

***REX – implémentation de la norme ISO 27001
en environnement infogéré***



11 juin 2009
Sébastien BOMBAL
AREVA - IT Operations

▶ **Leader mondial dans les métiers de l'énergie**

- ◆ N°1 sur l'ensemble du cycle nucléaire
- ◆ N°3 dans la transmission et distribution d'électricité

▶ **Notre mission**

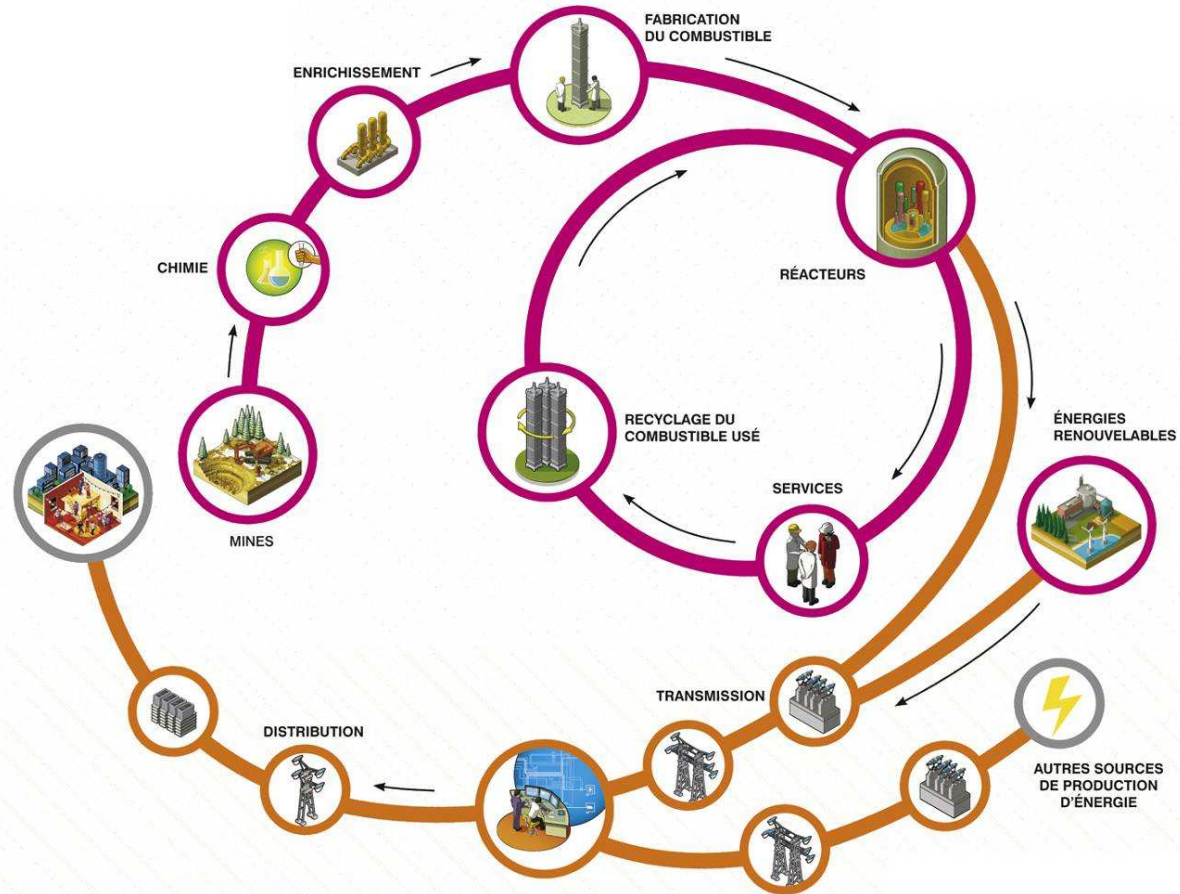
- ◆ **Permettre au plus grand nombre d'avoir accès à une énergie toujours plus propre, plus sûre et plus économique**

▶ **Notre stratégie**

- ◆ **Etre l'acteur de référence dans les solutions de production d'énergie sans CO₂ et d'acheminement d'électricité**
 - **Capitaliser sur notre modèle intégré pour mener la renaissance du nucléaire :**
 - Construire 1/3 des nouvelles capacités nucléaires
 - Sécuriser le cycle du combustible pour nos clients actuels et futurs
 - **Développer notre offre d'énergies renouvelables**
 - **Assurer une forte croissance rentable dans le T&D**

