MSS Alcatel une réponse aux contraintes légales (Sarbanes-Oxley, …)

Une approche de l'offre de services sécurité d'Alcatel

« SOC for SOX »

Les Assises de la Sécurité / Didier GRAS / 20-10-2005

Résumé

Au delà de la prise en compte de l'ensemble des dispositifs techniques (OS, réseaux, applicatifs, sécurité), de la couverture nécessaire du service rendu (24/7), l'enjeu de l'activité MSS – Managed Security Services repose sur la capacité à délivrer le service attendu de bout-en-bout au sein d'une relation de confiance.

Nous vous proposons de décrire par un exemple (respect d'une réglementation), les réponses apportées par l'offre MSS d'Alcatel afin de répondre concrètement aux besoins des entreprises.

Disposer d'un SOC dans le périmètre de l'entreprise étendue c'est permettre à cette entreprise de disposer d'un atout indéniable et de se focaliser sur son core-business. Le SOC est la réponse attendue face à une cybercriminalité toujours plus réactive et complexe !

AGENDA
SOC for SOX

L'introduction

La présentation de Sox – Sarbanes-Oxley

Une approche des services sécurité délivrés par Alcatel

Qu'apportent les services SOC à SOX ?

Les perspectives

AGENDA
L'introduction

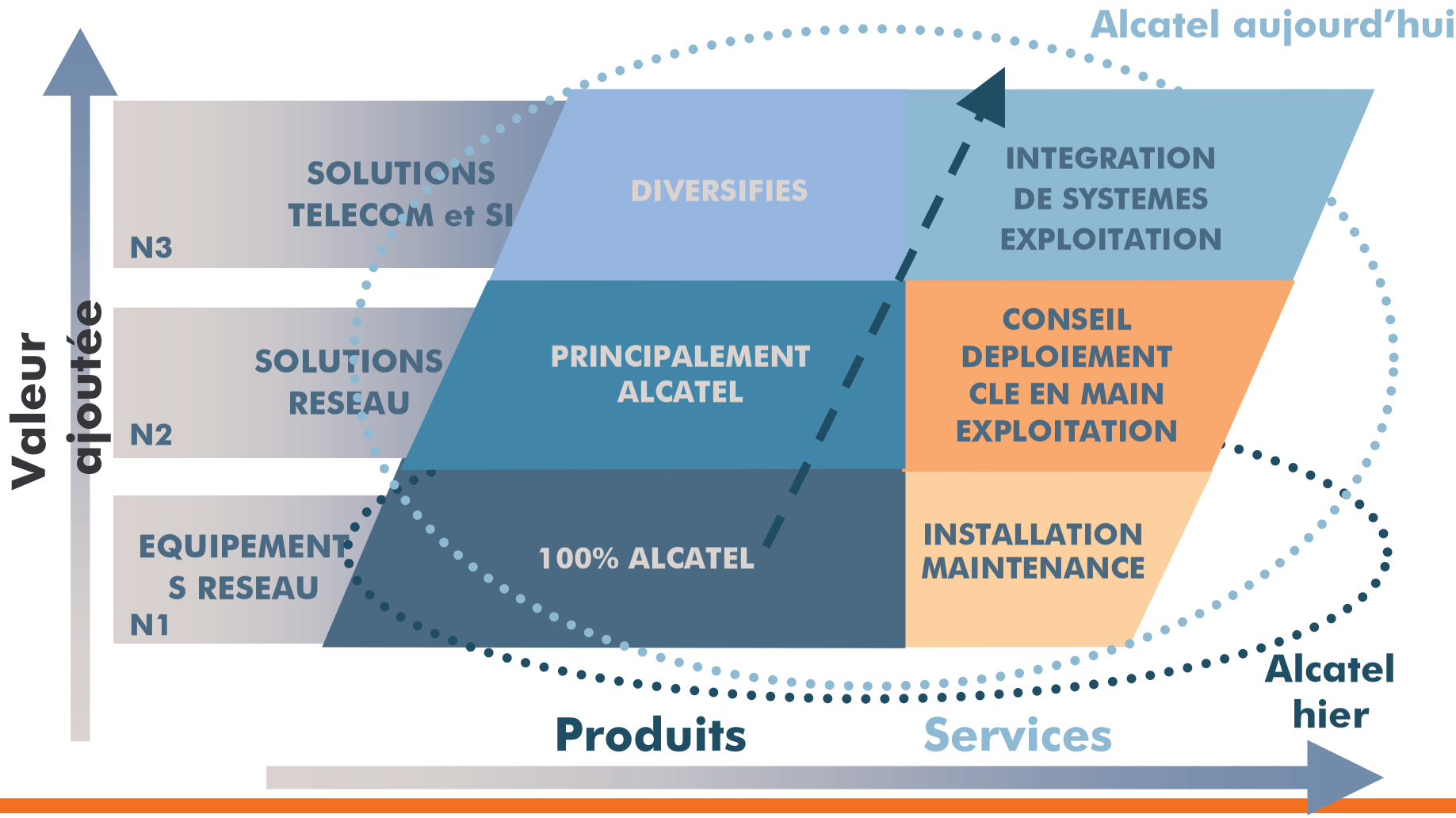
L'introduction

La présentation de Sox – Sarbanes-Oxley

Une approche des services sécurité délivrés par Alcatel

Qu'apportent les services SOC à SOX ?

Les perspectives



AGENDA
La présentation de Sox

L'introduction

La présentation de Sox – Sarbanes-Oxley

Une approche des services sécurité délivrés par Alcatel

Qu'apportent les services SOC à SOX ?

Les perspectives

Présentation de Sox
Une législation pour une meilleure gouvernance d'entreprise

Deux lois sur la sécurité financière ont été promulguées :

