UNIVERSITÉ DU QUÉBEC

ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

DÉPARTEMENT DU GÉNIE LOGICIEL ET DES T.I.

Travail de session

Intégration de Sarbanes-Oxley au modèle de maturité

présenté à Monsieur Alain April

par Alexandre Lauzon (LAUA09018003)

dans le cadre du cours

MGL804 Réalisation et maintenance de logiciels

Groupe 01

21 avril 2011

Table des matières

Liste des figures

Liste des tableaux

Lexique

Terme	Définition
Cobit	*Control objectives for Information and Technology* Cadre de référence ainsi qu'un ensemble d'outils pour assurer la maîtrise et surtout le suivi (audit) de la gouvernance des processus informatique. Site web : http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
COSO	*Committee Of Sponsoring Organizations of the Treadway Commission* Référentiel de contrôle interne utilisé dans le cadre de la mise en place des dispositions relevant des lois financières telle que la loi Sarbanes-Oxley. Site web: http://www.coso.org/
S3M	Modèle de maturité de la maintenance du logiciel visant une approche d'amélioration qui offre aux organisations les éléments essentiels pour l'optimisation des processus de la maintenance applicative du logiciel Site web : http://www.s3m.ca
SOX ou SOA	*Sarbanes-Oxley Act of 2002* Loi américaine sur la réforme de la comptabilité des sociétés cotées et la protection des investisseurs. Site web : http://www.sec.gov/about/laws/soa2002.pdf

1. Introduction

Mise en contexte

Au début des années 2000, quelques scandales financiers d'importance ont frappé de plein fouet le système économique des États-Unis. Au mois d'octobre 2001, le très médiatisé scandale de la compagnie Enron voit le jour. Encore de nos jours, les analystes affirment que ce scandale fut l'un des plus importants de l'histoire américaine. Et comment ! Au total, plusieurs milliards de dollars américains furent perdus par la totalité des actionnaires de cette compagnie du Texas. En quelques semaines seulement, le cours de l'action d'Enron est passé de 90$ US à moins de 1$ US. Finalement, au mois de décembre 2001, la compagnie Enron fait faillite et devient, par le fait même, la plus grande faillite d'une entreprise américaine. Cette marque fut malheureusement battue l'année suivante à la suite d'un autre scandale financier par la compagnie Worldcom.

L'origine du scandale d'Enron provient du fait que les hauts dirigeants avaient réussit à cacher au conseil d'administration d'importantes dettes et à gonfler artificiellement les profits de la compagnie. De plus, les gestionnaires de l'entreprise avaient également effectué des pressions auprès des auditeurs pour qu'ils ignorent cette situation dans les rapports financiers de la compagnie. Suite à ces falsifications des rapports financiers, il est évident que le cours de l'action à la bourse ne reflétait pas la juste réalité financière de l'entreprise. Cette fâcheuse situation a eu des répercussions néfastes sur les investisseurs, notons principalement d'importantes pertes financières ainsi qu'une perte de confiance envers l'intégrité du système financier.

Afin de répondre à ces scandales financiers à répétition et rétablir la confiance des investisseurs, la loi Sarbanes-Oxley a été adoptée par le congrès américain au mois de juillet 2002. Celle-ci est le fruit d'une initiative des sénateurs Paul Sarbanes et Michael G. Oxley. Cette loi est également connue sous le nom de « *Public Company Accounting Reform and Investor Protection Act of 2002* » ou plus simplement SOX ou SOA. Bien que cette loi soit américaine, elle touche la totalité des compagnies cotées à la bourse de New York. Ce faisant, certaines entreprises qui ont pignon sur rue en sol canadien doivent s'y conformer. Néanmoins, une loi canadienne similaire, soit la loi C-198, voit le jour quelques années plus tard et reprend essentiellement les grandes lignes de la loi américaine. Dans les deux cas, ces lois ont établit une série de nouvelles réglementations afin d'éviter la reproduction de scandales financiers à la Enron. Parmi ceux-ci, mentionnons notamment l'obligation pour les dirigeants des entreprises de garantir personnellement l'exactitude des rapports financiers et l'obligation d'avoir recours à des auditeurs indépendants pour assurer l'impartialité des audits effectués au sein de la compagnie. Suite à la création de la loi américaine, plusieurs autres pays ont emboîté le pas et ont créé à leur tour des lois pour protéger les investisseurs : France (Loi de sécurité financières - 2003), Australie (CLERP 9 - 2004) et Japon (J-SOX - 2006).

Survol de la loi Sarbanes-Oxley

La loi Sarbanes-Oxley [SOX02] comporte 11 sections qui regroupent plusieurs articles décrivant les différentes réglementations ou dispositions que les entreprises doivent respecter. Ces différentes sections couvrent principalement les sujets suivants : l'indépendance des vérificateurs,

l'importance d'une saine gouvernance des entreprises, l'évaluation du contrôle interne et amélioration de la communication financière. La loi décrit également la création d'un organisme à but non lucratif, soit le « *Public Company Accounting Oversight Board »,* qui a pour mission de définir les standards d'audits et de surveiller le suivi de ces standards par les vérificateurs internes des compagnies publiques [PCAOB]. Cet organisme a également comme mandat de promouvoir l'importance d'effectuer la préparation d'audits juste et indépendant.

