifs d'affaires.

L'objectif est d'activer le conseil d'administration à la compréhension de la direction stratégique de problèmes informatiques, tels que le rôle des TI, un aperçu technologique et des capacités. S'assurer qu'il y a une compréhension commune entre l'entreprise et les TI sur la contribution potentielle de l'informatique à la stratégie d'affaires.

6.2.1 Inducteur de risque

• Allocation et gestion inefficace des investissements informatiques.

• Les TI ne soutiennent pas les objectifs de l'entreprise.

• La planification stratégique n'est pas alignée avec la stratégie globale d'entreprise.

• Les directions TI ne sont pas définies et ne soutiennent pas les objectifs commerciaux.

6.2.2 Recommandations aux professionnels opérationnels des SI

1. Activer un processus d'entreprise, une planification stratégique efficace en assurant l'alignement entre l'entreprise et la stratégie informatique et une structure organisationnelle informatique qui complète le modèle d'entreprise et la direction.

2. Aligner et intégrer la stratégie TI avec les objectifs d'affaires. Fournir une orientation afin qu'il soit optimal permettant la stratégie de l'entreprise et que les opérations informatiques sont alignées avec les opérations commerciales. Il devrait y avoir de médiation appropriée entre les impératifs de l'entreprise et de la technologie.

3. Commanditaires directes des entreprises, responsables et propriétaires dans les grands investissements des TI.

6.2.3 Recommandations aux professionnels indépendants des SI

• Inspectez les documents de stratégie IT et évaluer si elle appuie l'orientation fournie par le conseil d'administration ou la direction. Il doit refléter les stratégies d'affaires et son alignement approprié avec les opérations commerciales.

• Déterminer si le processus de planification stratégique des TI comprend la participation des opérations commerciales et démontre l'alignement avec les stratégies et objectifs commerciaux.

• Examiner les documents de stratégie informatique et d'évaluer si elles comprennent le rôle des TI, les principes directeurs, de maximes d'affaires, comment elle surveille l'impact commercial de l'infrastructure informatique et de portefeuille d'applications, la contribution potentielle de l'informatique à la stratégie globale de l'entreprise.

6.3 SE4.3 : procuration de la valeur

Ce processus donne une visibilité sur le retour sur investissement en matière de technologie d'information. Il est important que la DSI ne soit pas perçu comme un centre consommateur de coûts.

Son objectif est de Gérer les programmes d'investissement des TI et autres ressources informatiques et de services pour s'assurer qu'ils offrent la meilleure valeur possible pour soutenir la stratégie de l'entreprise et ses objectifs.

6.3.1 Inducteurs de risque

• Mauvaise orientation des investissements en TI.

• Valeur non obtenue à partir des actifs et services informatiques.

• Diminuer la satisfaction du client.

• L'augmentation des coûts pour les investissements des TI et des opérations.

• Manque d'alignement entre les objectifs d'affaires et de l'architecture informatique

• Les bénéfices attendus ne sont pas réalisés.

6.3.2 Recommandations aux professionnels opérationnels des SI

1. Surveiller la livraison des services TI afin de s'assurer qu'elles bénéficient du soutien fourni aux processus d'affaires. Les investissements directs des programmes de TI assurent et offrent des avantages tangibles en harmonie avec les objectifs initiaux. Établir la coresponsabilité entre l'entreprise et de TI pour les investissements en TI.

2. Établir les architectures informatiques et d'affaires qui sont conçus pour générer de la valeur d'entreprise au maximum. Standardiser les architectures et les technologies pour réduire la complexité et atteindre l'optimisation des coûts.

3. Contrôler si les investissements informatiques sont basés sur un équilibre des risques et des avantages, avec des budgets qui sont acceptables et prendre en compte le retour et les aspects concurrentiels des investissements en TI.

6.3.3 Recommandations aux professionnels indépendants des SI

• Confirmer qu'il y a coresponsabilité entre les métiers et l'informatique pour tous les investissements en TI.

• Inspecter la documentation qui identifie comment il rencontre de la stratégie. Il devrait inclure la prestation dans les délais et le budget, avec des fonctionnalités appropriées et les avantages escomptés.

• Déterminer s'il y a un processus de TI efficaces de gestion de portefeuille qui est évalué sur une base régulière afin d'optimiser la valeur par rapport aux coûts et que les résultats de avantage concurrentiel, le temps écoulé pour la commande / service d'exécution, la satisfaction des clients, des employés productivité et la rentabilité.

6.4 SE4.4 : Gestion des ressources

Le sous processus gestion des ressources a pour but le suivi et le contrôle en vue de s'assurer que les ressources sont exploitées pour les raisons qu'elles ont été acquises.

L'objectif de ce sous processus est de superviser les investissements, l'utilisation et l'affectation des ressources informatiques grâce à des évaluations régulières des initiatives de TI et des opérations afin d'assurer les ressources appropriées et l'alignement avec les objectifs actuels et futurs impératifs stratégiques d'affaires.

6.4.1 Facteurs de risques

- Fragmentation inefficace des infrastructures.
- Les capacités et compétences insuffisantes des ressources pour atteindre les objectifs souhaités.
- Des objectifs stratégiques non atteints.
- Des priorités inappropriées utilisées pour l'allocation des ressources.

