La maîtrise
des Systèmes d'Information

Quel impact de la Loi Sarbanes-Oxley sur les systèmes d'information ?

Gina Gullà-Ménez

Benjamin Durieux

10 décembre 2004

Objectifs de la présentation

- Rappeler le contexte de la loi et ses exigences
- Présenter une démarche de prise en considération des impacts sur les systèmes d'information
- Faire un premier retour d'expérience

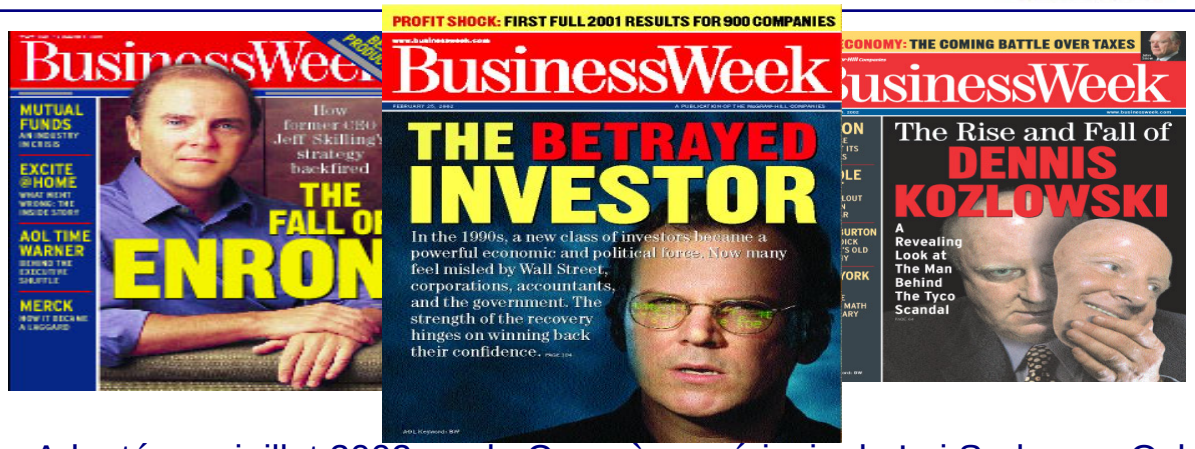
Plan de la présentation

I - Contexte	16:30
II - De la loi à l'implémentation	16:45
III - Conduite d'un programme SOA	17:00
IV - Retour d'expérience	17:15
V - Questions / Réponses	17:30

Le contexte et l'esprit de la Loi

U.S. SECURITIES AND EXCHANGE COMMISSION

"We are the investor's advocate."
William O. Douglas
SEC Chairman, 1937-1939



- Adoptée en juillet 2002 par le Congrès américain, la Loi Sarbanes-Oxley (SOA) implique que les Présidents des entreprises cotées aux Etats-Unis certifient leurs comptes auprès de la Securities and Exchanges Commission (SEC) l'organisme de régulation des marchés financiers US.
- Guidée par trois grands principes : l'exactitude et l'accessibilité de l'information, la responsabilité des gestionnaires et l'indépendance des vérificateurs/auditeurs
- Son objectif : restaurer la confiance des investisseurs et de renforcer la gouvernance[1] d'entreprise, largement entamée par les nombreux scandales financiers de 2001 et 2002

[1]**Gouvernance: structure de relations et de processus visant à diriger et contrôler l'entreprise pour qu'elle atteigne ses objectifs en générant de la valeur, tout en trouvant le bon équilibre entre les risques et les avantages des Technologies de l'Information et de leurs processus (COBIT).**

Le champ d'application

- Toutes les sociétés américaines cotées aux États Unis, dont la capitalisation boursière est supérieure à 75 millions de dollars doivent être conforme SOA 404 depuis le 15 novembre seront contraintes de déposer auprès de la SEC un rapport rédigé par la Direction portant sur le contrôle interne exercé sur le reporting financier en même temps que leur rapport financier annuel.
- Pour les autres entreprises cotées aux États Unis et/ou dont la capitalisation boursière est inférieure à 75 millions de dollars, la date est fixée au 15 juillet 2005.

Extraits d'une loi contenant plus de 60 articles

La maîtrise des Systèmes d'Information

Fiabiliser le reporting financier

302
- Certification des états financiers par le management

404
- Attestation de l'auditeur et du management sur l'évaluation du contrôle interne.

