ETS-RT - 2011-000

INTEGRATION DE LA LOI SARBANES-OXLEY AU MODÈLE DE MATURITÉ S^{3M}

HICHAM BELBSIR

ETS-RT - 2011-000

INTEGRATION DE LA LOI SARBANES-OXLEY AU MODÈLE DE MATURITÉ S^{3M}

RAPPORT TECHNIQUE DE L'ÉTS

HICHAM BELBSIR

Génie logiciel

ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
UNIVERSITÉ DU QUÉBEC

MONTRÉAL, 14 AVRIL 11

ETS-RT - 2011-000

INTEGRATION DE LA LOI SARBANES-OXLEY AU MODÈLE DE MATURITÉ S^{3M}

HICHAM BELBSIR
Génie logiciel
ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

La version électronique de ce rapport technique est disponible sur le site Web de l'École de technologie supérieure (http://www.etsmtl.ca).

Pour se procurer une copie papier, s'adresser à :

Service de la bibliothèque
École de technologie supérieure
1100, rue Notre-Dame Ouest
Montréal (Québec)
H3C 1K3

Téléphone : (514) 396-8946
Télécopieur : (514) 396-8633
Courriel : biblio@etsmtl.ca

ISBN x-xxxxxx-xx-x

Dépôt légal : Bibliothèque et Archives nationales du Québec, 2011
Dépôt légal : Bibliothèque et Archives Canada, 2011

INTEGRATION DE LA LOI SARBANES-OXLEY AU MODÈLE DE MATURITÉ S^{3M}

HICHAM BELBSIR

RÉSUMÉ

Ce travail s'inscrit dans le cadre du cours MGL804 : Réalisation et maintenance logiciels. Il correspond au travail de session n° 22 du chapitre-3- du livre « **Améliorer la maintenance du logiciel » April-Abran**, p.107 : « ***Étudiez la proposition Sarbane-Oxley (la loi canadienne équivalente) et indiquez comment cette nouvelle obligation peut être intégrée au modèle de maturité***»

Dans un premier temps, le document présente quelques définitions importantes suivies d'une description de la loi Sarbanes-Oxley : Historique, objectifs, principes exigence, sections importantes, interaction avec le système d'information. Ensuite, il y aura une brève description du référentiel de contrôle interne **COSO** ainsi que le référentiel pour la gouvernance des SI **COBIT.**

Après, le document essaie de mettre en évidence l'intégration de la loi Sarbanes-Oxley au modèle de maturité S^{3M}. Cette intégration sera divisée en deux parties : la première partie aligne la loi Sarbanes-Oxley et le référentiel **COBIT** afin de déterminer les objectifs de control IT à atteindre pour être conforme à la loi Sarbanes-Oxley .La deuxième partie aligne les objectifs dégagés, qui traitent de la maintenance, et le modèle de maturité S^{3M}.

À la fin, le document illustre un tableau récapitulatif d'alignement afin de bien voir la correspondance entre les objectifs de la loi Sarbanes-Oxley et ceux de S^{3M}.

AVANT-PROPOS

Ce document est le résultat du travail individuel de session réalisé dans le cadre du cours MGL804-**réalisation et maintenance logiciels**. Il s'adresse, principalement, au professeur **Alain April** et aux étudiants de ce cours. Mais il pourrait être un document de références pour certains futurs étudiants et aussi pour les entreprises qui adoptent le modèle de maturité S^{3M} et qui veulent savoir jusqu'à quel point elles sont conformes avec la loi Sarbanes-Oxley et spécifiquement par rapport au sujet de maintenance

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

1 GLOSSAIRE

SOX	Loi Sarbanes-Oxley
PCAOB	Le Public Company Accounting Oversight Board est un organisme sans but lucratif du secteur privé créé en 2002 par la loi Sarbanes-Oxley, chargé de surveiller les auditeurs de sociétés cotées afin de protéger les intérêts des investisseurs et l'intérêt public, grâce à la préparation de rapports d'audit informatifs, justes et indépendants
CEO	Directeur Général
CFO	Directeur Financier

2 LA LOI SARBANES OXLEY (SOX)

2.1 Historique de SOX

Aux États-Unis d'Amérique, la fin de l'année 2001, et le début l'année 2002, ont donné lieu à de nombreux scandales financiers (avec Enron, en tête, mais aussi Adelphia, Xerox, et surtout WorldCom) dont l'importance a gravement impacté la confiance placée dans l'économie et le fonctionnement des sociétés cotées. Les scandales ne sont pas le résultat d'agissements frauduleux de quelques-uns. Il s'agit de scandales financiers mettant en cause le fonctionnement de tout un système, celui des sociétés cotées et de leur autorégulation, dans un environnement ultralibéral de création de valeur actionnariale.

