Exposé sous le thème : **Audit des systèmes d'information**

Plan

Introduction

La mondialisation des échanges, la globalisation des marchés, l'innovation technologique constituent des facteurs de multiplication des risques qui rendent la position des entreprises de plus en plus difficile à une échelle économique mondiale. Cette problématique, dans un univers où la quantité d'information et son accessibilité augmentent et se complexifient, nécessite d'adopter une attitude "anticipatrice" par une exploitation permanente des informations vitales pour l'entreprise.

Une entreprise ne pourra survivre que si elle dispose d'un ensemble d'informations suffisantes (information disponible, pertinente, fiable, précise et récente) pour pouvoir agir avec efficacité, c'est à dire prendre les bonnes décisions au bon moment, d'un ensemble de technologies pour suivre l'évolution des marchés, ainsi qu'un personnel compétent, d'où la nécessité d'un système d'informations.

Aujourd’hui les choix en matière de système d'information sont au cœur de la recherche de l'avantage concurrentiel, et non plus seulement au niveau de la simple amélioration du fonctionnement de l'organisation

L'avantage concurrentiel des organisations, grandes et petites, s'adossant à un système d'information optimisé, à l'heure d'une compétition mondiale de plus en plus exacerbée est plus que jamais à l'ordre du jour

Les coûts engendrés par la maintenance d’un système d’information sont très importants. Ceux-ci dépendent de nombreuses dimensions telles que les ressources humaines, informatiques ainsi que les aspects organisationnels. L’audit du système d’information aura pour but de permettre à l’entreprise de maîtriser ses coûts mais aussi de permettre une évolution vers de nouvelles technologies.

Donc dans quelle mesure l’audit des systèmes d’informations contribuera-t-il à l’amélioration de la qualité des systèmes d’informations et par conséquent à la compétitivité des entreprises ?

Chapitre 1 : Evolution des systèmes d’informations

La pérennité de l’entreprise dans les milieux concurrentiels nationaux et internationaux exige de cette dernière d’être capable de disposer le plus vite possible, au bon moment et avec un coût raisonnable d’une information de qualité susceptible d’aider les membres de l’organisation dans l’exercice dans leurs activités. En effet, les entreprises capables de prévoir l’évolution des marchés, de tenir comptes de besoins potentiels, d’identifier toutes les innovations technologiques, d’anticiper les modifications de comportement des acteurs économique (interne et externe à l’entreprise), politiques et sociaux maintiendront la faculté d’être compétitives.

Définition et évolution historique des SI

Définition

Le terme système d’information possède plusieurs définitions on peut présenter l’une d’elles.

« Le système d'information (SI) est l'ensemble **des informations** circulant dans l'entreprise et **des moyens** mis en œuvre pour les gérer ».[1]

Un système d'Information (noté SI) représente l'ensemble des éléments participant à la gestion, au traitement, au transport et à la diffusion de l'information au sein de l'organisation.

C’est Un ensemble organisé de ressources (personnel, données, procédures, matériel, logiciel, …) permettant d'acquérir, de stocker, de structurer et de communiquer des informations sous forme de textes, images, sons, ou de données codées dans des organisations. Selon leur finalité principale, on distingue entre :

- Systèmes d’information fonctionnels

Généralement chaque organisation est structurée par fonctions, chacune regroupent un certain nombre d’activités. L’utilisation de systèmes d’information de gestion à pour but de soutenir chacune des fonctions de l’entreprise: Marketing, fabrication, gestion des ressources humaines, gestion des opérations et de la production, comptabilité et finance. Le système d’information fonctionnel est utilisé pour décrire les divers types de systèmes d’information de ces fonctions.

Planification & Organisation

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

Acquisition & Installation

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

Livraison & Support

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

Surveillance

Permet au management d’évaluer la qualité et la conformité des processus informatiques aux exigences de contrôle.

CobiT fournit aux gestionnaires, auditeurs et utilisateurs de TI (Technologies de l’Information), des indicateurs, des processus et des meilleures pratiques pour les aider à maximiser les avantages issus du recours à des technologies de l'information et à l'élaboration de la gouvernance et du contrôle d'une entreprise. Il les aide à comprendre leurs systèmes de TI et à déterminer le niveau de sécurité et de contrôle qui est nécessaire pour protéger leur entreprise, et ceci par le biais du développement d’un modèle de gouvernance IT tel que CobiT. Ainsi, CobiT fournit des indicateurs clés d’objectif, des

indicateurs clés de performance et des facteurs clés de succès pour chacun de ses processus. Le modèle CobiT se focalise sur ce que l'entreprise a besoin de faire et non sur la façon dont elle doit le faire.