6.4.2 Recommandations aux professionnels opérationnels des SI

1. Fournir des directives de haut niveau pour le sourcing et l'utilisation des ressources informatiques, par exemple, les alliances stratégiques.

2. Surveiller la façon dont la gestion détermine, comment les ressources informatiques sont nécessaires pour atteindre les objectifs stratégiques. Établir les priorités et allouer des ressources des TI afin de permettre des performances d'affaires efficaces.

3. Optimiser les investissements informatiques et l'utilisation des ressources pour obtenir l'équilibre global entre le maintien et la croissance de l'entreprise.

6.4.3 Recommandations aux professionnels indépendants des SI

• Confirmer par un questionnement de la direction qu'un haut niveau de direction existe pour l'approvisionnement et l'utilisation des ressources de TI.

• Revoir les politiques, procédures et processus en place pour la gestion des ressources et vérifier qu'ils fonctionnent efficacement pour :

- optimiser les investissements informatiques et l'utilisation des ressources pour obtenir l'équilibre global entre le maintien et la croissance de l'entreprise ;

- capitaliser les ressources des technologies de l'information et connaissances ;

- établir des priorités de l'entreprise afin que les ressources soient allouées pour permettre aux TI des performances efficaces.

6.5 SE4.5 : gestion des risques

Ce sous processus assure la gestion des risques liés à la gouvernance de SI.

Il permet la maitrise de ces risques. L'objectif de contrôle est de travailler avec le conseil d'administration pour définir l'appétit de l'entreprise pour les risques informatiques, et obtenir l'assurance raisonnable que les pratiques de gestion des risques informatiques sont appropriées

pour s'assurer que le risque informatique réel ne dépasse pas l'appétit du risque du conseil. Intégrer les responsabilités de gestion du risque dans l'organisation.

6.5.1 Inducteurs de risque

- Les risques identifiés sont gérés inefficacement.
- Augmentation des dépenses et coûts engagés pour gérer les risques imprévus.
- L'échec des services et des applications informatiques critiques.
- Manque d'appropriation des risques informatiques.

6.5.2 Recommandations aux professionnels opérationnels des SI

1. Fournir au Conseil des informations sur l'exposition aux risques informatiques et les mesures en place traitant du confinement des risques et des coûts associés. Confirmer la pertinence du plan de gestion du risque et son alignement avec l'appétit pour le risque.

2. Surveiller les pratiques en matière de gestion des risques afin de s'assurer que la gestion des risques d'exploitation se fait tel que requis ; les responsabilités de gestion des risques sont adéquatement et clairement assignés, et la gestion des ressources a été mise en place pour assurer une bonne gestion des risques informatiques.

3. Évaluer l'efficacité de la surveillance de la direction des risques informatiques.

6.5.3 Recommandations aux professionnels indépendants des SI

Vérifier si et confirmer que:

- Basé sur l'information de la direction, telles que l'exposition aux risques informatiques, les mesures de gestion des risques et des coûts associés ; le conseil définit, réévalue régulièrement et communique l'appétit pour le risque de l'entreprise.

- La direction examine les résultats de l'évaluation des risques des activités informatiques, afin de confirmer que l'exposition au risque total ne dépasse pas l'appétit pour le risque défini, compte tenu des contrôles d'atténuation en place, et supervise la mise en œuvre de contrôles supplémentaires d'atténuation pour réduire l'exposition globale au risque au besoin.

6.6 SE4.6 : Mesure du rendement

Il est question de pouvoir mesurer ici le rendement de l'investissement effectué sur les TI à travers l'objectif suivant. Confirmer que les objectifs IT retenus ont été atteints ou dépassés, ou que les progrès vers les objectifs IT répondent aux attentes. Où les objectifs convenus ont été manqués ou ne progressent pas comme prévu, la revue de l'action de redressement de direction. Rapport au conseil d'administration des portefeuilles concernés, le programme et les performances informatiques, étayées par des rapports pour permettre aux cadres supérieurs pour examiner les progrès de l'entreprise vers les objectifs identifiés.

6.6.1 Inducteurs de risques

- Lacunes de performance non identifiées de manière opportune.
- Diminution de la confiance des intervenants.
- Les écarts des services et des dégradations ne sont pas reconnus et traités, entraînant une défaillance d'expression des besoins de l'entreprise.
- Échecs de performances du Service provoquant des expositions aux conformités légales et réglementaires.

6.6.2 Recommandations aux professionnels opérationnels des SI

1. Évaluer le rendement des cadres supérieurs dans l'exécution et la réalisation des stratégies informatiques et l'alignement avec les stratégies d'affaires. Revue des défaillances importantes et fournir une orientation pour corriger les causes organisationnelles ou systémiques par le biais des actions correctives appropriées.

2. Obtenir la garantie de la performance satisfaisante de contrôle et de gestion des risques IT et que les grandes décisions informatiques ont été déployés de manière appropriée. Considérons une assurance indépendante, où un objectif ou un avis spécialisé est nécessaire.

6.6.3 Recommandations aux professionnels indépendants des SI

Vérifier si et confirmer que:

- les tableaux de bord de mesures des performances informatiques sont correctement alignés avec les tableaux de bord de mesures Business et acceptée par l'entreprise.