En terme de conformité, les articles de la loi Sarbanes-Oxley les plus importants sont sans aucun doute les articles 302 et 404. En effet, l'article 302 [SOX02, p. 33] met l'emphase sur les responsabilités des entreprises concernant la divulgation intègre des rapports financiers. Plus particulièrement, cet article explique l'obligation pour les dirigeants d'une entreprise d'apposer leur signature et de certifier l'exactitude des rapports financiers. Cet article stipule également que les dirigeants doivent divulguer tout changement effectué aux contrôles internes depuis la dernière évaluation. Pour sa part, l'article 404 [SOX02, p. 45] exige que les dirigeants produisent et divulguent un rapport de contrôle interne à même les rapports financiers annuels de la compagnie. Ce rapport doit mentionner la responsabilité de la haute direction de l'entreprise à mettre en place et de maintenir des procédures et des contrôles pour assurer l'intégrité des rapports financiers. De plus, le rapport de contrôle interne doit également contenir une évaluation de l'efficacité des contrôles déployés par l'entreprise. Finalement, cette évaluation doit être validée et attestée par une firme indépendante de vérificateurs.

Bref, ces deux articles de SOX décrivent les responsabilités des dirigeants à garantir l'exactitude du processus de création des rapports financiers pour permettre aux investisseurs d'avoir une représentation fidèle de la santé financière de leur entreprise. Cette nécessité de mettre en place des contrôles pour assurer l'intégrité des données amène son lot d'interrogations. Premièrement, quels sont les outils et les cadres de références que disposent les dirigeants d'entreprise pour les aider à répondre aux exigences de Sarbanes-Oxley? Plus particulièrement, quelles sont les mesures concrètes que doivent prendre les compagnies afin de répondre à ces exigences?

Dans un même ordre d'idée, pour être en mesure de certifier l'intégrité des données publiées dans les rapports financiers, les dirigeants doivent en premier lieu être capables de prouver qu'ils contrôlent les systèmes informatiques utilisés pour produire ces données. En effet, de nos jours, la grande majorité des données des rapports financiers proviennent de systèmes informatiques déployés au sein de l'entreprise. Or, les dirigeants devront démontrer l'existence et l'efficacité de processus permettant d'effectuer la gestion des accès et la protection adéquate des données financières contenues dans ces systèmes. Ainsi, dans un contexte de maintenance informatique, quelles sont les étapes nécessaires afin d'intégrer les obligations de Sarbanes-Oxley dans le modèle de maturité S3M?

La prochaine section de ce document fera une description sommaire des cadres de références présentement disponibles sur le marché pour répondre à SOX.

2. Cadres de références

COSO

Le COSO (*Committee Of Sponsoring Organizations of the Treadway Commission*) est un organisme à but non lucrative qui a été fondée en 1985 afin d'aider les organisations à améliorer la qualité de l'information financière par l'éthique des affaires, les contrôles internes et les bonnes pratiques de gouvernance d'entreprise. En 1992, cet organisme a défini un cadre de référence commun pour les contrôles internes sur lequel les entreprises peuvent se baser pour créer et évaluer leurs propres systèmes de contrôles internes. Ce cadre de référence est communément appelé le COSO, ou plus spécifiquement le « *Internal Control Framework* » [COS92]. Étant donné que la loi Sarbanes-Oxley exige l'utilisation d'un cadre de contrôle interne approprié, COSO fut le principal cadre de référence utilisé par les organisations afin de se conformer à SOX [ITG06 p. 57].

Le cadre de référence COSO définit le contrôle interne comme étant un processus effectué par les différents gestionnaires d'une entreprise afin de fournir une « assurance raisonnable » quant à la réalisation des objectifs suivants [COS92] :

- Efficacité et efficience des opérations;
- Fiabilité des informations financières;
- La conformité aux lois et règlements applicables.

Le cadre de référence COSO définit également 5 composantes nécessaires [COS92] afin de mettre en place des contrôles internes adéquats au sein d'une entreprise.

Tableau 1 - Les 5 composantes du COSO

Composante	Description
Environnement interne	Les individus avec leurs qualités individuelles, mais surtout leur intégrité, leur éthique, leur compétence et l'environnement dans lequel ils opèrent sont l'essence même de toute organisation. Ils en constituent le socle et le moteur
Évaluation des risques	L'entreprise doit être consciente des risques et les maîtriser. Elle doit fixer des objectifs et les intégrer à toutes ses activités. Elle doit également instaurer des mécanismes permettant d'identifier, analyser et gérer les risques correspondants.
Activités de contrôle	Les politiques et les procédures de contrôle doivent être élaborées et appliquées pour s'assurer que les mesures identifiées par les dirigeants sont exécutées efficacement pour réduire les risques liés à la réalisation des objectifs. Les activités de contrôles comprennent les revues du contrôle interne, les protections physiques, la séparation des tâches et les contrôles des systèmes d'information.

