

# SOMMAIRE

- Constat CLUSIF 2008: la mise en œuvre des politiques de sécurité reste un vœu pieux: Pourquoi?
- Comment arriver à la non régression de la sécurité de l'information ?
- Pourquoi l'ISO 27001 ?
- Comment présenter un projet ISO27001 à une direction générale
- ISO27001 & OSSTMM: implémentation
- Stratégie alternative pouvant mener à la certification
- Enjeux et défis
- Quelles réponses ?
- Conclusion

# Constat 2008: la mise en œuvre des politiques de sécurité reste un vœu pieux: Pourquoi ? (1/2)

## Les causes possibles:

- Manque de volonté politique de la direction générale > pourquoi ?
- La DSI/RSSI ne sait pas « vendre » la juste sécurité en interne par manque d'arguments: pourquoi ?
- L'approche sécurité se fait par les « moyens techniques »: pourquoi ?
- La sécurité de l'information reste une affaire de spécialistes liés à la DSI souvent démunie pour mettre en œuvre un projet qui dépasse largement le cadre de la DSI (découragement par manque de méthodologie avec une pression croissante liée à une activité de plus en plus exigeante et instable)

# Constat 2008: la mise en œuvre des politiques de sécurité reste un vœu pieux: pourquoi? (2/2)

## Les remèdes possibles (pour une sécurité justifiée):

- Avoir une approche « métiers » et coordonnée avec les hommes clés de l'entreprise: identifier risques/impacts/patrimoine informationnel
- Valoriser l'information par une analyse de risques: en déduire les arguments qui parlent à une direction générale (langage métier)
- Démontrer simplement la relation de causes à effets entre l'activité et le système d'information: impacts et mesures de réduction (mettre la DG en position de décider en connaissance de causes)
- Etre réaliste dans la mesure de ses moyens: viser la juste sécurité accessible, ne pas ignorer les menaces, accepter les efforts à fournir, course de fonds sans fin

Dans un environnement de plus en plus instable et incertain:  
Piloter sa sécurité est une nécessité



# Comment arriver à la non régression de la sécurité de l'information ? (1/2)

## 1. Par une démarche qualité et sécurité de type ISO27001:

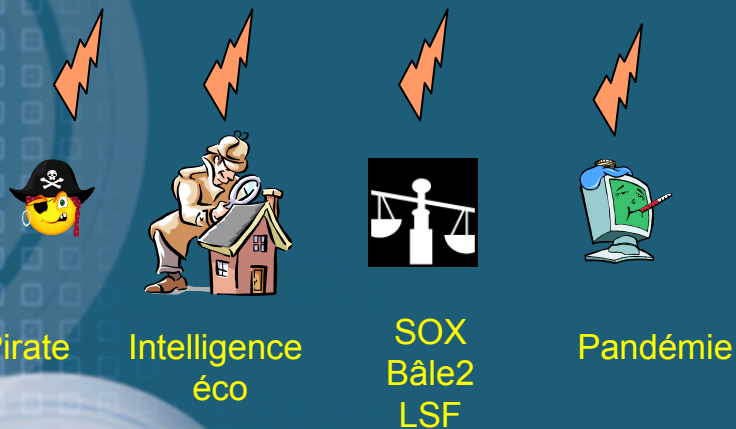
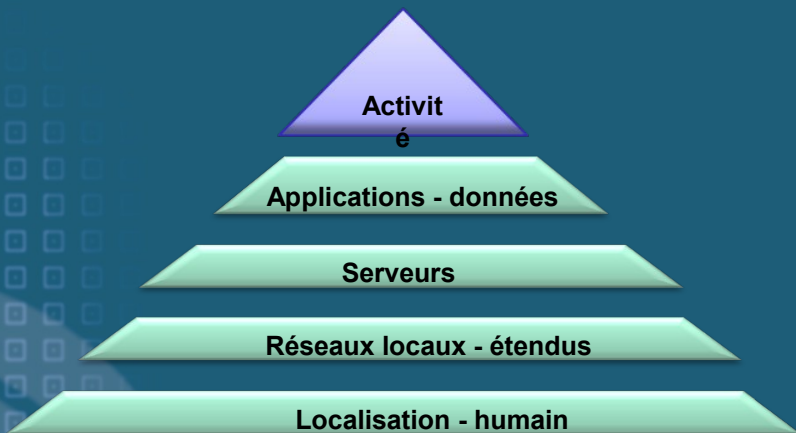
- Basée sur le modèle d'amélioration continue Plan-Do-Check-Act (PDCA)
- Qui intègre la gestion des risques (27005) et des indicateurs (27004)
- Dont les mesures de sécurité reposent sur les bonnes pratiques (27002)
- Qui n'a de raison d'être qu'à partir du moment où l'activité le justifie

*Ce qui est visé c'est la juste sécurité sur les biens sensibles  
Associée à une maîtrise des risques*

# Comment arriver à la non régression de la sécurité de l'information ? (1/2)

## pilotage et gestion de la sécurité

Joyaux ?      Quelle valeur / enjeux?