CMMI, le référentiel de conduite de projet

CMMI (Capability Maturity Model Integration) est un référentiel d'évaluation pour le développement de systèmes, de produits matériels et/ ou logiciels. Ce référentiel a été développé en 1987 et mis au point par le SEI (Software Engineering Institute) à Pittsburg afin de prendre le relais du CMM (Capability Maturity Model). C'est un référentiel de bonnes pratiques orienté vers le développement logiciel et la gestion de projet afférente. Il représente une avancée importante dans le monde de l'ingénierie des systèmes d'information.

Il permet aux entreprises de mesurer leurs pratiques de développement et de définir un plan d'actions en vue de tendre vers l'excellence.

CMMI évalue et certifie les organisations (ex. : département des études) et non les individus.

Il est structuré en 25 domaines de processus clés (process area) répartis en quatre disciplines (management des processus, management de projet, ingénierie et support). À chaque domaine de processus est attribuable un niveau de capacité qui lui est propre (de 1 à 5).

L'objectif principal du référentiel est d'améliorer l'efficacité du département des études.

ITIL, le référentiel de gestion des services informatiques

ITIL a été inventé en 1989 en Grande Bretagne par le Central Computer & Telecom Agency (CCTA). Cet outil rassemble dans une bibliothèque d'ouvrages un ensemble de bonnes pratiques destinées à répondre aux besoins des directions des système d'information dans le domaine de la gestion des services informatiques. Le référentiel ITIL accorde une importance particulière aux notions de qualité de service et de productivité.

L'adoption des bonnes pratiques de l'ITIL par une entreprise lui permet d'assurer à ses clients (internes comme externes) un service répondant à des normes de qualité pré-établies au niveau international. C'est donc un label de qualité proche des normes de l'ISO par exemple.

ITIL permet, grâce à une approche par processus clairement défini et contrôlé, d'améliorer la qualité des SI et du support aux utilisateurs en créant notamment la fonction (au sens "département de l'entreprise") de Centre de services ou « Service Desk » (extension du « help desk ») qui centralise et administre l'ensemble de la gestion des systèmes d'informations. ITIL est finalement une sorte de "règlement intérieur" du département informatique des entreprises qui l'adoptent.

La norme ISO, 27002

ISO / IEC 27002 est plus un code de pratique, qu'une véritable norme ou qu'une spécification formelle telle que l'ISO/IEC 27001. Elle présente une série de contrôles (39 objectifs de contrôle) qui suggèrent de tenir compte des risques de sécurité des informations relatives à la confidentialité, l'intégrité et les aspects de disponibilité. Les entreprises qui adoptent l'ISO/CEI 27002 doivent évaluer leurs propres risques de sécurité de l'information et appliquer les contrôles appropriés, en utilisant la norme pour orienter l'entreprise.

La norme ISO 27002 n'est pas une norme au sens habituel du terme. En effet, ce n'est pas une norme de nature technique, technologique ou orientée produit, ou une méthodologie d'évaluation d'équipement telle que les critères communs CC/ISO 15408. Elle n'a pas de caractère d'obligation, elle n'amène pas de certification, ce domaine étant couvert par la norme ISO/IEC 27001.

La conduite d'une mission audit des SI[8]

• *Les 6 phases de la mission d'audit informatique*

- Définition de la mission : Établissement de la lettre de mission
- La planification de la mission
- La collecte des faits, la réalisation de tests,...
- Entretiens avec les audités
- Rédaction du rapport final,
- Présentation et discussion de ce rapport

1 - Définition de la mission : Établissement de la lettre de mission

• Partir des attentes du demandeur d'audit

• Ne pas hésiter à passer du temps à bien les comprendre

• Si c'est nécessaire faire un pré-diagnostic

• Établir une liste des questions

• Faire une lettre de mission (C'est un mandat au sens du Code Civil)

2 - Planification de la mission : le choix de la démarche

• Il faut dès le départ annoncer la démarche suivie

• Il faut détailler le programme de travail

• Prévoir suffisamment à l'avance la collecte des faits et les tests à organiser (délais souvent longs)

• Savoir limité le nombre des entretiens (c'est un très gros consommateur de temps et de délais)

3 - La collecte des faits, la réalisation des tests,...