401, 409
- Prise en compte renforcée des transactions hors bilan et des événements critiques ayant un impact sur les comptes.

Renforcer la gouvernance

301
- Responsabilités et indépendance du Comité d'Audit
- Allocations budgetaires des auditeurs

Lutter contre les fraudes et les délits d'initiés

406
- Publication du code éthique

806
- "Whistle-Blower"

Renforcer les contrôles externes

104
- Rôle du PCAOB

Alourdir les sanctions

906
- Renforcement des mesures pénales pour les CEO/CFO

1102, 802
- Sanctions pénales renforcées en cas de destruction de preuves

Réaffirmer l'indépendance des auditeurs

201
- Interdiction explicite pour les auditeurs de fournir 9 types de services hors audit à leurs clients.

La loi Sarbanes - Oxley Act (2002)

La maîtrise des Systèmes d'Information

SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.

(a) RULES REQUIRED.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) INTERNAL CONTROL EVALUATION AND REPORTING.—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

La loi Sarbanes – Oxley

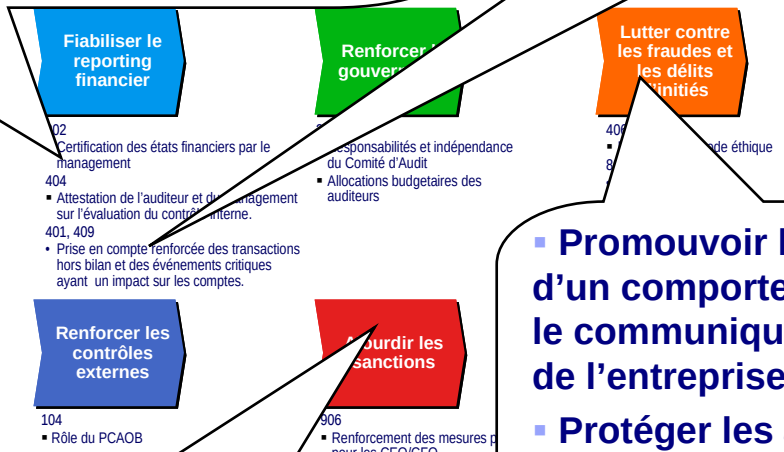
Une réponse règlementaire face à l'érosion critique de la confiance des investisseurs

Exemples de répercussions

La maîtrise des Systèmes d'Information

- **Améliorer la cartographie des processus et des contrôles internes.**
- **Évaluer le contrôle interne et rendre compte à la fois des défaillances et des plans d'amélioration.**

- **Faciliter la diffusion en temps réel des informations… mais de manière contrôlée.**



- **Promouvoir l'établissement d'un comportement éthique et le communiquer à l'ensemble de l'entreprise.**
- **Protéger les *alerteurs*[2] et mettre en place des processus d'alerte.**

- **Améliorer la gestion documentaire et les pratiques d'archivage des pièces.**

[2]De l'américain « Whistle Blowers »

Le Contrôle Interne

La maîtrise des Systèmes d'Information

- « Le contrôle interne est un processus défini et mis en œuvre par le conseil d'administration, le management et le personnel de l'entreprise, visant à fournir l'assurance raisonnable que les objectifs suivants sont atteints:
  - *Fiabilité de l'information comptable et financière,*
  - *Efficacité et efficience de la conduite des opérations de l'entreprise,*
  - *Respect des lois et des réglementations applicables ».*[3]

- Le contrôle interne est composé de deux niveaux de contrôle :
  - *les contrôles au niveau de l'entité qui constituent l'environnement de contrôle instauré par la direction générale qui, en fixant les principes directeurs, la politique et les procédures, instaure une culture du contrôle interne.*
  - *les contrôles au niveau des processus.*

[3]Définition du COSO (Committee of Sponsoring Organizations of the Treadway Commission)

En quoi les systèmes d'information sont-ils concernés ?

