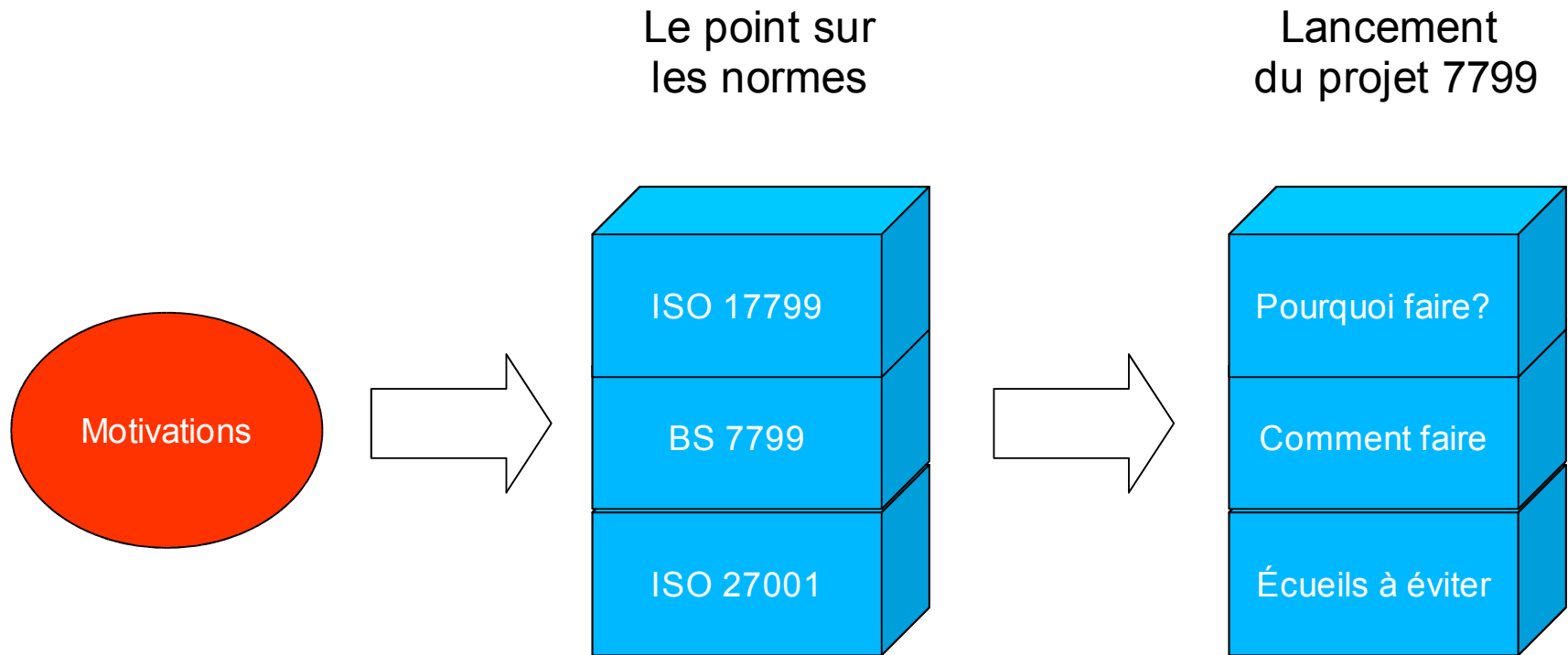


Pourquoi et comment lancer un projet 7799

Alexandre Fernandez

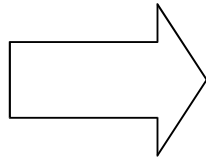
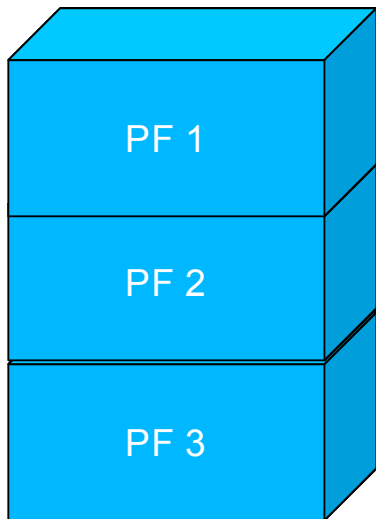
<Alexandre.Fernandez@hsc.fr>