Information et communication	Une communication efficace permet de s'assurer que l'information circule du haut vers le bas, et ce, à travers toutes les unités de l'organisation. Les contrôles internes sont communiqués et les employés reconnaissent leur responsabilité à les respecter. Il existe des procédures formalisées pour les gens à signaler les suspicions de fraude.
Surveillance	Un processus qui évalue la qualité des contrôles doit être mis en place au sein de l'organisation. Les déficiences qui sont trouvées lors des évaluations périodiques sont déclarées aux dirigeants et une action corrective voit le jour afin d'améliorer le contrôle interne délinquant.

Suite aux scandales financiers du début des années 2000, l'organisme COSO a mis en place une deuxième version améliorée de son cadre de référence. Cette nouvelle version accentue l'emphase sur la robustesse des contrôles internes à déployer et sur les pratiques de bonne gouvernance des entreprises. Malheureusement, les deux versions du COSO offrent très peu d'informations concernant les contrôles internes à mettre en place pour tout ce qui entoure la conformité des systèmes informatiques [ITG06 p. 57]. En fait, l'objectif principal du référentiel COSO est de décrire les composantes nécessaires pour mettre en place un système global de contrôles internes au sein d'une entreprise, et ce, sans mettre l'emphase spécifiquement sur le volet informatique. Suite à ce constat, les compagnies se sont plutôt tournées vers le cadre de référence COBIT pour adresser les problèmes de conformité de leurs départements informatiques.

COBIT

La première version du cadre de référence COBIT (*Control Objectives for Information and* related Technology) a été créée en 1996 par ISACA (*Information Systems Audit and Control Association*) et ITGI (*IT Governance Institute*). COBIT est en fait un répertoire de bonnes pratiques pour optimiser la gouvernance des TI. Ce cadre de référence met l'emphase sur la conformité réglementaire et est utilisé principalement par les auditeurs internes et externes pour déterminer si une compagnie est en contrôle de leur processus TI. Fait intéressant, COBIT a été élaboré en reprenant et en se basant sur les différents éléments des contrôles internes établis par le COSO. Ainsi, COBIT est présentement reconnu sur le marché comme le cadre de référence par excellence pour implémenter les contrôles internes dans les services informatiques [COB07].

La version actuelle de COBIT, soit la version 4.1, a été publiée en 2007. Elle comporte une définition de 34 processus TI et plus de 215 activités répartis sous 4 domaines [COB07] :

- la planification et l'organisation ;
- l'acquisition et la mise en place ;
- la distribution et le support ;
- la surveillance.

Comme l'illustre la figure 1, l'utilisation combinée des cadres de références COSO et COBIT permettent d'adresser adéquatement la réglementation des articles 302 et 404 de SOX [ITG06 p.

54]. En effet, comme il a été mentionné précédemment, COSO doit être principalement utilisé pour insérer des contrôles internes au niveau de l'entreprise, tandis que COBIT est la référence de prédilection afin de mettre en place ces contrôles dans les processus informatiques.

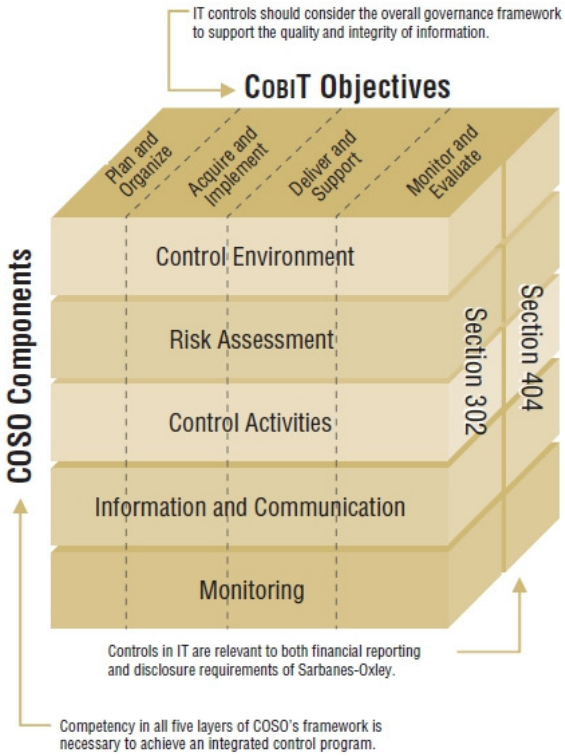

Figure 1 - Référence croisée de COSO et COBIT

Parmi les 34 différents processus définis dans COBIT, plusieurs décrivent des activités servant à respecter la conformité et deviennent, par le fait même, très utiles afin de respecter la réglementation de la loi Sarbanes-Oxley. Par contre, étant donné le nombre important de ces processus, le travail de recherche permettant à une organisation de déterminer les processus COBIT affectés par SOX pourrait s'avérer fastidieux. De plus, les personnes effectuant cette recherche pourrait oublier un processus important à considérer pour s'assurer d'une bonne conformité au sein de leur entreprise.