- Le Sarbanes-Oxley Act, aux USA, en Août 2002
  (loi applicable aux sociétés cotées aux USA)
- La Loi de Sécurité Financière, en France, en Août 2003

Ces deux lois vont dans le même sens et mettent l'accent sur :

- Une transparence accrue de l'information publiée
- Une plus grande efficacité du contrôle interne

Elles renforcent la responsabilité des gestionnaires et des commissaires aux comptes.

Le Sarbanes Oxley Act

➔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 (Loi de Sécurité Financière)

➔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**.

Présentation de Sox
Des efforts à produire et leur répartition

SOX Section	Requirement
§302,401, 403,406, 407,409, 501,906	Financial Reporting Disclosure; Disclosure of Ownership Changes; Code of Ethics Disclosure; Audit Committee Expertise Disclosure; Material Operating/Financial change Disclosure; etc.
§ 404	Management Assessment of Internal Controls
§103,408, 802,1102	Audit Record Retention and Security; Facilitation of SEC Review; Related Record Retention; etc.
§201,301, 306,402 806	Pre-approval of Non-Audit Services; Audit Committee Monitoring and Complaint Process; Insider Trading During Blackout Prevention; Personal Loan Prevention; Whistle Blower Process; etc.

Change Effort

PROCESS	DATA	PEOPLE	TECHNOLOGY
◑	●	◕	●
◕	●	◑	●
◕	◕	◕	◑
◕	◕	◕	◕

ALCATEL

Présentation de Sox
§404 Comment réaliser ces contrôles internes : COBIT

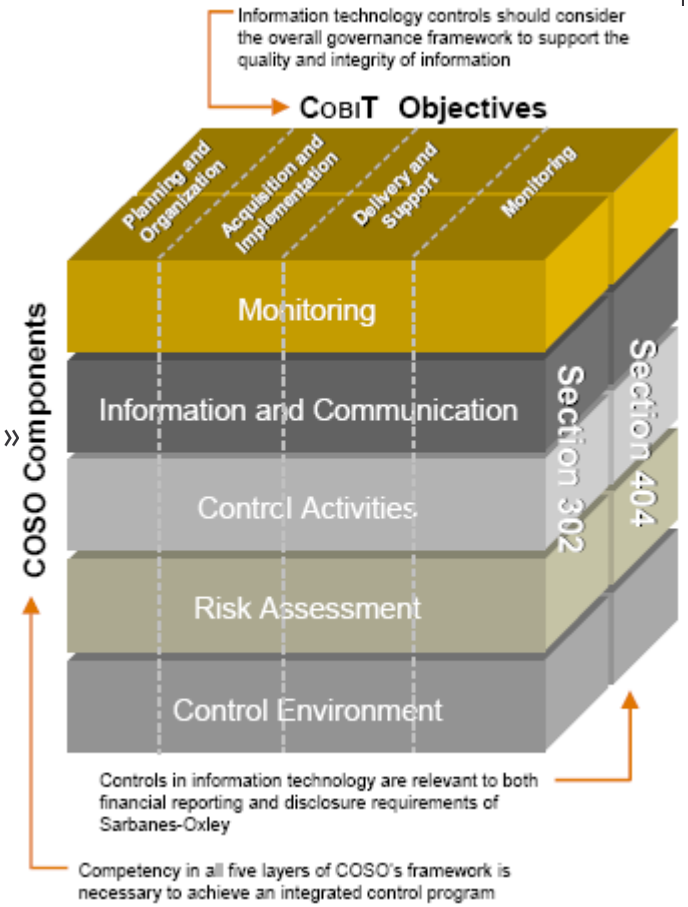
COSO
- COSO est le référentiel de contrôle suivi.
- Les 5 niveaux doivent être traités lors de l'évaluation par le contrôle interne

COBIT
- COBIT est le référentiel de contrôle IT communément accepté.
- COBIT est le référent afin de s'assurer de la qualité et de l'intégrité des informations
- Les contrôles COBIT abordent les 5 couches COSO.