Face à de tels scandales, un sénateur démocrate, M. P. Sarbanes, et un représentant républicain, M. M. Oxley, ont rédigé une proposition de loi dont le but est de réduire les fraudes et les conflits d'intérêts d'une part et augmenter la transparence financière et la confiance du public dans les marchés d'autre part. Cette loi sur la réforme de la comptabilité des sociétés cotées et la protection des investisseurs encore connue sous l'acronyme SOX, Sarbox, SOA ou d'après le nom de ses promoteurs Loi Sarbanes-Oxley. Celle-ci a ensuite été votée par le Congrès des États-Unis et ratifiée par le président Bush le 30 juillet 2002.

2.2 Les objectifs de SOX

Les principaux objectifs de la loi Sarbanes-Oxley sont :

- Contrôler plus finement les activités financières des entreprises.
- Renforcer et reconstituer la confiance du public envers la profession comptable.
- Renforcer l'application des lois sur les valeurs mobilières.
- Améliorer l'exemple et les responsabilités de la direction.

- Améliorer la performance des intermédiaires financiers.
- Protéger les investisseurs en améliorant l'exactitude et la fiabilité des divulgations de l'information financière.
- Réduire les fraudes et les conflits d'intérêts.

2.3 Les principes de SOX

Trois grands principes régissent la loi Sarbanes-Oxley :

- l'exactitude et l'accessibilité de l'information.
- la responsabilité des gestionnaires.
- l'indépendance des vérificateurs/auditeurs.

Ces trois principes définis par la loi Sarbanes-Oxley visent à augmenter la responsabilité corporative des instances dirigeantes et à mieux protéger les investisseurs. Leur but est de rétablir leur confiance dans le marché et d'imposer une réglementation stricte en matière de comptabilité et de transparence des états produits.

2.4 Les exigences de SOX

❖ La loi Sarbanes-Oxley a introduit :

- 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.
- 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 - 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 (le COSO).

2.5 Les Sections « importantes » de SOX

La loi Sarbanes-Oxley (SOX) est un document législatif très complexe qui comporte plusieurs sections. Les sections les plus pertinentes pour les technologies de l'information sont :

Section 302. Certification des états financiers

Le Directeur Général (CEO) et le Directeur Financier (CFO) de l'entreprise doivent préparer une déclaration, accompagnant le rapport des auditeurs, qui certifie la validité des états financiers et des indications hors bilan contenues dans le rapport annuel (ou les rapports périodiques). Cette déclaration doit aussi signaler que les états financiers présentent de manière sincère, dans tous leurs aspects significatifs, la situation financière et les résultats de l'activité de l'entreprise.

Section 404. Evaluation du contrôle interne

La section 404 précise que les auditeurs (financiers) doivent certifier les processus et les contrôles mis en œuvre lorsqu'une entreprise fait une déclaration financière (rapport financier). Elle implique donc une évaluation des mécanismes de contrôle tant au niveau des processus que du cadre lui-même.

La section 404 de Sarbanes-Oxley est souvent mise en avant pour expliquer et justifier la démarche de gouvernance des systèmes d'information. Rappelons ici que toute entreprise américaine cotée aux USA, dont la capitalisation boursière est égale ou

supérieure à 75 millions USD doit être conforme à la SOA 404 (Sarbanes-Oxley ACT 2002 - Section 404).

Le SOX et le SI

La loi Sarbanes-Oxley impacte également les systèmes d'information, à travers deux sections. D'une part, la section 409, dénommée « Real Time Issuer Disclosure », impose aux entreprises de pouvoir clôturer leurs comptes plus rapidement possibles (2 jours), d'autre part, la section 404 (Management Assessment of Internal Controls) qui se considère comme le véritable challenge du système d'information et qui oblige les entreprises à réaliser des contrôles internes dont l'efficacité doit pouvoir être prouvée.