Une offre intégrée au service des professionnels de l'énergie

Des solutions pour produire de l'énergie sans CO₂



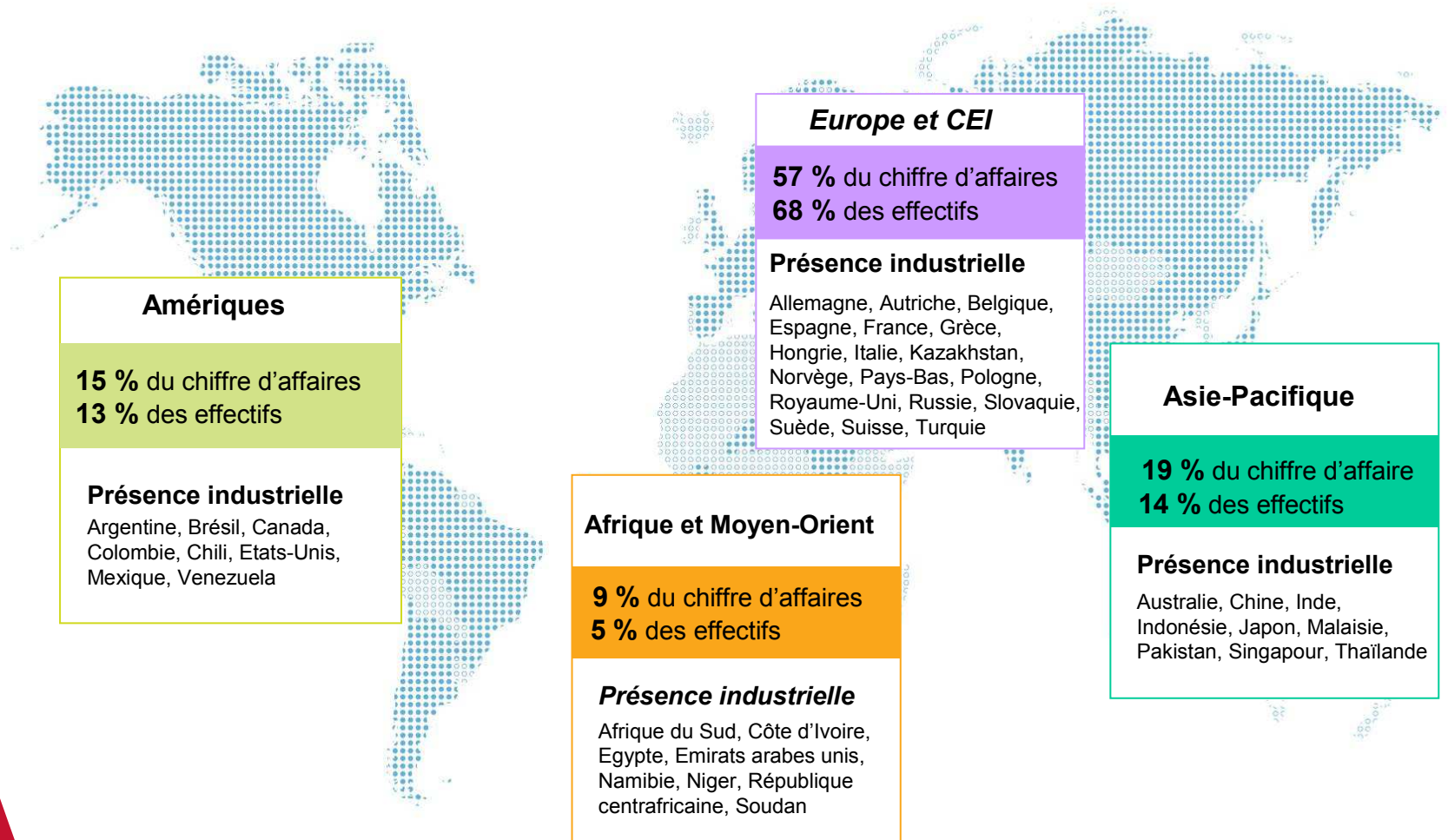
Des solutions pour acheminer l'électricité en toute fiabilité