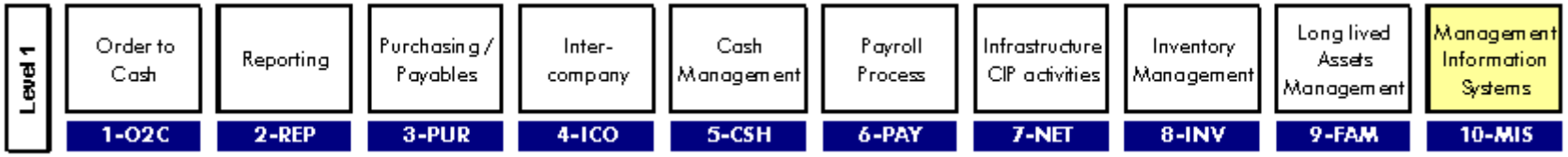
ISO17799
- ISO17799 fournit le référentiel afin de formaliser les politiques, règles et procédures implémentant les contrôles COBIT.

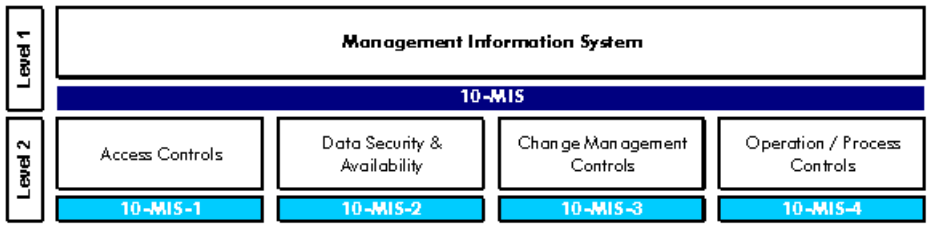
On s'attachera aux sections **302** et **404** mais surtout la « 404 »

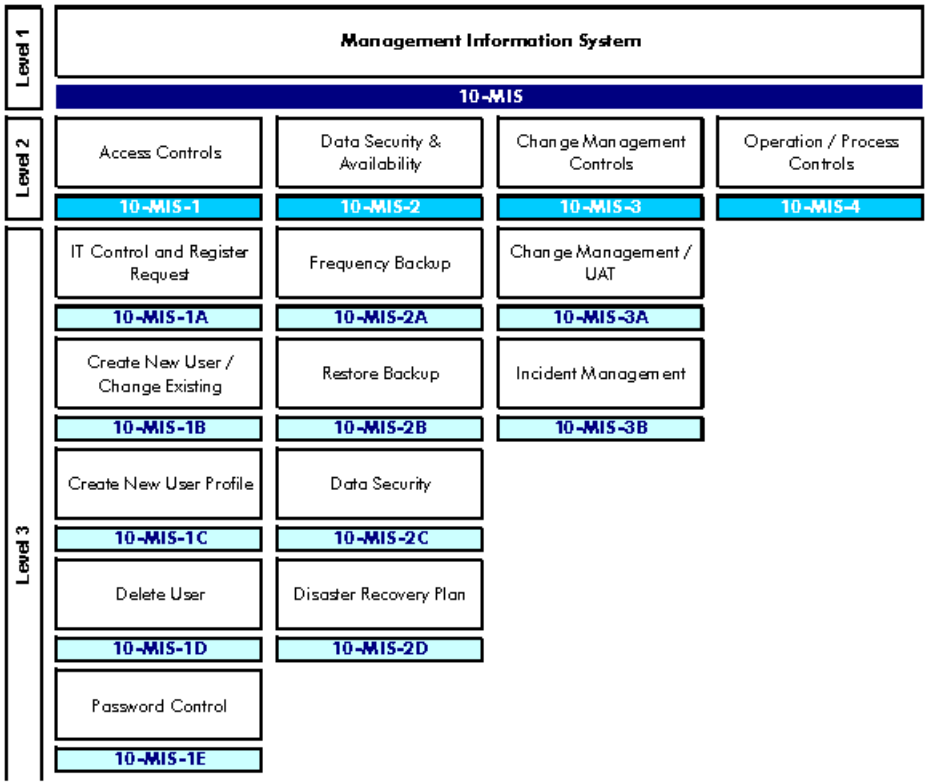
- **Section 302**
  - QUI : la direction (exécutive) de l'entreprise avec la participation du directeur financier et du directeur général
  - QUOI : Corporate Gouvernance
  - QUAND : Opérationnel à partir de Juillet 2002
  - Livrable(s) : Audits annuels et trimestriels
- **Section 404**
  - QUI : la direction (managériale)
  - QUOI : Mise en œuvre du mode de contrôle
  - QUAND : A partir du 15 Novembre 2004 (les filiales non présentes sur le sol américain à partir du 15 Juillet 2005).
  - Livrable(s) : Audit annuel par le management et des auditeurs indépendants