De même, le système d'information financier de l'entreprise doit permettre d'estimer rapidement les conséquences d'un évènement majeur de manière à pouvoir en informer les décideurs de l'entreprise incluent les actionnaires.

3 COSO

COSO (**Committee of Sponsoring Organizations of the Treadway Commission),** est une organisation de bénévoles du secteur privé à but non lucratif qui a publié en 1992 un document de définition standard du contrôle interne, intitulé « Internal Control - Integrated Framework », couramment appelé le « cadre du COSO » et illustré fréquemment sous la forme d'un cube, dit « cube du COSO » figure x , 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 :

- L'efficacité et l'efficience des **opérations**.
- La fiabilité des **rapports financiers** (l'importance principal de la loi SOX).
- **La conformité** aux lois et les règlements.

Le contrôle interne, tel que défini par le COSO, comporte cinq composants, il s'agit de :

1. **L'environnement de contrôle** : se résume par l'attribution de l'autorité et la responsabilité, la philosophie de gestion et le style de fonctionnement ainsi que les valeurs diffusées dans l'entreprise.
2. **L'évaluation des risques** : c'est la mise en place d'objectifs et la capacité à gérer les changements internes et externes.
3. **Les Activités de contrôle** : c'est la répartition des tâches, la documentation des règles et procédures mises en œuvre, les rapprochements et les approbations des transactions.

4. **L'information et la communication** : La bonne information doit acheminer à la bonne personne au bon moment.

5. **La surveillance** : c'est-à-dire le « contrôle du contrôle » interne (la fréquence des procédures de suivi, preuve que la surveillance a eu lieu…)

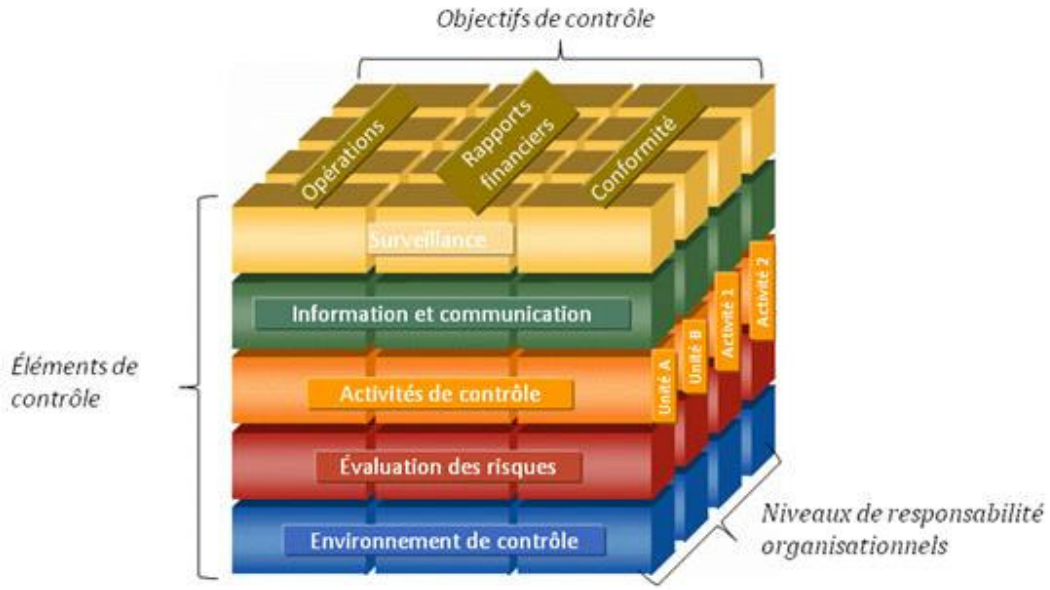

Figure 1: Le cube du COSO source : http://www.tbs-sct.gc.ca

4 COBIT

CobiT (Control Objectives for Information and related Techonology – Contrôle de l'Information et des Technologies Associées) est le modèle de référence en matière d'audit et de maîtrise des systèmes d'information, a été développé en 1994 (et publié en 1996) et qui permet d'établir un langage commun pour parler de la Gouvernance des systèmes d'information. Il est le résultat des travaux collectifs réalisés par les principaux acteurs de la profession, auditeurs internes ou externes, fédérés au sein de l'ISACA) (Information System Audit and Control Association).

Cobit fournit en détail les activités requises pour l'évaluation des contrôles IT afin de se conformer à SOA. Il comprend 4 domaines, 34 processus et 318 objectifs de contrôle.

