ÉTS
Le génie pour l'industrie
École de technologie supérieure
L'ÉTS est une constituante du réseau de l'Université du Québec

MGL804 groupe 01

Travail individuel de session

Travail remis le 14 avril 2011

Daniel Doucet

Table des matières

Introduction *3*

SOX (Sarbanes-Oxley) *4*

SOX au Canada *5*

Tableau sommaire SOX - C198 5

SOX pour les TI *6*

SOX vs Maintenance logiciel 6

Contrôles - Cadres de travail *7*

COSO *7*

Cube COSO (Réf. COSOCUBE) 7

COBIT (Control OBjectives for Information and related Technologies) *8*

Modèle COBIT 8

Les Contrôles TI & SOX *9*

Les niveaux de maturités SOX, COBIT & S3M *10*

Tableau récapitulatif des niveaux de maturités. 10

Objectifs de contrôle SOX & COBIT *11*

IT Control Objectives for Sarbanes-Oxley - IT Governance Institute 11

SOX - Contrôles - Maturité(S3M) *12*

Réponses au 2 questions : *13*

Comment SOX peut être intégrer au modèle de maturité S3M *13*

Groupe de maintenance rencontre les obligations de SOX *14*

Conclusion *15*

Références *16*

Annexe *17*

1. Introduction

Nous avions dans le cadre de travail personnel de session à choisir un sujet défini dans le livre *Améliorer la maintenance du logiciel (Réf: APRIL)*. Le sujet choisi est le travail de session numéro 22 du livre (APRIL, p.122); i.e.

> #22 – Étudiez la proposition Sarbanes-Oxley (la loi canadienne équivalente) et indiquer comment cette nouvelle obligation peut-être intégrée au modèle de maturité.

Pendant la réalisation de ce mandat, j'ai consulté Dr. April (via courriel, 22 février 2011) sur le sujet et il m'a aussi donné comme orientation que ce travail devait répondre à la question suivante :

> «Si tu avais à mettre des pratiques spécifiques pour évaluer si le groupe de maintenance rencontre les obligations de SOX quelles seraient-elles? »

L'objectif de ce travail est de répondre à ces 2 questions.

Je vais dans un premier temps, présenter les lois Sarbanes-Oxley (États-Unis), la loi C-198 (Canada) et leur applicabilité.

Dans un deuxième temps, je présenterai les cadres de travail reconnus (COSO, COBIT) utilisés dans l'industrie pour effectuer les contrôles de conformité SOX en entreprise. Je présenterai ces cadres et leur portée dans un contexte de contrôle de conformité SOX pour les TI. J'aborderai plus spécifiquement les contrôles de conformité SOX pour un groupe de maintenance logiciel. Prendre note que ce travail est réalisé dans une perspective que le groupe de maintenance logiciel oeuvre dans une entreprise canadienne.

Dans un troisième temps, je présenterai le modèle de maturité S3M, ses liens avec les cadres de contrôle utilisés et comment la proposition Sarbanes-Oxley peut s'intégrer à ce modèle de maturité.

Finalement une conclusion sur ce travail, permettra de faire un retour sur les objectifs et les apprentissages.

2. SOX (Sarbanes-Oxley)

La loi Sarbanes Oxley Act (Pub. L. No. 107-204, 116 Stat. 745), aussi connue sous le nom de Public Company Accounting Reform and Investor Protection Act of 2002 ou plus simplement SOX ou Sarbox, a été adoptée par le congrès américain en Juillet 2002. Cette loi est l'initiative de deux sénateurs américains, Paul Sarbanes et Michael G. Oxley. Cette loi est la réponse aux multiples scandales comptables et financiers (Enron, WorldCom, TycoInternational). Cette loi a introduit en juillet 2002 (réf: WIKISOX)

- *L'obligation pour les présidents et les directeurs financiers de certifier personnellement les comptes ;*
- *L'obligation de nommer des administrateurs indépendants au comité d'audit du conseil d'administration ;*
- *L'encadrement des avantages particuliers des dirigeants (perte de l'intéressement en cas de diffusion d'informations inexactes, interdiction des emprunts auprès de l'entreprise, possibilité donnée à la SEC - Securities and Exchange Commission, l'autorité de régulation des marchés boursiers américains - d'interdire tout mandat social pour les dirigeants soupçonnés de fraude).*
- *Cette loi oblige aussi à mettre en œuvre un contrôle interne s'appuyant sur un cadre conceptuel. En pratique le COSO est le référentiel le plus utilisé.*