Démarche

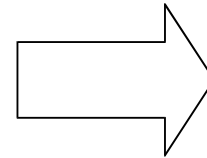


Volontairement

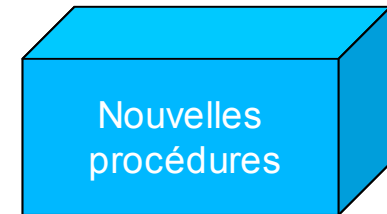
Interconnexion des différentes plates formes



Remise à plat de l'architecture



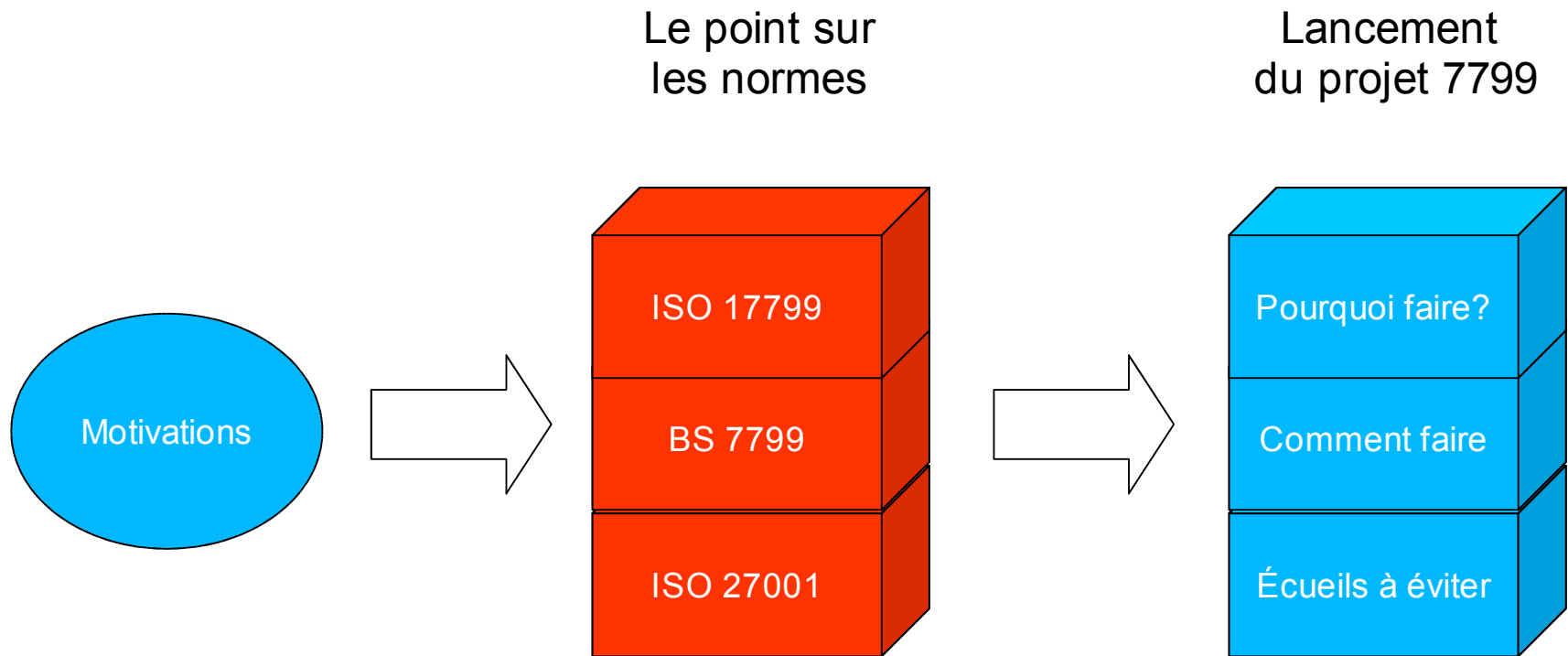
Remise à plat des procédures



- x De SoX
 - x Oblige à démontrer des bonnes pratiques en matière de SSI
 - x SAS70
 - x BS 7799
- x D'un partenaire
- x Des clients