Les 4 principaux domaines de Cobit sont :

- **Planification et Organisation** : c'est de savoir comment utiliser les techniques informatiques afin que l'entreprise atteigne ses objectifs Ex (Définition du plan stratégique informatique, Définition de l'architecture des informations...)
- **Acquisition et Installation** : c'est définir, acquérir et mettre en œuvre des technologies en les alignant avec les processus métiers de l'entreprise Ex (Identification des solutions automatiques, Acquisition et maintenance des applications informatiques…).
- **Livraison et Support** : c'est de garantir l'efficacité et l'efficience des systèmes technologiques en action Ex (Définition des niveaux de service, Garantie de la sécurité des systèmes …)
- **Surveillance et Évaluation**: c'est de vérifier si la solution mise en œuvre soit en adéquation avec les besoins de l'entreprise dans une vision stratégique Ex (Surveillance des processus, Audit par un organisme indépendant…).

CobiT est aujourd'hui l'outil de référence privilégié pour la prise en compte de la gouvernance de l'informatique dans la mise en œuvre des directives pour une démarche SOX.

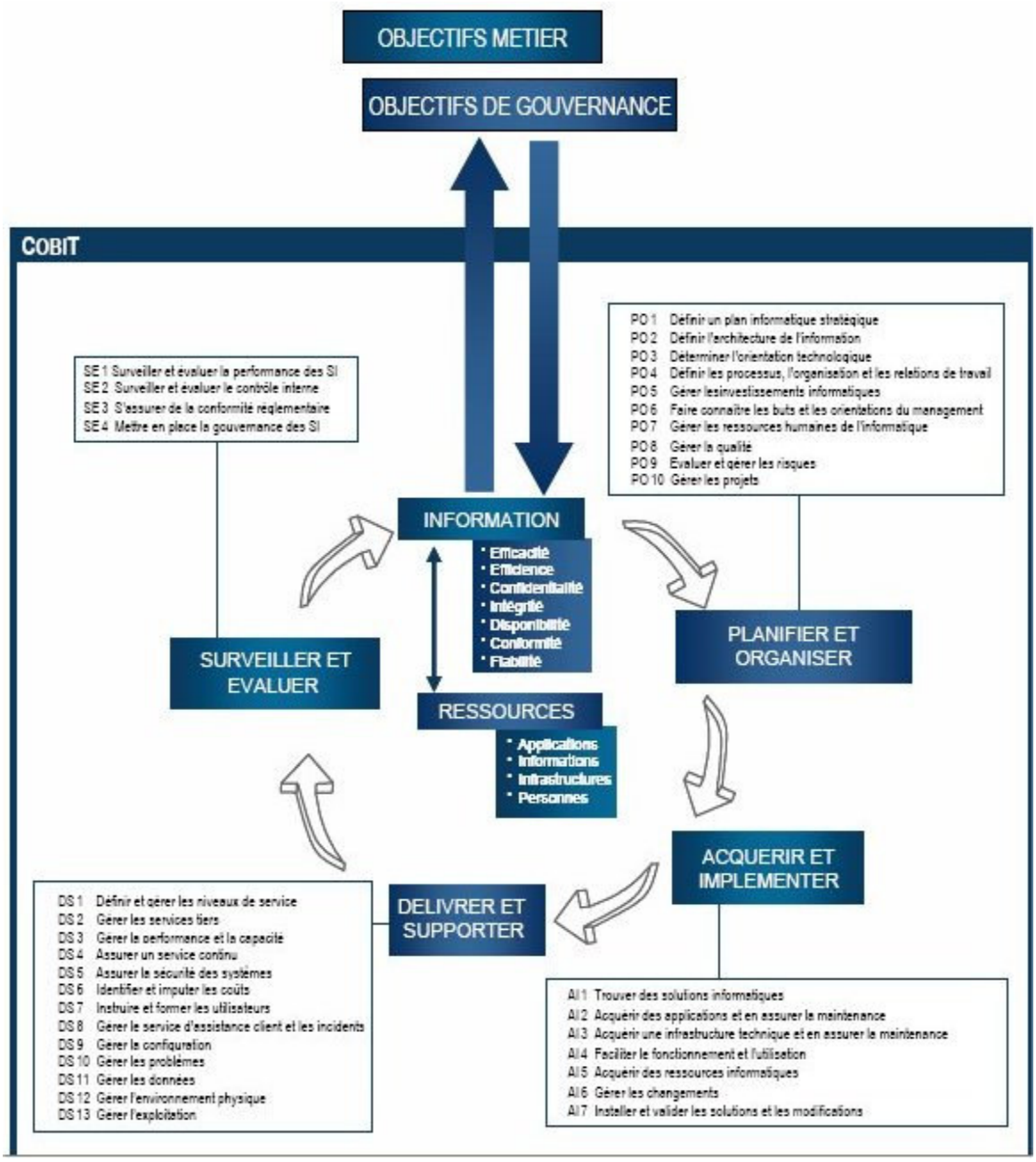

Figure 2 : vue d'ensemble de Cobit

Source : http://www.afai.fr

5 INTÉGRATION DE LA LOI SARBANES-OXLEY AU MODÈLE S^{3M}

La loi Sarbanes-Oxley exige que les organisations choisir et mettre en œuvre un cadre de contrôle interne approprié. COSO est devenu le cadre le plus couramment utilisé par les entreprises qui se conforment à la loi Sarbanes-Oxley.

Bien que COSO fait référence à l'importance des TI par rapport à l'environnement de contrôle global, mais, il ne fournit pas de directives détaillées pour les entreprises qui ont besoin pour concevoir et mettre en œuvre des contrôles informatiques spécifiques à leur environnement. Par conséquent, Cobit est la référence privilégiée pour la prise en compte de la gouvernance de l'informatique dans la mise en œuvre des directives pour une démarche SOX.

En effet, pour intégrer la loi Sarbanes-Oxley (SOX) au modèle S3M il va falloir passer par les étapes suivantes :

1. Aligner SOX avec COBIT.
2. Aligner Cobit avec S^{3M}.

5.1 Alignement du SOX avec Cobit