La loi Sarbanes Oxley (SOX), est une loi qui vise à protéger les investisseurs. La loi impose de nouvelles règles concernant la comptabilité et la transparence financière. SOX vise principalement à parer les investisseurs et s'assurer de l'intégrité des informations financières produites par les entreprises cotées en bourse.

Les obligations envers les dirigeants de produire et garantir des états financiers trimestriels intègres sont documentés dans les articles 302 et 404 de la loi SOX. Ces obligations ne s'arrêtent pas à la production des rapports mais englobe aussi la garantie que les données comptables et les logiciels utilisés à les produire sont intègrent. Afin de rencontrer ces obligations, l'entreprise devra documenter qui a des accès à ces données et s'assurer que ces informations sont communiquées.

L'entreprise aura l'obligation de communiquer quels sont les dirigeants et les responsables ayant accès aux données financières et s'assurer d'une disponibilité maximale des systèmes responsables de l'information financière.

3. SOX au Canada

La loi SOX est une loi américaine et s'applique à toutes les entreprises cotées en bourse américaine. La loi s'applique aux entreprises cotées aux États-Unis, pour cette raison, la législation canadienne a tenté d'arrimer sa loi aux obligations américaines. Au Canada SOX est la loi C-198 et se veut une loi qui est adaptée au contexte canadien. Elle s'applique aux grandes entreprises.

Parce que les grandes entreprises sont généralement cotées aux États-Unis elles sont soumises à SOX 404. Pour la petite et la moyenne entreprise, qui ne sont généralement pas cotés aux États-Unis, pourraient être exemptées à SOX 404 ou le règlement 52-111 de la loi C-198.

Le tableau suivant présente les principaux règlements relatifs à l'information financière.

SOX États-Unis	C-198 Canada
Compagnies publiques et filiales 2002	Compagnies publiques et filiales 2004
SOX 302 | Règlement 52-109 Attestation trimestrielle et annuelle concernant la **divulgation de l'information financière** Rapports Financiers	
SOX 404 | Règlement 52-111 **Rapport annuel sur les contrôles internes à l'égard de l'information financière** Contrôles Internes	

Tableau sommaire SOX - C198

Le 10 mars 2006, les Autorités canadiennes en valeurs mobilières (les « ACVM ») ont annoncé après une vaste consultation, de ne pas mettre en vigueur le projet de Règlement 52-111 sur les rapports sur le contrôle interne à l'égard de l'information financière. Les ACVM proposent plutôt de modifier le Règlement 52-109 sur l'attestation de l'information présentée dans les documents annuels et intermédiaires des émetteurs afin d'y inclure des dispositions additionnelles sur le contrôle interne à l'égard de l'information financière.

Les entreprises dont les actions transigent au Canada et aux États-Unis sont obligées de se conformer aux deux lois.