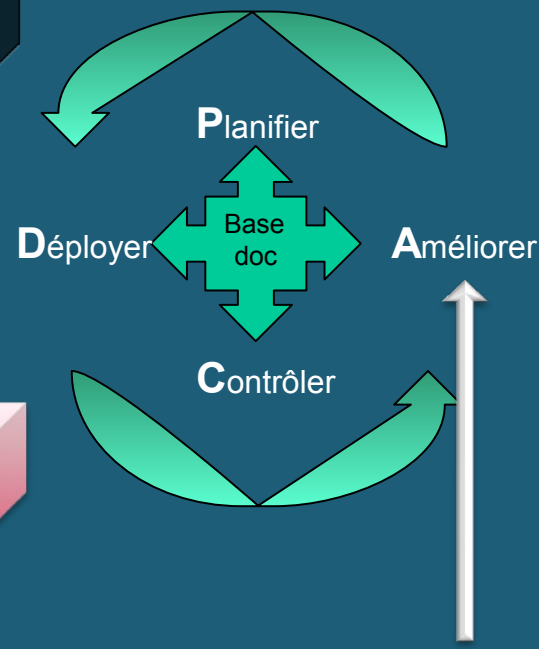
ISO 27001  
Système Management Sécurité Information

PCA → ISO 2700? MCA

Risque mesuré → ISO 27005 Gestion risques

ISO 27002 Mesures (17799)

ISO 27004 Indicateurs





# Comment arriver à la non régression de la sécurité de l'information ? (2/2)

## 2. Par un contrôle régulier du niveau réel de sécurité:

- Basée sur le modèle d'amélioration continue Plan-Do-Check-Act (PDCA)
- Indépendant (pas juge et partie)
- Qui reposent sur les bonnes pratiques (OSSTMM, OWASP)
- Qui peuvent conduire à la certification du niveau de sécurité (infrastructure, site web)
- Qui s'intègre parfaitement dans l'ISO 27001

# Comment arriver à la non régression de la sécurité de l'information ? (2/2)

## La méthode OSSTMM: complément de l'ISO 27001

- OSSTMM: Open Source Security Testing Methodology manual  
Méthode indépendante de tests de sécurité 
- Créée par une communauté de chercheurs en 2001 et éditée par l'ISECOM (.org) 
- Conçue pour mesurer le niveau de sécurité des systèmes opérationnels (infrastructures, applications, processus, personnels)
- Repose sur une métrique de sécurité (transparente, reproductible): le RAV (Risk Assessment value), se mesure en %
- Certification possible à partir de 90%: vs bonnes pratiques OSSTMM 3.0, OWASP (Open Web Application Security Project)



# Comment arriver à la non régression de la sécurité de l'information ? (2/2)

Objectifs métier et de sécurité

Activité

Applications - données

Serveurs

Réseaux locaux - étendus

Localisation - humain



Auditeur

Testeur

Analyste

Open Source  
Security  
Testing  
Methodology  
Manual  
(OSSTMM)

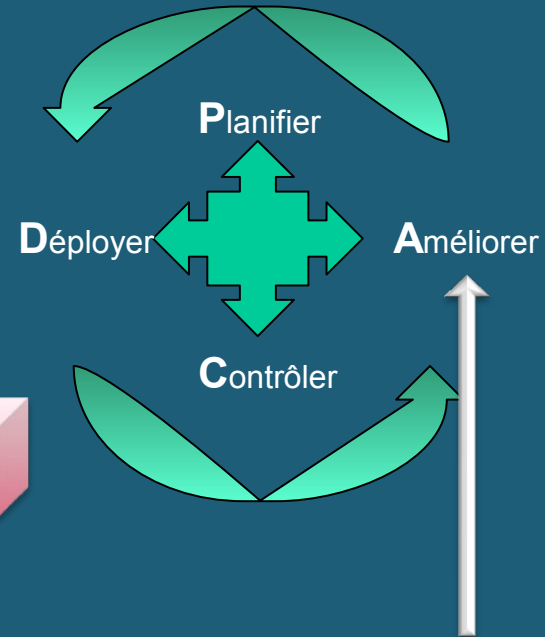
Métrique risques  
RAV

ISO 27001  
Système Management Sécurité Information

ISO 27005  
Gestion risques

ISO 27002  
Mesures (17799)