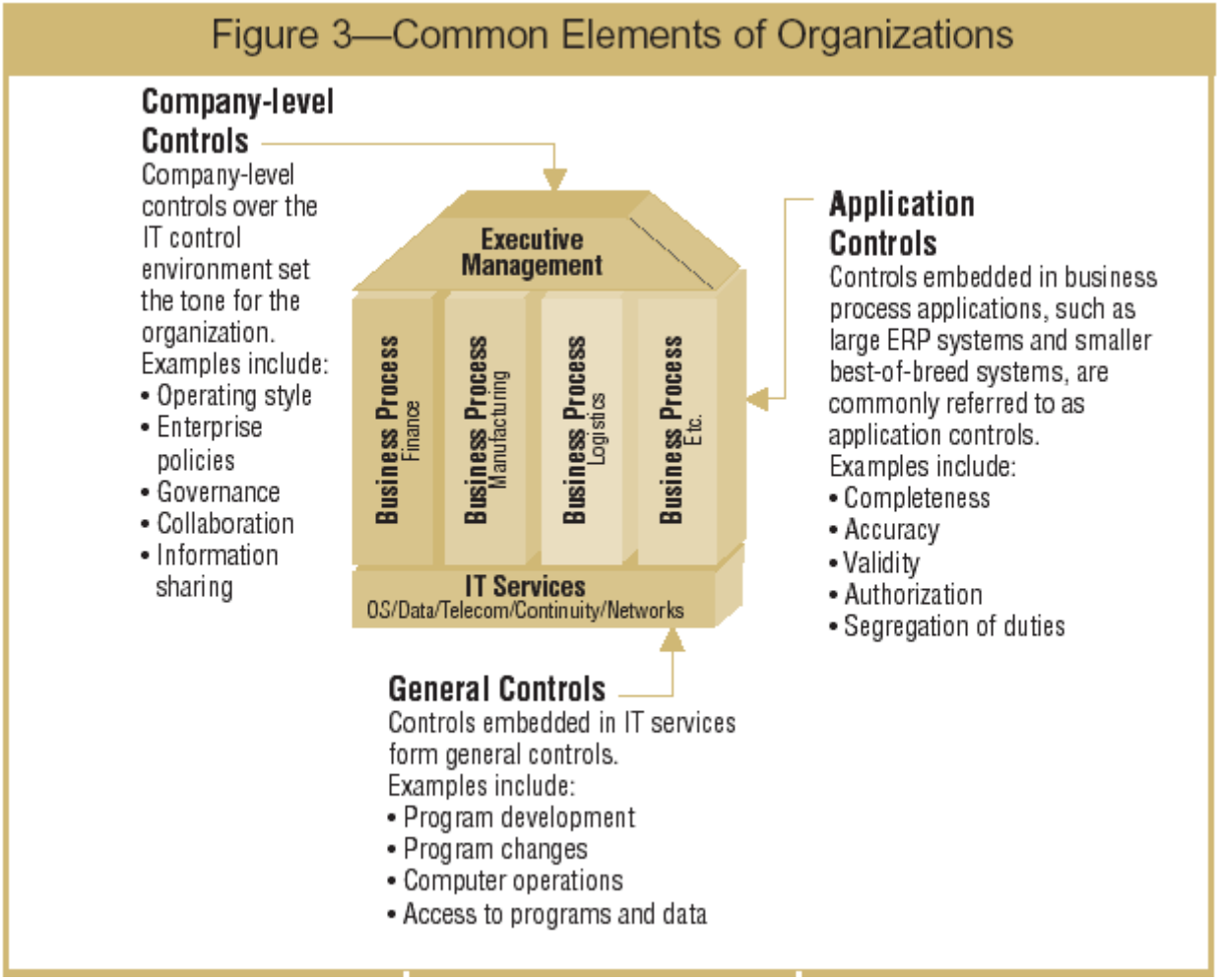
- Les SI sont indissociables des processus de l'entreprise en général et du processus de reporting financier en particulier. La maîtrise des applications et leur bonne gestion et administration sont, à ce titre, une partie intégrante du contrôle interne.
- Les systèmes d'information sont impliqués en tant que processus (sous la responsabilité SI) et dans le cadre de mise en œuvre de fonctionnalités (sous la responsabilité des utilisateurs).

Le contrôle interne informatique

- Les contrôles au niveau de l'entité sont le reflet de l'environnement de contrôle et de l'impulsion que lui donne la direction générale. Ces contrôles généraux concernent généralement les différents environnements techniques et l'ensemble des applications, et définissent le cadre général qui permet de maintenir et de contrôler les processus et l'intégrité des données. (développements et infrastructures techniques).