• On ne peut pas se contenter des «dires» des audités, il faut se baser sur des faits

• On s'organise pour trouver les faits dont on a besoin :

Les tests, les jeux d’essais,…

Les mesures de performances (temps de réponses...)

Les incidents d’exploitation, les anomalies, les erreurs, les bugs,…….

• Les faits, rien que les faits, tous les faits

• La mission, toute la mission, rien que la mission

4 - Entretiens avec les audités

• Au contraire, spontanément les auditeurs se méfient des faits et ils ont tendance à préférer les opinions

• Au cours des entretiens, ne pas se disperser. Cibler les questions

• Se méfier des check-lists. Avoir une liste de thèmes

• Le nombre d’entretiens est une variable importante expliquant la durée de l’opération et la charge de travail

5 - Le rapport d’audit : la conception, la rédaction, la présentation

• Le rapport d’audit est un document de référence

• Importance de définir à qui il est destiné et comment il sera diffusé

• Commencer à le rédiger à partir de la moitié de la mission. Sur une mission de deux mois dès la fin du 1er mois

• Le corps du rapport doit, dans la mesure du possible, être traité dans l’ordre des questions d’audit se trouvant dans la lettre de mission

• Les recommandations doivent être classées en mesures à court terme, à moyen terme et à long terme

• Faire une synthèse en 2 pages (plus souvent 4)

Bâtir un plan d’action

La liste des recommandations ne fait pas un plan d’action

• Un certain nombre d’opérations complémentaires sont nécessaires :

Sélectionner les mesures et les hiérarchiser

Approfondir et compléter les actions

Effectuer des analyses complémentaires

Fixer les responsabilités

….

• Le plan d’action doit être validé par le management (Comité de direction ; comité de pilotage ; commission informatique …)

Souvent des moyens spécifiques doivent lui être affectés

Le suivi des recommandations et du plan d’action

Il est nécessaire de mettre en place un dispositif de suivi des recommandations et du plan d’action

• L’expérience montre que si on ne met pas en place un suivi des recommandations, elles ne sont pas appliquées, ou du moins on applique que celles qui ne posent pas de problèmes et les autres sont laissées à leur triste sort

• Il est donc nécessaire de mettre en place un suivi des mesures choisies

• Faire un point périodique sur le degré de mise en place des recommandations (tous les 3 ou tous les 6 mois)

• L’efficacité des audits informatiques se joue en partie sur la mise en place d’un suivi

Chapitre 4 : Etude de cas :

Mission : Sécurité des Systèmes d’Information et de Données de Maroc Télécom

Groupe Maroc Telecom

La norme internationale ISO 27001 publiée en novembre 2005 couvre tous les types d’organismes et :

- *Spécifie les exigences relatives à l’établissement à la mise en œuvre, au fonctio*nnement, à la surveillance et au réexamen, à la mise à jour et à l’amélioration d’un système de management de la Sécurité de l’Information (SMSI) dans le contexte des risques globaux liés aux activités de l’entreprise ;
- *A pour objectif principal la protec*tion de l’entreprise. Elle vise à préserver et valoriser l’image de marque, à prévenir les pertes financières, garantir la continuité de l’activité, protéger l’entreprise contre les attaques logique ou physique, les sabotages, les fuites d’informations et réduire le risque que l’information stratégique s’ébruite ou se perde ;
- *Constitue un code de bonnes pratiques pour la gestion de la sécurité de l’information et un référentiel international de certification des entreprises* **;**

Principales réalisations

***Col*lecte des documents existants en matière de sécurité de l’information :**

Un préalable indispensable à l’élaboration de la politique de sécurité de l’information, l’identification des vulnérabilités, des risques et des menaces des actifs informationnels de Maroc Télécom et l’évaluation de l’étendue des mesures de sécurité déjà en place réalisés par des cabinets internationaux:

Audits des Systèmes d’Informations ;

Audits de sécurisation des infrastructures techniques (Fixe, Mobile, Entreprise) ;

Environnement incendiaire ;

Étude de sécurisation des plates formes RI prépayées ;