CARNET DE COMMANDES	48 246 M€	+ 21,1 %
CHIFFRE D'AFFAIRES	13 160 M€	+ 10,4 %
RESULTAT OPERATIONNEL	417 M€	<i>soit une marge opérationnelle de 3,2 %</i>
RESULTAT NET part du groupe	589 M€	<i>soit 16,62 € par action</i>
COLLABORATEURS	75 414	+ 15 %

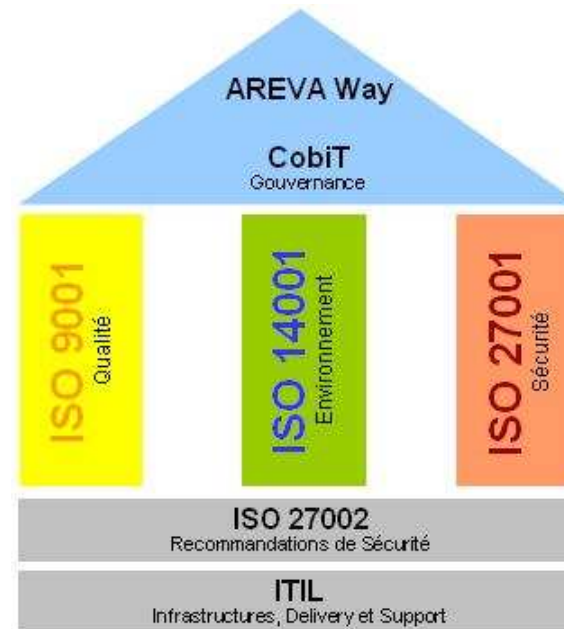
43 pays
présence industrielle

+ de 100 pays
présence commerciale

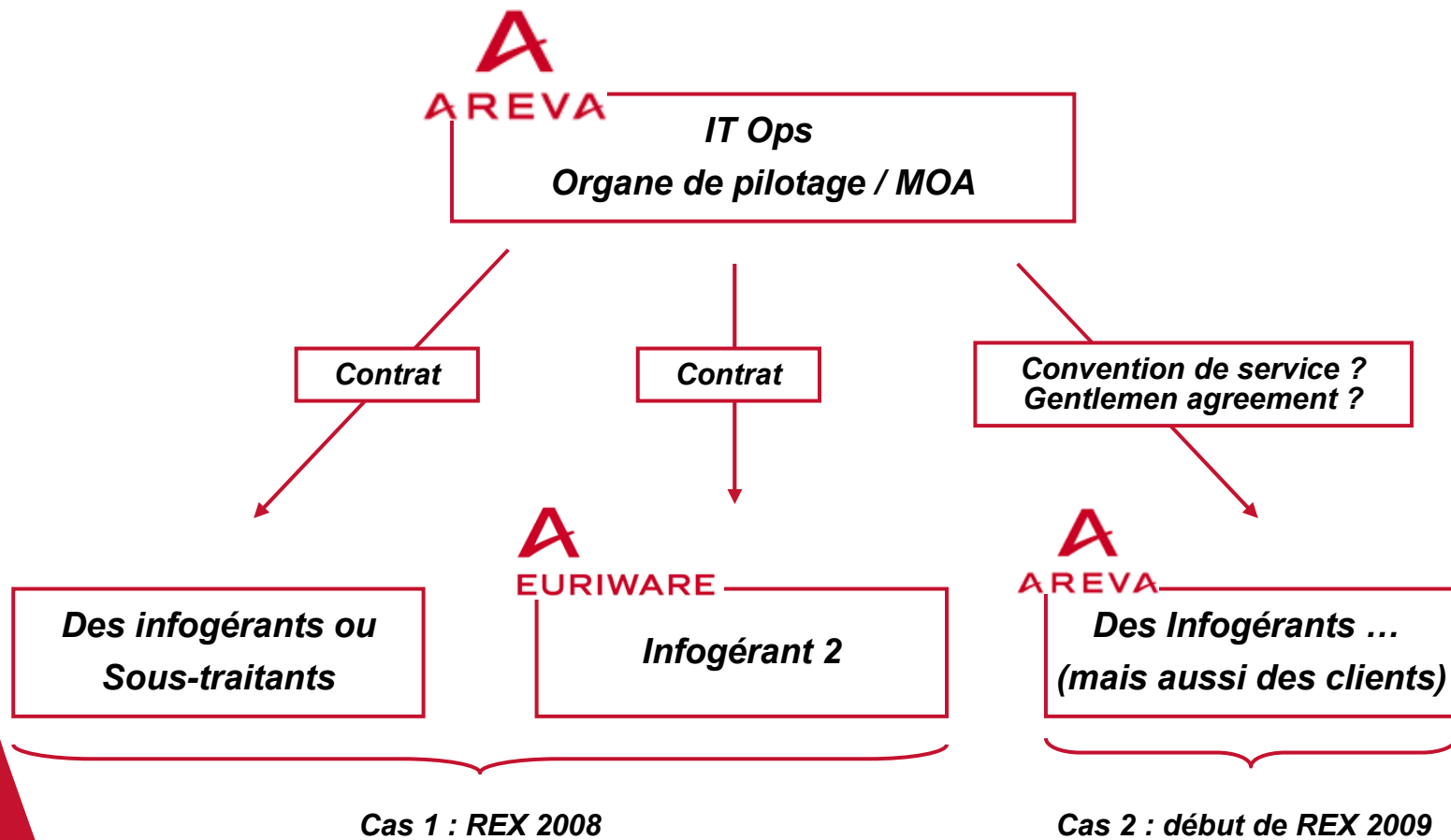
2/3 du chiffre d'affaires
réalisés hors de France