- x Vis-à-vis des clients
- x Vis-à-vis des assurances

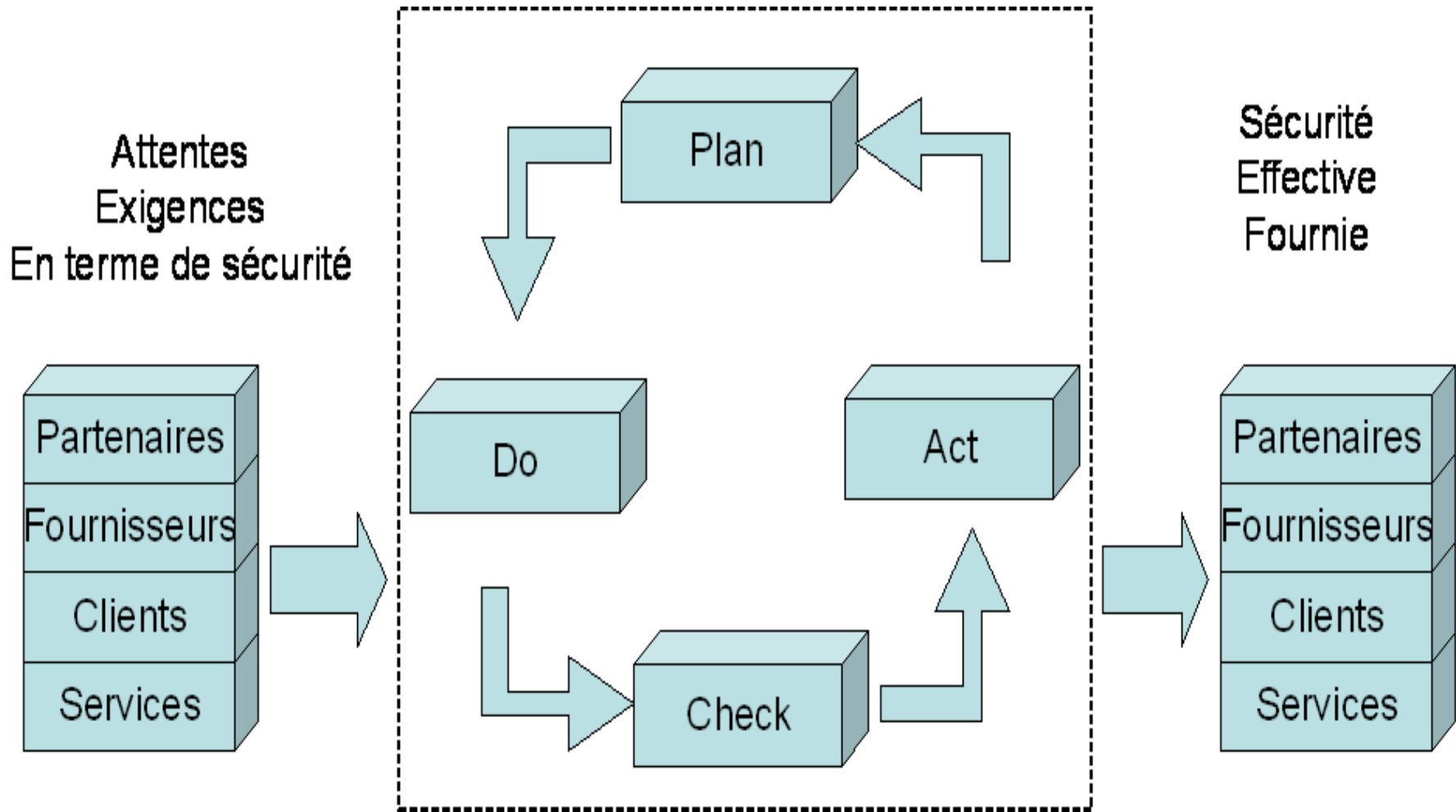
Démarche



- x Titre : « *Code of practice for information security management* »
- x Ensemble de mesures de sécurité pouvant être appliqués
 - x Description de la mesure de sécurité
 - x Description de l'indication de cette mesure de sécurité
- x « Control » = Mesure de sécurité