Présentation de Sox
Management Information System / SOX







AGENDA
Une approche des services sécurité Alcatel

L'introduction

La présentation de Sox – Sarbanes-Oxley

Une approche des services sécurité délivrés par Alcatel

Qu'apportent les services SOC à SOX ?

Les perspectives

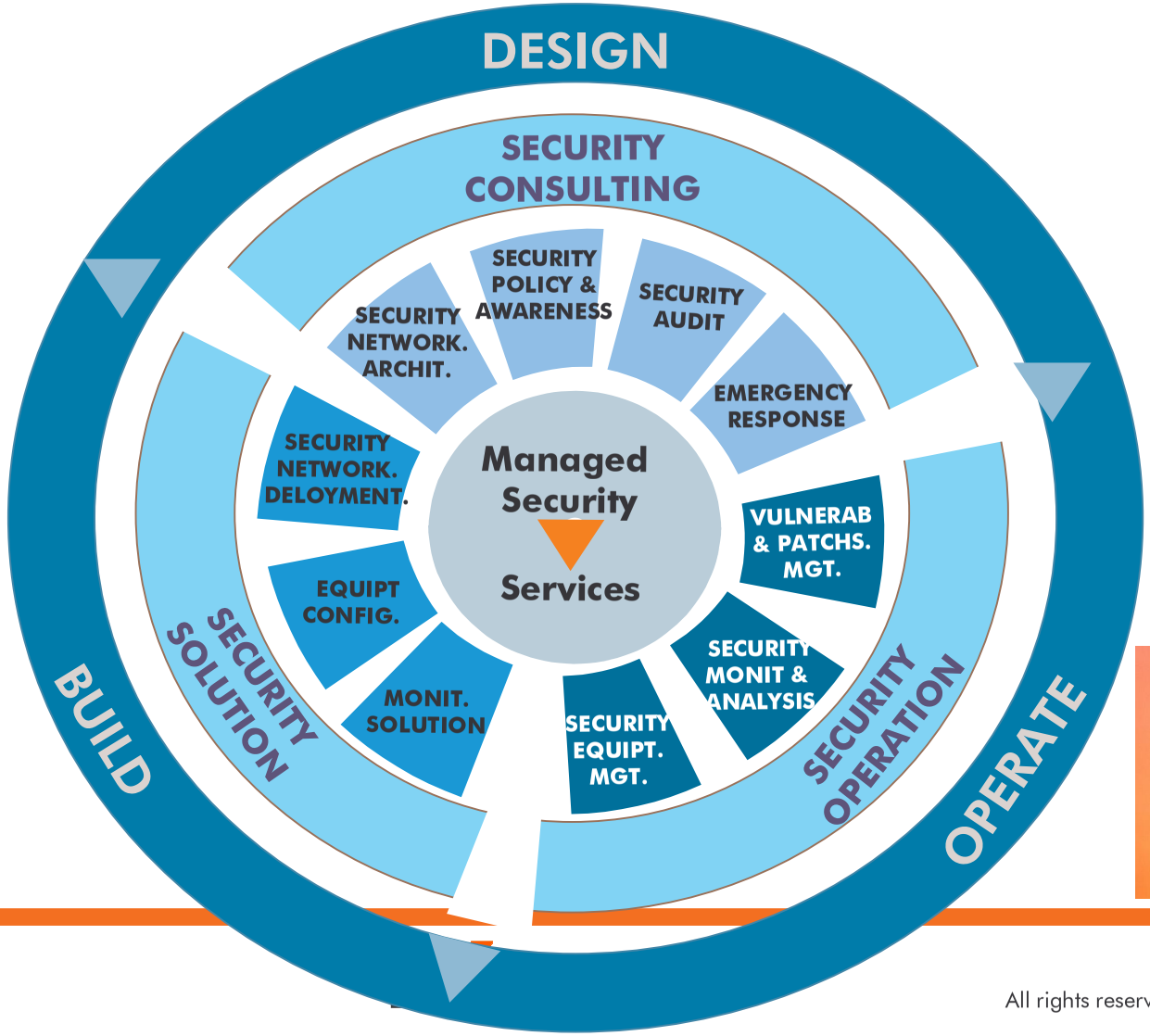
L'approche Alcatel
Que représente l'activité sécurité ?

