

Club 27001-Toulouse

ISO/IEC/27001 / ISO/IEC 27005 / EBIOS

Quelques réflexions

Anne MUR

Anne.mur@edelweb.fr

<http://www.on-x.com/> <http://www.edelweb.fr/>

Objectif de la présentation

**Débattre sur des sujets d'actualité autour de la question :
Qu'elle est la meilleure approche pour maîtriser les risques liés
au système d'information en conformité avec
l'ISO/IEC/27001**

Sommaire

- **Introduction**
 - Approche globale de la sécurité
 - Quelques mots clé

- **ISO/IEC/27xxx**

- **EBIOS**

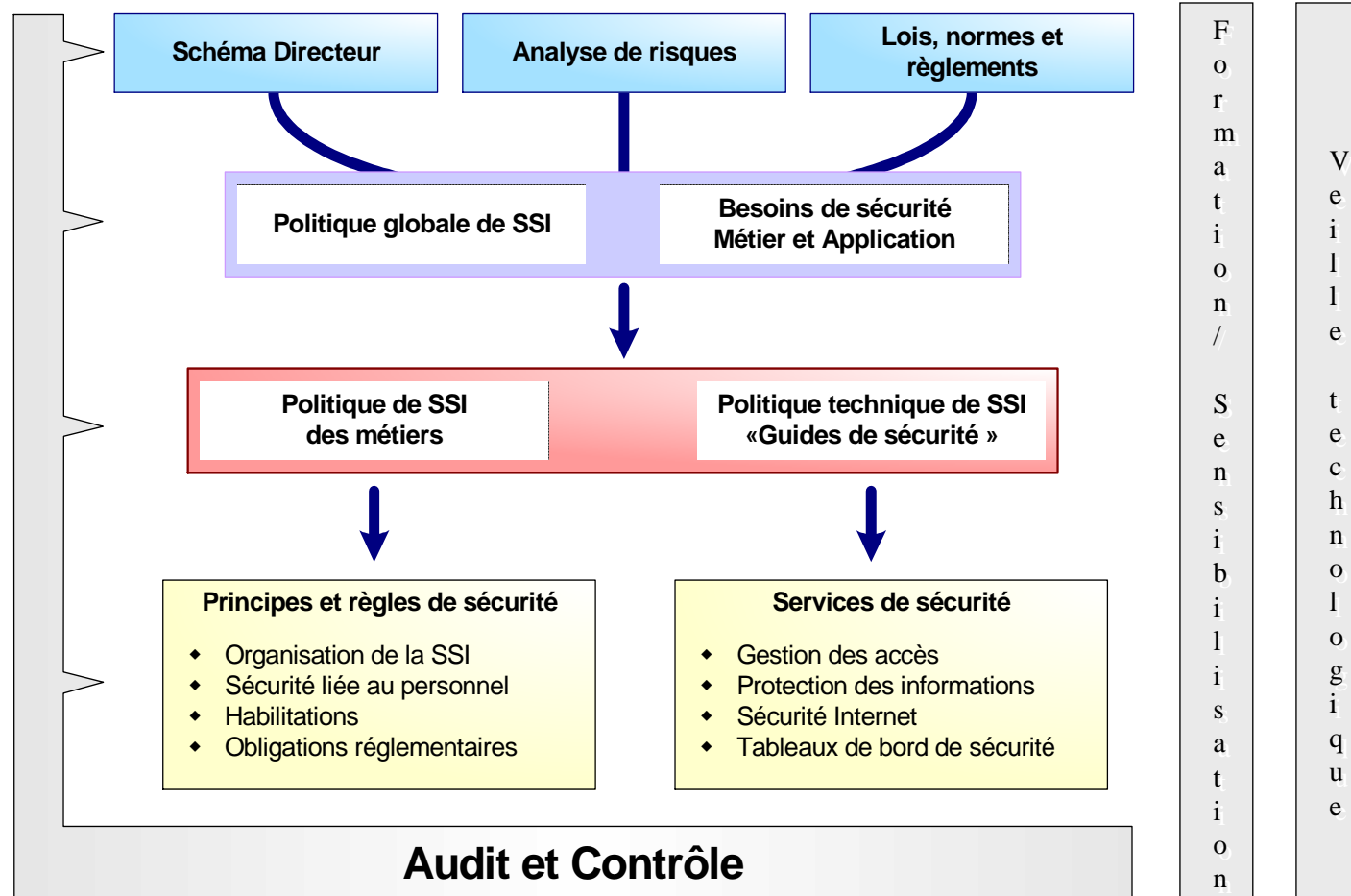
- **ISO/IEC/27001**

- **ISO/IEC/27005**

- **EBIOS / ISO27001 / ISO 27005**

Introduction (1/4)

Une approche globale de la sécurité



Introduction (2/4)

Quelques mots clé

➤ **Norme**

« Document, établi par consensus et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné. » « (définition de l'ISO/CEI).

➤ **Méthode**

Démarche organisée rationnellement pour aboutir à un résultat.