- ▶ Echanges sur la norme ISO 27001 lorsqu'un périmètre est totalement ou partiellement infogéré par un ou plusieurs prestataires
- ▶ Comment AREVA - IT Ops a implémenté la norme ?
- ▶ Les chantiers et points clés
- ▶ L'importance du contrôle et de la gouvernance

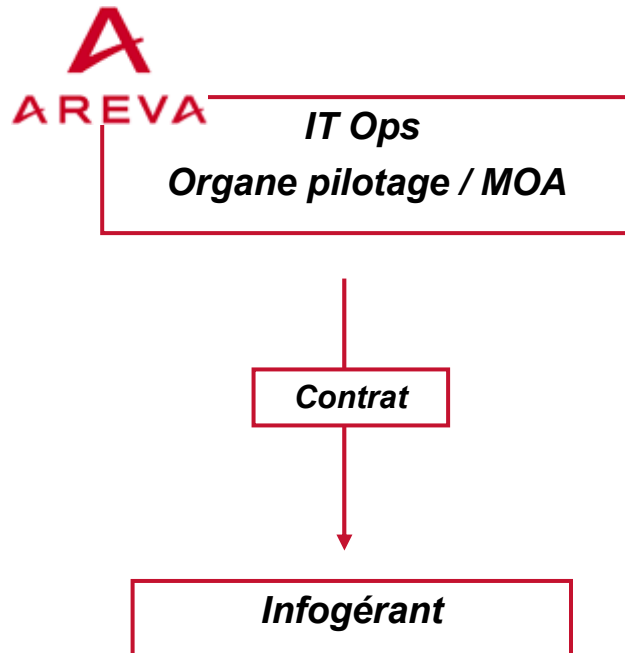


- ▶ **Quelle est la frontière du système de management d'IT Ops sachant que le SMSI s'applique à toute la fonction SI du groupe AREVA ?**



Cas 1 : frontière du SMSI et chantiers d'implémentation

- ▶ **Cas simple : le SMSI s'arrête chez IT Ops**
 - ◆ Implique que l'auditeur ne va pas au-delà...



Les chantiers 27001

- ▶ **Classification des actifs**
- ▶ **Les contrats !**
- ▶ **La gestion des risques**
- ▶ **L'opérationnel**
 - ◆ Les audits / contrôles
 - ◆ La gestion d'incidents
- ▶ **Les tableaux de bord**
- ▶ **La sensibilisation**

Cas 1 : Classification des actifs

► **Le plus long dans la classification des actifs est l'inventaire**

- ◆ La gestion d'inventaire est un processus difficile

Typologie d'actif	Remarque
Inventaire des applications, logiciels, matériels	Incitation à la qualité du référentiel nativement !
Sites physiques	Généralement spécifié dans les contrats dans les conditions d'exploitation
Ressources humaines	A contrôler mais pas d'inventaire nécessaire au niveau du client
Documentations, contrats de sous-traitance, etc.	A contrôler mais pas d'inventaire nécessaire au niveau du client

► **Cela peut même être encore plus simple**

- ◆ Cas de la location financière
- ◆ Cas des applications ASP
- ◆ ...