La publication en décembre 2005 de la version 4.0 de CobiT4 a été l'occasion d'aligner systématiquement ce référentiel sur les règles du PCAOB. Le document publié par l'IT Governance Institute « IT Control Objectives for Sarbanes-Oxley » qui reprend les éléments du COBIT et du COSO dans le but de répondre aux exigences du SOX, a aligné 12 objectifs de contrôle de Cobit avec la norme d'audit PCAOB « PCAOB Auditing Satandard No. 2 ».

Le tableau suivant présente un alignement de haut niveau des objectifs de contrôle TI pour le SOX avec les objectifs de COBIT :

Figure 1—Mapping to PCAOB and COBIT

IT Control Objectives for Sarbanes-Oxley	COBIT	PCAOB IT General Controls			
	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			●	●

Table 1. Alignment SOX avec COBIT

Source: IT Control Objectives for Sarbanes-Oxley, 2nd Edition

En se basant sur les données de ce tableau, on peut constater qu'il y a juste ces 7 objectifs qui ont une relation avec la maintenance de logiciels:

- **AI2 : Aquire and maintain application software**
- **AI3 : Acquire and maintain technology infrastructure**
- **AI4 : Enable operations**
- **AI6 : Manage changes**
- **AI7 : Install and accredit solutions and changes**
- **DS1: Define and manage service levels**
- **DS2 : Manage third-party services**

Mais, il faut signaler que parmi les 5 autres objectifs, il y en a ceux qui doivent être considérés parmi les objectifs de maintenance comme l'objectif 8 : **Ensure systems security et l'objectif** 9 : **Manage the configuration.**

5.2 Alignement du Cobit et S3M

Après l'alignement du SOX avec Cobit dans la section 5.1, on va prendre ces objectifs définis dans la section précédente pour essayer de les mettre en correspondances avec les objectifs des itinéraires de S3M.

5.2.1 Acquérir et Implémenter (AI)

AI2 Acquire and Maintain Application Software:

Parmi les 10 objectifs qui composent cet objectif il y a seulement 4 sous objectifs qui font partie du processus de la maintenance. Les autres appartiennent au processus de développement.

AI2.6 Major Upgrades to Existing Systems:
In the event of major changes to existing systems that result in significant change in current designs and/or functionality, follow a similar development process as that used for the development of new systems.

Le modèle S^{3M} considère le traitement des mises à niveau majeures des systèmes existants comme des nouveaux projets de maintenance. Il faut, prendre en note, que la durée typique acceptée d'une petite maintenance soit de 5 jours.