- La direction évalue et accepte l'efficacité des processus, l'exactitude et l'exhaustivité des livrables pour mesurer la performance par rapport à la réalisation des objectifs stratégiques IT et en faire rapport au conseil d'administration. Vérifier que les rapports d'état, mentionnent la mesure dans laquelle les objectifs prévus ont été atteints, les produits livrables obtenus et les objectifs de performance atteints.

6.7 SE4.7 : Assurance indépendants

Le sous processus d'assurance indépendance vise à apprécier la mise en œuvre de la gouvernance par une tierce partie autre que la haute direction et la direction des systèmes d'information.

Obtenir une garantie indépendante (interne ou externe) au sujet de la conformité de l'informatique avec les lois et règlements pertinents, les politiques de l'organisation, les normes et procédures, les pratiques généralement acceptées, et l'exécution efficace et efficiente des TI.

6.7.1 Inducteurs de risques

- Dommages à la réputation par l'échec à détecter ou à prévenir la dégradation de la performance du service.
- La gouvernance des TI, la gestion des risques et les dispositifs de contrôle interne sont Inefficaces.
- Les comportements déloyaux adoptés et acceptés.

6.7.2 Recommandations aux professionnels opérationnels des SI

1 Définir et mettre en œuvre une structure organisationnelle afin d'obtenir une assurance indépendante. Cela comprend généralement un comité de vérification et de soutien technique au niveau des comités de conseil, le cas échéant, avec pour mandat d'examiner quels sont les risques significatifs. Évaluer la façon dont ils sont identifiés, évalués et gérés ; commission informatique et les audits de sécurité, et avec rigueur le suivi de la réalisation des recommandations.

2. Obtenir des examens indépendants et des certifications de conformité aux politiques informatiques, normes et procédures à l'aide d'audit interne et / ou des parties externes.

3. Considérer les critères de sélection suivants conseiller en obtenant l'assurance équilibrée: l'indépendance, l'objectivité, la confidentialité, l'intégrité, la compétence et la diligence professionnelle et les qualifications / certifications pour effectuer le travail.

6.7.3 Recommandations aux professionnels indépendants des SI

• Vérifier si et confirmer que le comité de vérification a été établi avec pour mandat d'examiner quels sont les risques significatifs, d'évaluer la façon dont ils sont identifiés, évalués et gérés; Commission informatique et les audits de sécurité; et rigoureusement suivi la fermeture des recommandations subséquentes.

• Interview du comité de vérification et évaluer ses connaissances et la sensibilisation de ses responsabilités. Déterminer si le comité d'audit créé fonctionne efficacement.

• Vérifier si et confirmer que des examens indépendants, certifications ou agréments de la conformité aux politiques informatiques, normes et procédures ont été obtenus.

Inspecter physiquement pour l'adéquation des documents produits par les examens indépendants.

Dans le présent chapitre, objectifs de contrôles, inducteurs de risques, inducteurs de coûts, recommandations aux professionnels opérationnels des SI et recommandations aux professionnels indépendants des SI sont intégralement pris des travaux du comité COBIT et associés aux référentiels COBIT.

La deuxième partie que nous venons de lire, permettra à toute personne qui a la volonté de s'assurer de la santé ne serait-ce que de façon sommaire et sans connaissances accrues des systèmes d'information d'avoir une opinion très objective et réaliste des SI.

Ceci est possible en mettant en œuvre les procédures d'évaluation en chapitre 5 associés au diagnostic proposé par le COBIT que nous avons déployé en chapitre 6.

Cette partie se veut donc être le plus simple possible pour permettre à toute personne ayant la méthodologie d'audit de s'assurer de la mise en œuvre de la gouvernance des SI dans une organisation.

CONCLUSION GENERALE

La gouvernance des technologies de l'information se présente à l'heure actuelle comme indispensable à la pratique de la bonne gouvernance de l'entreprise. A cet effet, son évaluation est incontournable dans l'appréciation de la gouvernance d'entreprise et du système d'information de l'entreprise.

L'opinion de l'auditeur, d'un commissaire aux comptes ou encore d'un spécialiste, dépend de la qualité de l'information qu'il reçoit. Ceci l'oblige donc à vérifier le système qui produit l'information qui lui sert d'entrer en amont, pour produit en aval une opinion raisonnable.

A défaut d'avoir la compétence requise pour se prononcer sur la qualité du système d'information, la mise en application de manuel de procédure sus élaboré, leur permet de constaté si le minimum de diligence est fait pour rendre les informations sortant du système fiables.

Cet outil vient à point pour satisfaire les auditeurs et contrôleurs dans la mise en œuvre des diligences nécessaires pour les libérer à la fois de leurs obligations tant déontologiques que pénales.

Ledit manuel de procédure, est le fruit d'un référentiel complet et fédérateur (COBIT). Ceci lui permet alors d'incorporer les bonnes pratiques universellement adoptées pour assurer à l'entreprise de façon générale une bonne gouvernance.

La mise en application dudit manuel nous a permis avec le CECA lors d'un audit des SI de résorber le problème de gouvernance d'une institution de micro-finance à partir d'un diagnostic de la gouvernance des systèmes d'information et de sa mise en œuvre de cette dernière conformément aux exigences du référentiel COBIT. Nous parvenons ainsi respecter les exigences de gouvernance du COSO, de management de la qualité d'ISO et le « Capability Maturity Model Intégrate (CMMI) ».