- x Différents types de mesures de sécurité
 - x Politique de sécurité
 - x Sécurité organisationnelle
 - x Classification et contrôle des actifs
 - x Sécurité du personnel
 - x Sécurité physique
 - x Procédures opérationnelles et communication
 - x Contrôle d'accès
 - x Développement et maintenance du système
 - x Plan de continuité de l'activité
 - x Conformité aux réglementations

- x Titre : « *ISMS Specification with guidance for use* »
- x SMSI = Système de Management de la Sécurité de l'Information (*ISMS en anglais*)
- x Qu'est-ce qu'un SMSI
 - x C'est un ensemble de mesures
 - x Organisationnelles
 - x Techniques
- x A quoi sert un SMSI
 - x A assurer la sécurité dans la durée
 - x A rendre vérifiable de façon formelle cette sécurité
 - x Fournit de la confiance aux parties prenantes



- x Planification (Plan)
 - x Périmètre du SMSI
 - x Identification et évaluation des risques
 - x Plan de gestion des risques
 - x Méthode choisie pour gérer le risque
 - x Contrôles mis en place
 - x Traitement du risque
 - x Acceptation
 - x Transfert
 - x Réduction du risque à un niveau acceptable
 - x ==> Document : Statement of applicability (SoA)
 - x Document obligatoire en vue d'une certification

- x Execution (Do)
 - x Allocation de ressources
 - x Personnes, temps, argent
 - x Rédaction de la documentation
 - x Formation du personnel concerné
 - x Gestion du risque
 - x Pour les risques acceptés : Rien à faire
 - x Pour les risques transférés : Assurance, partenariats etc.
 - x Pour les risques à réduire :
 - x Implémenter les contrôles identifiés dans la phase précédente
 - x Assignation des responsabilités
 - x Identifier des risques résiduels

x Vérification (Check)

- x Vérification de routine

- x Apprendre des autres

- x Audit de l'ISMS

 - x Audit annuel

 - x Sur la base de

 - x Documents

 - x Traces système

- x Conduit à

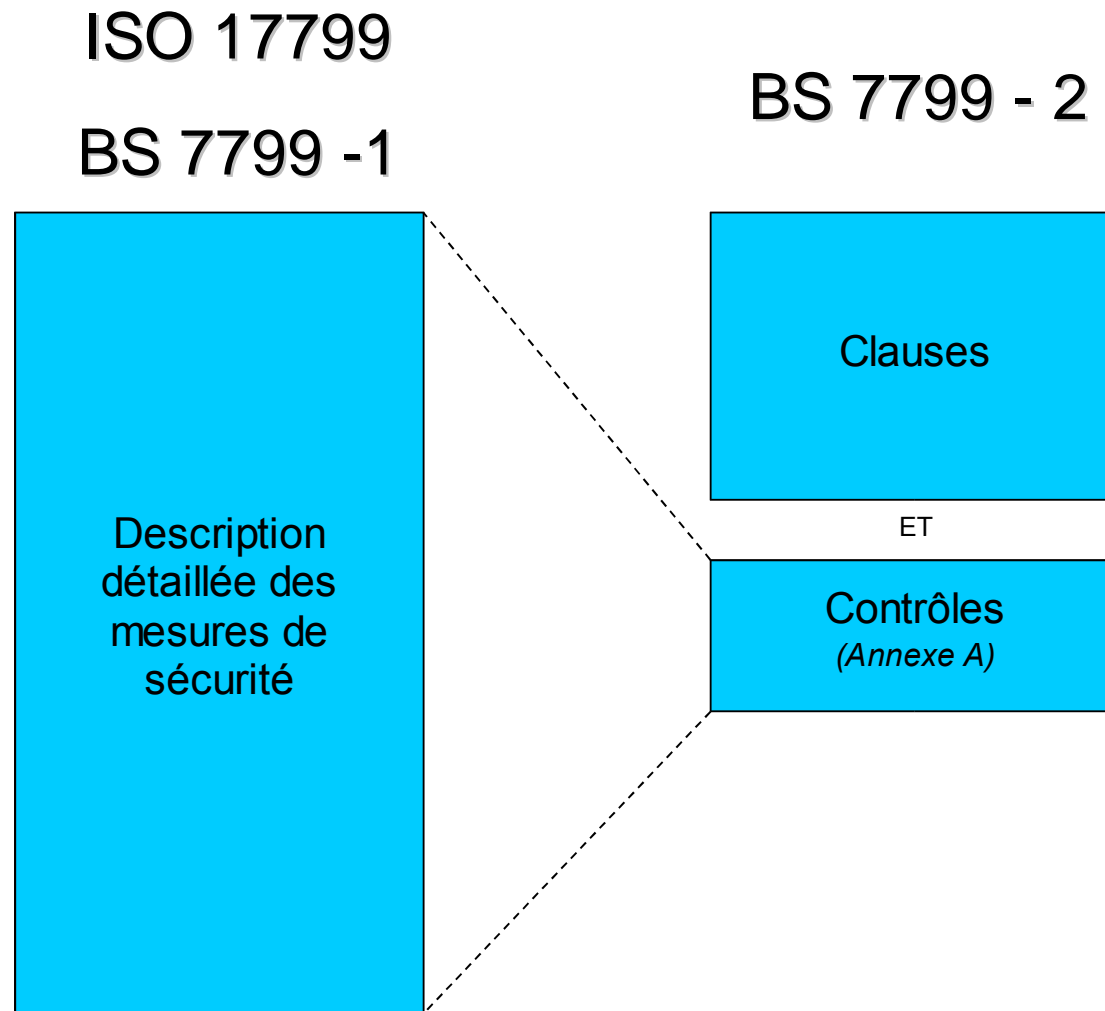
 - x Constatation que les contrôles ne réduisent pas de façon effective les risques pour lesquels ils ont été mis en place