AI2.8 Software Quality Assurance
Develop, resource and execute a software QA plan to obtain the quality specified in the requirements definition and the organisation's quality policies and procedures

Cet objectif est respecté par le modèle S^{3M} à travers l'itinéraire sup2 « assurance qualité des processus, des services et des logiciels » sous le domaine de processus

« Support à l'ingénierie d'évolution » et qui a comme objectifs du processus d'offrir un support à la livraison des produits et des services de haute qualité.

AI2.9 Applications Requirements Management
Track the status of individual requirements (including all rejected requirements) during the design, development and implementation, and approve changes to requirements through an established change management process.

S^{3M} propose dans le domaine de processus « ingénierie de l'évolution » un itinéraire Evo3 (Évolution/correction du logiciel) qui correspond à cet objectif. On peut voir cette correspondance dans les objectifs du processus :

- Le mainteneur s'assure de gérer les exigences de la clientèle, avec une conception détaillée.
- Le mainteneur poursuit la mise en œuvre des changements des essais unitaires et d'intégration.
- Le mainteneur poursuit la documentation des changements.

On peut voir cette correspondance aussi dans les résultats attendus du processus :

- Les exigences sont documentées.
- La modification est documentée (il y a traçabilité des changements et des composants de la conception détaillée, des éléments de codage et des essais).
- Les essais sont réalisés, documentés, vérifiés et révisés.

AI2.10 Application Software Maintenance
Develop a strategy and plan for the maintenance of software applications

S^{3M} respecte parfaitement cet objectif, on trouve ça au niveau de l'itinéraire Req2 (Planification de la maintenance du logiciel) du 2ème domaine de processus du modèle S^{3M} « Gestion des requêtes » .

AI3 Acquire and Maintain Technology Infrastructure

S^{3M} ne traite pas de la maintenance de l'infrastructure technologique

AI4 Enable Operation and Use

Cet objectif comprend 4 sous objectifs, mais seulement le 4ème sous objectif qui a une relation avec la maintenance.

AI4.4 Knowledge Transfer to Operations and Support Staff
Transfer knowledge and skills to enable operations and technical support staff to effectively and efficiently deliver, support and maintain the system and associated infrastructure.

Cet objectif est respecté par S^{3M} dans l'itinéraire Evo1 « transition du logiciel vers la maintenance » sous le domaine de processus « ingénierie d'évolution », et plus précisément la facette du suivi de la formation et du transfert de connaissance avant la transition d'un logiciel.

AI6 Manage Changes

Le but de cet objectif est de contrôler touts les changements, y compris la maintenance d'urgence et les correctifs, relatif à l'infrastructure et les applications au sein de l'environnement de production ainsi que les modifications « y compris celles des procédures, des processus, des systèmes et des paramètres de services » sont identifiés, évalués et autorisés et examiné par rapport aux résultats prévus avant la mise en œuvre. Tout ça implique que cet objectif concerne presque en totalité la maintenance.

AI6.1 Change Standards and Procedures
Set up formal change management procedures to handle in a standardised manner all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.

S^{3M} respecte les exigences de cet objectif qui exige la mise en place de procédures formelles pour la gestion des changements pour traiter de manière standardisée toutes les requêtes au niveau de la facette « documentation et normalisation des

processus et des services » de l'itinéraire Pro2 « définition des processus/services de la maintenance » du premier domaine de processus « Gestion des processus de la maintenance du logiciel ».

AI6.2 Impact Assessment, Prioritisation and Authorisation
Assess all requests for change in a structured way to determine the impact on the operational system and its functionality. Ensure that changes are categorised, prioritised and authorised.

La correspondance entre cet objectif et le S^{3M} se fait par la pratique Req2.2.17, qui désigne le responsable de la maintenance comme le responsable d'analyse d'impact, et la pratique Req2.2.19 qui permet de prioriser les différentes requêtes en collaboration avec le client, conformément à une procédure documentée. Ces deux pratiques sont sous la **facette de l'analyse d'une requête de modifications** de l'itinéraire Req2 « Planification de la maintenance du logiciel » du domaine de processus « gestion des requêtes ».