Mise à part cette opportunité qu'offre ce manuel, ses limites s'élèvent dès l'instant qu'intervient la nécessité de mise en œuvre de l'audit des systèmes d'information.

Enfin, nous pensons que la certification des comptes d'une organisation digne du nom, ne saurait être validée sans l'intervention préalable d'une assurance de la fiabilité du système d'information. Car, le niveau de pénétration des technologies de l'information dans les organisations est très

élevé. Tout ce qui précède nous permet d'estimer que l'audit des systèmes d'information est la profession de l'ère technologique dans laquelle nous sommes depuis l'an 2000 et dans laquelle l'Afrique subit une pleine phagocytose accélérée et non maîtrisable.

ANNEXES

Annexe1 : RACI

ACTIVITÉS	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif	Bureau projet	Conformité, audit, risque et sécurité
Lier objectifs métier et objectifs informatiques.	C	I	A/R	R	C						
Identifier les dépendances critiques et les performances actuelles.	C	C	R	A/ R	C	C	C	C	C		C
Construire un plan informatique stratégique.	A	C	C	R	I	C	C	C	C	I	C
Élaborer des plans informatiques tactiques.	C	I		A	C	C	C	C	C	R	I
Analyser les portefeuilles de programmes et gérer les portefeuilles de projets et de services.	C	I	I	A	R	R	C	R	C	C	I

Annexes 2 : modèle de maturité

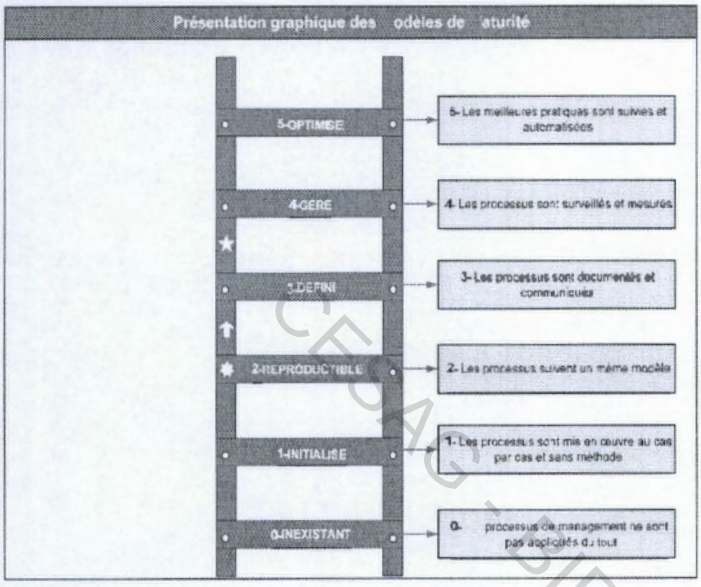


Figure 3-2 : Modèle de maturité

Annexe 3 : Documents liés à Cobit

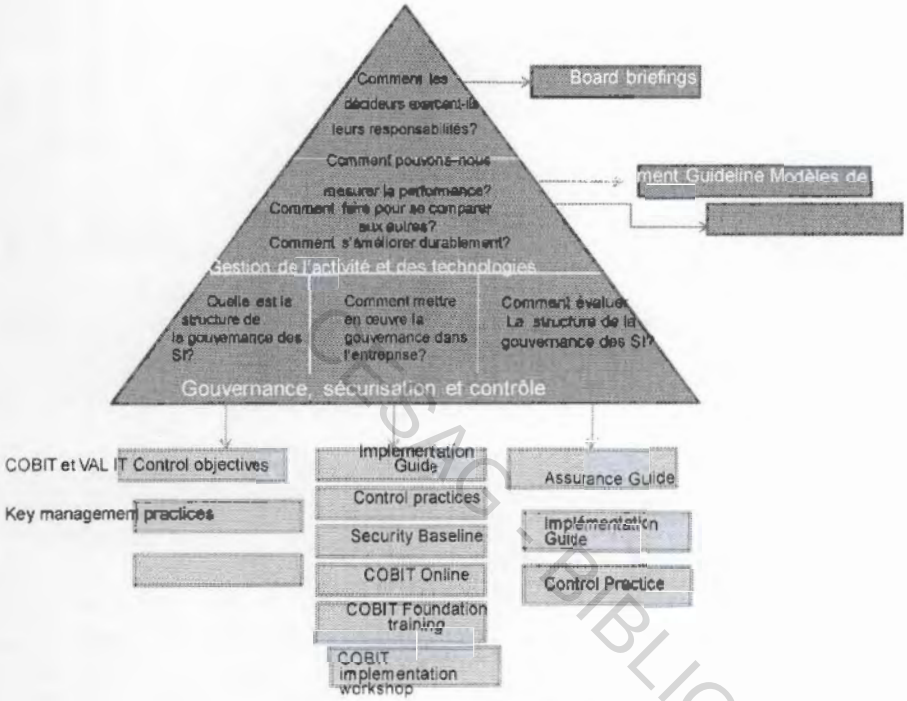


Figure 3-3 : Documents liés à CobiT

Annexe4 : niveaux de responsabilité pour une bonne gouvernance de la sécurité des SI