ISO 27004 Indicateurs



OSSTMM: compatible ISO27001



# Pourquoi l'ISO27001 ? (1/2)

Quelles sont les motivations possibles:

- adopter les bonnes pratiques (mesures de sécurité, démarche qualité)
- structurant par la démarche (personnel certifié pour la mise en œuvre)
- augmenter la confiance des parties prenantes (certification d'un périmètre stratégique): actionnaires, clients, fournisseurs, salariés, partenaires...
- avantage concurrentiel pour gagner des parts de marché (garanties d'une bonne gestion de la sécurité sur des marchés sensibles: hébergement, e-commerce...)
- économie d'énergie et d'efforts à fournir: puisque les mesures à appliquer peuvent être limitées au périmètre stratégique et limitées aux mesures attendues par l'ISO



## Pourquoi l'ISO27001 ? (2/2)

### Les erreurs à éviter:

- couvrir un périmètre trop important (risque de découragement) ou trop petit (pas significatif pour l'activité)
- penser qu'entamer la démarche est suffisant pour obtenir des résultats : c'est un projet d'entreprise qui doit être sponsorisé par la DG
- assimiler l'ISO27001 à l'ISO9000: beaucoup plus léger puisqu'on peut l'appliquer sur un périmètre limité mais significatif (2 serveurs hébergeant un site marchand)
- la certification est du luxe : c'est un aiguillon indispensable si on veut obtenir des résultats rapidement
- Ne pas impliquer la DG: indispensable puisqu'on touche à ce qui est stratégique au plus haut niveau de l'entreprise



# Comment présenter un projet ISO27001 à une direction générale ?

En tant qu'outil de pilotage et de maîtrise des risques d'entreprise:

- basé sur les objectifs « métier » en termes financiers et de satisfaction clients
- qui protège les parties vitales de l'entreprise dans un processus d'amélioration continu

Doit être justifié pour l'activité de l'entreprise:

- stratégique pour la DG: augmentation CA, avantage concurrentiel, rassurer en vue d'une fusion/acquisition...imposé de fait par un organisme de contrôle (Banque de France)
- structurant pour la DSI/RSSI: augmente la fiabilité du SI par l'adoption des bonnes pratiques

# ISO 27001 & OSSTMM: implémentation (1/4)

OSSTMM:  
vecteurs  
D'attaque\*

OSSTMM:  
indicateurs: RAV\*

OSSTMM:  
Identification vul.\*

OSSTMM:  
certification

## ISO27001 Phase 1

Analyse  
préalable:

- Justifié ?
- État des lieux
- Options du périmètre\*

## ISO27001 Phase 2

Mise en place  
structure de  
base:

- Gouvernance
  - Doc
- Audit interne\*
- Formation
- Indicateurs\*

## ISO27001 Phase 3

Intégration  
processus:

- Appréciation des risques\*
- Adaptation mesures existantes
- Mise en place mesures manquantes
- Mise en place revue SMSI

## ISO27001 Phase 4

Démarrage  
SMSI:

- Revue SMSI
- Prép. Audit
- Audit à blanc
  - Actions correctives & préventives

\* Points communs



# ISO 27001 & OSSTMM: implémentation (2/4)

| ISO 27001           |  | OSSTMM  | Démarche traditionnelle        |
|---------------------|--|---|--------------------------------|
| <b>Introduction</b> | lancement du projet                                |   |                                |
| <b>Phase 1</b>      | <u>Analyse préalable</u>                           |   |                                |
|                     | Etude d'opportunité                                | apports de l'OSSTMM à l'organisme               | apport à l'organisme           |
|                     | Etat des lieux                                     |   | analyse de risques             |
|                     | Etude des scénarios/options périmètre & politique  | Choix des vecteurs d'attaque                    |                                |
| <b>Phase 2</b>      | <u>mise en place structure de base</u>             |   |                                |
|                     | Gouvernance  | implication de la direction                     |                                |
|                     | Documentation                                      | à intégrer dans le SMSI                         |                                |
|                     | Audit interne suivi d'actions                      | à intégrer dans le SMSI                         | Diag/audit général             |
|                     | Formation Sensibilisation                          | OPST/OPSA                                       |                                |
|                     | Indicateurs  | alimente le SMSI                                |                                |
| <b>Phase 3</b>      | <u>mise en place des processus</u>                 |   |                                |
|                     | Appréciation des risques                           | application méthode OSSTMM: recherche infos     | tests                          |
|                     | Adaptation des mesures de sécurité existantes      | PDCAifier les processus OSSTMM                  |                                |
|                     | Mise en place des mesures de sécurité managériales | appliquer les recommandations issues de l'audit | mettre en œuvre plan d'actions |
|                     | Mise en place de la revue du SMSI                  |   |                                |
| <b>Phase 4</b>      | <u>Démarrage du SMSI</u>                           |   |                                |
|                     | Revue du SMSI                                      |   |                                |
|                     | Préparation à l'audit                              | idem SMSI                                       |                                |
|                     | Audit à blanc                                      | idem SMSI                                       |                                |
|                     | Actions correctives et préventives                 | idem SMSI                                       |                                |