AI6.4 Change Status Tracking and Reporting
Establish a tracking and reporting system to document rejected changes, communicate the status of approved and in-process changes, and complete changes. Make certain that approved changes are implemented as planned

Cet objectif, qui demande de mettre en oeuvre un système de suivi et de rapports pour documenter les changements, peut être assuré par S3M à un certain point par le biais de la facette du suivi des activités planifiées et approuvées de l'itinéraire Req3 « Suivi et supervision des requêtes de la maintenance du logiciel » du domaine de processus « Ingénierie d'évolution » .

AI6.5 Change Closure and Documentation
Whenever changes are implemented, update the associated system and user documentation and procedures accordingly

La facette **de la documentation** de l'itinéraire Evo3 (Évolution/Correction du logiciel) du domaine de processus « Ingénierie d'évolution » du modèle S3M répond à cet objectif qui exige la mise à jour de la documentation après qu'une modification soit implémentée.

AI7 Install and Accredit Solutions and Changes

Les nouveaux systèmes (nouveaux ou modifiés) doivent être opérationnels une fois que le développement est terminé.

AI7.1 Training
Train the staff members of the affected user departments and the operations group of the IT function in accordance with the defined training and implementation plan and associated materials, as part of every information systems development, implementation or modification project.

S^{3M} satisfait la demande de cet objectif via **la facette du suivi de la formation et du transfert de connaissance avant la transition** dans le domaine « l'ingénierie d'évolution », et précisément la pratique Evo1.2.8 de l'itinéraire Evo1 « transition du logiciel vers la maintenance » qui exige à l'entité organisationnelle de la maintenance d'évaluer l'efficacité de la formation des utilisateurs (développeurs et clients).

AI7.2 Test Plan
Establish a test plan based on organization wide standards that defines roles, responsibilities, and entry and exit criteria. Ensure that the plan is approved by relevant parties.

Cet objectif est respecté par S^{3M} au niveau de la **facette des essais unitaires et d'intégration** qui appartiennent au domaine de processus « Ingénierie d'évolution », et plus précisément les pratiques Evo3.2.7 et Evo3.2.8 de l'itinéraire Evo3 « transition du logiciel vers la maintenance » et qui demandent aux mainteneurs de développer des plans de test.

AI7.3 Implementation Plan
Establish an implementation and fallback/backout plan. Obtain approval from relevant parties.

On peut dire que l'itinéraire Sup1 « Management de la configuration et des environnements» du domaine de processus « Support à l'ingénierie d'évolution », respect les exigences de cet objectif.

AI7.6 Testing of Changes
Test changes independently in accordance with the defined test plan prior to migration to the operational environment. Ensure that the plan considers security and performance.

AI7.7 Final Acceptance Test
Ensure that business process owners and IT stakeholders evaluate the outcome of the testing process as determined by the test plan. Remediate significant errors identified in the testing process, having completed the suite of tests identified in the test plan and any necessary regression tests. Following evaluation, approve promotion to production.

S^{3M} respecte ces 2 objectifs à travers l'itinéraire Evo4 «Vérification et Validation » au niveau de la **facette des essais systèmes et d'acceptation** du domaine de processus « Ingénierie d'évolution ».

AI7.8 Promotion to Production
Following testing, control the handover of the changed system to operations, keeping it in line with the implementation plan. Obtain approval of the key stakeholders, such as users, system owner and operational management. Where appropriate, run the system in parallel with the old system for a while, and compare behaviour and results

Cet objectif est respecté par S^{3M} dans le domaine du processus « Ingénierie d'évolution », au niveau de la **facette de la mise en opération d'un changement ou d'une version,** itinéraire Evo4 « Vérification et Validation », plus précisément la

pratique Evo.4.2.5 qui encourage la mise en production soit effectuée conformément à une procédure documentée et avec le consentement de la clientèle.

AI7.9 Post-implementation Review
Establish procedures in line with the organisational change management standards to require a post-implementation review as set out in the implementation plan.

Cet objectif est atteint par S^{3M} dans le domaine de processus « Ingénierie d'évolution », itinéraire Evo4 «Vérification et Validation » au niveau de la **facette des essais systèmes et d'acceptation** (pratique Evo.4.2.4)

5.2.2 Livraison et support (DS)

DS1 Define and Manage Service Levels
Effective communication between IT management and business customers regarding services required is enabled by a documented definition of and agreement on IT services and service levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels. This process enables alignment between IT services and the related business requirements.