Audit de sécurité d’accès physique des sites de Rabat et de Casablanca;

Étude des vulnérabilités et conséquence d’un désastre ;

Audits financiers ;

Audits Assurance ;

Document de la Qualité ISO 9001 ;

Code d'éthique

Convention collective pour l'ensemble des employés

Audits et prestations réalisés par la Direction Contrôle Général de Maroc Télécom ;

Maroc Télécom dispose ainsi d'éléments concrets et objectifs lui permettant d'évaluer ses vulnérabilités, de mesurer les enjeux et de définir la cible de sécurité

Intégration des composantes Sécurité de l'Information dans la cartographie des processus;

Formation certifiante théorique et pratique de 52 RSLs "Lead Auditor ISO 27001 :2005" ;

Campagne de sensibilisation de 11 000 collaborateurs, soit plus 95%de participation ;

Accord de confidentialité et clauses contractuelles « Sécurité de l'Information » de Maroc Télécom intégré depuis 2006 dans tous les contrats avec les tiers au niveau central et régional ;

Plus de 320 procédures et documents sécurité de l'information (Référentiel, Charte, Guides, Modes opératoires…) ;

PRA de l'ensemble des activités y compris les RHs ;

Plus de 190 Guides et modes opératoires informatiques et techniques ;

Sécurisation des réseaux de transmission et des centres de commutation ;

Contrats d'assurance couvrant tout le patrimoine d'IAM contre les dommages matériels et les pertes d'exploitation après dommages ;

Environ 3000h/j effectués par une équipe ;

*Plus de 700 managers ont suivi une formation pratique aux outils de la sé*curité de l'information ;

Plus de 350 audits opérationnels ont été réalisés (Centres techniques, Actels, Délégations, …)

Un audit à blanc est effectué en décembre 2006 par un cabinet externe qui conclut la conformité à 70%

FPRIVATE "TYPE=PICT;ALT=Votre navigateur ne "

Enjeux :

Poursuivre la mise en œuvre de la politique de sécurité et les contrôles de manière

Homogène sur les systèmes, ainsi que sa déclinaison sur l'ensemble du périmètre SI, réseaux et services ;

Maintenir la certification ISO 27001:2005 ;

Conclusions :

Le processus de certification a permit de contribuer à l'amélioration de l'efficacité,

la

*conduite du changement et la confiance des clients, des actionnaires e*t des collaborateurs;

*La SÉCURITÉ de l'INFORMATION et la PERFORMANCE ne sont finale*ment pas des concepts contradictoires. La mise en œuvre de solutions de sécurité peut engendrer des économies substantielles et contribuer à améliorer la productivité de l'entreprise.

Conclusion :

Généralement, les risques liés au fonctionnement courant du système d'information sont cernés par le commissaire aux comptes et intégrés dans son approche de la mission. Mais tout système comprend des exceptions qui dérogent aux règles de contrôle interne. Le système d'information n'échappe pas à cet état de fait. Ces exceptions sont nécessaires au bon fonctionnement de l'entreprise, elle lui confère une meilleure réactivité. Il est crucial pour le commissaire aux comptes de déceler ces exceptions et d'évaluer leur nuisance potentielle, car mal maîtrisées en interne, elles peuvent s'avérer très préjudiciables à la pérennité de l'entreprise.

Bibliographie :

- Les techniques de l’audit informatique, Yann DERRIEN, DUNOD
- L’audit informatique : Méthodes, règles, normes. M.Thorin, Edition Masson, Paris 1991
- Audit informatique : Approche juridique et sociale, J-P.Ravalic, Edition Delmas, Paris 1991
- Construire le système d’information de l’entreprise. C. Grenier et C. Moine, Edition Foucher, Paris, 2003.
- Management des systèmes d’informations. Marie-Helene, DUNOD 2003
- Stratégie appliquée à l’audit des systèmes d’informations. Carlier Alphonse 1994

Articles :

- Journée de Réflexion sur l’Audit Démarche d’audit des Systèmes d ’information Cabinet MASNAOUI MAZARS ; ENCG Agadir, le 1 Mars 2003

Web :

- www.aud-it.ch/audit informatique.html
- www.octo.com/Audit-de-SI.28
- www.auditsi.eu/?p=428
- www.auditware.fr/missions/auditsecSI.htm