➤ **Guide**

Publication donnant des orientations, conseils, recommandations sur un sujet d'ordre général lié à la normalisation.

➤ **Standard**

Convention fondée sur un consensus plus restreint que pour la norme, généralement élaboré entre des industriels au sein de forums ou de consortiums.
Lorsqu'une méthode ou une technologie est adoptée par une majorité d'industriels et d'utilisateurs et qu'elle est considérée comme "standard", on parle alors de "standard de fait" (standard de facto.)

Introduction (3/4)

Quelques mots clé

- **Bien « Asset »**
« Tout élément représentant de la valeur pour l'organisme »
- **Évènement lié à la sécurité de l'information**
« occurrence identifiée d'un état d'un système, d'un service ou d'un réseau, indiquant une brèche possible dans la politique de sécurité de l'information, ou, un échec des moyens de protection, ou, une situation inconnue pouvant relever de la sécurité »
- **Menace**
« cause potentielle d'un incident indésirable, pouvant entraîner des dommages au sein d'un système ou d'un organisme »
- **Vulnérabilité**
« Faiblesse d'un bien ou d'un groupe de biens pouvant faire l'objet d'une menace »
- **Mesure - ATTENTION au terme anglais « control »**
« moyen de gérer un risque, comprenant la politique, les procédures, les lignes directrices, et les pratiques ou structures organisationnelles, et pouvant être de nature administrative, technique, gestionnaire ou juridique »

Introduction (4/4)

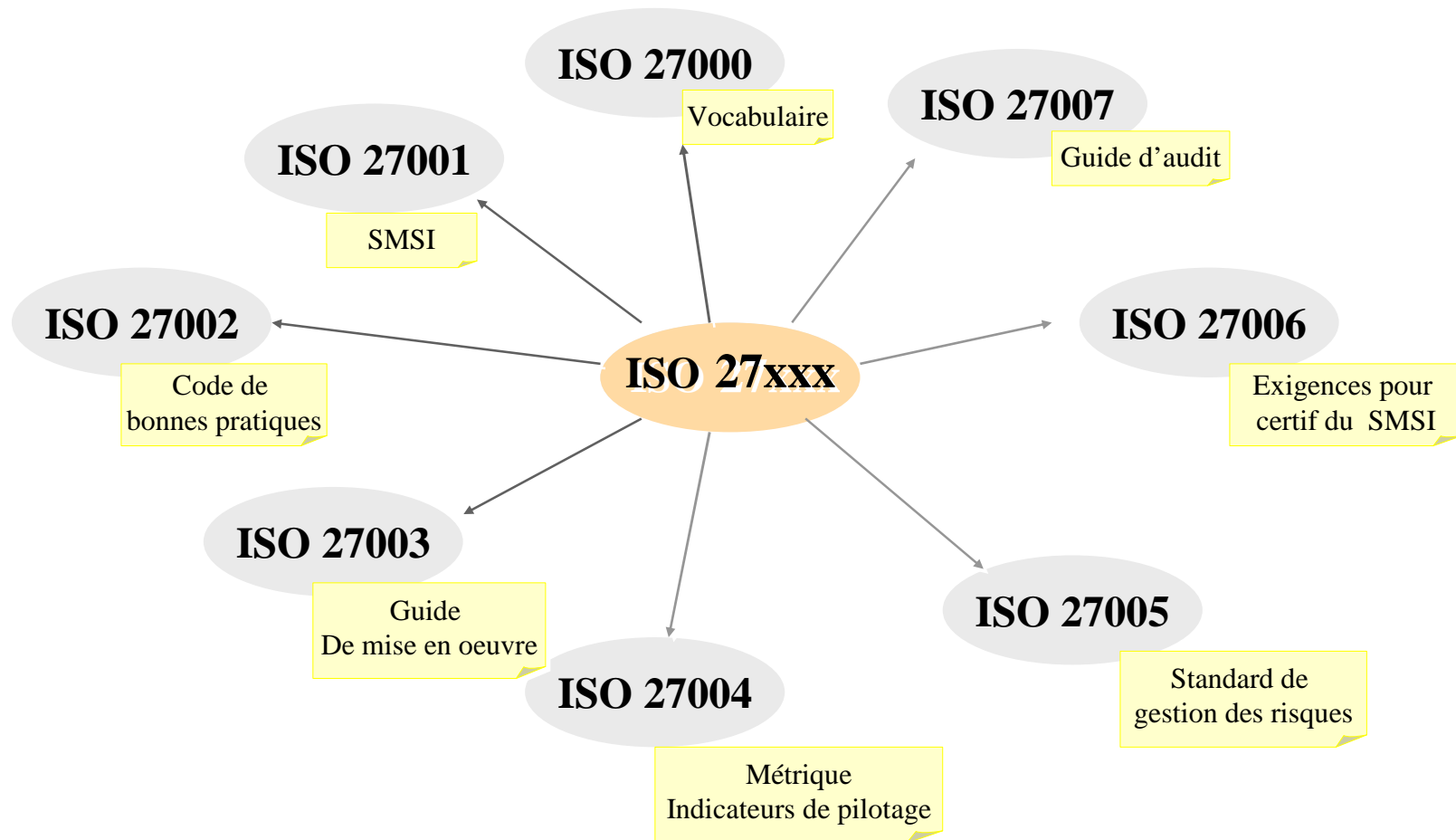
Quelques mots clé

➤ Risque

« combinaison de la probabilité d'un évènement et de ses conséquences » [Guide ISO/IEC 73]