4. SOX pour les TI

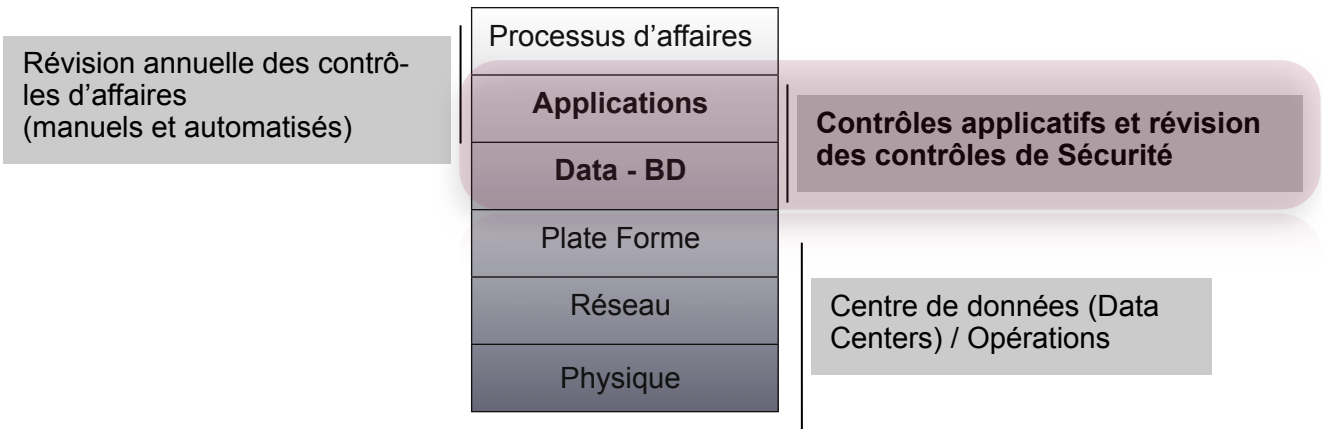
La composition actuelle des entreprises est principalement ses ressources, ses processus d'affaires et ses outils (people, process & tools). L'information et la TI sont des actifs de l'entreprise, on parle de plus en plus de ressource informationnelle (réf: RESSINFO).

> Ressource informationnelle: **Définition** : Ressource utilisée par une entreprise ou une organisation, dans le cadre direct de ses activités de traitement de l'information, pour mener à bien sa mission, pour la prise de décision, ou encore pour la résolution de problèmes. **Note** : Une ressource informationnelle peut être une ressource humaine, matérielle ou financière directement affectée à la gestion, à l'acquisition, au développement, à l'entretien, à l'exploitation, à l'accès, à l'utilisation, à la protection, à la conservation et à la destruction des éléments d'information. Une ressource peut donc être une personne, un fichier ou le système informatique lui-même.

Afin de rencontrer les obligations de SOX, il devient donc impératif pour les entreprises de définir et gérer des contrôles sur les ressources TI (information et processus). TI est impliqué dans la production des rapports financiers de l'entreprise, SOX oblige les dirigeant de l'entreprise à gérer (contrôler et maitriser) ses ressources informatiques afin de s'assurer que l'information des états financiers soit complète, exacte, validée et autorisée.

Considérant le fait que ses processus clés sont dépendants des TI, que la gestion des risques liés aux TI est une composante de la gouvernance d'entreprise, il est essentiel de mettre en place des contrôles sur l'intégrité de l'information et de sa gestion.

Dans le cadre de ce travail, comme nous considérons l'impact de SOX sur les groupes de maintenance logiciel, nous ne considèrerons que les contrôles applicatifs et de sécurités relatives aux applications logiciels, bases de données.



SOX vs Maintenance logiciel

5. Contrôles - Cadres de travail

Dans le cadre de ce travail, nous assumerons que l'entreprise a en place un cadre de gouvernance et les contrôles permettant une gestion des risques au niveau de l'entreprise. Le travail se concentre sur les impacts de SOX sur les groupes de maintenance et comment cette règlementation peut être intégrer au modèle de maturité de la maintenance de logiciel.

5.1. COSO

Le référentiel COSO (réf: COSOORG, *traduction libre*) défini le contrôle interne comme un processus mis en œuvre par le conseil d'administration, les dirigeants et le personnel d'une organisation, destiné à fournir une assurance raisonnable quant à la réalisation des 3 objectifs suivants :

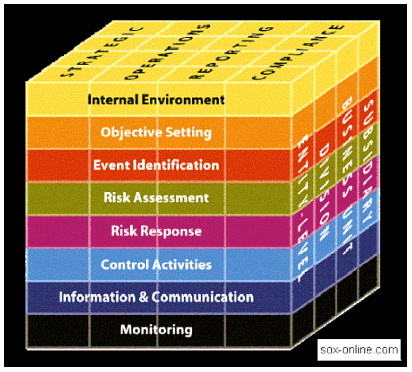
- L'efficacité et l'efficience des opérations,
- La fiabilité des informations financières,
- La conformité aux lois et règlements.

