Le projet SOX chez Alcatel

Forum CERT-IST, 08/06/2006

Alcatel • ICT Services

ALCATEL

Présentation SOX

Qu’est-ce que SOX ?

Le projet SOX

Le champ d’application

L’organisation

Le déroulement

La vie après SOX…

La Loi Sarbanes-Oxley

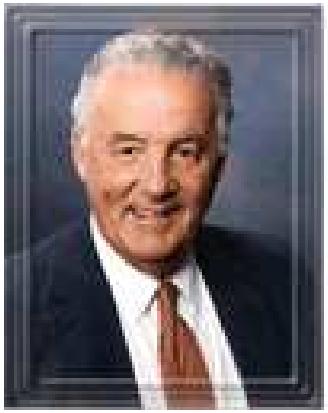
La loi Sarbanes-Oxley (Sarbanes-Oxley Act, ou SOX) a été introduite aux USA en Juillet 2002 à la suite des scandales des affaires Enron, Worldcom, Global Crossing, Tyco, etc.

Elle a pour objectif de s'assurer que les entreprises mettent en place les bons **contrôles** en matière financière, et dans ce cadre elle s'intéresse en particulier :

- **à la sécurité financière**
- **aux règles de comptabilité**

La Loi Sarbanes-Oxley

Elle tire son nom du nom de ses deux promoteurs, les sénateurs américains Paul Sarbanes et Michael Oxley :



Paul S. Sarbanes , US Senator from Maryland, serves as Member of the Senate Banking, Housing and Urban Affairs Committee, and is a senior member of the Foreign Relations, Budget and Joint Economic Committees. and is a senior member of the Foreign Relations, Budget and Joint Economic Committees.

Congressman ***Michael G. Oxley*** is serving his eleventh term in the US House of Representatives (4th District of Ohio) and is Chairman of the House Committee on Financial Services.

La Loi Sarbanes-Oxley

La loi SOX est basée sur trois principes:

- L'exactitude et l'accessibilité de l'information
- La responsabilité des managers
- L'indépendance des auditeurs

Toute société désirant se conformer à SOX doit :

- Mettre en place les contrôles internes sur les processus financiers, ainsi que **IS et IT** comme supports de ces processus
- Être certifiée par des auditeurs externes
- Maintenir un suivi du cycle de vie des documents
- Archiver toutes les données pour une période d'au moins cinq ans

La Loi Sarbanes-Oxley

En effet la loi a été créer essentiellement pour aider les entreprises à mettre en place suffisamment de **contrôles** internes pour éviter:

- La fraude
- L'utilisation erronée de données financières
- La perte de transactions financières

Un des aspects clé de la loi Sarbanes-Oxley est de s'assurer qu'aucun individu ne soit en mesure de manipuler les données financières d'une manière frauduleuse.

La non-conformité peut conduire (aux USA) à:

- L'exclusion d'une société de la bourse américaine
- Des sanctions civiles sévères (amendes financières)
- Des sanctions criminelles sévères (emprisonnement des dirigeants)

SOX : Responsabilité du CEO et du CFO, sections 302 et 404

Responsible for ensuring the organization is in compliance with the requirements of sections 302 and 404 and other requirements of the SOX Act

- Section 302 requires management to evaluate and report on the effectiveness of disclosure controls and procedures with respect to the quarterly and annual reports. The CEO and CFO must certify that they
  - Are responsible for disclosure controls
  - Have designed controls to ensure that material information is known to them
  - Have evaluated the effectiveness of controls
  - Have presented their conclusions in the filing
  - Have disclosed to the audit committee and auditors significant control deficiencies and acts of fraud
  - Have indicated in the report significant changes to controls
- Section 404 requires management to document and evaluate the design and operation, and report on the effectiveness, of its internal control over financial reporting. The internal control report includes the following components :
  - Management's recognition of its responsibility for establishing and maintaining adequate internal control and procedures for financial reporting
  - The framework used in the evaluation
  - Management's assessment of the effectiveness of internal control over financial reporting. Any material weaknesses must be disclosed.
  - A statement indicating that external auditors have issued an attestation report on Management's assessment of effectiveness of internal control over financial reporting