- **Analyse de risque :**
« utilisation systématique d'information pour identifier les sources et pour estimer le risque »
- **Évaluation du risque :**
« processus de comparaison du risque estimé avec des critères de risque donnés pour déterminer l'importance d'un risque »
- **Appréciation du risque :**
« ensemble du processus d'analyse du risque et d'évaluation du risque »
- **Management du risque :**
« activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque »
- **Traitement du risque :**
« processus de sélection et de mise en œuvre de mesures visant à modifier le risque »

ISO/IEC/27xxx



La méthode EBIOS

Expression des besoins et Identification des objectifs de sécurité

➤ Historique

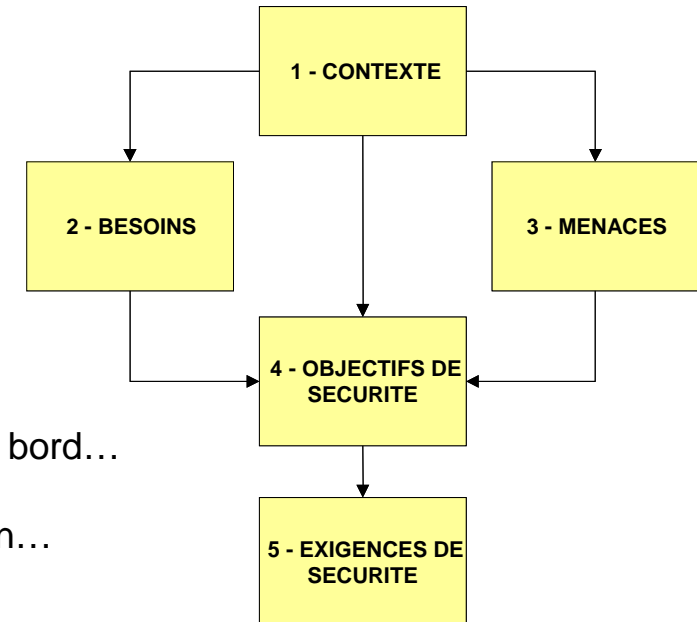
- Apparue en 1995
- Méthode d'analyse de risque, développée par la DCSSI
- Maintenu aujourd'hui par le Club EBIOS (DCSSI, FT, CNAM/TS, SAGEM, ... et EDELWEB)

➤ Objectif

- **Contribue à des démarches globales de SSI pour la formalisation de:**
 - schéma directeur, politique de sécurité, tableaux de bord...
 - spécifications SSI : FEROS, cible de sécurité, PP,
 - spécifications pour la maîtrise d'œuvre, plan d'action...
- Implique tous les acteurs
- Permet d'effectuer des arbitrages