 - x Identification de nouveaux risques non traités

 - x Tout autre type d'inadaptation de ce qui est mis en place.

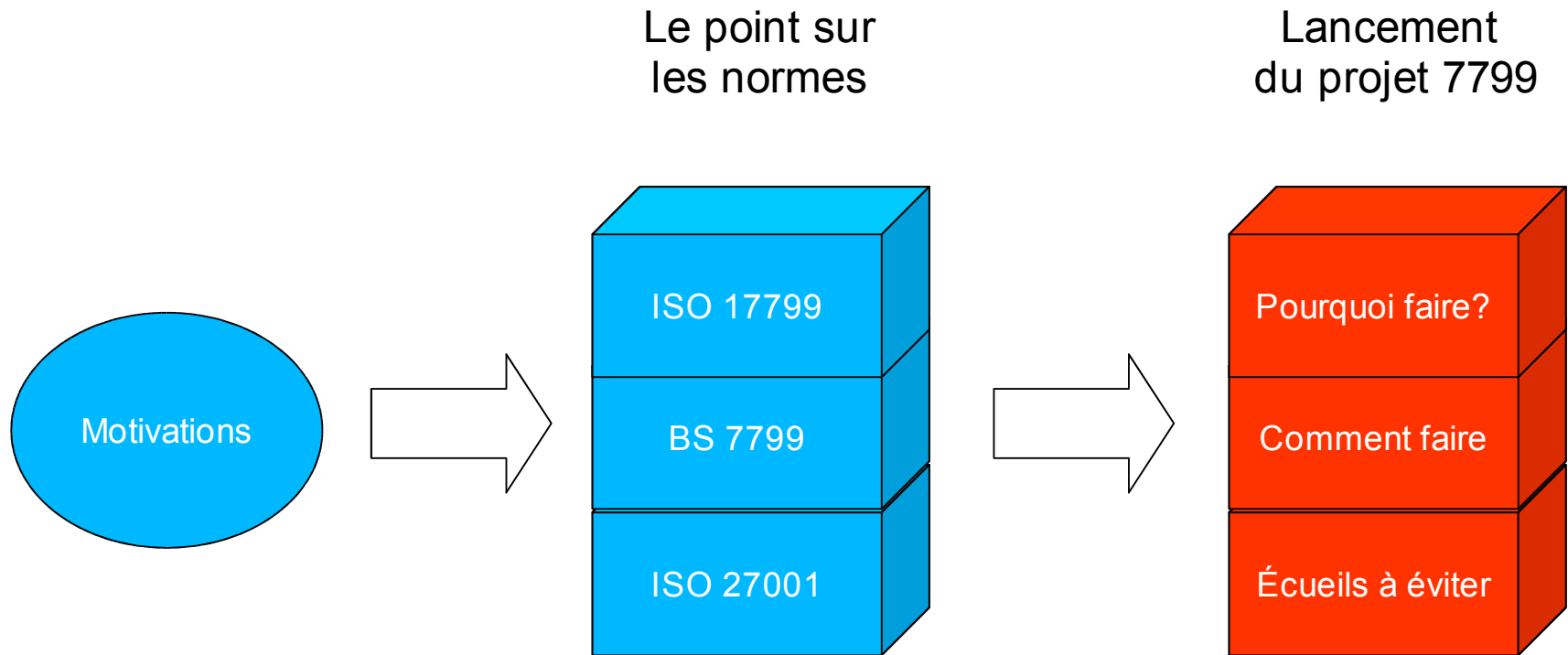
x Action (Act)