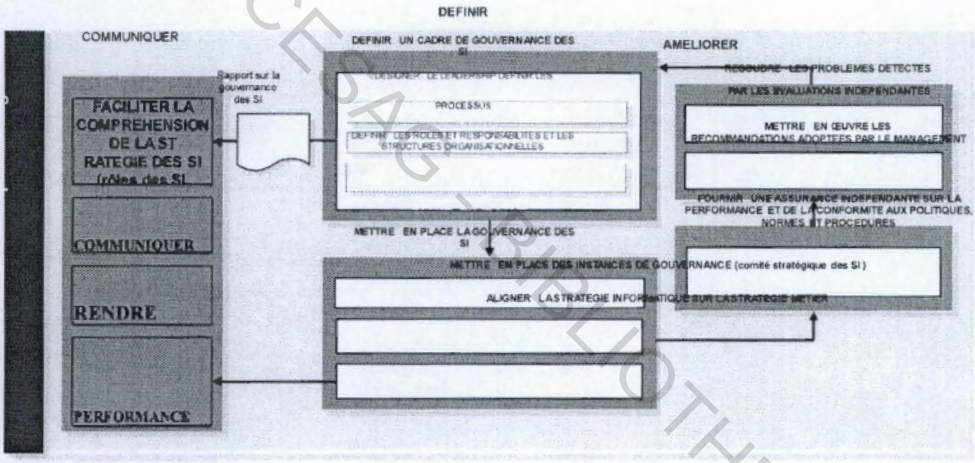
Niveau de direction	Alignement stratégique	Gestion des risques	Offres de valeur	Mesure du rendement	Gestion des ressources	Intégration de processus
Conseil d'administration	Exiger un alignement démontrable	- établir la tolérance au risque. - établir une politique de gestion des risques. - assurer la conformité à la réglementation .	Exiger des rapports sur les coûts des activités de sécurité.	Exiger des rapports sur l'efficacité de la sécurité	Etablir une politique de gestion des connaissances et l'utilisation des ressources	Etablir une politique d'assurance de l'intégration des processus
Haute direction	Etablir des processus pour intégrer la sécurité aux objectifs opérationnels	- Assurer les rôles, responsabilités , inclure la gestion des risques dans toute activité. - Surveiller la conformité à la réglementation	Exiger des études de cas sur les initiatives en matière de sécurité	Exiger la surveillance et la mesure des activités relatives à la sécurité	Assurer des processus pour la saisie des connaissances et pour la mesure de l'efficacité	Fournir une surveillance d'assurance de toutes les fonctions et de tous les projets d'intégration
Comité directeur	-Examiner la stratégie de sécurité et les efforts	Déterminer les nouveaux risques, promouvoir les	Examiner le caractère adéquat des initiatives de	Examiner les initiatives de sécurité, donner des	Examiner les processus de saisie et de disséminatio	-Déterminer les processus administratifs et les

	d'intégration. -Veiller à ce que les propriétaires de l'entreprise soutiennent l'intégration	pratiques de sécurité des unités fonctionnelles et déterminer les problèmes de conformité	sécurité pour que celles-ci soient au service des fonctions opérationnelle s	conseils par rapport à celle-ci et veiller à ce qu'elles respectent les objectifs opérationnels	n des connaissance s	certificateurs. -Diriger les efforts d'intégration
Responsable de la sécurité de l'information	Elaborer une stratégie de sécurité, surveiller le programme et les initiatives de sécurité et assurer la liaison avec les responsables des procédés administratifs pour un alignement continu	-Assurer l'évaluation des impacts opérationnels. -Elaborer des stratégies de réduction des risques. -Faire respecter la politique et la conformité à la règlementation	Surveiller l'utilisation et l'efficacité des ressources de sécurité	Elaborer et mettre en place des approches de surveillance et mesure, et diriger et surveiller les activités	Elaborer des méthodes de saisie et de disséminatio n des connaissance s et développer des mesures d'efficacité et d'efficience	-Assurer la liaison avec d'autres certificateurs -Veiller à ce que les lacunes et les chevauchemen ts soient déterminés et corrigés
Dirigeants d'audit	Evaluer et faire un rapport sur le degré d'alignement	Evaluer et faire un rapport sur les pratiques de gestion du risque de l'entreprise et des résultats	Evaluer et faire un rapport sur l'efficacité	Evaluer et faire un rapport sur le degré d'efficacité des mesures en place et des paramètres utilisés	Evaluer et faire un rapport sur l'efficacité de la gestion des ressources	Evaluer et faire un rapport sur l'efficacité des processus d'assurance effectués par divers secteurs de la direction.

Annexe 5 : Objectifs et détailles d'étapes d'audit

Obj. 02	Réagir aux exigences de la gouvernance en accord avec les orientations du CA.
Obj. 12	S'assurer de la transparence et de la bonne compréhension des coûts, bénéfices, stratégie, politiques et niveaux de services des SI.
Obj. 27	Assurer la conformité de l'informatique aux lois et aux règlements.
Obj. 28	S'assurer que l'informatique fait preuve d'une qualité de service efficiente en matière de coûts, d'amélioration continue et de capacité à s'adapter à des changements futurs.

ure 7-11 représente les flux internes du processus SE4.