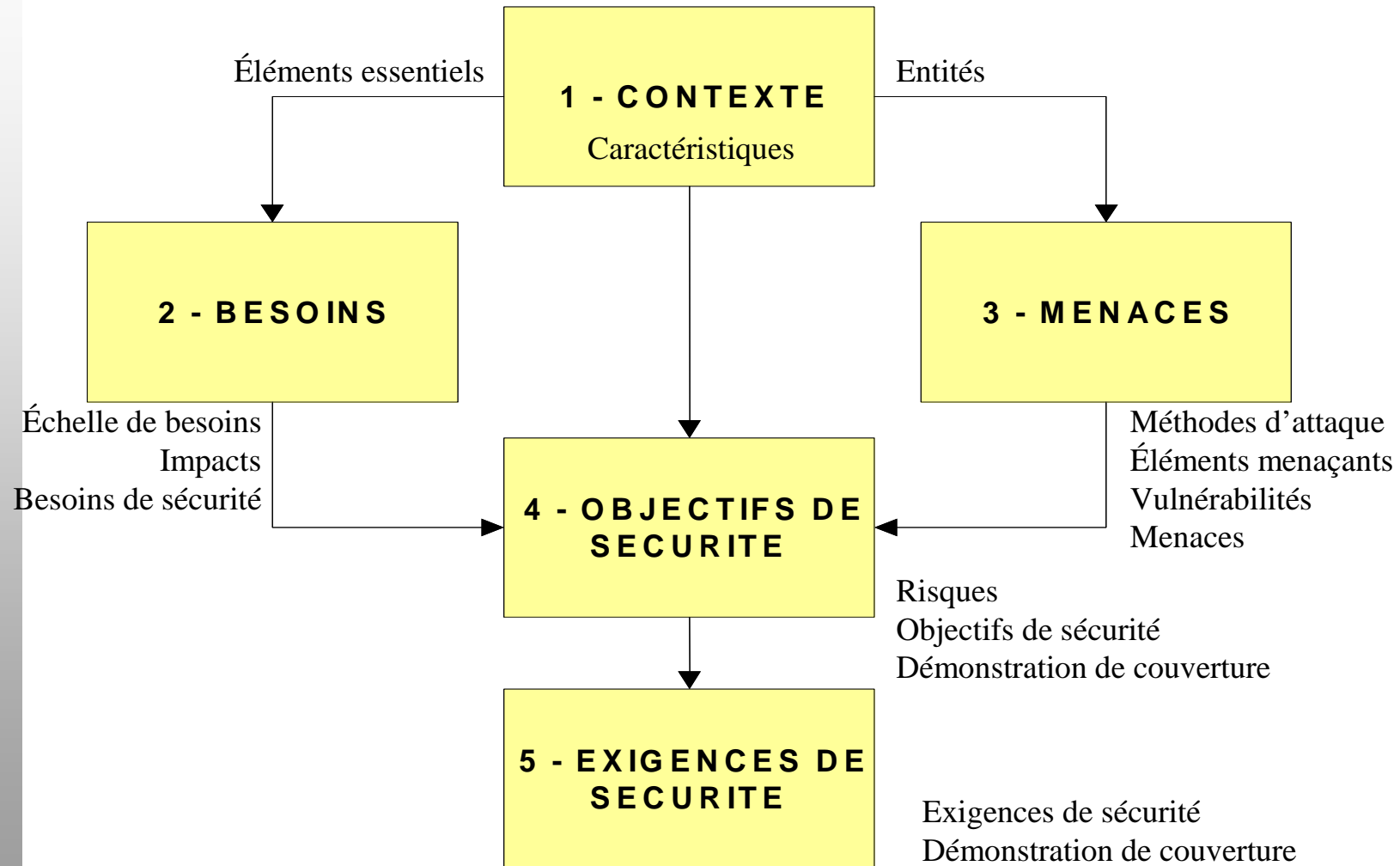
➤ Contenu

- **5 étapes d'analyse**
 - Contexte
 - Expression des besoins de sécurité
 - Analyse des menaces
 - Identification des objectifs de sécurité
 - Expression des exigences de sécurité (lien avec ISO 15408 et ISO 27002)
- **Méthode et outillage gratuits**