SOX : L'équipe Project Alcatel

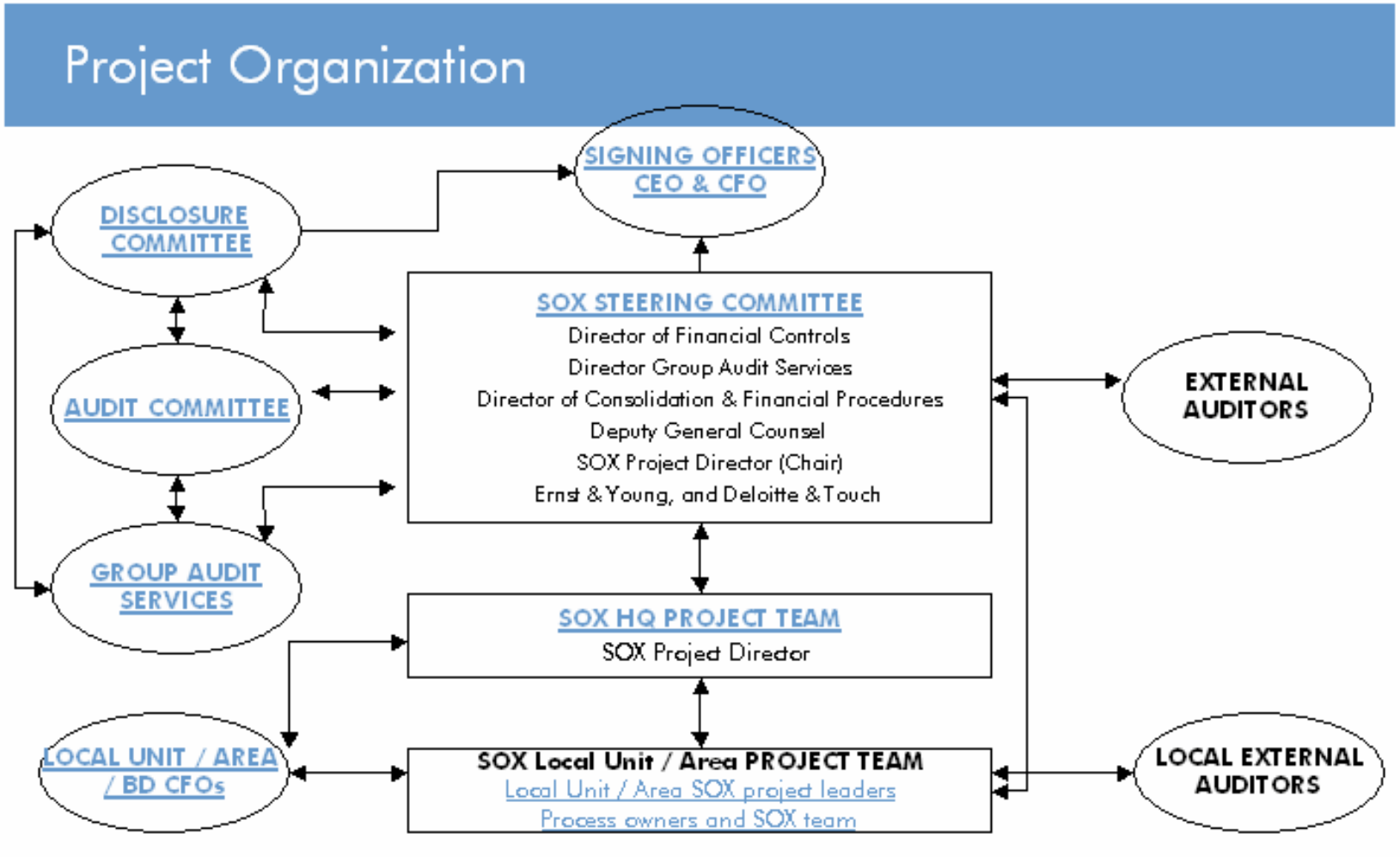
Chez Alcatel, SOX est géré comme un projet à part entière, impliquant :

- le Corporate
- les trois Régions (Amérique Nord, Europe+Amérique Sud, Asie)
- les équipes internes de l'infrastructure IT
- les équipes internes des applications IS
- le Groupe Audit interne

Au total, 110 personnes ont été, en plus de leurs missions courantes, investies de missions de management spécifiques pendant les 30 mois du projet.

Plusieurs centaines de personnes ont été impliquées à un moment ou à un autre du projet.