DS2 Manage Third-party Services
The need to assure that services provided by third parties (suppliers, vendors and partners) meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimises the business risk associated with non-performing suppliers.process…

Ces 2 grands objectifs DS1 et DS2 sont traités parfaitement par S3M au niveau de l'itinéraire Req4 « Gestion de l'entente de services et de sous-traitants » du 2ème domaine de capacité (Gestion des requêtes)

5.3 Résumé de la correspondance entre SOX et S3M

Sarbanes-Oxley		S3M
Acquire and maintain (AI)		
AI2. Acquire and maintain application software	AI2.6 Major Upgrades to Existing Systems	**S3m** propose de traiter les mises à niveau majeures des systèmes existant comme des **projets** de maintenance
	AI2.8 Software quality assurance	sup2. Assurance qualité des processus, des services et des logiciels
	AI2.9 application requirements management	Evo3 Évolution/correction du logiciel
	AI2.10 application software maintenance	Req2 .Planification de la maintenance du logiciel
AI3. Acquire and Maintain Technology Infrastructure		S3M ne traite pas la maintenance de l'infrastructure technologique
AI.4 Enable Operation and Use	AI.4.4 knowledge transfer to operations and support staff	Evo1. Transition du logiciel vers la maintenance
AI.6 Manage Changes	AI.6.1 Change standards and procedures	Pro2.Définition des processus/services de la maintenance
	AI.6.2 Impact assessment, prioritization and Authorisation	Req2 : Req2.2.17 et Req2.2.19
	AI.6.4 Change Status Tracking and Reporting	Req3.Suivi et supervision des requêtes de la maintenance du logiciel
	AI.6.5 Change Closure and Documentation	Evo3.Evolution/Correction du logiciel
AI7 Install and Accredit Solutions and Changes	AI.7.1 Training	Evo1. transition du logiciel vers la maintenance
	AI.7.2 Test Plan	Evo3 : Evo3.2.7 et Evo3.2.8
	AI.7.3 Implementation Plan	Sup 1
	AI.7.6 Testing of Changes	Evo4 .Vérification et Validation
	AI.7.7 Final Acceptance Test	Evo4 .Vérification et Validation
	AI.7.8 Promotion to Production	Evo4 .Vérification et Validation : Evo.4.2.5
	AI.7.9 Post-implementation Review	Evo4.Vérification et Validation : Evo.4.2.4

Deliver and support (DS)	
DS1 Define and Manage Service Levels	Req4 : Gestion de l'entente de services et de sous-traitants
DS2 Manage Third-party Services	

Table 2. Correspondance entre SOX et S3M

6 CONCLUSION

En conclusion, on peut constater que le modèle de maturité S^{3M} est en grande partie conforme à la loi Sarbanes-Oxley. Par conséquent, pour toutes les entreprises qui utilisent le modèle de maturité S^{3M} et qui veulent être conforme à la loi Sarbanes-Oxley il suffit d'apporter quelques modifications et quelques ajustements pour que tous les objectifs de contrôle IT de Cobit soient respectés par le modèle.

Par ailleurs, il faut signaler aussi, que ces conclusions sont vraies si seulement elles seront approuvées par une étude expérimentale sur terrain pour valider les résultats obtenus de l'alignement des objectifs des contrôles TI de Cobit avec le modèle de maturité S^{3M}. Cela permettra d'assurer que les correspondances suggérées par ce document auront plus de crédibilité et efficacité. De plus, ces résultats quantitatifs permettront d'ajuster l'alignement stipulé et de le modifier en conséquence.

BIBLIOGRAPHIE

April-Abran 2006. Améliorer la maintenance du logiciel.

IT Governance Institute. COBIT 4.1

IT Governance Institute. IT Control Objectives for Sarbanes-Oxley, 2nd Edition -2006

Alain A. April, Reiner R. Dumke, Alain Abran, SMmm Model to Evaluate and Improve the Quality of the Software Maintenance Process, Arbeitsgruppe Softwaretechnik – Software Measurement Laboratory SMl@b ,GÉLOG – Laboratoire de Génie Logiciel,

SOX 404 & IT Controls IT Control Recommendations For Small and Mid-size companies by Ike Ugochuku, CIA, CISA TLK Enterprise 2006.

Terence Sheppy and Ross McGill. Sarbanes-Oxley (Building Working Strategies for Compliance) - 2007

http://fr.wikipedia.org/