Afin d'aider les compagnies à évaluer et mettre en place des contrôles internes adéquats, le *IT Governance Institute* a créé au mois d'avril 2004 une liste de 12 objectifs qui doivent être pris en considération pour se conformer aux exigences de SOX [ITG06 p. 11]. Ces différents objectifs enrobent les principales activités d'un département informatique, en passant par les processus d'achat de logiciels, la gestion de l'infrastructure, les opérations, la gestion des changements et la gestion des données. Tel que spécifié par le *IT Governance Institute*, les entreprises ont la responsabilité de déterminer les éléments qui s'appliquent à leur contexte parmi la liste de ces 12 objectifs.

Le *IT Governance Institute* a également poussé leur recherche plus loin en établissant la relation entre la liste de leurs 12 objectifs et les processus définis dans le cadre de référence COBIT

[ITG06 p. 11]. La figure 2 ci-dessous illustre cette relation en identifiant les 12 objectifs du *IT Governance Institute* et la liste de tous les processus COBIT qui sont requis afin de répondre aux exigences des articles 302 et 404 de SOX. Ce travail de recherche constitue donc un élément essentiel pour toute organisation qui désire implémenter des contrôles internes pour répondre aux obligations de SOX dans leur département informatique. Étant donné que le travail de définition des processus requis COBIT a déjà été effectué, le travail de mise en place de contrôles internes autour de ces processus est grandement facilité.

Figure 1—Mapping to PCAOB and COBIT

	COBIT	PCAOB IT General Controls			
IT Control Objectives for Sarbanes-Oxley	**Mapping to COBIT 4.0 Processes**	**Program Development**	**Program Changes**	**Computer Operations**	**Access to Programs and Data**
1. Acquire and maintain application software.	AI2	●	●	●	●
2. Acquire and maintain technology infrastructure.	AI3	●	●	●	
3. Enable operations.	AI4	●	●	●	●
4. Install and accredit solutions and changes.	AI7	●	●	●	●
5. Manage changes.	AI6		●		●
6. Define and manage service levels.	DS1	●	●	●	●
7. Manage third-party services.	DS2	●	●	●	●
8. Ensure systems security.	DS5			●	●
9. Manage the configuration.	DS9			●	●
10. Manage problems and incidents.	DS8, DS10			●	
11. Manage data.	DS11			●	●
12. Manage the physical environment and operations.	DS12, DS13			●	●

Figure 2 - Relation entre les objectifs de contrôle IT et les processus de COBIT

3. Intégration de SOX dans S3M

Vue sommaire de la démarche

Comme nous l'avons vu à la section précédente, le travail de recherche effectué par le *IT Governance Institute* a clairement identité la liste des processus du cadre de référence COBIT impactés par la loi Sarbanes-Oxley. Cette liste de processus est facilement accessible pour une entreprise qui désire implémenter des contrôles internes au sein de ses processus organisationnels. Afin d'intégrer les obligations de SOX au modèle de maturité pour la maintenance, il sera nécessaire d'effectuer le même type de recherche et d'effectuer à nouveau la relation entre cette liste de processus COBIT et les processus du S3M.

La première étape de ce travail consiste donc à trouver un processus du S3M qui s'arrime et répond aux exigences de chaque processus COBIT qui se retrouve dans la liste définit par le *IT Governance Institute* (voir figure 2 à la section précédente). Or, pour il est possible d'éliminer immédiatement quelques processus de cet exercice de recherche. En effet, certains de ces processus ne concernent pas le domaine de la maintenance. En fait, cette situation touche plus spécifiquement quatre processus, soit « *AI3 – Acquire and maintain technology insfrastructure* », « *DS5 – Ensure systems security* », « *DS11 – Manage Data* » et « *DS12 – Manage the physical environment* ».

Le processus « *AI3 – Acquire and maintain technology insfrastructure* » [COB07 p. 81] concerne tout ce qui a attrait à l'infrastructure technique à mettre en place pour être en mesure de fournir un service informatique adéquat au sein de l'entreprise. Ce processus décrit entre autre la nécessité de produire un plan d'acquisition et de maintenance de l'infrastructure technologique et de s'assurer que cette infrastructure respecte les standards définis par l'organisation. De plus, ce processus explique toute l'importance de créer des environnements de développement et de tests pour supporter les tests qui seront effectués sur les différents logiciels de l'entreprise. Bien que le groupe de maintenance profite de la présence de cette infrastructure, les personnes qui auront à l'implémenter sont principalement le personnel d'infrastructure et des opérations. Bref, ce processus ne possède aucun lien concret avec le groupe de maintenance logicielle et ne doit pas être couvert par le modèle de maturité du S3M.

Pour sa part, le processus « *DS5 – Ensure systems security* » [COB07 p. 117] met l'emphase sur l'importance de protéger l'intégrité de l'information et de l'infrastructure physique des systèmes informatiques de l'organisation. Pour ce faire, le processus décrit la nécessité de définir une politique de sécurité informatique, d'effectuer la gestion des accès aux utilisateurs et de mettre en place des contrôles internes afin de surveiller et détecter les failles de sécurité au réseau informatique de l'entreprise. Encore une fois, les exigences de ce processus n'ont aucun lien direct avec le groupe de maintenance, mais seront plutôt adressées par le groupe de sécurité du département informatique.