Annexe 6 : Objectifs du système d'information et processus selon le cobit

Tableau II-1 : Objectifs du système d'information et processus du domaine Planifier et Organiser

Objectifs		Processus						
		AI1 : Trouver des solutions informatiques	AI2 : Acquérir des applications et en assurer la maintenance	AI3 : Acquérir une infrastructure technique et en assurer la maintenance	AI4 : Faciliter le fonctionnement et l'utilisation	AI5 : Acquérir des ressources informatiques	AI6 : Gérer les changements	AI7 : Installer et valider des solutions et des modifications
Obj. 16	Réduire le nombre de défauts et de retraitements touchant à la fourniture de solutions et de services.				✔		✔	✔
Obj. 17	Protéger l'atteinte des objectifs informatiques.							
Obj. 18	Montrer clairement les conséquences pour l'entreprise des risques liés aux objectifs et aux ressources informatiques.							
Obj. 19	S'assurer que l'information critique et confidentielle n'est pas accessible à ceux qui ne doivent pas y accéder.							
Obj. 20	S'assurer que les transactions métier automatisées et les échanges d'informations sont fiables.							✔
Obj. 21	S'assurer que les services et l'infrastructure informatique peuvent résister/se rétablir convenablement en cas de panne due à une erreur, à une attaque délibérée ou à un sinistre.							✔
Obj. 22	S'assurer qu'un incident ou une modification dans la fourniture d'un service informatique n'a qu'un impact minimum sur l'activité.						✔	
Obj. 23	S'assurer que les services informatiques sont disponibles dans les conditions requises.							
Obj. 24	Améliorer la rentabilité de l'informatique et sa contribution à la profitabilité de l'entreprise.							
Obj. 25	Livrer les projets à temps et dans les limites budgétaires en respectant les standards de qualité.							
Obj. 26	Maintenir l'intégrité de l'information et de l'infrastructure de traitement.						✔	
Obj. 27	Assurer la conformité de l'informatique aux lois et aux réglements.							
Obj. 28	S'assurer que l'informatique fait preuve d'une qualité de service efficiente en matière de coûts, d'amélioration continue et de capacité à s'adapter à des changements futurs.							

Tableau II-2 : Objectifs du système d'information et processus du domaine Acquérir et Implémenter

Objectifs		Processus												
		DS1 : Définir et gérer...	DS2 : Gérer les services tiers	DS3 : Gérer la performance...	DS4 : Assurer un service continu	DS5 : Assurer la sécurité...	DS6 : Identifier et imputer...	DS7 : Instruire et former...	DS8 : Gérer le service...	DS9 : Gérer la configuration	DS10 : Gérer les problèmes	DS11 : Gérer les données	DS12 : Gérer l'environnement physique	DS13 : Gérer l'exploitation
Obj. 01	Réagir aux exigences métier en accord avec la stratégie métier.	✔		✔										
Obj. 02	Réagir aux exigences de la gouvernance en accord avec les orientations du CA.													
Obj. 03	S'assurer de la satisfaction des utilisateurs finaux à l'égard des offres et des niveaux de services.	✔	✔					✔	✔		✔			✔
Obj. 04	Optimiser l'utilisation de l'information.											✔		
Obj. 05	Donner de l'agilité à l'informatique.													
Obj. 06	Déterminer comment traduire les exigences métier de fonctionnement et de contrôle en solutions automatisées efficaces et efficientes.													
Obj. 07	Acquérir et maintenir fonctionnels des systèmes applicatifs intégrés et standardisés.													
Obj. 08	Acquérir et maintenir opérationnelle une infrastructure informatique intégrée et													
Obj. 09	Se procurer et conserver les compétences nécessaires à la mise en œuvre de la stratégie informatique.													
Obj. 10	S'assurer de la satisfaction réciproque dans les relations avec les tiers.		✔											
Obj. 11	S'assurer de l'intégration progressive des solutions informatiques aux processus métier.													
Obj. 12	S'assurer de la transparence et de la bonne compréhension des coûts, bénéfices, stratégie, politiques et niveaux de services des SI.	✔	✔				✔							
Obj. 13	S'assurer d'une bonne utilisation et des bonnes performances des applications et des solutions informatiques.							✔	✔					
Obj. 14	Protéger tous les actifs informatiques et en être comptable.					✔				✔			✔	
Obj. 15	Optimiser l'infrastructure, les ressources et les capacités informatiques.			✔				✔		✔				

Tableau II-3 : Objectifs du système d'information et processus du domaine Délivrer et Supporter