- x Prendre les mesures résultant des constatations faites lors de la phase de vérification
- x Actions possibles
 - x Passage à la phase de planification
 - x Si de nouveaux risques ont été identifiés
 - x Passage à la phase d'exécution
 - x Si la phase de vérification en montre le besoin
 - x Constatation de non conformité
 - x Actions correctives ou préventives
 - x Actions entreprises immédiatement
 - x Planification d'actions sur le moyen et long terme



- x Nouvelle norme ISO 27001
 - x Annoncée pour l'année prochaine
 - x Reprendra la BS 7799-2
 - x Permettra de certifier
 - x Compatible avec la BS 7799-2
- x **Il faut s'habituer à parler de 27001**

Démarche



- x **Pour les tableaux de bord**
 - x ISO 17799
 - x Usage le plus répandu à ce jour
 - x Approche très pragmatique

- x **Pour les audits**
 - x ISO 17799
 - x Les conclusions font référence à la norme
 - x Espéranto de la sécurité

- x Pour adopter les bonnes pratiques
 - x BS 7799-2
 - x Constat **objectif** que vous adoptez les bonnes pratiques en matière de SSI
 - x Permet d'évoluer, le moment venu, vers une certification
 - x Risque : Non-conformité avec la norme

- x Pour donner une image de sérieux aux partenaires
 - x BS 7799-2
 - x Constat, **extérieur** et **objectif** que vous adoptez les bonnes pratiques en matière de SSI
 - x Permet d'évoluer, le moment venu, vers une certification

Pourquoi faire?

- x Pour être certifié BS 7799-2:2002
 - x BS 7799-2
 - x Constat **impartial**, **objectif** et **officiel** que vous adoptez les bonnes pratiques en matière de SSI
 - x Engagement dans la durée

- x Démarche incontournable
 - x Définir le périmètre
 - x Faire l'inventaire des actifs
 - x Faire une analyse de risques (Vulnérabilités + Menaces etc.)
 - x Traiter le risque (Accepter, Transférer, Réduire)
 - x Mettre en place les mesures de sécurité
 - x Auditer
 - x Boucler

- x Le lancement d'un projet de mise en conformité BS7799 est un projet à part entière
- x Quel type de projet?
 - x Le produit final est décrit de façon formelle dans la norme
 - x Projet transversal
 - x Concerne potentiellement tous les services
- x Les techniques classiques de gestion de projet s'appliquent

- x Comme la mise en place de la BS 7799 est un projet à part entière, il est exposé aux risques projets suivants
 - x Définition imprécise de l'objectif à atteindre
 - x Manque de participation des personnes concernées
 - x Non acceptation de la démarche
 - x Mauvaise estimation des charges et des délais
 - x Manque de dialogue entre les différents interlocuteurs
 - x Non implication des utilisateurs
 - x Inadéquation de l'application de la BS 7799
 - x Problèmes d'organisation de l'équipe
 - x Compétences mal distribuées
 - x Faible visibilité sur l'avancement du projet