SOX : Project organization

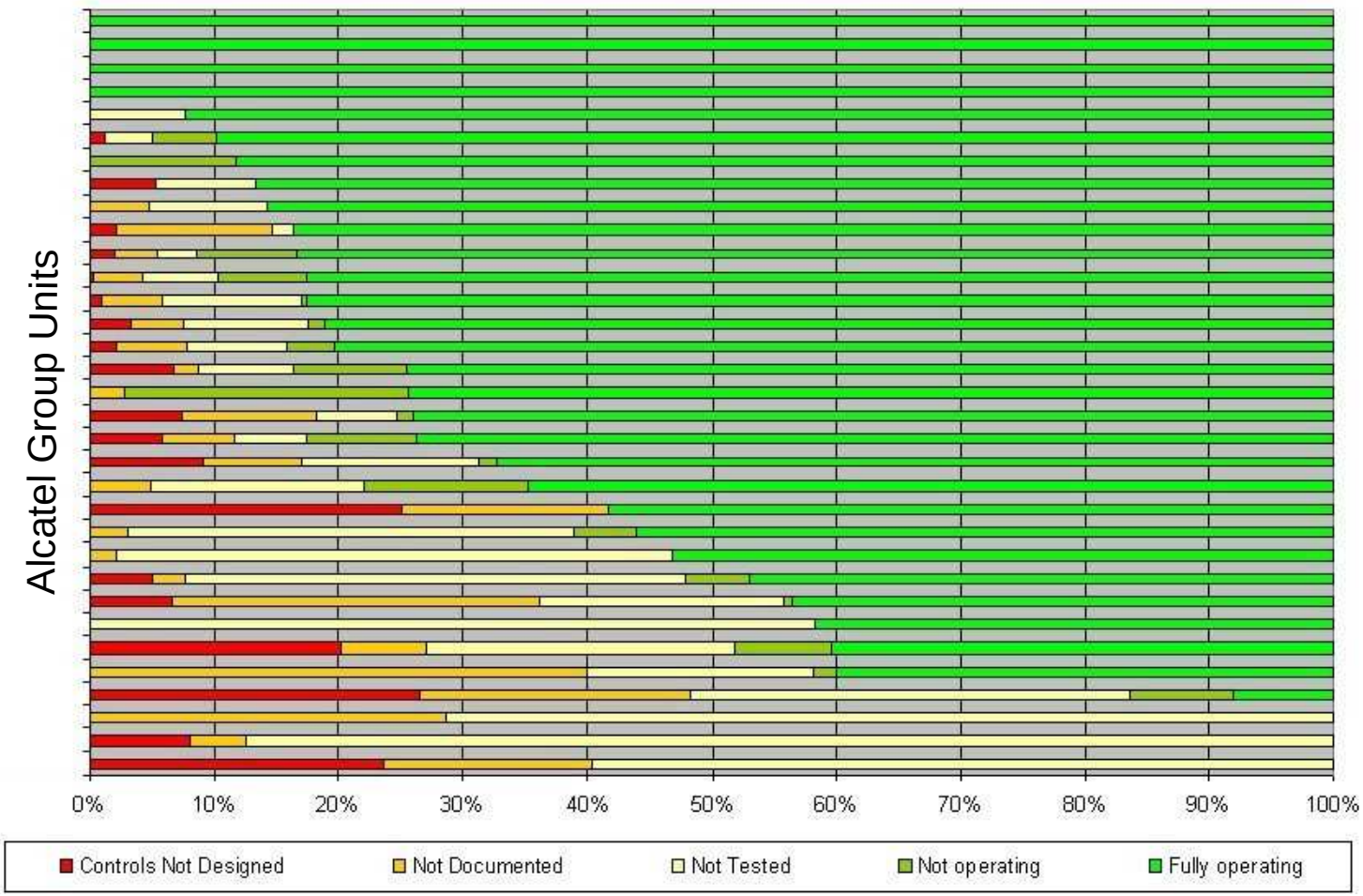


SOX : Phases du Projet

Les phases de Projet SOX sont:

- **Documentation des contrôles**
- **Identification et Implémentation des actions correctives**
- **Audit par les auditeurs internes Alcatel GAS**
- **Audit par les auditeurs externes**
- **Signature du rapport par le CEO et le CFO**
- **-> Conformité SOX**

SOX : Vue d'ensemble des progrès (01/2005)