# ISO 27001 & OSSTMM: implémentation (3/4)

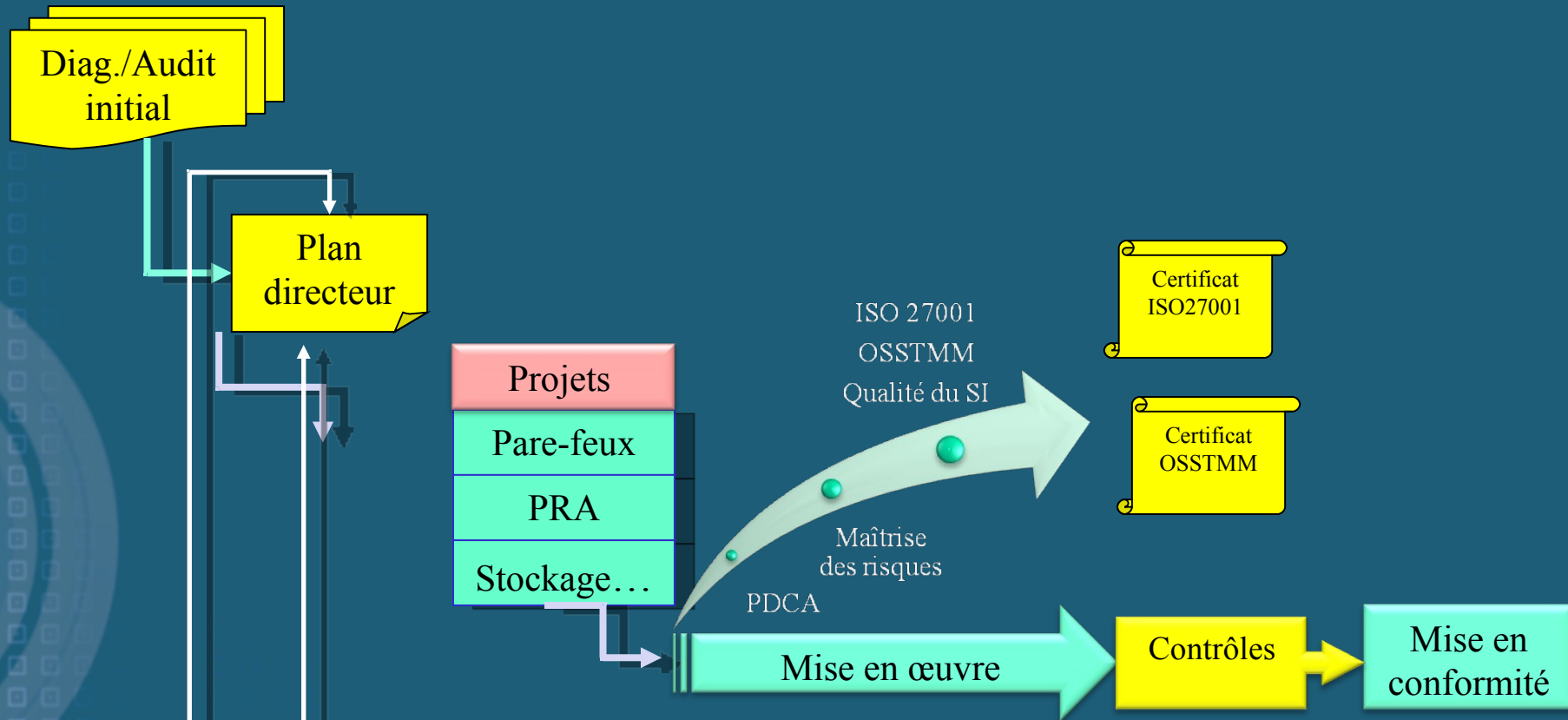
## ISO 27001

| Phase 1        | Analyse préalable                      |   | Livrables   |
|----------------|--|---|---|
|                |  | Etude d'opportunité   |   |
|                |  | Etat des lieux  |   |
|                |  | Etude des scénarios/options périmètre & politique   | Périmètre du SMSI<br>Politique du SMSI  |
| <b>Phase 2</b> | <u>mise en place structure de base</u> |   |   |
|                |  | Conseil SMSI; Fiches descriptives des instances de gouvernance; Planning des réunions des différentes instances |   |
|                |  | Documentation   | procédure de gestion de la documentation; Documents du SMSI                         |
|                |  | Audit interne suivi d'actions   |   |
|                |  | Formation Sensibilisation   |   |
|                |  | Indicateurs   |   |
| <b>Phase 3</b> | <u>mise en place des processus</u>     |   |   |
|                |  | Appréciation des risques  | Critères d'acceptation des risques; Inventaire des actifs; Appréciation des risques |
|                |  | Adaptation des mesures de sécurité existantes   |   |
|                |  | Mise en place des mesures de sécurité manquantes  | Déclaration d'applicabilité   |
|                |  | Mise en place de la revue du SMSI   |   |
| <b>Phase 4</b> | <u>Démarage du SMSI</u>                |   |   |
|                |  | Revue du SMSI   |   |
|                |  | Préparation à l'audit   |   |
|                |  | Audit à blanc   |   |
|                |  | Actions correctives et préventives  |   |



# ISO 27001 & OSSTMM: implémentation (4/4)

## ISO 27001 & OSSTMM: intégration dans la démarche globale de sécurité



# Stratégie alternative pouvant mener à la certification

## 1. Démarche classique:

- A partir des objectifs « métier » identifier les risques/impacts/patrimoine informationnel
- En déduire le périmètre du système d'information à prendre en compte

## 2. Y ajouter un volet ISO27001:

- retenir les mesures de sécurité obligatoires par l'ISO
- y ajouter les mesures spécifiques au projet d'entreprise (ex: e-commerce)
- commencer à PDCA-ifier les processus les plus importants

## 3. Compléter progressivement le dispositif en vue d'évoluer vers un SMSI voire une certification



# Enjeux et défis

- Les enjeux se situent:
  - dans la prise de conscience des directions générales
  - au niveau du réglage des organisations (gouvernance, manque de compétences)
  - et juridiques (vides liés à Internet, mondialisation de l'économie)
- Accentué par des technologies qui évoluent de plus en plus vite et des compétences qui ont du mal à suivre...

Pour résumer, les risques augmentent avec des exigences et une pression économiques de plus en plus fortes, associé à une connaissance diffuse voire inexistante du niveau réel de sécurité.

# Quelles réponses à ces enjeux ?

- Piloter sa sécurité
- Contrôler le niveau réel de sécurité dans le cadre de communautés de confiance (chaînes de valeurs: utilisateur-fournisseur-certificateur)
  - La confiance repose sur:
    - L'indépendance (auditeurs, certificateurs),
    - La transparence (référentiels normes et bonnes pratiques)
    - Des repères communs (normes, règles internationales...)

# Conclusion

L'insécurité de nos entreprises n'est pas une fatalité.

Il ne faut pas être naïf face aux nouvelles menaces d'un monde de plus en plus imprévisible et penser global (marché mondial, entreprise étendue, diffusion instantanée de l'information)

L'anticipation est un des moyens de maîtriser un peu mieux l'imprévu.

Le discours « sécurité informatique » est dépassé depuis longtemps.

L'entreprise pour rester dans la course doit être agile et rentable. Pour cela elle augmente de jour en jour sa dépendance au système d'information et son attractivité sur le marché (concurrence) , si en plus elle est vulnérable ou pire pense être sécurisée (méconnaissance de la sécurité réelle): alors elle prend des risques inconsidérés (engagement personnel de la direction).

Une partie de la réponse est dans un pilotage de sa sécurité de plus en plus lié à celui de son activité.

Tout peut être fait avec ou sans gestion des risques, on peut voir les premiers résultats dans l'actualité...