- x Choisir un CdP
 - x 1 - Avec l'expérience de la BS 7799
 - x Très rare
 - x 2 - Avec l'expérience de l'ISO 9001
 - x Rare
 - x 3 – Expérimenté et expert en sécurité
 - x Rare
 - x 4 – Expérimenté

- x Profil

- x *Lead Auditor*

- x Un *lead auditor* sait très bien ce qu'est la norme BS7799

- x Il sait aussi comment auditer le SMSI en regard de la norme BS7799

- x Il ne sait pas forcément comment mettre en place le SMSI

- x Il n'a pas forcément les compétences de management nécessaires

- x Suffisamment technique pour parler aux techniciens

- x Suffisamment organisationnel

- x Pour convaincre la direction

- x Comprendre et se faire comprendre des utilisateurs

- x Compétent en gestion de projets

- x Des documents de sécurité existent-ils déjà?
 - x Sont ils adaptés au besoin?
- x Les applications ont-elles un dossier de sécurité
 - x Toutes, ou seulement les plus récentes?
 - x Le dossier est-il à jour
- x Une méthode d'analyse de risques est-elle appliquée
 - x Est elle adaptée
 - x Trop lourde,
 - x Pas assez formelle
- x Les informations sont elles classifiées?

- × Les conséquences d'une erreur de périmètre peuvent être très lourdes en termes de
 - × Coûts
 - × Délais
 - × Crédibilité de la démarche BS 7799

- × Si CdP de type 3 ou 4, alors
 - × Dans un premier temps : choisir un périmètre restreint
 - × Utiliser les techniques classiques de retour d'expérience projet
 - × Dans un second temps : élargir le périmètre

Choisir un périmètre

| Appli 1 | Appli 2 | Appli 3 | Appli 4 | Appli 5 |
|--------------------|--------------------|--------------------|--------------------|--------------------|
| Code | Code | Code | Code | Code |
| Utili- sateurs | Utili- sateurs | Utili- sateurs | Utili- sateurs | Utili- sateurs |
| Entrées Sorties | Entrées Sorties | Entrées Sorties | Entrées Sorties | Entrées Sorties |
| Veille | Veille | Veille | Veille | Veille |
| Journaux | Journaux | Journaux | Journaux | Journaux |
| Svg | Svg | Svg | Svg | Svg |
| Arch | Arch | Arch | Arch | Arch |
| Doc | Doc | Doc | Doc | Doc |
| PCA | PCA | PCA | PCA | PCA |

Choisir un périmètre

| Appli 1 | Appli 2 | Appli 3 | Appli 4 | Appli 5 | |
|---------|---------|---------|---------|---------|------------------------|
| | | | | | Veille |
| | | | | | Gestion des journaux |
| | | | | | Sauvegardes |
| | | | | | Archivage |
| | | | | | Documentation générale |
| | | | | | PCA / PRA |

- x Travailler tout seul
- x Ne pas définir clairement l'objectif du projet 7799
- x Choisir un périmètre trop ambitieux
- x Vouloir sous-traiter tout le travail
 - x Le prestataire est indispensable
 - x Il peut et doit vous conseiller
 - x Il peut et doit vous aider
 - x Il ne **doit pas** faire le travail à votre place

- x La BS 7799
 - x C'est la transposition en SSI de la démarche qualité
 - x Mise en place d'un système de management de la sécurité
 - x Bonnes pratiques
 - x Dire ce que l'on va faire, puis faire ce que l'on a dit
 - x Être en conformité avec la norme
 - x Conséquences
 - x Augmente la sécurité du périmètre mis en conformité
 - x Augmente la confiance des parties prenantes

- x Les littéraires
 - x Ont tendance à formaliser
 - x Planifient
 - x Communiquent
 - x **Comment faire de la sécurité sans eux?**

- x Les techniciens
 - x Focalisés sur des problèmes concrets
 - x Généralement à court terme
 - x Exigent des solutions pratiques
 - x Très pragmatiques
 - x **Comment faire de la sécurité sans eux?**