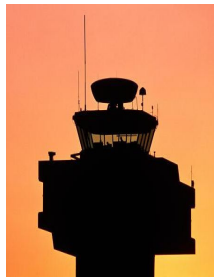
Plus de 12 ans d'existence

Premiers à effectuer de l'audit d'intrusion en France (1995)

Précurseurs dans le domaine de la détection d'intrusion (1998)

Premier CERT Industrie Service et Tertiaire en France (1999)





L'approche Alcatel
Description en 7 points

Focus sur le monitoring !

L'originalité de l'approche d'Alcatel repose les éléments suivants

- Les domaines couverts
- Les outils utilisés
- La démarche retenue
- Les processus (ITIL)
- Les services sécurité délivrés
- L 'organisation mise en place

L'approche Alcatel
Domaines couverts

Les domaines couverts

- Ce projet retient une approche globale de la sécurité au sein de l 'entreprise. Trop souvent, le cloisonnement est tel dans les entreprises que l 'on ne traite que de manière incomplète la problématique de la sécurité.
- Par conséquent nous abordons les 4 domaines de la sécurité

- [**CONTENANT**]

La sécurité de l 'infrastructure c 'est l 'ensemble des architectures dites techniques (informatiques, télécoms) [systèmes, réseaux, applicatifs, sécurité]

- [**CONTENU**]

La sécurité de l 'infostructure c 'est l 'analyse des flux d 'information

- [**UTILISATEUR**]

La sécurité physique des biens et des personnes

- [**CONTEXTE**]

La sécurité dite environnementale c 'est le CONTEXTE dans lequel se trouve l 'UTILISATEUR accédant à un CONTENU véhiculé dans un CONTENANT.

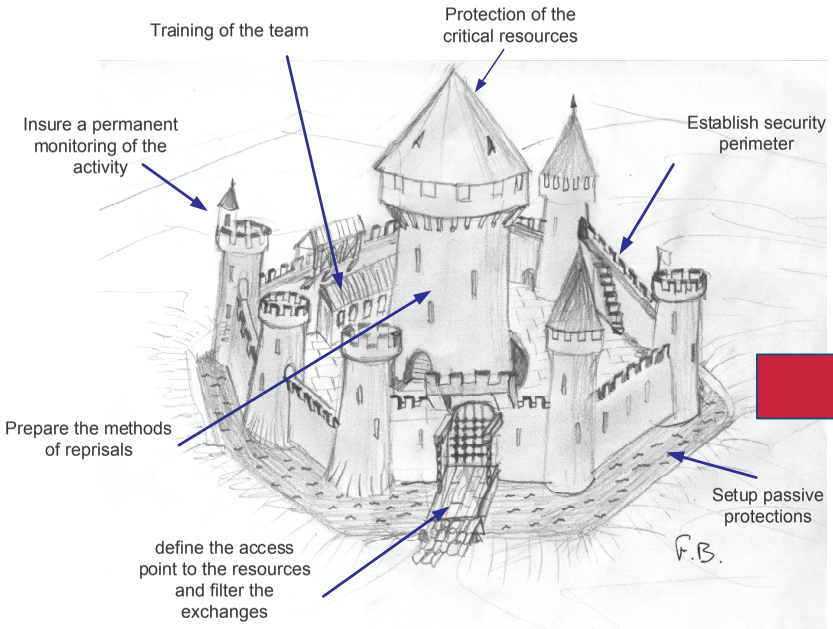
L 'atout majeur réside dans l 'association de deux domaines généralement abordés de manière distincte : l 'infrastructure et l 'infostructure de la sécurité.

Ce mariage réussi répond aux attentes à tous les niveaux (opérationnel, décisionnel, stratégique) de l 'entreprises !

L'approche Alcatel
La Tour de Contrôle …

Les outils utilisés

- Ce projet repose sur une TOUR DE CONTRÔLE, autrement dit un SOC - Security Operation Center.