SOX : Processus financiers

Alcatel financial applications

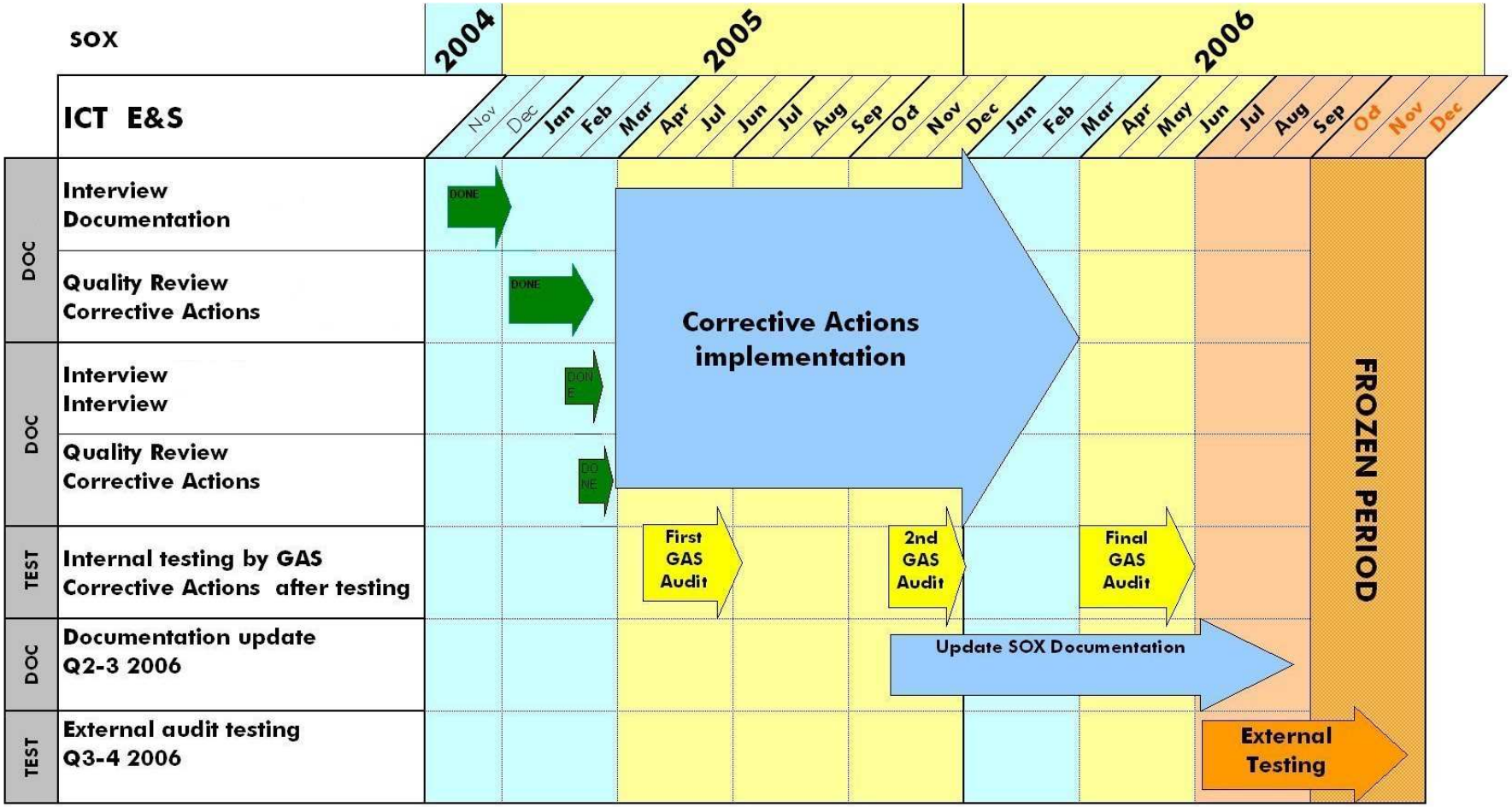
Alcatel countries

Tier 1 units										
				x		x	x	x	x	x
	x	x	x	x	x	x	x	x	x	x
	x	x	x	x		x	x	x	x	x
	x			x		x	x	x	x	x
	x	x	x	x	x	x	x	x	x	x
		x	x	x	x	x	x	x	x	x
		x	x	x	x	x	x	x	x	x
	x	x	x	x		x	x	x	x	x
	x	x	x	x		x	x	x	x	x
	x		x	x		x	x	x	x	x
	x			x		x	x	x	x	x
	x				x	x		x	x	x
Tier 2 units										
	x					x			x	
				x	x	x			x	x
				x	x	x			x	x
					x					
					x	x			x	
									x	
	x								x	
						x		x		
						x			x	x
	x									
					x	x	x			x	x
					?					?	
					x						
					x						
		x									
					x						
							x				
		x									
	x				x	x					
		x									
		x									
										x	