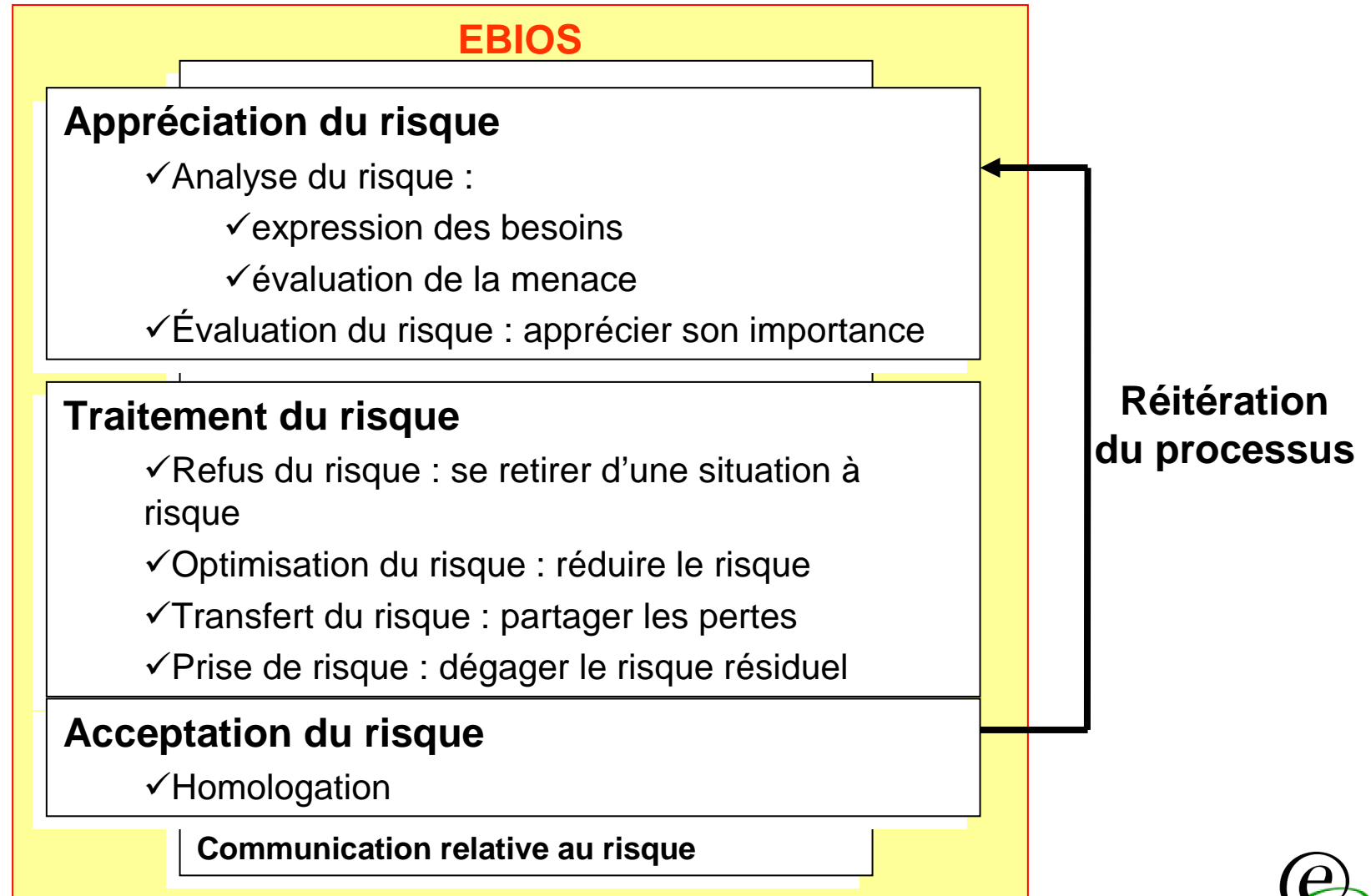
La méthode EBIOS

Les étapes de la méthode



La méthode EBIOS

L'analyse de risque



Club 27001 – Toulouse le 28/09/07

ISO/IEC/27001

SMSI

➤ Historique

- Origine britannique (BS7799 part 2)

➤ Objectif : Certifier que les **moyens de management** sont bien en place pour obtenir le niveau de sécurité adéquat

➤ Contenu

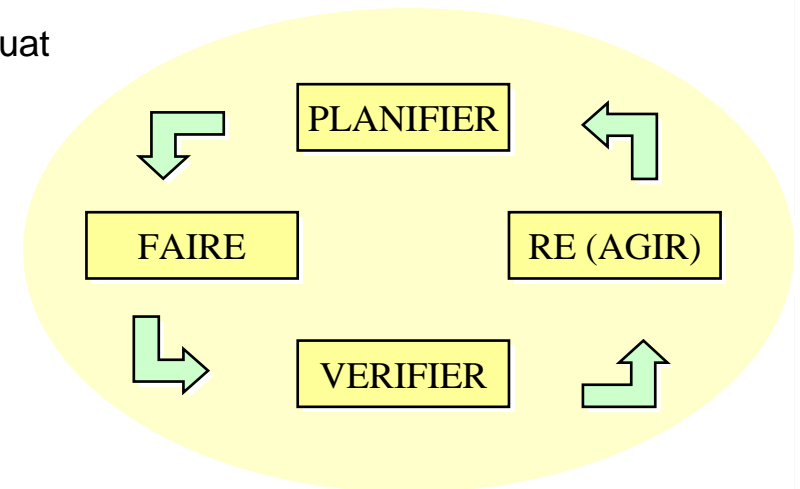
- Démarche et exigences pour la mise en œuvre d'un SMSI

➤ Approche de gestion des risques

- Formaliser une démarche de management de la sécurité de l'information
- Mettre en œuvre la sécurité de l'information
- Améliorer continuellement la sécurité de l'information
- Auditer la sécurité de l'information