- Les contrôles au niveau des processus du SI sont composés :
  - ***des contrôles généraux informatiques :*** *contrôles internes au sein des processus de gestion et d'administration des systèmes d'information, mis en œuvre par les informaticiens au niveau d'un site ou d'une plate-forme technique ou par des utilisateurs, généralement responsables des applications,*
  - ***des contrôles applicatifs*** *qui contribuent à assurer l'exhaustivité, la réalité et l'intégrité des données restituées par les applications informatiques.*

Les contrôles informatiques



Company-Level Controls Exemple

Points to Consider	Responses	Comments
IT Strategic Planning		
1. Has management prepared strategic plans for IT that align business objectives with IT strategies? Does the planning approach include mechanisms to solicit input from relevant internal and external stakeholders affected by the IT strategic plans?	☐ Yes ☐ No	Comments
2. Does management obtain feedback from business process owners and users regarding the quality and usefulness of its IT plans for use in the ongoing risk assessment process?	☐ Yes ☐ No	Comments
3. Does an IT planning or steering committee exist to oversee the IT function and its activities? Does committee membership include representatives from senior management, user management and the IT function?	☐ Yes ☐ No	Comments
4. Are IT strategies and ongoing operations formally communicated to senior management and the board of directors, e.g., through periodic meetings of an IT steering committee?	☐ Yes ☐ No	Comments
5. Does the IT organization ensure that IT plans are communicated to business process owners and other relevant parties across the organization?	☐ Yes ☐ No	Comments
6. Does IT management communicate its activities, challenges and risks on a regular basis with the CEO and CFO? Is this information also shared with the board of directors?	☐ Yes ☐ No	Comments
7. Does the IT organization monitor its progress against the strategic plan and react accordingly to meet established objectives?	☐ Yes ☐ No	Comments

General IT controls Exemple

Figure 22—Manage Operations	
Control Guidance	
Control Objective—Controls provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing, error monitoring and system availability.	
Rationale—Managing operations addresses how an organization maintains reliable application systems in support of the business to initiate, record, process and report financial information. Deficiencies in this area could significantly impact an entity's financial reporting. For instance, lapses in the continuity of application systems may prevent an organization from recording financial transactions and thereby undermine its integrity.	
Illustrative Controls	**Illustrative Tests of Controls**
Management has established and documented standard procedures for IT operations, including scheduling, managing, monitoring and responding to security, availability and processing integrity events.	Determine if management has documented its procedures for IT operations, and operations are reviewed periodically to ensure compliance. Review a sample of events to confirm that response procedures are operating effectively. When used, review the job scheduling process and the procedures in place to monitor job completeness.
System event data are sufficiently retained to provide chronological information and logs to enable the review, examination and reconstruction of system and data processing.	Determine if sufficient chronological information is being recorded and stored in logs, and it is useable for reconstruction, if necessary. Obtain a sample of the log entries, to determine if they sufficiently allow for reconstruction.

Application Controls

Figure 24—Application Control Objectives for the Purchasing Cycle

Illustrative Control Objectives	Financial Statement Assertions
Purchase orders are placed only for approved requisitions.	Validity
Purchase orders are accurately entered.	Valuation
All purchase orders issued are input and processed.	Completeness
Amounts posted to accounts payable represent goods or services received.	Validity
Accounts payable amounts are accurately calculated and recorded.	Valuation
All amounts for goods or services received are input and processed to accounts payable.	Completeness
Amounts for goods or services received are recorded in the appropriate period.	Valuation Occurrence
Accounts payable are adjusted only for valid reasons.	Completeness Validity
Credit notes and other adjustments are accurately calculated and recorded.	Valuation
All valid credit notes and other adjustments related to accounts payable are input and processed.	Completeness Validity

Plan de la présentation

Référentiel pour les systèmes d'information

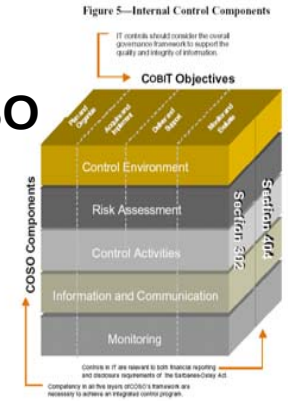
U.S. SECURITIES AND EXCHANGE COMMISSION

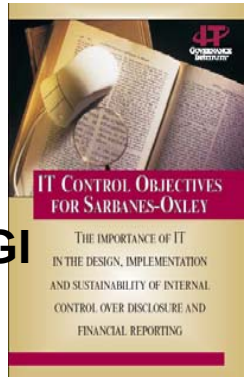
"We are the investor's advocate."
William O. Douglas
SEC Chairman, 1937-1939

PCAOB

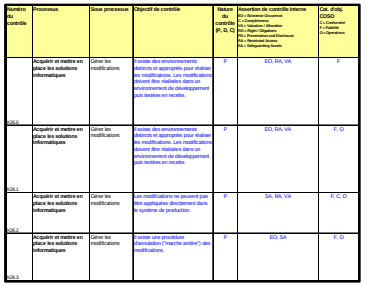
ITGI

COSO





ITGI



Matrice de contrôle interne informatique

PCAOB Auditing Std n°2

PCAOB (Public Company Accounting Oversight Board) est en charge de l'établissement des règles de la profession et de la surveillance des auditeurs.