Le contrôle interne, tel que défini par le COSO, comporte cinq composantes. Ces composantes procurent un cadre pour décrire et analyser le contrôle interne mis en place dans une organisation. Ces composantes sont :

- L'environnement de contrôle, qui correspond, pour l'essentiel, aux valeurs diffusées dans l'entreprise ;
- L'évaluation des risques à l'aune de leur importance et fréquence ;
- Les activités de contrôle, définies comme les règles et procédures mises en œuvre pour traiter les risques, le COSO imposant la matérialisation factuelle des contrôles ;
- L'information et la communication, qu'il s'agit d'optimiser ;
- La supervision, c'est-à-dire le « contrôle du contrôle » interne.

Sommairement COSO, se représente sous la forme de ce cube (COSO Cube) et est composé de :

- 4 catégories :
  - *Stratégique, Opérationnel, Reporting, Conformité*
- 8 éléments du dispositif de management des risques :
  - *Environnement interne, Fixation des objectifs,*
  - *Identification des événements, Evaluation des risques,*
  - *Traitement des risques, Activités de contrôle,*
  - *Information et communication, Pilotage*
- La troisième dimension sont les unités de l'organisation



Cube COSO (Réf. COSOCUBE)

SOX oblige les sociétés cotées en bourse (faisant appel à l'épargne publique) à évaluer leurs contrôles internes et à en publier leurs conclusions dans les états demandés par la Securities and Exchange Commission. SOX demande la définition d'un cadre conceptuel de gestion des risques, le SOX Act a favorisé l'adoption du COSO comme référentiel.

5.2. COBIT (Control OBjectives for Information and related Technologies)

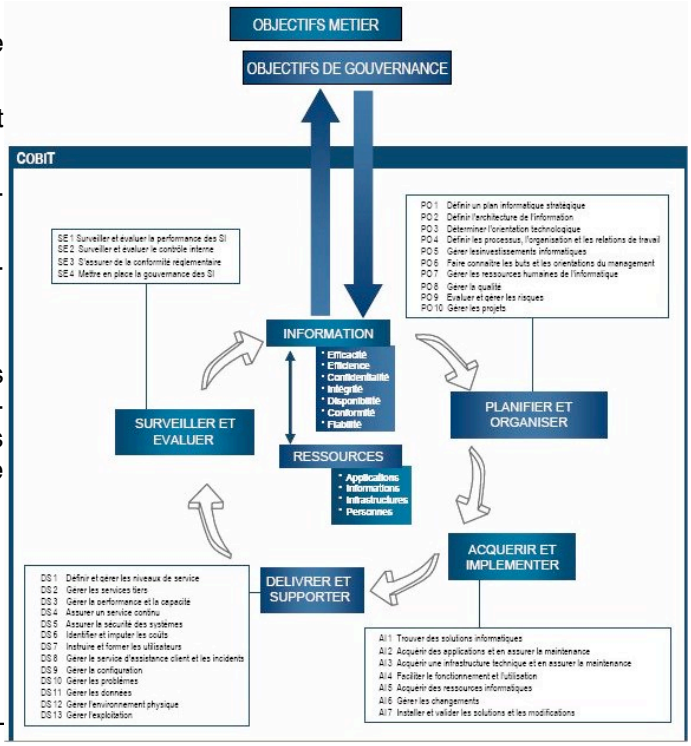
COSO propose un cadre de référence à très haut niveau pour la gestion des contrôles internes en entreprise, ce cadre se doit d'être associé à un référentiel plus détaillé comme COBIT ou ISO27002 afin de le rendre *opérationnelle*, i.e. permettre sa mise en opération ou de l'opérationnaliser.

COBIT est un cadre de référence international conçu à partir des meilleures pratiques mondiales en audit et maitrise des TI.

COBIT contribue à la gouvernance des TI en s'assurant que les :

- Les systèmes d'information (SI) sont alignés sur le métier de l'entreprise,
- Les SI apportent un plus au métier, et maximisent ses résultats,
- Les ressources des TI sont utilisées de façon responsable,
- Les risques liés aux TI sont gérés comme il convient.