Passer du concept de château-fort à … l'aéroport (HUB D'INFORMATION)

L'approche Alcatel
Une tour de contrôle à plusieurs niveaux

Direction

STRATEGIQUE

Respecter les engagements
Anticiper les évolutions

SSC
Security Strategic Center

Responsable de Service

DECISIONNEL

Mesurer les écarts
Analyser le comportement

SMC
Security Management Center

Administrateur

OPERATIONNEL

Diagnostiquer en temps réel
Agir sur les composants

SOC
Security Operation Center

L'approche Alcatel
Une tour de contrôle à plusieurs niveaux

Mots Clefs
- États, alarmes
- Configuration
- Inventaire
- Télédistribution
- Sauvegarde
- Archivage…

Administrateur

OPERATIONNEL

Diagnostiquer en temps réel
Agir sur les composants

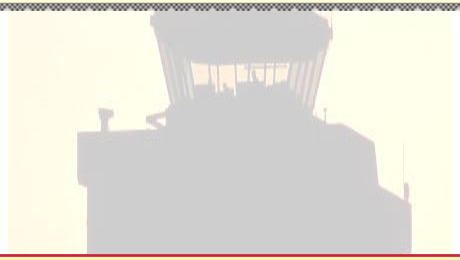
Diagnostiquer & Agir
sur l'Infrastructure

Les Enjeux
- **Les délais d'intervention et de mise en service**
- **La fiabilité et régularité des services d'acheminement**
- **Offrir un service 24h/24h**

Les Engagements
- **Diagnostiquer les dysfonctionnements**
- **Assurer la surveillance des applications critiques**
- **Assurer la sécurité des données du S.I.**

L'approche Alcatel
Une tour de contrôle à plusieurs niveaux

Mots Clefs
- Fault Management
- Filtres
- Corrélation
- Hypervision
- Dépassement de seuils
- SLA / SLM
- Reporting…



Responsable de Service

DECISIONNEL

Mesurer les écarts
Analyser le comportement

Mesurer & Analyser
Une Vision d'Ensemble

Les Enjeux
- **Améliorer la réactivité**
- **Faciliter l'exploitation**
- **Centraliser l'information**
- **Maîtriser les évolutions**
- **Analyser les tendances**
- **Rapporter**

Les Engagements
- **Gestion Globale des ressources**
- **Définir des normes de bon fonctionnement**
- **Gérer les comportements hors normes**

L'approche Alcatel
Une tour de contrôle à plusieurs niveaux

Mots Clefs
- Chaîne de Valeur
- Process View
- Impact Client
- Simulation
- QoS de bout en bout
- Capacity Planning…

Direction

STRATEGIQUE

Respecter les engagements
Anticiper les évolutions

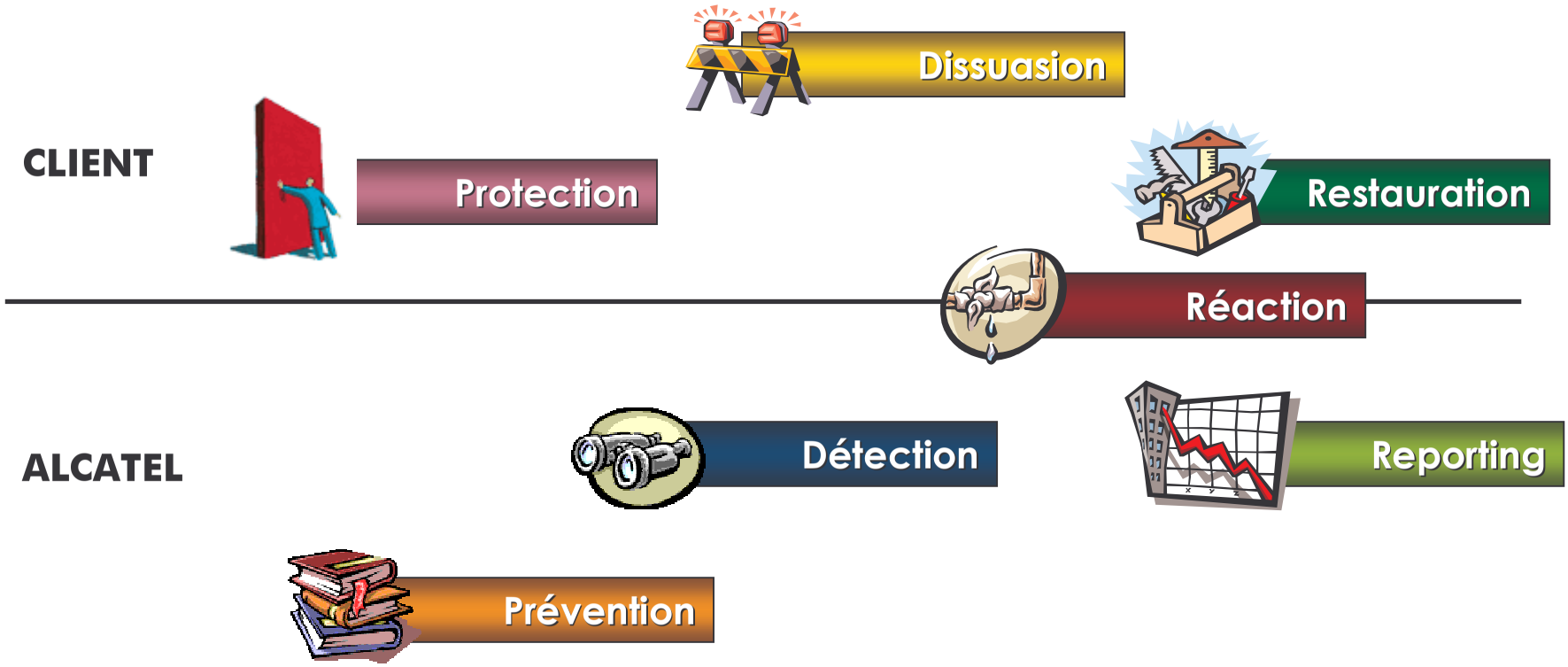
Respecter & Anticiper
Le Pilotage Métier