50. Some controls (such as company-level controls, described in paragraph 53) might have a pervasive effect on the achievement of many overall objectives of the control criteria. For example, information technology general controls over program development, program changes, computer operations, and access to programs and data help ensure that specific controls over the processing of transactions are operating effectively. In contrast, other controls are designed to achieve specific objectives of the control criteria. For example, management generally establishes specific controls, such as accounting for all shipping documents, to ensure that all valid sales are recorded.

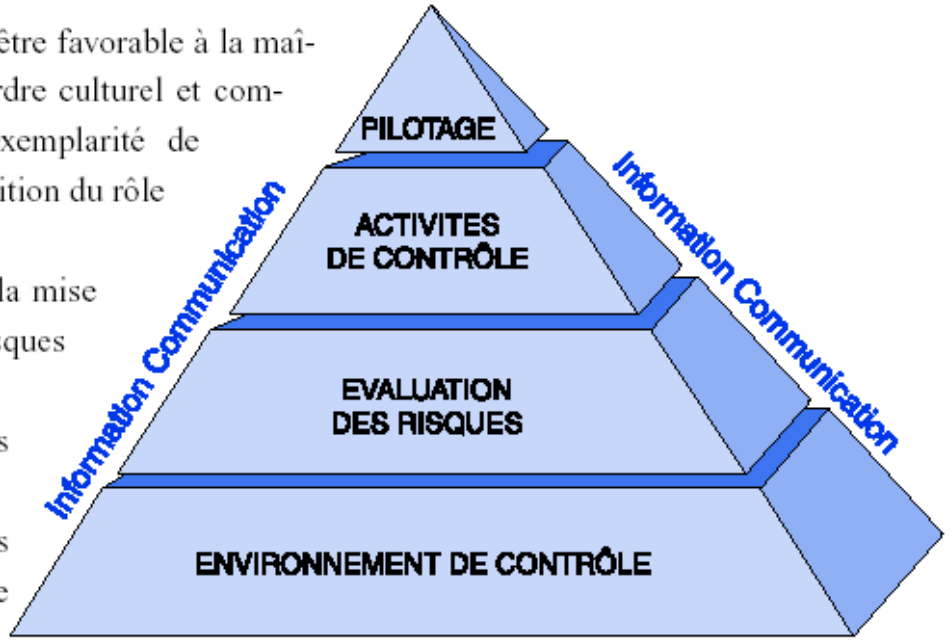
Le COSO Committee of Sponsoring Organizations

SOA ne fournit pas de directives spécifiques quant à la définition du contrôle interne approprié, ce dernier pouvant varier sensiblement d'une entreprise à l'autre.
Cependant, dans ses règles finales édictées en juin 2003, la SEC a identifié l'infrastructure de contrôle interne COSO en tant qu'infrastructure répondant à ses critères en matière de recommandations pour l'évaluation et le développement des contrôles.
Le COSO : trois objectifs, cinq composants, p processus pour un contrôle interne efficace.

Le COSO*

L'environnement de contrôle, qui doit être favorable à la maîtrise des risques est essentiellement d'ordre culturel et comportemental : intégrité et éthique, l'exemplarité de l'attitude du management, la bonne définition du rôle de chacun et le respect des structures.

L'évaluation des risques, essentielle à la mise en œuvre de stratégies de maîtrise de risques adaptées.



Les activités de contrôle interne mises en œuvre par chaque manager :

- des objectifs clairs, cohérents avec les missions du manager et la stratégie de l'entreprise ;
- des moyens adaptés ;
- un système d'information, qui permet de mesurer la réalisation des objectifs ;
- l'organisation qui met en œuvre le bon fonctionnement des moyens ;
- les méthodes et procédures pour bien opérer les tâches définies ;
- la supervision pour vérifier l'avancement des objectifs et les faire évoluer en fonction du contexte.

L'information et la communication entre les différents acteurs de l'entreprise.

Le pilotage du Système de Contrôle Interne.