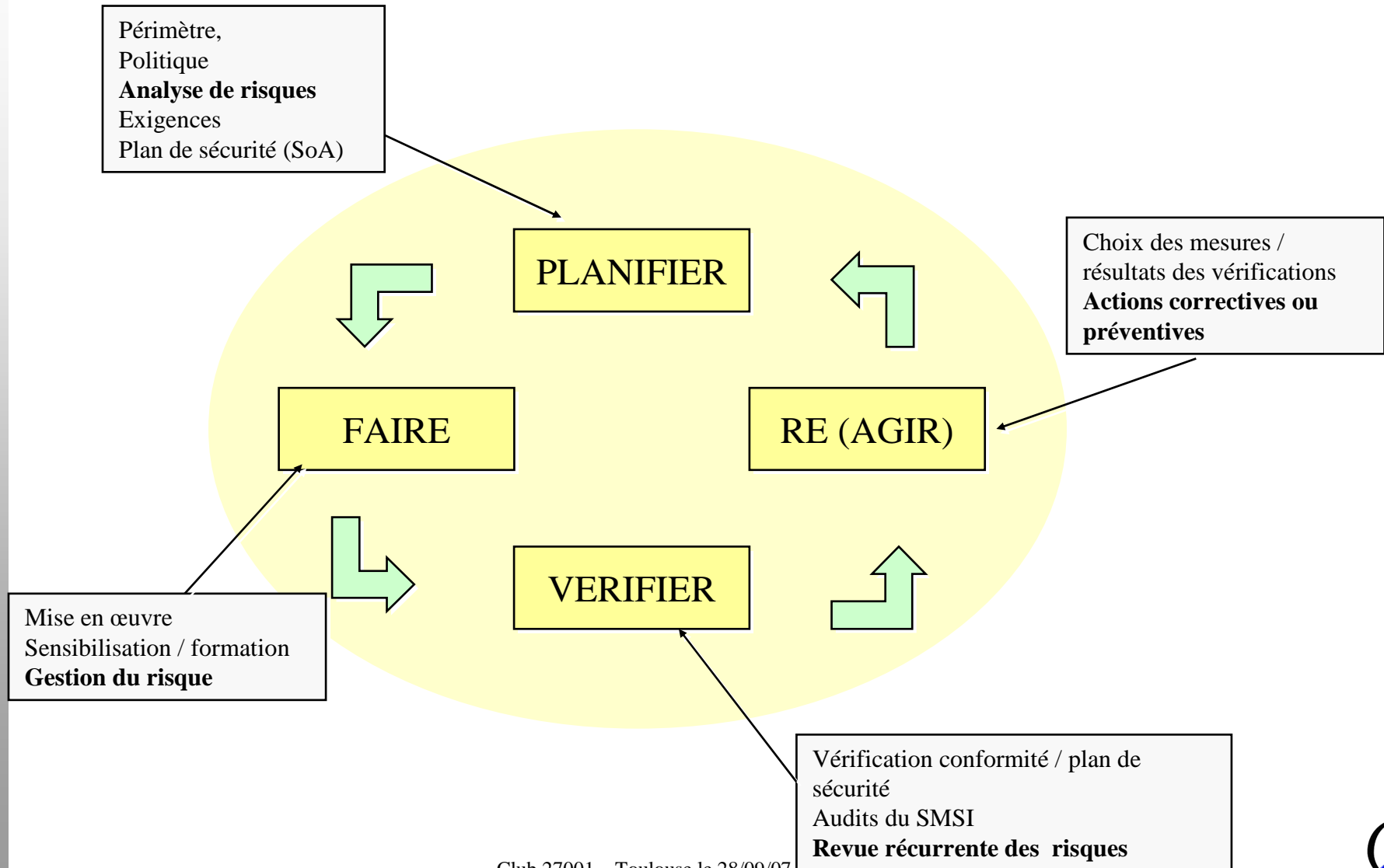
➤ Processus continu (Roue de Deming – voir ci-après)

- Identifier en permanence les évolutions ayant un impact sur le système
- Intégrer les évolutions dans le SMSI



ISO/IEC/27001

Roue de deming



ISO/IEC/27005

Standard de gestion du risque

➤ Objectif

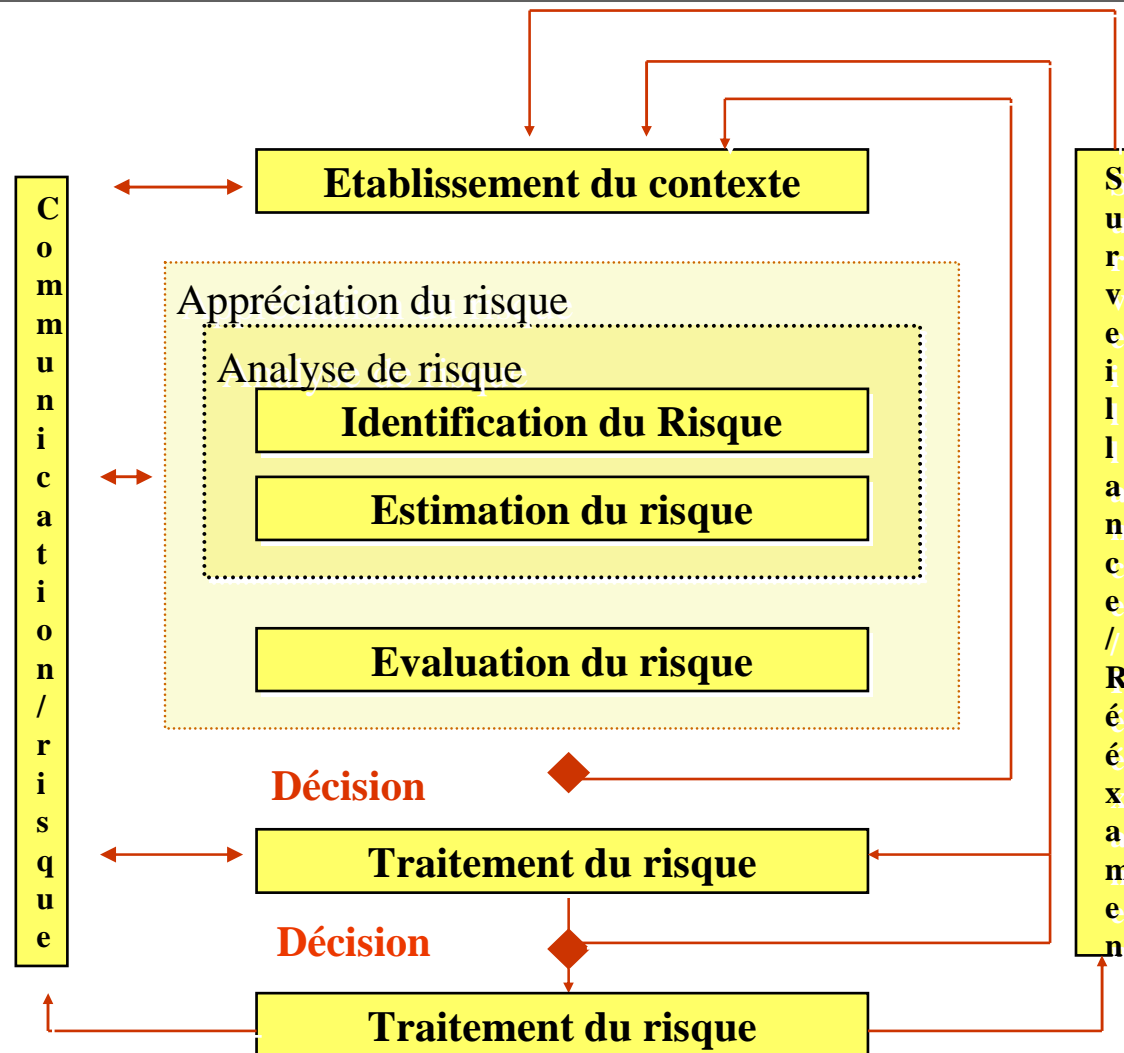
- Recommandations pour la gestion du risque dans un SMSI