Les Enjeux
- **Afficher le service rendu en temps réel**
- **Respecter les engagements**
- **Détecter les dérives**
- **Calculer l'impact métier**
- **Anticiper & Valider les évolutions**
- **Justifier les services offerts**

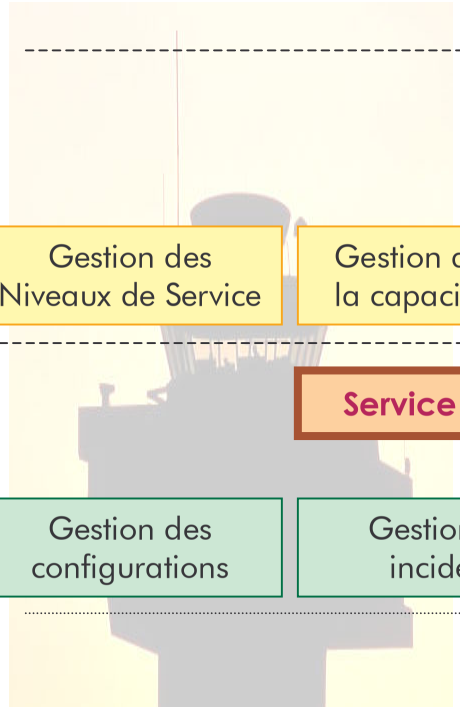
Les Engagements
- **Vitalité des services vendus**
- **Capacité d'évolutions**
- **QoS de bout en bout**
- **Satisfaction clients**

L'approche Alcatel
Démarche retenue

Alcatel ➔ Rôle essentiel de contrôle



L'approche Alcatel
Processus ITIL



Perspectives METIERS

STRATEGIQUE

Long terme

Fourniture des SERVICES

DECISIONNEL

Moyen terme

Gestion des Niveaux de Service | Gestion de la capacité | Prévention des menaces | Gestion des menaces | Reporting sécurité | Gestion de crise

Service Desk

Support aux SERVICES

OPERATIONNEL

Court terme

Gestion des configurations | Gestion des incidents | Gestion des demandes | Gestion des changements | Gestion des mises en production

OPERATIONS

OPERATIONNEL

Gestion des données | Gestion de l'infrastructures | Gestion des outils de sécurité | Gestion des applications | Gestion des utilisateurs

ALCATEL

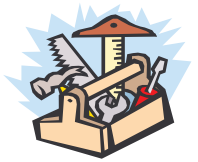
CLIENT

L'approche Alcatel
Services sécurité délivrés

Les services proposés ⇨ basés sur le monitoring

- **Collecte & Filtrage**
  - Collecte des événements
  - Filtrage et corrélation selon règles standards
  - Retransmission des alertes potentielles

- **Gestion de la menace**
  - Service de base + Analyse de risques
  - Filtrage et corrélation selon règles dédiées
  - Analyse des menaces issues de la corrélation



- **Prévention des menaces**
  - Analyse préventive des menaces du périmètre suivant l'actualité

- **Gestion de crise**
  - Accès au Hub de gestion de crise du CERT-IST

- **Reporting spécifique**
  - Définition et mise en œuvre de reporting personnalisé

L'approche Alcatel
Organisation mise en place

L'organisation mise en place

Niv 0 **WELCOME CENTER**

- **24/7**
- Langues retenues : FR, UK, SP, NL

Change Management

Niv 1/2 **SOC**

- **24/7**
- Langues retenues : FR, UK

Prévention des Menaces

Gestion des Menaces

Incident Management (résolution de l'incident)