Tant qu'à lui, le processus « *DS11 – Manage Data* » [COB07 p. 141] expose la nécessite de protéger et assurer la disponibilité des données de l'entreprise. Pour effectuer cette tâche, le processus détaille la nécessité d'effectuer la gestion des bases de données, de procéder à des copies de sauvegarde des données (incluant la gestion d'entrepôts de données externes à

l'entreprise) et à concevoir des plans de restauration des données. Ce processus ne touche en rien à la maintenance logicielle et impliquera plutôt la participation des administrateurs de bases de données. Ces derniers font encore une fois partie du groupe d'infrastructure et des opérations.

Finalement, le processus « *DS12 – Manage the physical environment* » [COB07 p. 145] explique la nécessité d'assurer la protection de l'environnement physique de l'infrastructure informatique d'une organisation. Par exemple, le processus mentionne l'importance de mettre en place des mesures de sécurité pour protéger l'accès aux serveurs seulement au personnel qualifié. De plus, le processus décrit la nécessité de bien sélectionner l'emplacement des serveurs afin de diminuer les interruptions des activités de l'entreprise et d'assurer la protection du matériel et des données vis-à-vis l'environnement extérieur. À nouveau, ce processus est clairement sous la responsabilité du groupe de l'infrastructure et des opérations et ne possède aucun lien avec le groupe de maintenance.

En excluant ces 4 processus de la liste initiale, il nous reste donc un total de 10 processus COBIT pour lesquels on doit trouver un itinéraire S3M équivalent. La section suivante comprend donc le détail de cette recherche.

Itinéraires S3M requis pour SOX

Le processus « *AI2 – Acquire and maintain application software* » [COB07 p. 77] met l'emphase sur l'importance de mettre en place un processus de développement de logiciel performant afin d'aligner les applications informatiques avec les besoins d'affaires et opérationnels de l'entreprise, et ce, dans un coût et un délai de temps raisonnable. D'un point de vue de la maintenance, l'objectif de contrôle qui nous intéresse le plus est « *AI2.10 Application Software Maintenance* » qui indique que le service informatique doit développer une stratégie et un plan pour supporter les applications informatiques des usagers. Pour ce qui est du modèle de maturité du S3M, cet objectif est couvert par l'itinéraire « Évo3 – Évolution et correction du logiciel ». En effet, cet itinéraire stipule que l'évolution et la correction du logiciel font appel aux activités de mise en œuvre similaires aux activités du développeur afin d'implanter ces modifications [Apr06 p. 243]. Plus spécifiquement, cet itinéraire mentionne également que toutes les activités nécessaires pour modifier le logiciel doivent suivre un processus normalisé. Un autre objectif important de cet itinéraire est que le mainteneur s'assure de bien modifier le logiciel afin de répondre aux exigences du client.

Le processus « *AI4 – Enable operation and use* » mentionne que la connaissance des nouveaux systèmes doit être mise à la disposition aux utilisateurs et personnel des TI par la création de documentation, de manuels et de la formation qui permettra une bonne utilisation des systèmes [COB07 p. 85]. Parmi les différents objectifs de contrôle de ce processus, celui qui nous intéresse le plus en terme de maintenance est l'objectif « *AI4.4 Knowledge Transfer to Operations and Support Staff* ». En effet, cet objectif stipule qu'un transfert de connaissances sur un logiciel doit être fait pour permettre au personnel technique d'assurer un support efficient et une maintenance adéquate sur le logiciel. Du côté du S3M, l'itinéraire « Évo1 – Transition du logiciel vers la maintenance » du S3M est directement en lien avec cet objectif et décrit la transition du logiciel comme un des processus clés de la maintenance du logiciel [Apr06 p. 231]. D'ailleurs, un des buts de cet itinéraire est d'obtenir de l'information et les connaissances nécessaires afin de permettre au personnel de la maintenance de prendre en charge un logiciel.

Le processus « *AI6 – Manage changes* » met l'emphase sur le fait que tous les changements, y compris l'entretien d'urgence et des correctifs apportés à un logiciel dans l'environnement de production, sont officiellement gérés de manière contrôlée [COB07 p. 93]. En terme de maintenance, l'objectif de contrôle qui nous intéresse le plus est « *AI6.2 Impact Assessment, Prioritisation and Autorisation* ». Cet objectif décrit l'importance d'évaluer toute demande de changement et de s'assurer que chacune de ces demandes sont priorisées, catégorisées et autorisées. Or, l'itinéraire « Req1 – Gestion des requêtes de service et des événements » du S3M est directement en lien avec cet objectif. En effet, les buts de cet itinéraire sont justement d'identifier les nouvelles requêtes de services, d'en évaluer l'importance vis-à-vis le travail présentement effectué et de s'assurer auprès des utilisateurs que l'on travaille sur les bonnes priorités [Apr06 p. 195].