(*) voir site IFACI

Le COBIT

- L'infrastructure COSO donne peu d'informations concernant les contrôles IT spécifiques. Par conséquent, nombreuses sont les entreprises qui ont choisi l'infrastructure COBIT (Control Objectives for Information and related Technology).
- Pour rappel, le COBIT :
  - *est rédigé par l'IT Governance Institute, édité par l'ISACA (Information System Audit & Control Association). La version française est publiée par l'AFAI (Association Française de l'Audit et du conseil Informatique).*
  - *est le modèle de référence en matière d'audit et de maîtrise des systèmes d'information.*
  - *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.

Le document de l'ISACA/ITGI

Ce document établi la correspondance entre les contrôles généraux IT du PCAOB, les objectifs de contrôle du COBIT et les objectifs du COSO.

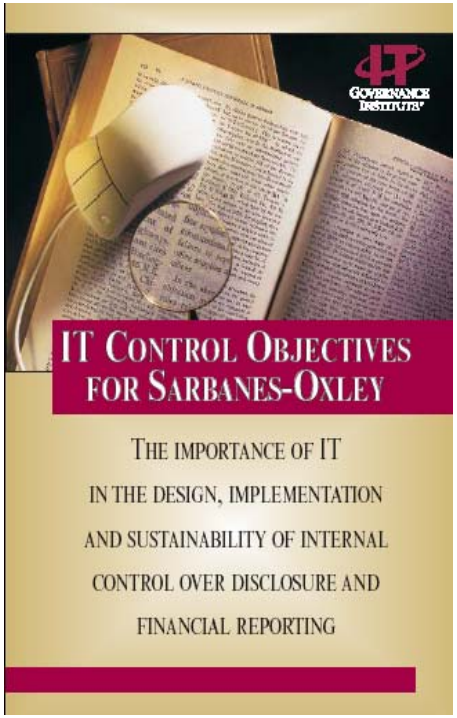


Figure 1—Control Processes

CobiT Control Objective Heading	PCAOB IT General Control Heading: Program Development	Program Changes	Computer Operations	Access to Programs and Data
1. Acquire or develop application software.	●	●	●	●
2. Acquire technology infrastructure.	●	●	●	
3. Develop and maintain policies and procedures.	●	●	●	●
4. Install and test application software and technology infrastructure.	●	●	●	●
5. Manage changes.		●		●
6. Define and manage service levels.	●	●	●	●
7. Manage third-party services.	●	●	●	●
8. Ensure systems security.			●	●
9. Manage the configuration.			●	●
10. Manage problems and incidents.			●	
11. Manage data.			●	●
12. Manage operations.			●	●