Objectifs		Processus													
		DS1 : Définir et gérer...	DS2 : Gérer les services tiers	DS3 : Gérer la performance...	DS4 : Assurer un service continu	DS5 : Assurer la sécurité...	DS6 : Identifier et imputer...	DS7 : Instruire et former...	DS8 : Gérer le service...	DS9 : Gérer la configuration	DS10 : Gérer les problèmes	DS11 : Gérer les données	DS12 : Gérer l'environnement physique	DS13 : Gérer l'exploitation
Obj. 16	Réduire le nombre de défauts et de retraitements touchant la fourniture de solutions et de services.										✔			
Obj. 17	Protéger l'atteinte des objectifs informatiques.										✔			
Obj. 18	Montrer clairement les conséquences pour l'entreprise des risques liés aux objectifs et aux ressources informatiques.										✔			
Obj. 19	S'assurer que l'information critique et confidentielle n'est pas accessible à ceux qui ne doivent pas y accéder.					✔						✔	✔	
Obj. 20	S'assurer que les transactions métier automatisées et les échanges d'informations sont fiables.					✔								
Obj. 21	S'assurer que les services et l'infrastructure informatique peuvent résister/se rétablir convenablement en cas de panne due à une erreur, à une attaque délibérée ou à un sinistre.				✔	✔							✔	✔
Obj. 22	S'assurer qu'un incident ou une modification dans la fourniture d'un service informatique n'a qu'un impact minime sur l'activité.				✔								✔	
Obj. 23	S'assurer que les services informatiques sont disponibles dans les conditions requises.			✔	✔				✔					✔
Obj. 24	Améliorer la rentabilité de l'informatique et sa contribution à la profitabilité de l'entreprise.						✔							
Obj. 25	Livrer les projets à temps et dans les limites budgétaires en respectant les standards de qualité													
Obj. 26	Maintenir l'intégrité de l'information et de l'infrastructure de traitement.					✔								
Obj. 27	Assurer la conformité de l'informatique aux lois et aux règlements.											✔		
Obj. 28	S'assurer que l'informatique fait preuve d'une qualité de services efficiente en matière de coûts, d'amélioration continue et de capacité à s'adapter à des changements futurs.						✔							

Tableau II-4 : Objectifs du système d'information et processus du domaine Surveiller et Évaluer

Objectifs		Processus			
		SE1 : Surveiller et évaluer la performance du SI	SE2 : Surveiller et évaluer le contrôle interne	SE3 : S'assurer de la conformité aux obligations externes	SE4 : Mettre en place une gouvernance des SI
Obj. 01	Réagir aux exigences métier en accord avec la stratégie métier.	✔			
Obj. 02	Réagir aux exigences de la gouvernance en accord avec les orientations du CA.	✔			✔
Obj. 03	S'assurer de la satisfaction des utilisateurs finaux à l'égard des offres et des niveaux de services.				
Obj. 04	Optimiser l'utilisation de l'information.				
Obj. 05	Donner de l'agilité à l'informatique.				
Obj. 06	Déterminer comment traduire les exigences métier de fonctionnement et de contrôle en solutions automatisées efficaces et efficientes.				
Obj. 07	Acquérir et maintenir fonctionnels des systèmes applicatifs intégrés et standardisés.				
Obj. 08	Acquérir et maintenir opérationnelle une infrastructure informatique intégrée et standardisée.				
Obj. 09	Se procurer et conserver les compétences nécessaires à la mise en œuvre de la stratégie informatique.				
Obj. 10	S'assurer de la satisfaction réciproque dans les relations avec les tiers.				
Obj. 11	S'assurer de l'intégration progressive des solutions informatiques aux processus métier.				
Obj. 12	S'assurer de la transparence et de la bonne compréhension des coûts, bénéfices, stratégie, politiques et niveaux de services des SI.	✔		✔	
Obj. 13	S'assurer d'une bonne utilisation et des bonnes performances des applications et des solutions informatiques.				
Obj. 14	Protéger tous les actifs informatiques et en être comptable.		✔		
Obj. 15	Optimiser l'infrastructure, les ressources et les capacités informatiques.				
Obj. 16	Réduire le nombre de défauts et de retraitements touchant à la fourniture de solutions et de services.				
Obj. 17	Protéger l'atteinte des objectifs informatiques.		✔		

BIBLIOGRAPHIE

1. ANGOT Hugues, FISCHER Christian, THEUNISSEN Baudouin (2004), *Audit comptable, audit informatique*, 3e édition, De Boeck Université, Bruxelles, 300.

2. AUTISSIER David, DELAYE Valérie (2008), *Mesurer la performance du système d'information,* groupe EYROLLES, Paris, 214 pages.

3. BALLAND Stéphane, BOUVIER Anne-Marie (2007), *Management des entreprises en 24 fiches*, DUNOD, Paris, 149 pages.

4. BARBIER Etienne (1999), *Mieux piloter et mieux utiliser l'audit*, MAXIMA, Paris, 132 pages.

5. BENNASAR MATTHIEU (2010), Plan de continuité d'activité et système d'information : vers l'entreprise résiliente, DUNOD, Paris, 303 pages.

6. BESLUAU Emmanuel (2008), *Management de la continuité d'activité*, EYROLLES, Paris, 254 pages.

7. BITTERLI Peter R., BRUN Jürg, BUCHER Thomas, CHRIST Brigitte, HAMBERGER Bernhard, HUISSOUD Michel, KÜNG Daniel, TOGGWYLER Andreas, WYNIGER Daniel, BERWEILER Georges (2008), *Guide d'audit des applications informatiques*, AFAI, 48 pages.

8. BOHNKÉ Sabine (2010), Moderniser son système d'information, groupe EYROLLES, Paris, 290 pages.

9. BORGHINO Pascal, DASINI Olivier, GADAL Arnaud (2010), *Audit et Optimisation MySQL 5 : Bonnes pratiques pour l'administrateur*, EYROLLES, Paris, 266 pages.

10. CATTAN Michel (2008), *Guide des processus : passons à la pratique !*, 2ème édition, AFNOR, La Plaine Saint-Denis, 314 pages.

11. CHALLANDE François, LEQUEUX Jean-Louis (2009), *Le grand livre du DSI : Mettre en œuvre la direction des systèmes d'information 2.0,* version 2.0, édition d'organisation Groupe EYROLLES, Paris, 352 pages.