- COBIT est illustrée par un modèle de processus qui subdivise l'informatique en 34 processus répartis entre les quatre domaines de responsabilités que sont donnant ainsi une vision complète de l'activité informatique - Réf:Présentation COBIT
  - Planifier et Organiser (Plan and Organize),
  - Acquérir et implémenter (Acquire & Implement),
  - Delivrer et Supporter (Deliver and Support)
  - Surveiller et Évaluer (Monitor and Evaluate)



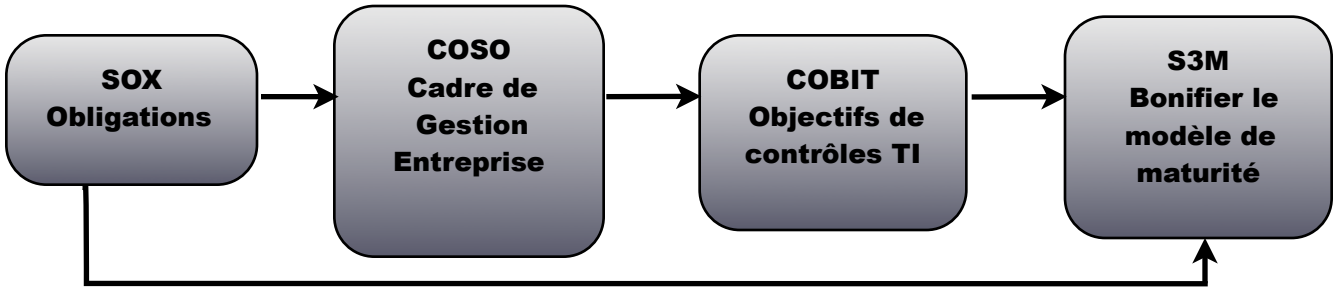
Modèle COBIT

COBIT intègre dans son modèle une orientation métier qui assure un meilleur alignement de l'informatique sur les activités de l'entreprise et une meilleur compréhension du management des activités de l'informatique. L'approche par processus, permet une attribution claire des propriétés et des responsabilités. COBIT est reconnu et apporte un préjugé favorable de la part des organismes de contrôles externes et respecte les exigences du COSO en matière de contrôle des environnement informatique.

6. Les Contrôles TI & SOX

Dans le cadre de ce travail, nous travaillerons avec 3 « cadres de référence » pour démontrer le lien entre SOX et le modèle de maturité.

Dans un premier temps SOX impose la mise en place d'un cadre de gestion des contrôles internes qui sera assumé par COSO et ne fait pas parti du présent travail. Ensuite nous utiliserons COBIT comme cadre de gestion des risques TI pour établir le lien avec le modèle de maturité. Ces cadres ne font pas strictes au sens qu'ils demeurent tous sujet à l'interprétation, i.e. que la portée du contrôle et le nombre de contrôles sont laissés à l'entreprise et qu'aucun de ces cadres imposent ou fournissent une description claire du contrôle à mettre en place pour assurer la conformité à SOX.



Il en revient donc à l'entreprise, son groupe de vérification interne et externes d'établir une saine définition de ces contrôles sans tomber dans l'exagération. Il y a un coût associé à la mise en place de ces activités de contrôles et au maintient de celles-ci.

Il existe un document de référence produit par l'organisme IT Governance Institute qui s'intitule ***IT CONTROL OBJECTIVES FOR SARBANES-OXLEY*** (réf: ITCTRLSOX) que j'ai utilisé comme base de travail. Ce document présente un premier mapping entre les objectifs de contrôle TI de SOX, de COBIT et du PCAOB (Public Company Accounting Oversight Board). Le PCAOB est l'autorité de surveillance indépendante pour les sociétés de révision. Cette autorité a été introduite aux Etats-Unis dans le cadre du projet de loi SOX pour répondre aux exigences de qualité et d'indépendances imposées aux auditeurs.

6.1. Les niveaux de maturités SOX, COBIT & S3M

Avant de procéder au mapping entre les obligations SOX et les cadres de travail utilisés, j'ai consolidé dans un même tableau la définition des niveaux de maturité des différents cadre afin de valider les interprétations des différentes autorités.

Le tableau ci-inclus démontre que SOX, COBIT et S3M ont plus ou moins la même définition des différents niveaux de maturités.