Alcatel countries

X : full documentation and tests of controls with the software tool

SOX : example de plan de projet (partie IT E&S)



SOX : Après le projet

Chaque année, l'entreprise doit démontrer l'efficacité des contrôles internes:

- Les contrôles de documents doivent être maintenus
- L'efficacité de contrôles est évaluée par l'Audit interne
- Les disfonctionnements doivent être résolus dans le plus bref délais

La loi SOX, qui a une envergure internationale, aura été considérée par les **responsables de la sécurité** comme un remarquable **outil pour accélérer des améliorations** qui sans elle auraient été beaucoup plus difficiles à mettre en place aussi rapidement.

SOX et le Cert-IST

C'est au travers de la couverture des exigences ISO 17799 listées ci-dessous que le Cert-IST aide à satisfaire les exigences SOX
(car l'ISO 17799 répond aux exigences de la section 404 de SOX sur l'implantation des contrôles liés à la sécurité de l'information financière).

6.1.7 Contact with special interest groups

- Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.

12.6.1 Control of technical vulnerabilities

- Timely information about technical vulnerabilities of information systems being used should beobtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measurestaken to address the associated risk.

13.2 Management of information security incidents and improvements

- Responsibilities and procedures should be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of information security incidents.Where evidence is required, it should be collected to ensure compliance with legal requirements.

SOX, le Cert-IST, et Alcatel *(Shangai Bell …)*

Hello,

For the following step:
09.020.c010 step 1 : All available patches are analysed by IT security team for potential implementation.
We have implemented a process for the datacenter of Velizy based on the analysis of the CERT alerts. To be available also for ASB it request the problem management process implemented in ASB with Vega OPS. P. Bailly told me that the plan is to have it available for ASB in Q1 Y06. Can you confirm the plan?

09.060.c010 step 3 : Yearly security self-assessment is conducted by ISO according to corporate security self-assessment questionnaire. (can not change date). We have no plan for a global security self-assessment. In the other area, the local ISO performs a yearly self-assessment. This is part of his mission. In addition to that we have security audits from GAS with a correction plan that can be added to the results of the local self-assessment.

For the following step:
09.020.c010 step 1 :
All available patches are analysed by IT security team for potential implementation.
09.060.c010 step 3 :
Yearly security self-assessment is conducted by ISO according to corporate security self-assessment questionnaire.

As you know, ASB wants to take advantage of the global ICT process on patch qualification. But ASB and APAC don't have a plan of PMP implementation before 2Q or 3Q of the year. I am afraid it will be late for SOX compliance testing. So could you suggest is there any way to keep ASB security administrators informed about the CERT-IST advisories? For instance, let one or two ASB colleagues be the member of AES security administrators.

Let me know what is your suggestion.

As you know, ASB wants to take advantage of the global ICT process on patch qualification. But ASB and APAC don't have a plan of PMP implementation before 2Q or 3Q of the year.
I am afraid it will be late for SOX compliance testing.

Herve CHAPPE/FR/ALCATEL @ALCATEL
Sent by: certist@cert-ist.com
10/02/2006 09:39

To: certist@cert-ist.com
cc:
Subject: Fw: CERT and SOX issue

Cher CERT-IST,

Merci d'abonner les employés Alcatel suivants aux avis du CERT en ANGLAIS.
Pour votre information, Alcatel Shangai-Bell est la filiale chinoise du groupe.

pengmao.zhou@alcatel-sbell.com.cn

rong.f.cui@alcatel-sbell.com.cn

Dong.Yang@alcatel-sbell.com.cn

Cher CERT-IST,
Merci d'abonner les employés Alcatel suivants aux avis du CERT en ANGLAIS.
Pour votre information, Alcatel Shangai-Bell est la filiale chinoise du groupe.

BROADEN YOUR LIFE

Alcatel • ICT Services

ALCATEL