



Club ISO 27001 15 Février 2007

La Sécurité : Quelle Approche pour Sarbanes Oxley ?

Claude SERRE
DSSI OrangeFrance





Agenda

- Quelques éléments de contexte :

Groupe France Telecom

- Conformité Sarbanne Oxley

La question : Quelle approche avec quel référentiel ?

La solution : Le Système de Management Intégré

- La Méthode

Le diagnostic : analyse d'écart

Le design : contrôles, plans de test

La cohérence : tests de cheminement

La Conformité : testing

- Conclusion

L'ISO 27001, le grand Véhicule ?...





un des principaux opérateurs de télécoms dans le monde

- une présence dans **220** pays & territoires
- **145,2** millions de clients dans le monde
- CA 2005 : **49** mds d'euros
- résultat net 2005 : **5,7** mds d'euros
- **203 000** salariés



une des toutes 1ères marques mondiales de communication

chiffres au 31/12/05





des positions de 1er plan

mobile
84,3

fixe
49,2

internet
11,7

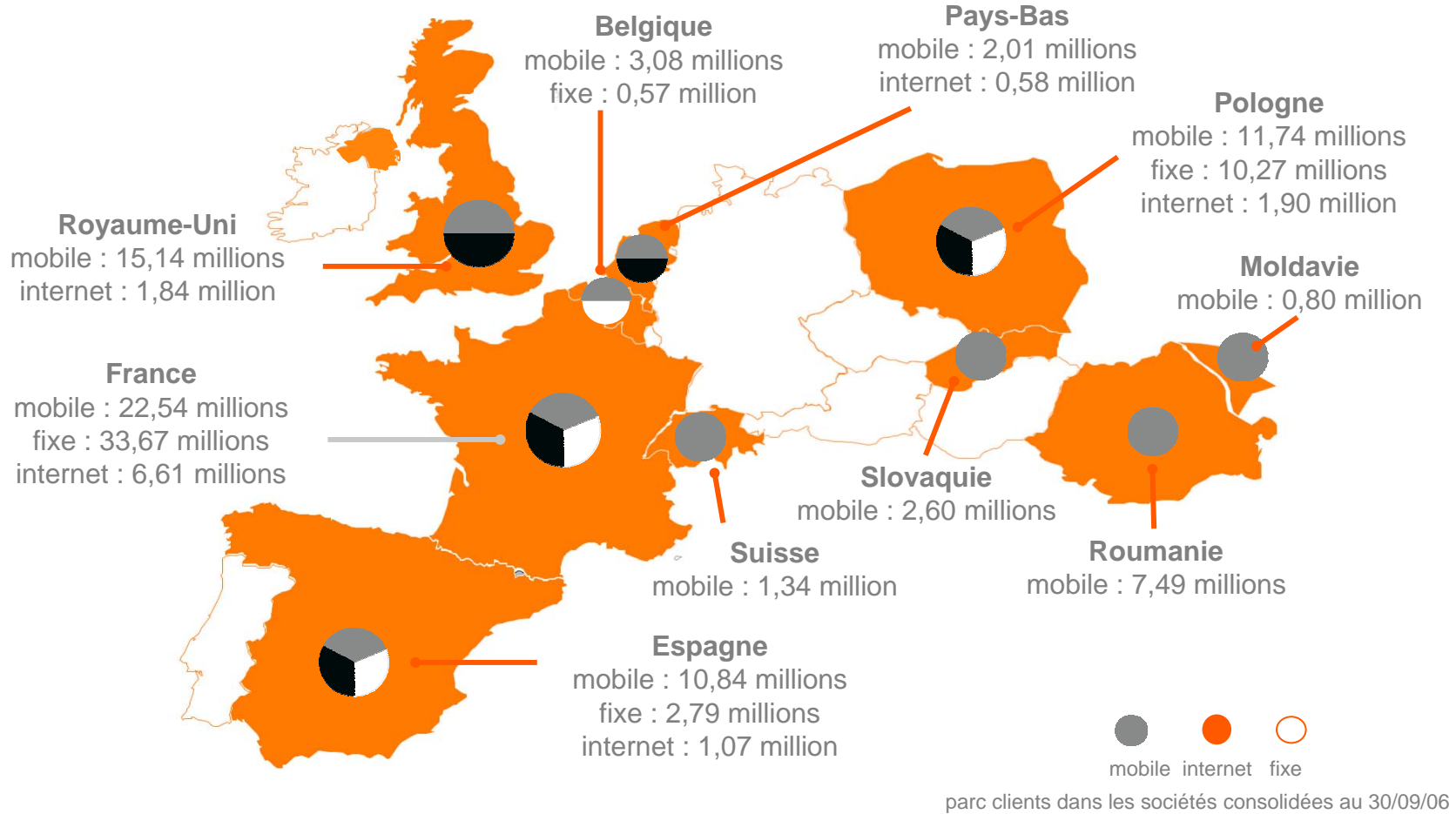
millions de clients dans le monde

parc clients dans les sociétés contrôlées au
31/12/05





1^{er} opérateur intégré en Europe





Agenda

- Quelques éléments de contexte

Groupe France Telecom

- Conformité Sarbanes Oxley

La question : Quelle approche avec quel référentiel ?

La solution : Le Système de Management Intégré

- La Méthode

Le diagnostic : analyse d'écart

Le design : contrôles, plans de test

La cohérence : tests de cheminement

La Conformité : testing

- Conclusion

L'ISO 27001, le grand Véhicule ?...