Niveau	SOX	Cobit (qualité des contrôles)	S3M (maturité)
0	L'organisation ne peut être conforme à ce niveau. À ce niveau il y a manque total de contrôle, de procédures, impossible d'être conforme.	Stage 0 - Inexistant	Inexistant
1	Contrôles ne sont pas en place et la documentation est insuffisantes. Les employés ne sont pas avisés et ne connaissent par leurs responsabilité . Le niveau d'effort pour se conformer très significatif.	Stage 1 - Initial / Ad Hoc	Initial Improvisé
2	Contrôles, procédures et documentation sont en place mais incomplètes et insuffisantes pour supporter une certification de la direction. Le niveau d'effort pour documenter et tester les contrôles est significatif.	Stage 2 - Répétable mais intuitif	Discipliné Répétable
3	Contrôles, procédures et documentation sont en place, conformes et peu supporter une certification de la direction.	Stage 3 - Procédure définies	Processus Personnalisé
4	L'efficience opérationnel des contrôles est fait périodiquement. L'utilisation des TI est limitée et primaire, i.e documentation des processus, des objectifs de contrôles et des	Stage 4 - Géré et mesurable	Géré quantitativement et mesurable
5	Pleine utilisation des TI pour la documentation des processus, des objectifs de contrôles, des «gaps» et de l'évaluation de l'efficacité des contrôles.	Stage 5 - En optimisation	En optimisation

Tableau récapitulatif des niveaux de maturités.

6.2. Objectifs de contrôle SOX & COBIT

La tableau ci-inclus est un extrait du document de référence *IT CONTROL OBJECTIVES FOR SARBANES-OXLEY* (réf: ITCTRLSOX) dans lequel le mapping entre des objectifs de contrôles TI de SOX et les processus COBIT.

Cette première étape de mapping permettra d'établir un lien entre un objectif SOX et un processus COBIT. La seconde étape est d'établir le lien entre le processus COBIT, son objectif de contrôle, son contrôle et le modèle de maturité S3M.

IT Control Objectives for Sarbanes-Oxley - IT Governance Institute
Traduction libre partielle

	OBJECTIFS DE CONTROLE TI - SOX	COBIT	S3M
1	Acquisition et maintenance logiciel applicatif	AI2	PRO
2	Acquisition et maintenance des infrastructures technologiques	AI3	PRO
3	Enable Operations	AI4	PRO
4	Install and accredit solutions and changes	AI7	SUP
5	Gères les changements	AI6	REQ, EVO
6	Défini et gère les niveaux de service (SLA)	DS1	REQ4
7	Gère les «third party services»	DS2	REQ4
8	Assure la sécurité des systèmes	DS5	SUP, EVO
9	Gestion de la configuration	DS9	SUP
10	Gestion des problèmes et des incidents	DS8,DS9	REQ
11	Gestion / Gouvernance des données	DS11	PRO
12	Gestion des environnements physiques et des opérations	DS12,DS13	SUP

Ce mapping à très haut niveau permet de faire une corrélation entre les processus, contrôles COBIT et les domaines du modèle de maturité de la maintenance (S3M). Dans le cadre de ce travail, il n'y aura pas de mapping exhaustif mais bien la présentation d'une démarche pour intégrer les obligations SOX au modèle de maturité.

7. SOX - Contrôles - Maturité(S3M)

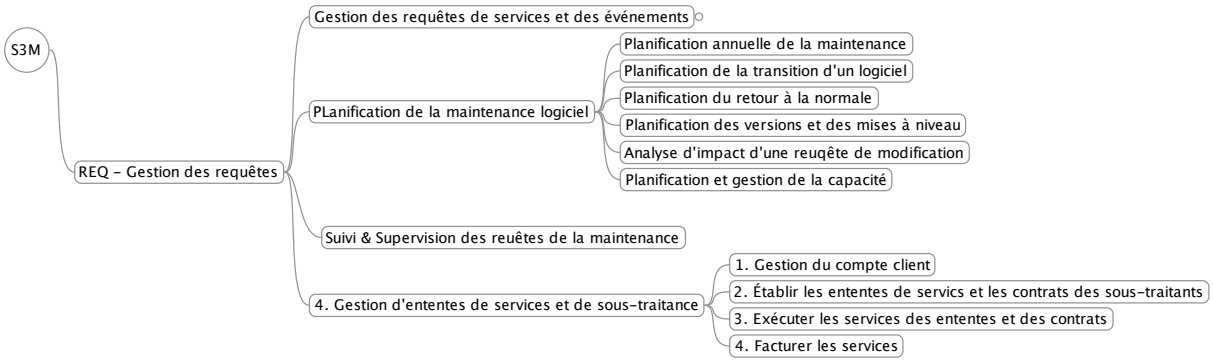
S3M est un modèle de maturité composé de 4 domaines, 18 itinéraires et 75 facettes. Les domaines sont :