12. DELLIERE Claude (2004), *Management de l'entreprise performante : apprendre par l'action*, Robert Jauze, France, 280 pages.

13. DELORME Pierre (1990), *Théories et pratiques actuelles du management*, Presses de l'Université du Québec, Québec, 203 pages.

14. DUMONT Christian (2007), *ITIL - Pour un service informatique optimal,* 2e édition, EYROLLES, Paris, 377 pages.

15. FIGARI Gérard (1994), Évaluer, quel référentiel, De Boeck Université, Bruxelles, 194 pages.

16. FOX Christopher, ZONNEVELD Paul **(2006), *It control objectives for sarbanes-oxley : the role of it in the design and implementation of internal control over financial reporting***, 2e edition , ISACA, United States of America, 130 pages.

17. GALLAIRE Jean-Marc (2008), Les outils *de la performance industrielle*, édition d'organisation groupe EYROLLES, Paris, 200 pages.

18. HENRY Alain, Ignace MONKAM-DAVERAT (2001), *rédiger les procédures de l'entreprise: guide pratique*, 3e édition, édition d'organisation, Paris, 185 pages.

19. ISACA (2007), *IT Assurance Framework : Draf*, ISACA, USA, 66 pages.

20. ISACA (2008), *ITAF : A professional Practices Framework for IT Assurance*, ISACA, USA, 80 pages.

21. ISACA (2009), *Implementing And Continually Improving IT governance*, ISACA, USA, 74 pages.

22. ISACA (2009), *Security, Audit and Control Features: Oracle Database*, 3rd edition, ISACA, USA, 28 pages.

23. ISACA (2010), Monitoring Internal Control Systems and IT, ISACA, 124 pages.

24. ISACA (2011), *Certified Information Systems Auditor: Manual de Préparation CISA2011*, ISACA, 508 pages.

25. ITGI (2007), *COBIT Control Practices : Guidance to Achieve Control Objectives for Successful*, IT GOVERNANCE, 2nd edition, ISACA, USA, 184 pages.

26. ITGI (2007), *CobiT Quickstart*, 2nd edition, ISACA, USA, 60 pages.

27. ITGI (2007), *CobiT Security Base: An Information Security Survival Kit*, ISACA, USA, 48 pages.

28. ITGI (2007), IT Assurance Guide Using COBIT, ISACA, 270 pages.

29. ITGI (2007), *IT Control Objectives For Base BASEL II: THE IMPORTANCE OF GOVERNANCE AND RISK MANAGEMENT FOR COMPLIANCE*, ISACA, USA, 105 pages.

30. ITGI (2008), IT Governance and Process Maturity, ISACA, USA, 102 pages.

31. ITGI (2009), *CobiT® User Guide for Service Managers*, ISACA, USA, 55 pages.

32. KLOSTERBOER Larry (2011), *ITIL.Capacity.Management*, Version 3, RECYCLED PAPER, Massachusetts, 205 pages.

33. LONGIN Pierre, DENET Henri (2008), *Construisez votre qualité : toutes les clés pour une démarche qualité gagnante*, 2e édition, DUNOD, Paris, 338 pages.

34. LÖNING Hélène, MALLERET Véronique, MERIC Jérôme, PESQUEUX Yvon, CHIAPELLO Ève, MICHEL Daniel, SOLE Andreù (2008), *Le contrôle de gestion : organisation, outils et pratiques*, 3e édition, DUNOD, Paris, 304 pages.

35. MARTIN Robert (2009), Coder proprement, PEARSON, 481 pages.

36. MEIER Olivier (2009), *DICO du manager*, DUNOD, Paris, 228 pages.

37. MOISAND Dominique, GARNIER DE LABAREYRE Fabrice (2009), *CobiT : Pour une meilleure gouvernance des systèmes d'information*, version 4.1, EYROLLES, Paris, 258 pages.

38. MORLEY Chantal (2008), *Management d'un projet système d'information : Principes, techniques, mise en œuvre et outils*, 6e édition, DUNOD, Paris, 458 pages.

39. MORLEY Chantal, BIA-FIGUEIREDO Marie, GILLETTE Yves (2011), Processus métiers et systèmes d'information, 3e édition, DUNOD, Paris, 309 pages.

40. MOUTON Daniel (2008), *La validation intégrée,* DUNOD, Paris, 210 pages.

41. OBERT Robert, MAIRESSE Marie-Pierre (2009), *DSCG 4 Comptabilité et audit : manuel et applications*, 2e édition, DUNOD, Paris, 625 pages.

42. OTTER Martine, SIDI Jacqueline, HANAUD Laurent (2009), *Guide des certifications SI,* 2e édition, DUNOD, Paris, 271 pages.

43. PRUD'HOMME Lionel (2009), *Performance des comités exécutifs,* édition d'organisation groupe EYROLLES, Paris, 196 pages.

44. REGNIER-PECASTAING Franck, GABASSI Michel, FINET Jacques (2008), *MDM enjeux et méthodes de la gestion des données,* DUNOD, Paris, 287 pages.

45. RENARD Jacques (2010), *Théorie et pratique de l'audit interne*, 7e édition, EYROLLES, Paris, 470 pages.