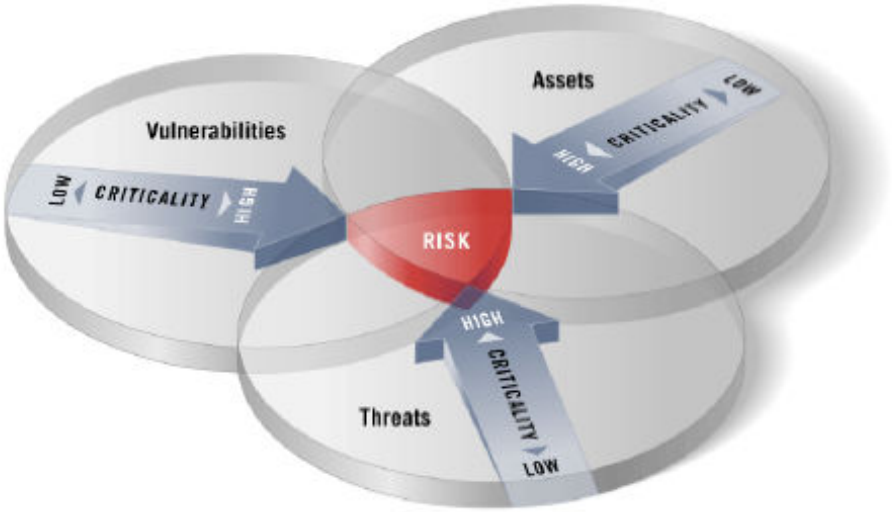
Problem Management (résolution de la cause)

Niv 3 **HUB DE CRISE**

L'approche Alcatel
Objectif visé : La gestion des risques opérationnels

Il s'agit de fournir aux clients la réponse appropriée à la gestion de ses risques opérationnels(*).

LA SECURITE AU BON ENDROIT, AU BON MOMENT ET AU MEILLEUR COUT !



(*) Risque opérationnel = Risques de pertes dues à une inadéquation ou à une défaillance des procédures, personnels, systèmes internes ou à des événements extérieurs.

AGENDA
Qu'apportent les services SOC à SOX ?

La présentation d'Alcatel

Les services sécurité délivrés par Alcatel

La présentation de Sox – Sarbanes-Oxley

Qu'apportent les services SOC à SOX ?

Les perspectives

Qu'apportent les services SOC à SOX ?

- **La difficulté ne réside pas dans la formulation des contrôles à réaliser MAIS plutôt dans la capacité à les réaliser**
  - **De manière automatique**
  - **Récurrent**

SECTION 404

- **Mise en place des contrôles : réponses apportées par**
  - **collecte et filtrage**
  - **gestion de la menace**
- **Change Management : réponses apportées par**
  - **prévention des menaces**
- **Reporting spécifique : réponse apportée par**
  - **reporting spécifique (orienté SOX)**

SECTIONS 802 / 1102

- **Gestion des fichiers logs : archivage légal**
- **Habilitations du personnel et Procédures**

Qu'apportent les services SOC à SOX ?

- **Des contrôles récurrents et des rapports**

AGENDA
Les perspectives

L'introduction

La présentation de Sox – Sarbanes-Oxley

Une approche des services sécurité délivrés par Alcatel

Qu'apportent les services SOC à SOX ?

Les perspectives

Les perspectives

La vision

- **Mutualisation**
  - Ce qui est fondamental c'est d'avoir une approche mutualisation et de créer une communauté d'intérêts car
    ➔ Face à l'adversité (durant un incident de sécurité), le DSI, DSSI, RSSI, les opérationnels en général sont très seuls … et l'équipe sécurité Alcatel intervient en support
    ➔ Il n'existe pas de vérité absolue et seul le partage d'information au sein d'un espace de confiance permet de corréler sur le terrain les informations obtenues du SOC. Un échange permanent d'information du SOC vers la communauté et de la communauté vers le SOC permet d'affiner les informations opérationnelles collectées et analysées.
  - Alcatel a su créer depuis quelques années cette communauté de confiance avec des sociétés qui ont des profils et des problématiques variés.

Rappel de quelques critères fondamentaux

- **Pragmatisme**
  - La capacité à délivrer des services sur des périmètres limités et maîtrisés permet de s'affranchir des « usines à gaz » (notion de « Trial »)
- **Approche services**
  - Ce qui est fondamental c'est de démontrer la capacité à délivrer un service (input, output, SLA mesurable, processus, …) + Tour de contrôle
- Ne pas oublier l'essentiel : **le savoir-faire** !
  - Face à un incident de sécurité, au delà des outils c'est la capacité de disposer de **personnes compétentes et expérimentées** (personnes formées et certifiées qui ont déjà été confrontées à un incident réel de sécurité).

ALCATEL