- PRO - Gestion des processus
- REQ - Gestion des requêtes
- EVO - Ingénierie des solutions
- SUP - Support à l'ingénierie d'évolution

Ce modèle propose une approche pratique, les itinéraires et les facettes sont très appliqués et permettent d'établir un diagnostic et une base terminologique dans un domaine de génie logiciel qui n'est pas encore normalisé.

Nous sommes à l'étape d'établir le lien entre l'objectif de contrôle SOX, le processus COBIT et le modèle de maturité S3M. Afin de démontrer comment les obligations SOX peuvent être intégrés au modèle de maturité, je propose la démarche suivante :

- À partir de l'objectif de contrôle SOX no.7 (considérons cet objectif dans le cadre de cette démonstration), faire référence au tableau de la page précédente, i.e. Manage third-party services.
- Cet objectif est adressé par le processus DS de COBIT et est en lien avec le domaine REQ du S3M.
- Le domaine 4 - Gestion d'entente de services et de sous-traitance
- La facette 3 - Exécuter les services des ententes et des contrats



Ceci nous permet de conclure sur 2 aspects,

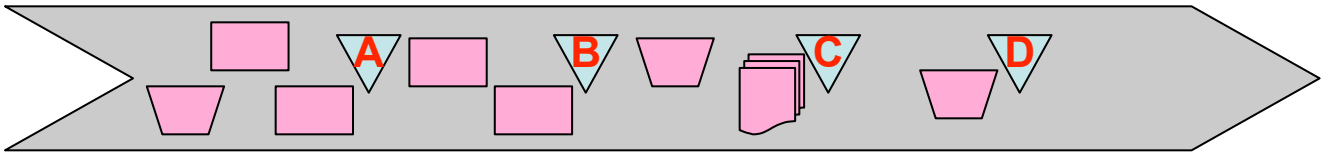
- Le modèle de maturité S3M intègre les bonnes pratiques des normes, il existe déjà une correspondance entre l'itinéraire et COBIT
- les niveaux de maturité sont alignés

8. Réponses au 2 questions :

8.1. Comment SOX peut être intégrer au modèle de maturité S3M

En considérant que les contrôles devraient être adaptés au contexte de l'entreprise, il faut établir une correspondance entre les objectifs de contrôles TI de SOX, les contrôles COBIT à définir et les itinéraires du modèle de maturité de la maintenance de logiciel.

Il faut intégrer et répartir les contrôles COBIT dans les processus de l'entreprise et aux itinéraires-facettes du modèle. Et finalement proposer des tests de contrôles (A, B, C, D) de conformité spécifique et une production d'artefacts conformes aux attentes de la règlementation.



	OBJECTIF DE CONTROLE TI - SOX	S3M	COBIT
7	Gère les «third party services»	REQ4.2.3	Manage «Third Party» Servives DS2.1, 2.2, 2.3, 2.4

8.2. Groupe de maintenance rencontre les obligations de SOX

«Si tu avais à mettre des pratiques spécifiques pour évaluer si le groupe de maintenance rencontre les obligations de SOX quelles seraient-elles? »

Il fut dans un premier temps évaluer le niveau de maturité, ceci nous permettra d'évaluer les efforts à la démarche. Il faut noter que les organisations dont le niveau de maturité est de 0 et 1 se retrouvent dans une situation où les efforts seront trop importants. De plus, les artefacts seront très inconsistants.