► **Il ne faut pas oublier les actifs MOA !**

- ◆ Ressources humaines, sites physiques, documentation, serveurs de fichiers...

Focus : les contrats, les étapes de la démarche

► Step 1 : Faire une analyse d'écart sur les mesures sélectionnées

Ref.	Objectifs et mesures de sécurité	SoA	Plan de traitement des risques global	PSSI	Partie de la PSSI	Présent dans contrat actuel	Partie du contrat actuel	Présent dans le contrat d'application IT OPS	Partie du contrat d'application
A.5	Politique de sécurité								
A.5.1	Politique de sécurité de l'information <u>Objectif</u> : apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.								
A.5.1.1	Document de politique de sécurité du SI Un document de politique de sécurité de l'information doit être approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés.	Oui	Oui	Oui	1	Oui	Annexe 1 Charte AREVAnet	Oui	Annexe 2.1 - Partie 8.7
A.5.1.2	Maintien de la politique de sécurité Pour garantir la pertinence, l'adéquation et l'efficacité de la politique de sécurité de l'information, il convient de réexaminer la politique à intervalles fixés préalablement ou en cas de changements majeurs.	Oui	Oui	Oui	2.6	N/A		N/A	

► Step 2 : Modifier les documents et processus en conséquence

- Pour inclure des éléments sur les mesures (références documentaires, processus, rôles et responsabilités, etc.)

► Step 3 : Injecter le résultat dans les analyses de risques et la grille d'audit