Le processus « *AI7 – Install and accredit solutions and changes* » [COB07 p. 97] mentionne qu'un nouveau système ou un système modifié doit être fonctionnel sans défauts majeurs à la suite de la livraison aux utilisateurs. Pour ce faire, le processus définit la nécessité d'effectuer des tests dans un environnement de test, de s'assurer que l'application se comporte comme prévu et répond aux exigences des utilisateurs. Ce processus comporte plusieurs objectifs de contrôles qui sont très importants dans un contexte de maintenance. Par exemple, l'objectif « *AI7.2 Test Plan* » exprime la nécessité de créer un plan de test pour les changements apportés au logiciel. Pour sa part, l'objectif « *AI7.6 Testing of Changes* » s'occupe d'effectuer les tests définis dans le plan de test. Puis, l'objectif « *AI7.7 Final Acceptance Test* » mentionne l'importante d'effectuer une revue des résultats obtenus lors des tests, de s'assurer que les changements apportés répondent aux exigences et d'obtenir l'autorisation des utilisateurs afin de procéder à la mise en production de la modification. Du côté du modèle de maturité S3M, nous retrouvons également un itinéraire qui s'occupe de toute activité entourant le processus des tests, soit l'itinéraire « Évo4 – Vérification et validation ». En effet, l'objectif principal de cet itinéraire est de s'assurer qu'il y a une planification des activités de vérification et validation et de démontrer que le travail de maintenance rencontre les exigences spécifiées [Apr06 p. 250].

Le processus « *DS1 – Define and manage service levels* » [COB07 p. 101] définit la nécessité de définir et d'effectuer la gestion les ententes de services (SLA) avec les utilisateurs des systèmes informatique supportés par le groupe de maintenance. Pour sa part, le processus « *DS2 – Manage third-party services* » [COB07 p. 105] définit la nécessité d'effectuer une saine gestion des sous-traitants afin de rencontrer les niveaux de services établis avec les utilisateurs. Pour ce faire, le service informatique doit clairement définir les rôles et responsabilités des sous-traitants et mettre en place un processus de surveillance du bon respect des contrats signés entre ceux-ci et l'entreprise. Le modèle de maturité du S3M possède déjà un itinéraire qui est en lien avec les besoins de ces deux processus du COBIT. En effet, les principaux objectifs de l'itinéraire « Req4 – Gestion des requêtes de service et des événements » sont de déterminer les types de services requis pour chacun des logiciels, établir les ententes de service avec les utilisateurs et les sous-traitants, et mettre en place une structure pour assurer le respect de ces ententes [Apr06 p. 213]. Cet itinéraire mentionne également l'importance d'effectuer une évaluation périodique afin de modifier, au besoin, les ententes de services et renégocier les contrats avec les sous-traitants.

Le processus « *DS8 – Manage service desk and incidents* » [COB07 p. 129] explique les avantages à se doter d'un bureau d'aide afin de supporter plus efficacement et d'apporter des

résolutions rapides aux requêtes des utilisateurs. Bien que cela soit le personnel du bureau d'aide qui communique directement avec la clientèle lors d'une nouvelle requête, il n'en demeure pas moins que la groupe de maintenance sera appelé à jouer un rôle primordial dans la résolution du problème et pour respecter les ententes de services établies auprès des utilisateurs. Or, d'un point de vue maintenance, l'objectif de contrôle qui nous intéresse le plus dans ce processus est « *DS8.2 Registration of Customer Queries* ». En effet, cet objectif définit plus précisément qu'il faut mettre en place un processus et une application qui permet d'effectuer une saine gestion et le suivi des requêtes des utilisateurs. De plus, les requêtes doivent être catégorisées et priorisées selon les besoins de l'entreprise. Pour sa part, le modèle de maturité S3M comporte déjà un itinéraire d'améliorations qui est directement en lien avec ce processus, soit « Req1 – Gestion des requêtes de service et des événements ». Comme nous l'avons vu précédemment, un des objectifs de cet itinéraire est d'identifier et de catégoriser les nouvelles requêtes de services et de les prioriser selon les besoins de la clientèle [Apr06 p. 195].

Le processus « *DS9 – Manage the configuration* » [COB07 p. 133] définit la nécessité de garantir l'intégrité des configurations des composantes matérielles et logicielles qui entourent les systèmes informatiques. Pour ce faire, le processus décrit l'importance de la création d'un référentiel central pour effectuer la gestion de la configuration. D'un point de vue maintenance, l'objectif de contrôle qui nous intéresse le plus est « *DS9.1 Configuration Repository and Baseline* » qui mentionne l'utilisation d'un outil technique afin d'effectuer une saine gestion de ce référentiel de configuration. L'itinéraire « Sup1 – Management de la configuration et des environnements » du S3M est en lien direct avec ce processus. En effet, l'un des objectifs de cet itinéraire est l'utilisation d'un logiciel de support pour conserver une image de la configuration d'un logiciel [Apr06 p. 262]. Cette configuration peut contenir plusieurs éléments, dont le code source, la documentation et les documents d'analyse. En rendant cette information disponible à tout le personnel du groupe de maintenance, on s'assure que chacun des mainteneurs possèdent la dernière version de la documentation et du code source d'un logiciel spécifique.