La documentation des processus de l'entreprise est requises pour effectuer ce genre d'évaluation. Les pratiques à mettre en place pour déterminer si le groupe de maintenance rencontre les obligations de SOX sont les suivantes :

- Identifier les processus et les applications qui supportent la production des états financiers
- Évaluer les risques
- Identifier les contrôles COBIT pour mitiger les risques
- Priorité au Contrôles clés et à plus haut risque
  - *Gestion des données (DS11)*
  - *Gestion des changements (AI6, AI7)*
  - *Gestions des accès et ségrégation des tâches (DS5)*
  - *Gestion de la Sécurité (DS5)*
- Documenter et tester les contrôles

9. Conclusion

Dans le cadre de ce travail, il m'a été permis de constater qu'il existe de nombreux ouvrages, sites, organismes et documentation de disponible sur le sujet.

Les contrôles et les objectifs sont «flexibles», la législation n'impose pas de contrôles spécifiques, il n'y a rien d'imposer. Il faut rencontrer des objectifs relativement peu clairs et il est difficile pour les entreprises de déterminer la quantité de contrôle requis pour assurer la conformité.

On doit éviter de mettre des contrôles pour mettre des contrôles ou de mettre en place COBIT et oublier l'objectif principal, assurer une conformité à SOX. Ce contexte à favoriser le monde de la consultation et de l'audit.

L'entreprise qui désire se conformer à SOX doit avoir une pratique et un minimum de maturité (documentation et processus) en place pour identifier les risques et fixer les contrôles adéquats.

On doit accorder la priorité à une saine gestion des risques, prioriser une approche progressive corporative et s'assurer d'avoir le support des Hauts Dirigeants.

Dans certains cas des entreprises vont au-delà des obligations législatives et révisent leurs processus afin de les optimiser et les rendre plus sures. D'autres vont faire que le minimum et je présume que certains attendront les pénalités pour se conformer.

En guise de conclusion, je crois qu'il serait approprié d'intégrer à la législation, des contrôles spécifiques. Il existe des normes claires et précises dans certains domaines de l'ingénierie, nous devrions être en mesure de faire de même pour le génie logiciel. L'ambiguité et le manque de précision pénalisent les entreprises. Les autorités devraient et doivent assumer leur part d'imputabilité et de responsabilités vis-à-vis des investisseurs qui sont démunis devant les entreprises «délinquantes». Je crois que les rapports de conformité devraient être rendus publiques afin d'en aviser les investisseurs.

10. Références

APRIL : Améliorer la maintenance du logiciel, Alain April / Alain Abran, Éditeur : LOZE-DION, ISBN : 9782921180887,Parution : 2006

ITCtrlSOX : ISBN 1-933284-76-5, IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition (IT Control Objectives for Sarbanes-Oxley, 2nd Edition)

WIKISOX : http://fr.wikipedia.org/wiki/Loi_Sarbanes-Oxley

RESSINFO: http://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/terminologie_sec_informatique/ressource_informationnelle.html

WIKICOSO : http://fr.wikipedia.org/wiki/COSO

COSOORG: http://www.coso.org/

COSOORG Francais : http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary_french.pdf

ITCTRLSOX : IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition, ISBN 1-933284-76-5

http://www.coso.org/documents/COSO_ERM_ExecutiveSummary_french.pdf

http://www.coso.org/documents/COSO_Guidance_On_Monitoring_Intro_online1_002.pdf

COSOCUBE: sox-online.com, http://www.sox-online.com/coso_cobit_coso_cube-new.html)

COBITFRANCAIS: http://www.afai.fr/index.php?m=29

www.itgi.org

www.isaca.org

http://www.soxlaw.com/

http://www.piloter.org/gouvernance-entreprise/sarbanes-oxley.htm

11. Annexe

Ma présentation donnée en classe le 3 mars 2011 (format PowerPoint)

Public Law 107-204--July 30, 2002 116 STAt.745 (loi américaine Sarbanes-Oxley de 2002)

La réponse du Canada à la loi américaine Sarbanes-Oxley de 2002.

Le management des risques de l’entreprise Cadre de Référence, Synthèse (COSO ORg)