Contrats



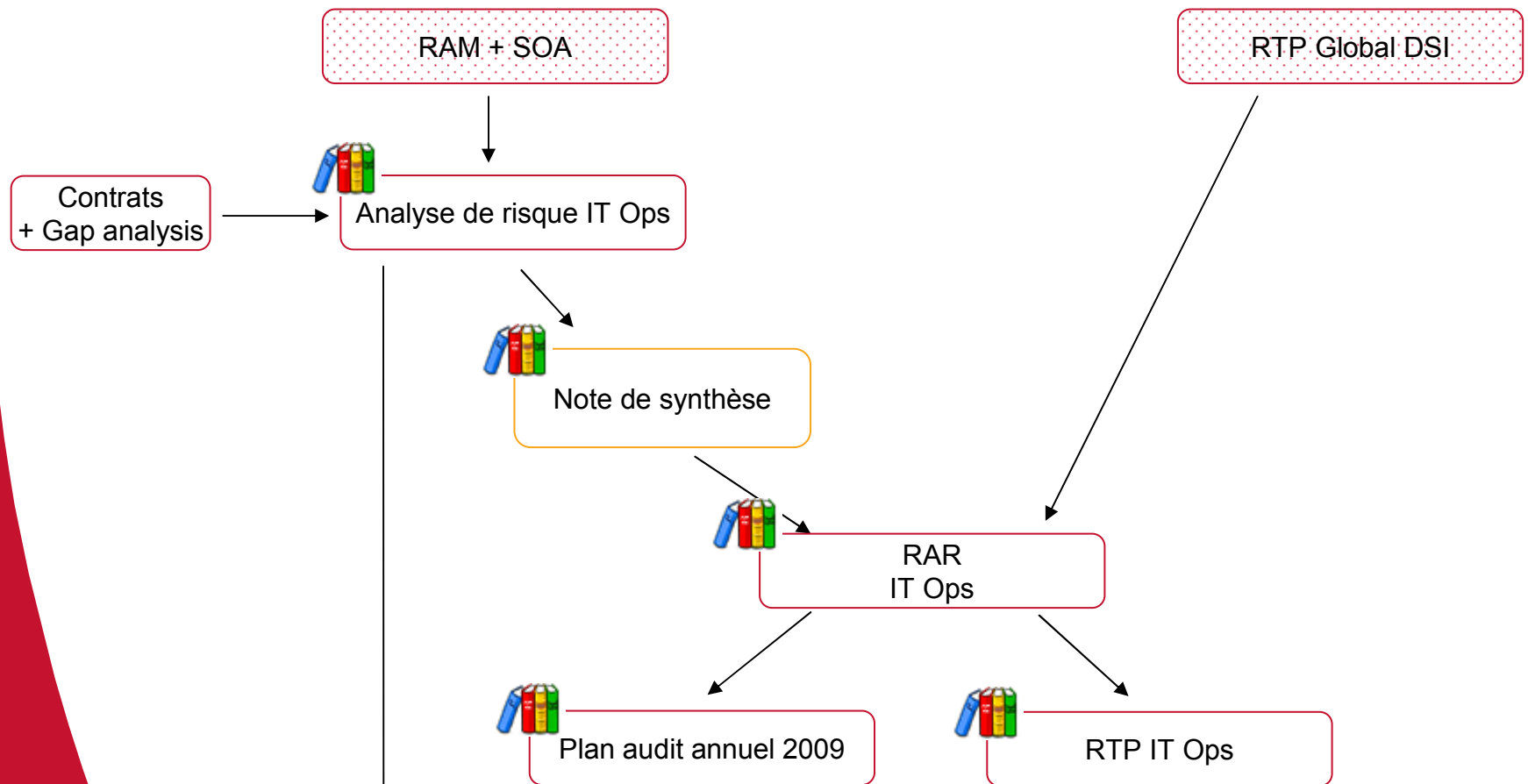
Analyse d'écart



Futurs contrats, templates...

Cas 1 : La gestion des risques (1/2)

Focus : Cycle de gestion des risques biannuel et remonté au corporate de ces résultats pour la boucle d'amélioration



Préparation du référentiel documentaire pour justifier les réponses à l'auditeur

Cas 1 : La gestion des risques (2/2)

- ▶ **Probablement le processus et le levier le plus important lors de l'implémentation de la norme**
 - ◆ Repositionnement de l'activité en soutien du management
 - ◆ Etablissement de deux roadmaps claires et des chantiers de fond
 - Plan d'audit
 - Plan de traitement des risques

- ▶ **Effets de bord**
 - ◆ Le financement / les ressources ad-hoc
 - ◆ Tous les chantiers ne sont pas portés par la sécurité
 - Positionnement en contributeur (prescription/financier) et en contrôleur

- ▶ **Attention à l'usage du transfert de risques**
 - ◆ Comme instrument de réduction du risques ou pour le financement

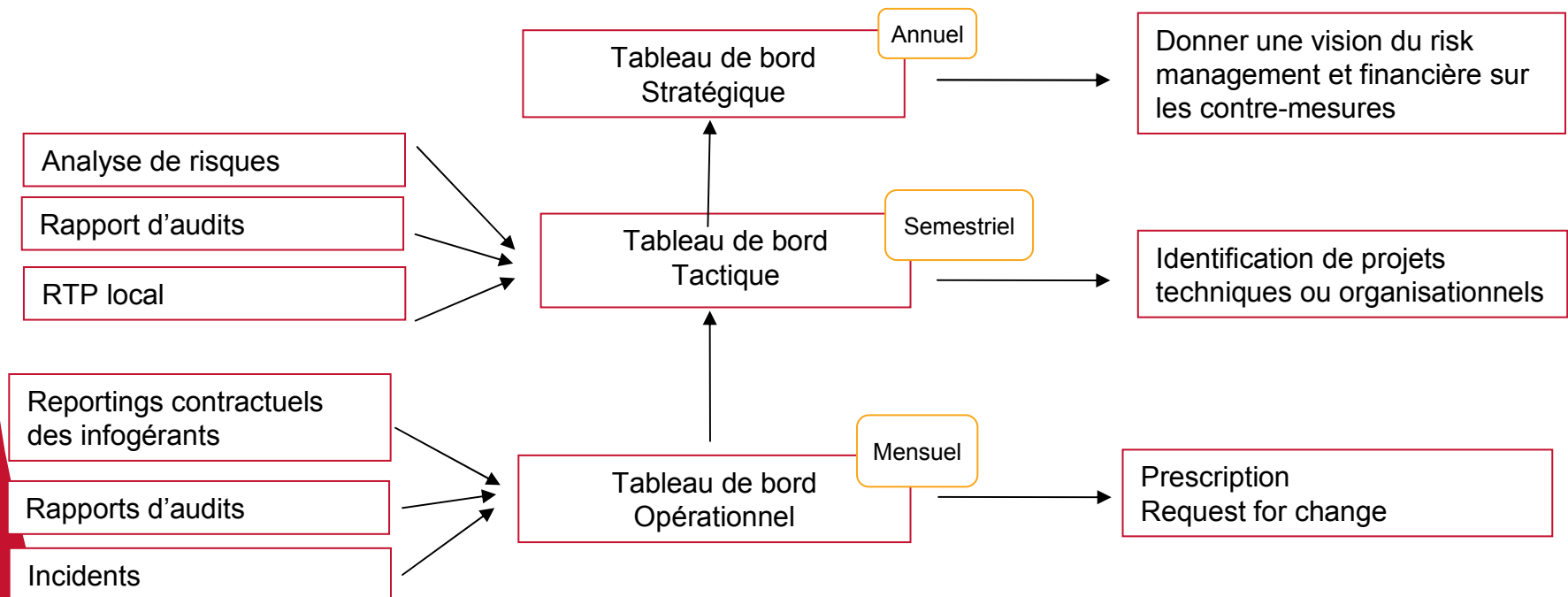
- ▶ **La gestion des risques est un processus itératif, comportant des jalons**
 - ◆ Il faut livrer !
 - ◆ Et évoluer en incluant les couvertures de responsabilités, les instruments de réduction, de financement, etc.