Le processus « *DS10 – Manage problems* » [COB07 p. 137] décrit l'importance de mettre en place une gestion efficace des problèmes afin d'assurer la satisfaction des clients et de rencontrer les niveaux de services établis avec ces derniers. Pour ce faire, le processus mentionne que l'on doit identifier et classifier le problème, analyser et rechercher la cause principale, suivre l'évolution de la demande de modification et finalement résoudre le problème. Il existe encore une fois un processus du S3M qui est directement en lien avec ce processus du COBIT. En effet, l'objectif de l'itinéraire « Req1 – Gestion des requêtes de service et des événements » est de s'assurer que les défaillances et autres requêtes de support opérationnel soient identifiées, classées, ordonnées par priorités et traitées de façon à respecter les niveaux de services définis avec le client [Apr06 p. 195].

Finalement, le processus « *DS13 – Manage operations* » [COB07 p. 149] explique la nécessité d'assurer le bon fonctionnement des opérations des services informatiques et de respecter les niveaux de service attendus avec les utilisateurs. Par exemple, le processus mentionne l'importance d'effectuer de la maintenance préventive sur l'infrastructure et les composantes matérielles du réseau informatique de l'organisation. De plus, le processus décrit la nécessité de faire une saine gestion et d'optimiser la cédule de production pour assurer le bon déroulement des opérations. C'est à ce niveau que le groupe de maintenance peut jouer un rôle très important. En effet, pour permettre l'optimisation de la cédule de production et assurer le bon déroulement

des opérations, il faut prévoir effectuer du support en dehors des plages horaires régulières de travail. Il existe au sein du S3M un itinéraire, soit le « Évo2 – Support opérationnel », qui mentionne cet élément fort important de la maintenance. Cet itinéraire a pour but d'effectuer toutes les activités de support opérationnel qui ne comporte aucune modification au logiciel. Ainsi, l'un des objectifs principal de cet itinéraire est d'offrir un support adéquat des opérations en dehors des heures du travail [Apr06 p. 239].

Finalement, suite à ce travail de recherche, il est possible de constater avec la figure ci-dessous qu'il est possible d'effectuer une relation entre la grande majorité des processus COBIT qui sont impactés par SOX et les itinéraires du S3M. En fait, si on exclut les processus qui ne concernent pas spécifiquement le domaine de la maintenance, on peut constater que le S3M couvre adéquatement les requis de SOX selon les travaux effectués par le *IT Governance Institute.*

Processus de Cobit 4.1	Processus S^{3M}
AI2 – Acquire and maintain application software	Évo3
AI3 – Acquire and maintain technology infrastructure	Non applicable
AI4 – Enable operation and use	Évo1
AI6 – Manage changes	Req1
AI7 – Install and accredit solutions and changes	Évo4
DS1 – Define and manage service levels	Req4
DS2 – Manage third-party services	Req4
DS5 – Ensure systems security	Non applicable
DS8 – Manage service desk and incidents	Req1
DS9 – Manage the configuration	Sup1
DS10 – Manage problems	Req1
DS11 – Manage data	Non applicable
DS12 – Manage the physical environment	Non applicable
DS13 – Manage operations	Évo2

Figure 3 – Sommaire des relations entre les processus COBIT requis pour SOX et S3M

Assurance qualité de la conformité

La section précédente a permis d'effectuer la relation entre les processus COBIT requis pour SOX et les itinéraires du modèle de maturité du S3M. Par contre, afin de se conformer adéquatement à l'article 404 de Sarbanes-Oxley, il faut s'assurer du suivi de ces itinéraires par les différents employés du groupe de maintenance. En effet, il ne suffit pas seulement de définir les processus à mettre en place au sein de l'organisation, il est également requis d'effectuer un suivi constant du respect de ces processus afin de prouver hors de doute que la conformité n'est pas seulement un sujet d'actualité quelques semaines avant la venue d'un auditeur externe ! En fait, lors de la visite de l'un de ces auditeurs, il faudra justement lui démontrer que la conformité à SOX s'effectue sur une base régulière et que le groupe de maintenance possède la maturité nécessaire afin de respecter les procédures établies. Tout ceci amène donc la nécessité pour les

entreprises d'effectuer de l'assurance qualité du suivi des processus requis pour SOX et de suivre l'évolution de la conformité à l'aide de métriques.

Heureusement, le modèle de maturité du S3M a déjà prévu un itinéraire qui permet la gestion de l'assurance qualité des processus. En effet, l'itinéraire « Sup2 – Assurance qualité des processus, des services et des logiciels » permet de procéder à des révisions indépendantes et objectives des services et des produits de la maintenance [Apr06 p. 267]. À l'aide de cet itinéraire, un des membres de l'équipe d'assurance qualité pourra évaluer adéquatement le suivi des processus par le personnel de la maintenance. Afin d'obtenir une évaluation représentative et juste, il est essentiel que cette évaluation soit effectuée par un service interne de l'organisation, mais indépendant du groupe de maintenance informatique. Pour les besoins de la conformité, ce service devra donc vérifier sur une base régulière que toutes les activités entourant un processus impacté par SOX soient effectuées selon les procédures et la documentation de l'entreprise. Malheureusement, il est très fréquent que cette vérification soit manuelle et nécessite une charge de travail considérable.