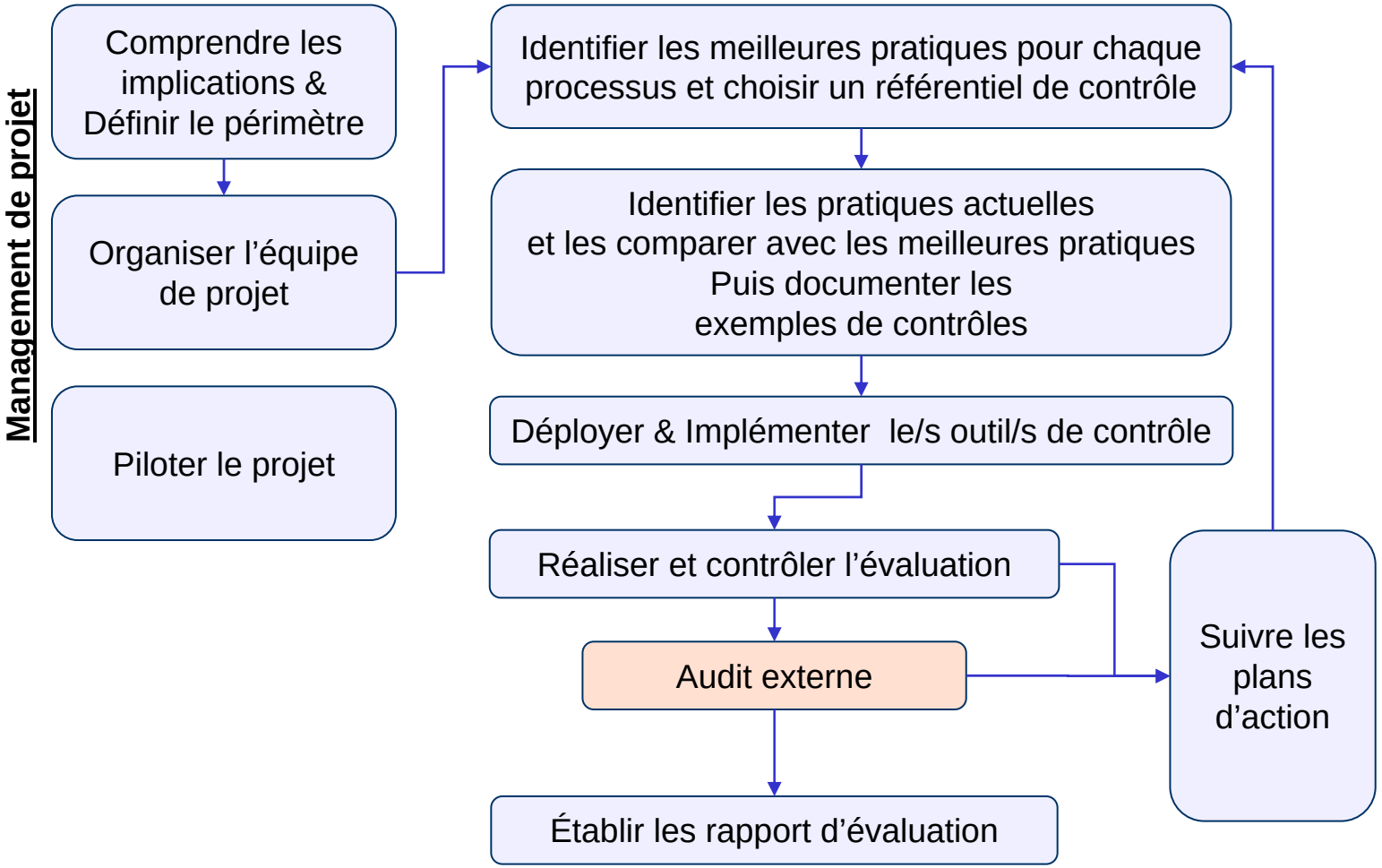
Un exemple de modèle de matrice de contrôle

Processus	Sous-processus	Objectif de contrôle	Nature du risque	Exemple de contrôle	Exemple de test de contrôle	Element du COSO
Acquérir et mettre en place les solutions informatiques	Gérer les modifications	S'assurer qu'aucune modification sur un système est effectuée de façon inappropriée ou frauduleuse	Une modification sur un système, effectuée de façon inappropriée ou frauduleuse, pourrait impacter la fiabilité du reporting financier, la disponibilité du système ou l'intégrité du dispositif de contrôle interne.	Les mises en production ne peuvent être effectuées qu'après l'obtention d'une validation appropriée (validation du demandeur, autorisation de mise en production).	=> Sélectionner un échantillon de mise en production (application et système) et vérifier que ces évolutions ont été dûment testées et approuvées préalablement à leur mise en production (vérifier l'existence d'une preuve formelle de l'approbation).	Activités de contrôle Monitoring

Plan de la présentation

I - Contexte	16:30
II - De la loi à l'implémentation	16:45
III -Conduite d'un programme SOA	17:00
IV -Retour d'expérience	17:15
V - Questions / Réponses	17:30

Une démarche de projet



Type de documentation produite

- 3 niveaux de contrôles sont à prendre en compte et doivent être documentés de manière appropriée.
  - *« Company Level Controls »*
  - *« General Controls »*
  - *« Application Controls »*
- La documentation doit démontrer la traçabilité entre les risques liés à la production des états financiers, les objectifs de contrôle, les activités contrôles, les tests et les plans d'action.
  - *Avant la phase d'évaluation, des documents standards sont réalisés, de manière à assurer la cohérence d'ensemble de la documentation. Ces documents sont particulièrement importants dans le cadre d'une grande entreprise.*
  - *Pendant la phase d'évaluation, les documents finaux, qui sont réalisés au niveau de chaque entité.*

Quelques inducteurs de charge

- Complexité de l'organisation:
  - *Nombre d'entités juridiques*
  - *Type d'organisation (identification plus ou moins facile des « process owners »)*
  - *Nombre de métiers différents*
  - *Couverture géographique*
- Complexité du SI
  - *Nombre d'applications*
  - *Niveau de mutualisation des systèmes et des pratiques*
  - *Types d'applications (ERP ou développements internes)*
- Référentiel et culture
  - *Pré-existence d'un référentiel de bonnes pratiques en interne et niveau de partage*
  - *Niveau et cohérence de la documentation des applications (existence d'autres cadres réglementaires)*
  - *Objectifs du projet SOA (notion de « juste nécessaire »)*