➤ Contenu

- Introduction : périmètre, vocabulaire, structure
Document présenté comme étant un standard
- Processus de gestion du risque (6)
- Etablissement du contexte (7)
- Appréciation du risque (8)
- Traitement du risque (9)
- Acceptation du risque (10)
- Communication du risque (11)
- Surveillance et réexamen du risque (12)

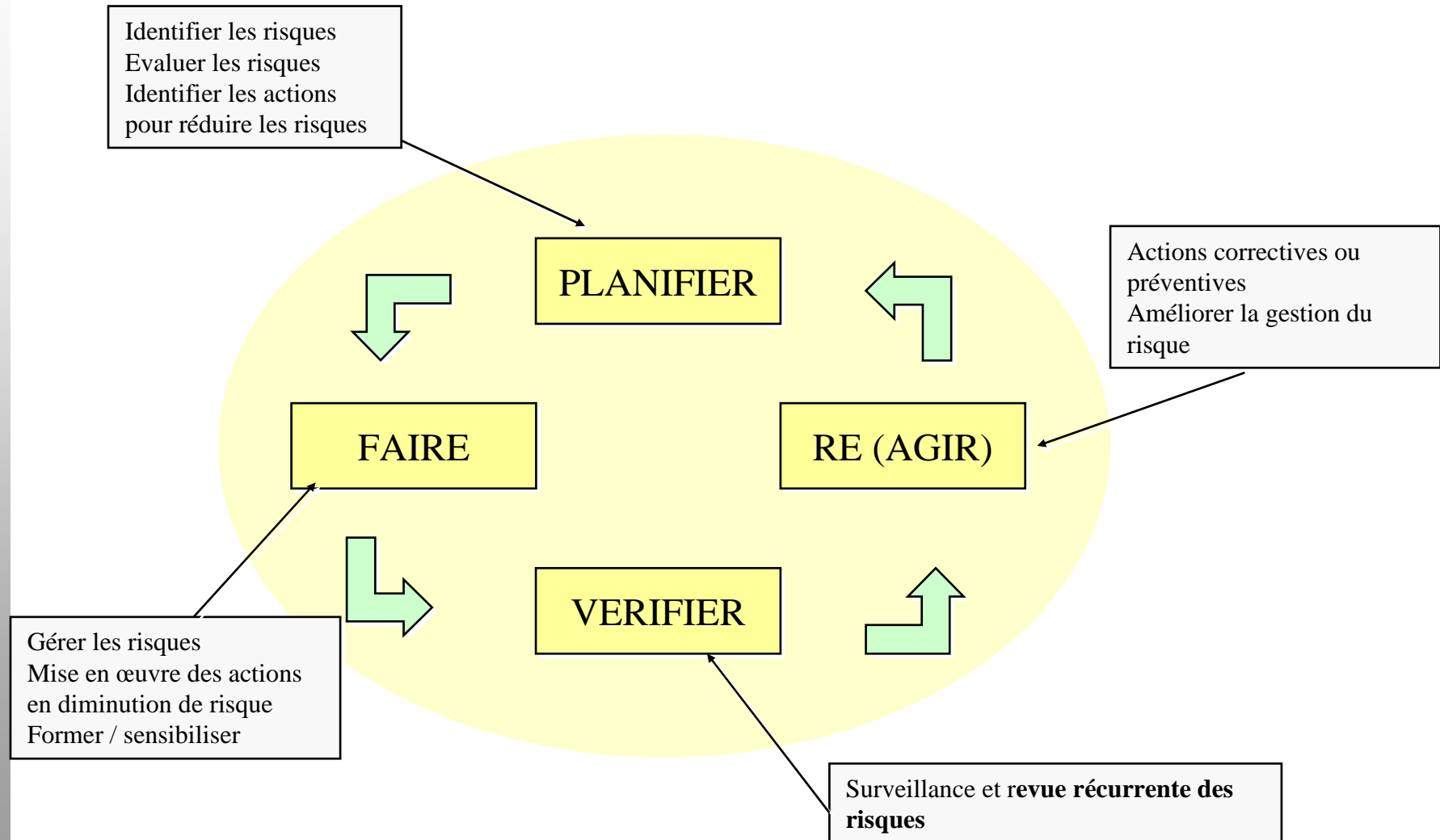
ISO/IEC/27005

Les étapes



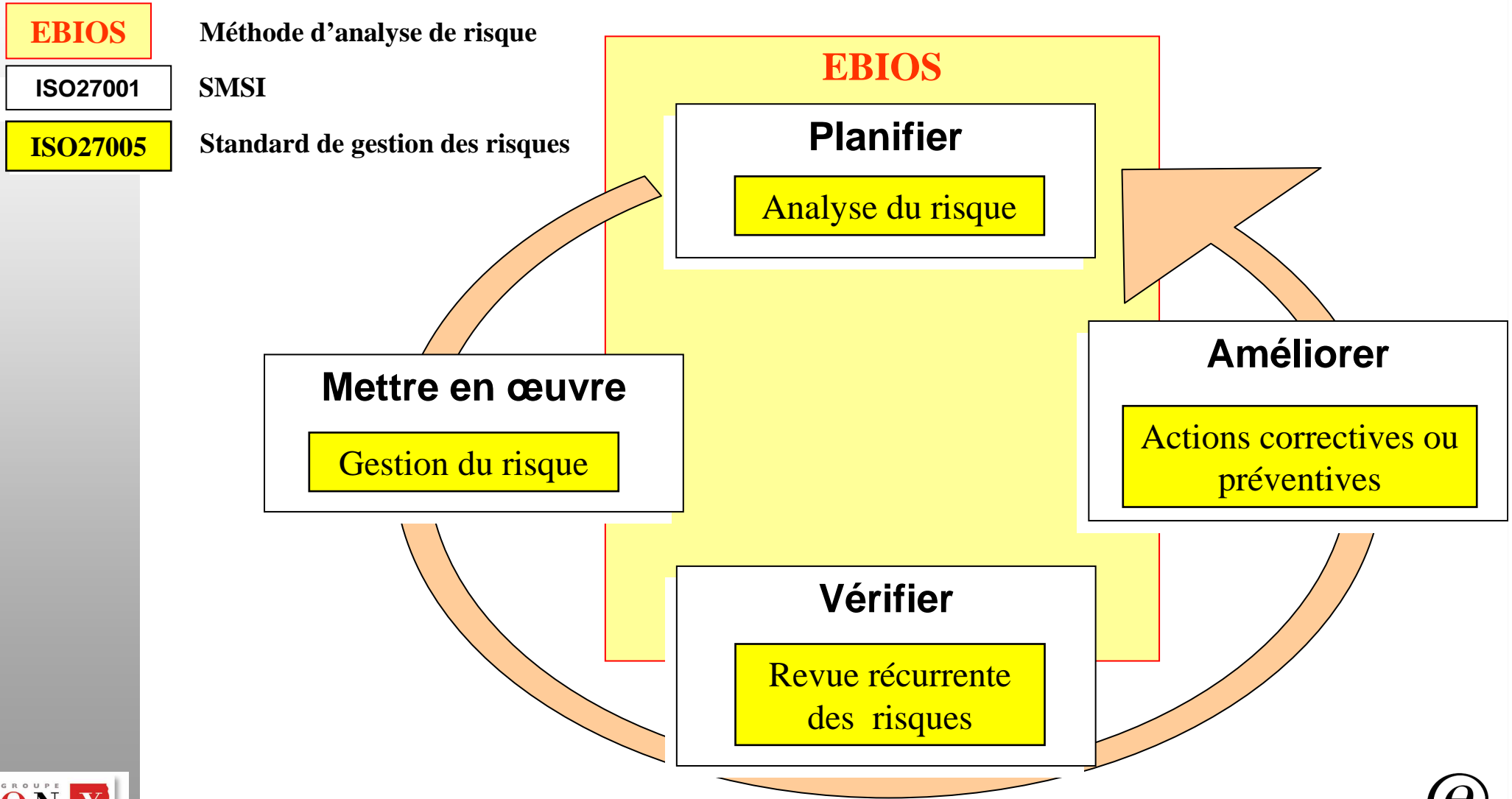
ISO/IEC/27005

Roue de deming



EBIOS/ISO27001/ISO27005

Positionnement



EBIOS/ISO27001/ISO 27005

Débat