À la suite d'une évaluation, l'auditeur doit préparer un rapport de conformité et communiquer le résultat aux employés du groupe de maintenance et aux différents gestionnaires TI. En cas de non-conformité, l'auditeur doit également documenter les défauts et des actions devront être prises afin de corriger le tir. Pour ce faire, l'auditeur doit en informer le responsable du groupe de maintenance et suggérer des moyens pour corriger la situation. En tout temps, l'auditeur doit obtenir le support des gestionnaires pour régler les cas problématiques.

Pour ce qui des métriques, l'auditeur devra identifier à l'aide du groupe de maintenance les processus clés à mesurer ou les processus problématiques qui nécessitent une attention particulière. Certaines métriques pourront donc voir le jour afin de suivre des processus non performants ou le non respect de certains contrôles internes. La diffusion de ces métriques peut facilement s'effectuer à l'aide de simples graphiques comprenant des mesures hebdomadaires ou mensuelles. L'objectif principal est de mesurer la performance du groupe de maintenance à respecter les contrôles internes et de visualiser rapidement l'évolution de la conformité des processus SOX par chacun des employés. La mise en place de ces métriques sera fort utile afin de discerner un relâchement du suivi des procédures et d'enclencher le processus d'actions correctives pour corriger la situation.

4. Conclusion

Pour conclure, l'objectif de ce travail de recherche était d'étudier la loi Sarbanes-Oxley et d'indiquer comment cette nouvelle obligation pouvait être intégrée au modèle de maturité pour la maintenance. Comme nous l'avons vu, il existe présentement plusieurs cadres de références sur le marché qui sont à la disposition des entreprises afin d'intégrer les exigences de SOX dans leur opérations quotidiennes. Bien que le COSO soit le cadre de référence généralement utilisé par les organisations pour adresser les problèmes de conformité, il a été démontré que celui-ci ne répondait pas aux besoins des entreprises d'un point de vue informatique. Pour cette raison, les auditeurs externes qui sont responsables de certifier la conformité des processus entourant les services et systèmes informatiques se sont plutôt tournés vers un autre cadre de référence, soit le COBIT. Afin d'aider les entreprises à bien utiliser ce cadre de référence pour rencontrer les obligations de SOX, le *IT Governance Institute* a également définit la liste de tous les processus définis à l'intérieur du COBIT qui sont impactés par la loi américaine. Or, pour intégrer les obligations de cette loi au modèle de maturité, il nous suffit tout simplement d'effectuer la relation entre la liste des processus COBIT impactés par SOX et les différents itinéraires du S3M. Ce travail d'association a été réalisé à l'intérieur de ce document et a permis de constater que le modèle de maturité du S3M offre déjà tous les itinéraires d'améliorations requis pour supporter un groupe de maintenance à respecter les exigences de SOX.

Toutefois, il a également été démontré que cette relation entre les processus du COBIT et du S3M n'était pas suffisante afin d'adresser les besoins de Sarbanes-Oxley. En effet, il ne suffit pas tout simplement de bien documenter les processus de la maintenance, mais il faut également s'assurer de les suivre. D'ailleurs, c'est à cette étape où la conformité prend tout son sens. Une organisation a beau posséder les meilleurs processus et contrôles internes, il faut néanmoins qu'elle soit en mesure de prouver qu'elle les contrôle, qu'elle les utilise à bon escient et que ses employés comprennent toute l'importance de leur raison d'être. À cet égard, l'auditeur interne a un très grand rôle à jouer et aide les gestionnaires de l'entreprise à rectifier le tir en cas de non-conformité. Par le fait même, l'utilisation de métrique devient essentielle pour vérifier le respect des contrôles internes et s'assurer de la conformité quotidienne des différents processus de l'entreprise.

5. Références

[Apr06] April, A. et Abran, A., Améliorer la maintenance du logiciel, 2006

[COB07] IT Governance Institute, COBIT Framework 4.1, 2007, [En ligne] : <http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT_4.1.pdf> (Consulté le 12 mars 2011)

[COS92] COSO, Internal Control - Integrated Framework, 1992, [En ligne] : <http://www.coso.org/IC-IntegratedFramework-summary.htm> (Consulté le 10 mars 2011)

[ITG06] IT Governance Institute, IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition, 2006, [En ligne] : <http://www.isaca.org/Knowledge-Center/cobit/Documents/ITCO-Sarbanes-OxleyResearch.pdf> (Consulté le 12 mars 2011)

[SOX02] Sarbanes-Oxley Act of 2002, 2002, [En ligne] : <http://www.sec.gov/about/laws/soa2002.pdf> (Consulté le 10 mars 2011)

[PCAOB] Public Company Accounting Oversight Board, [En ligne] : <http://pcaobus.org/Pages/default.aspx> (Consulté le 12 mars 2011)