- ▶ **La gestion des incidents**
- ▶ **Les audits**
 - ◆ **Plan d'audit**
 - ◆ **En réaction à un incident, un problème...**
 - ◆ **Suite à des changements**
 - ◆ **En continu**
- ▶ **L'implémentation du plan de traitement des risques**

Le respect de la norme entraîne un nombre d'actions préventives ou correctives important qu'il faut suivre avec discipline !

Et dans une seconde phase, un outillage...

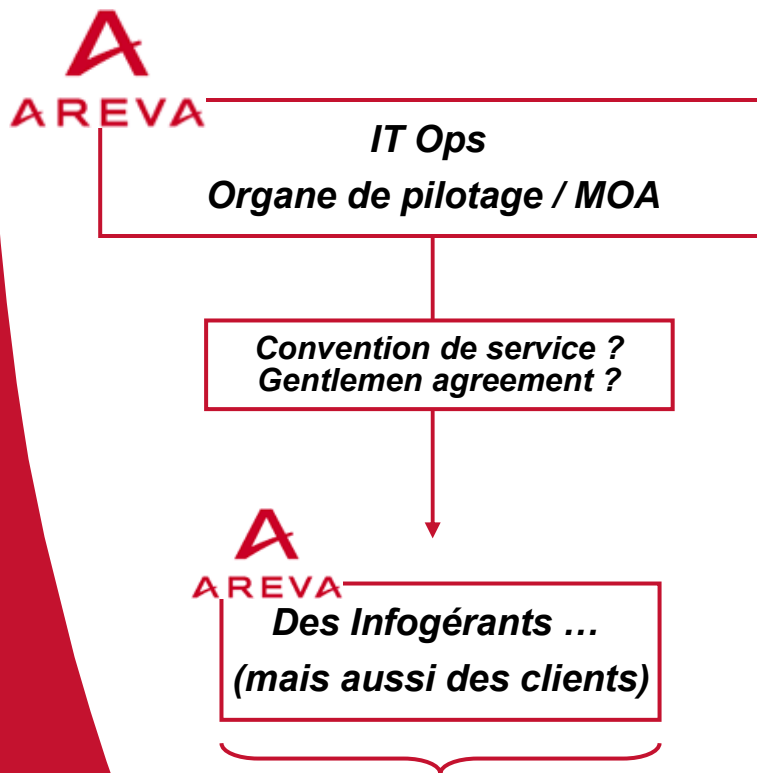
- ▶ La notion « d'indicateurs » imposée par la norme, mais...
 - ◆ Que doit-on remonter ? Comment ? A quelle fréquence ?
- ▶ Avant tout, c'est un outil de pilotage et de communication



- ▶ Mais il faut rapidement se doter d'outillage pour mesurer l'efficacité des infogérants et surtout être indépendant dans les mesures
 - ◆ Outils de vulnerability management, SIEM, etc...

Cas 2 : frontière du SMSI et chantiers d'implémentation

- ▶ Cas plus complexe : le SMSI s'arrête chez... ?
 - ▶ IT Ops aussi...



- ▶ Même chantier que précédemment
 - ♦ Etablissement de conventions de services systématiquement
 - ♦ Commencer par une gestion de risques par silo (par contrat / convention) dans un premier temps

Cas 2 : notre REX 2009

Des questions ?



11 juin 2009
Sébastien BOMBAL
AREVA - IT Operations