Sarbanes Oxley : Les fondamentaux

■ Des objectifs communs :

Une transparence accrue de l'information publiée

Une plus grande efficacité du contrôle interne

■ Une responsabilité renforcée

Des Gestionnaires de l'entreprise

Du Commissariat aux Comptes

SOX

- Le directeur général et le directeur financier s'engagent à titre personnel ; ils sont passibles de sanctions pénales lourdes en cas de défaillance caractérisée.
- Ils sont tenus chaque année de certifier l'existence de procédures de contrôle interne et d'attester de la véracité des publications financières (section 302 – déjà en vigueur).
- Le bon fonctionnement du contrôle interne de tous les processus qui concourent à l'élaboration de l'information financière publiée doit être attesté par le management et les Commissaires aux Comptes (section 404 – à partir des comptes 2005).



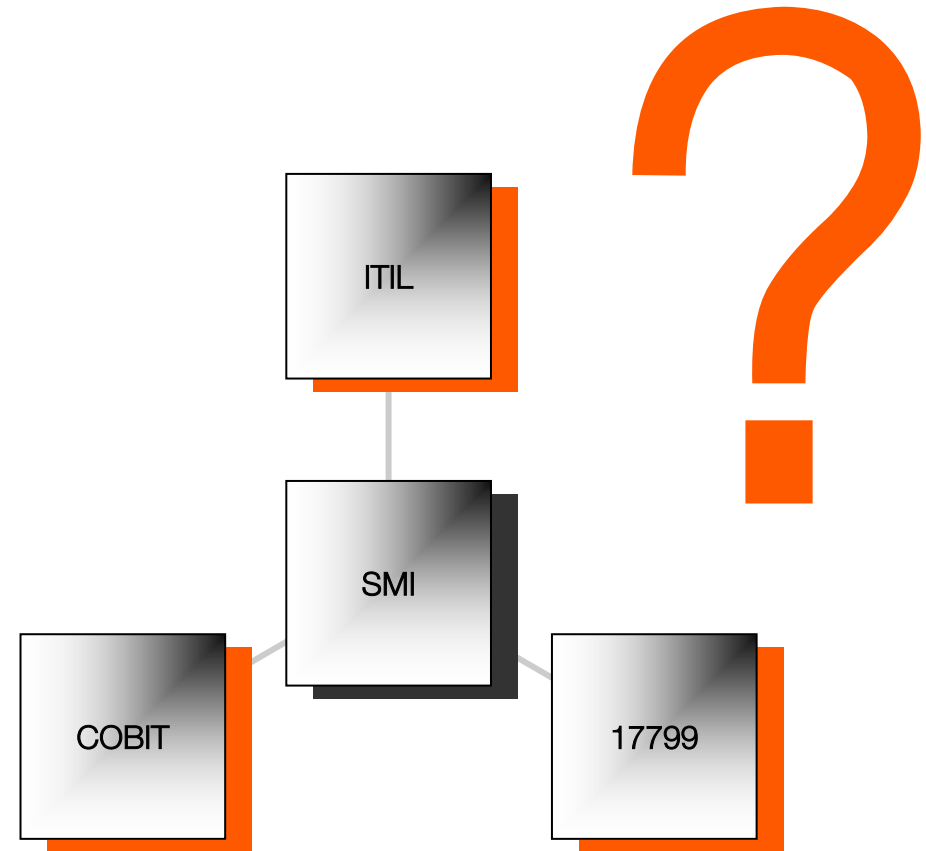
LSF

- Le Président du Conseil d'Administration est tenu de présenter à l'Assemblée Générale annuelle un rapport sur les procédures de contrôle interne mises en place (Article 117)
- Les Commissaires aux Comptes présentent dans un rapport joint à leur rapport sur les comptes, leurs observations sur le rapport du Président du Conseil (Article 120)
- Ces deux rapports seront établis dès la publication des comptes 2003 et seront publiés par les sociétés cotées.

Conformité Sarbanes Oxley

■ **La question :** Quelle approche avec quel référentiel ?

■ **La solution :** L'utilisation du Système de Management de la Qualité ?





Agenda

- Quelques éléments de contexte

Groupe France Telecom

- Conformité Sarbanes Oxley

La question : Quelle approche avec quel référentiel ?
La solution : Le Système de Management Intégré

- La Méthode

Le diagnostic	:	analyse d'écart
Le design	:	contrôles, plans de test
La cohérence	:	tests de cheminement
La Conformité	:	testing

- Conclusion

L'ISO 27001, le grand Véhicule ?...



La Méthode : La Vision Système

- **Le Diagnostic** : Analyse d'écart
ISO 17799 11 Chapitres
ISO 17799 39 Objectifs de sécurité
- **Le Design** : Approche processus
Le contrôle, quelle pertinence ?
Le plan de de test, quelle stratégie ?
- **La Cohérence** : Par la pertinence
Système de Management de la Qualité
Cheminement « bout en bout »
- **La Conformité** : Par le testing
Des contrôles Optimisés





Agenda

- Quelques éléments de contexte

Groupe France Telecom

- Conformité Sarbanes Oxley

La question : Quelle approche avec quel référentiel ?
La solution : Le Système de Management Intégré

- La Méthode

Le diagnostic	:	analyse d'écart
Le design	:	contrôles, plans de test
La cohérence	:	tests de cheminement
La Conformité	:	testing

- Conclusion

L'ISO 27001, le grand Véhicule ?...



Conclusion

- **ISO 27001 : Le Grand Véhicule !**

SOX 302 SOX 404

Un référentiel Opposable ?

Au Commissariat Aux Comptes : PCAOB
, Cobit for Sox





Qui veut gravir une montagne commence par le bas

Proverbe Chinois

MERCI