Plan de la présentation

I - Contexte	16:30
II - De la loi à l'implémentation	16:45
III - Conduite d'un programme SOA	17:00
IV -Retour d'expérience	**17:15**
V - Questions / Réponses	17:30

Attentes de l'auditeur externe *

- Processus informatique soit un processus à part entière
- Contrôles pouvant s'aligner sur le Cobit
- Formalisation des contrôles
- Points clé : Change control et Logical security
- Période de fonctionnement des contrôles suffisamment longue

(*) extrait de la présentation de KPMG – LSF/SOX et informatique : retour d'expérience vécues par les auditeurs
16 novembre 2004 (AFAI/IFACI)

Difficultés habituelles rencontrées*

- Sous-estimation de la charge de documentation
- Hétérogénéité des pratiques IT, des applications et des systèmes
- Superposition avec des normes déjà en place (ISO, Qualité)
- Impossibilité pratique à effectuer des actions de rémédiation dans les délais
- Prestataires ne pouvant pas fournir de rapport SAS 70 type II

(*) extrait de la présentation de KPMG – LSF/SOX et informatique : retour d'expérience vécues par les auditeurs
16 novembre 2004 (AFAI/IFACI)

Conclusion

La maîtrise des Systèmes d'Information

Le SI joue un rôle essentiel sur le contrôle interne.

Extrait du PCAOB Auditing Standard No. 2

« The nature and characteristics of a company's use of information technology in its information system affect the company's internal control over financial reporting. »

Liens (1/2)

- La loi en PDF : news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf
- Le site Sarbanes-Oxley : www.sarbanes-oxley.com
- 404 institute : www.404institute.com
- PCAOB : www.pcaobus.org/rules/Release-20040308-2.pdf
- FEI survey – Sarbanes-Oxley compliance cost estimates : www.fei.org/news/404_july.cfm
- IT control Objectives for Sarbanes-Oxley : www.itgi.org
- Association française d'audit et de conseil informatique (AFAI) : www.afai.fr/
- Institut de l'Audit interne(IFACI) : www.ifaci.com
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) : *www.coso.org*

Liens (2/2)

- Protiviti : bulletin consacré à l'impact de la Loi de Sécurité Financière sur le contrôle interne informatique
  http://www.protiviti.fr/downloads/PRO/pro-fr/lebulletin03.pdf
- US Securities and Exchange Commission, USA, June 2003, Final Rule
  www.sec.gov/rules/final/33-8238.htm
- "Taking Control, A Guide to Compliance with Section 404 of the Sarbanes- Oxley Act of 2002," Deloitte & Touche, 2003
- "The Defining Issues—Implications of Proposed Auditing Standard on Internal Control," KPMG, 2003
- "The Sarbanes-Oxley Act of 2002, Strategies for Meeting New Internal Control Reporting Challenges," PricewaterhouseCoopers, 2003
- "The Sarbanes-Oxley Act of 2002, The Current Landscape—Rules, Updates and Business Trends," Ernst & Young, 2003

Conclusion

La maîtrise des Systèmes d'Information

Notre approche :

Transformer une contrainte réglementaire en levier d'amélioration de la performance opérationnelle

SOA

Effet d'aubaine

ou

Risque du "pompier-pyromane" ?

Plan de la présentation

I - Contexte	16:30
II - De la loi à l'implémentation	16:45
III -Conduite d'un programme SOA	17:00
IV -Retour d'expérience	17:15
V - Questions / Réponses	**17:30**

La maîtrise des Systèmes d'Information

Questions - réponses

La maîtrise des Systèmes d'Information

Extraits du discours de John A. Thain - CEO / NYSE (27/05/2004) à l'Economic Club of New York City

« The Sarbanes-Oxley is the most important securities legislation since the original federal securities laws of the 1930's. The new governance and accountability standards are far-reaching. » Chairman Donaldson

« The strength of the legislation, reinforced by the efforts of (….) the PCAOB, is helping to restore investor confidence in U.S. companies. »

« Compliance efforts have required an average of 12,000 hours of internal work and 5,000 hours of external work – at least double original estimates. »

« Since the inception of Sarbanes-Oxley, fees paid to outside auditors have increased by double digits year over year. »