GR – Les normes ISO27001-27002

UNIV-PAU / LP

Les normes ISO27001 et 27002

Qu'est ce qu'un SMSI

- Système de Management de la Sécurité de l'Information
- Constat
  - Sécurité de l'information = parent pauvre en entreprise
  - On constate une anarchie = chacun fait ce qu'il veut dans son coin
  - Nécessité d'avoir un chef d'orchestre.
  - Ce chef d'orchestre s'appelle le « SMSI »

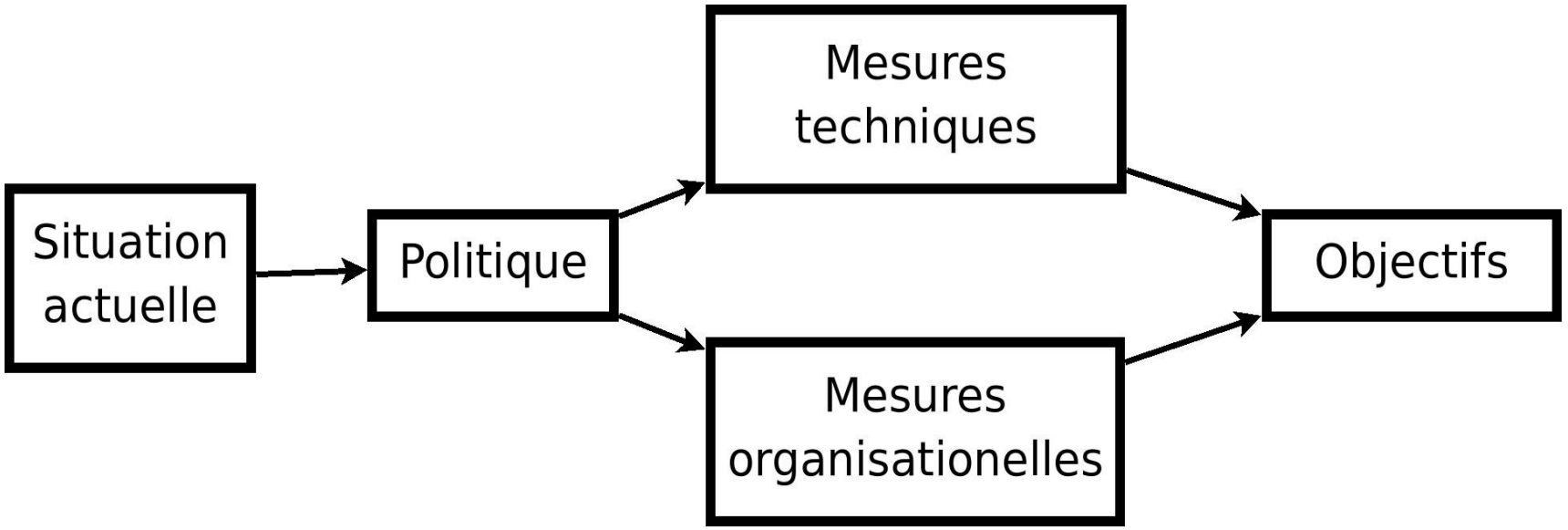
Qu'est ce qu'un SMSI

- Système de Management de la Sécurité de l'Information => 2 composantes :
  - **Système de management**
  - Sécurité de l'information

Qu'est-ce qu'un système de management ?

- C'est un système qui permet :
  - d'établir **une politique**
  - d'établir **des objectifs**
  - d'**atteindre** ces objectifs
- Quand l'objectif est atteint, il faut **maintenir** le niveau atteint et éventuellement le dépasser.

Système de management



Propriétés de systèmes de management

- Large spectre de métiers et de compétences
  - c'est l'approche transversale
- Un projet fédérateur et mobilisateur
  - C'est l'approche verticale => de la direction aux employés (toute la hiérarchie est concernée)
- Importance de l'écrit
- Auditabilité

apport des systèmes de management

- Mettre en place un système de management coûte cher (définition de politiques, rédaction de procédure, audit, mobilisation)
- Donc => Qu'est-ce que ça apporte ?
  - L'adoption de bonnes pratiques
  - L'augmentation de la fiabilité
  - La confiance (l'apport le plus important)

L'adoption de bonnes pratiques

- Chaque SM a son guide de bonnes pratiques (qualité - ISO-9001, environnement ISO-14001, sécurité alimentaire ISO-22000).
- Un SMSI (ISO-27001) permettra d'adopter des bonnes pratiques permettant d'améliorer la sécurité de l'information :
  - Quels sont les biens les plus sensibles ?
  - Où déployer en priorité les mesures de sécurité ?
  - Comment cloisonner les réseaux ?
  - Comment détecter les incidents ?
  - Comment réagir rapidement aux intrusions ?
  - ...

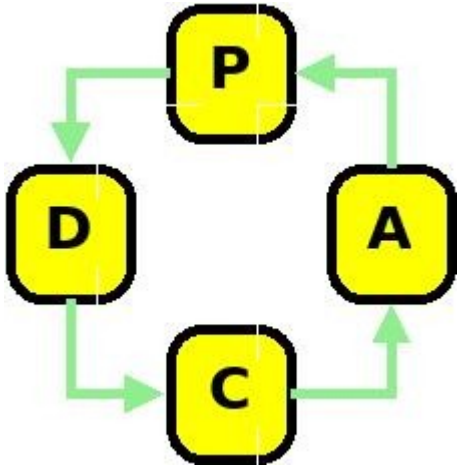
L'augmentation de la fiabilité

- Conséquence de l'adoption de bonnes pratiques
- + notion d'amélioration continue favorisant la capitalisation sur les retours d'expérience.

La confiance

- C'est bien d'être « bon » (apport 1 et 2) encore faut-il que ça se sache. Pour obtenir un avantage commercial par exemple.
  - Notion de partie-prenante : Les actionnaires, directeurs de projet, les clients, les fournisseurs, les partenaires, les banques et assurances (exemple du transfert de risque), le personnel, l'opinion publique.
- Ce sont les parties prenantes qui nous obligent à mettre en place un SM.
- C'est grâce à la confiance que l'on gagne de l'argent (permet les relations entre les clients et les fournisseurs)
- C'est la notion de **certification** qui apporte la confiance.

Le modèle PDCA



- le modèle en quatre temps Plan, Do, Check, Act
  - Planifier : On dit et on écrit ce que l'on va faire sur le domaine qui nous concerne
  - Faire : On met en place
  - Vérifier : On mesure les écarts entre ce que l'on a dit et ce qui est fait réellement
  - Corriger : On entreprend les actions pour corriger les écarts
- 2 propriétés :
  - Cyclique => amélioration continue
  - Fractale => Se retrouve à tous les niveaux de l'entreprise

La norme ISO-27001

- Elle concerne la mise en place d'un Système de Management pour la sécurité de l'information
- Historique de la norme
  - **1995** : la BSI (British Standard Institution) => publie la norme BS7799
    - Catalogue de bonnes pratiques
    - Pas de notion de SMSI
  - **1998** : BSI => BS7799-2 (ce n'est pas la version 2)
    - c'est la deuxième partie de la norme
    - Elle précise les exigences pour mettre en place un SMSI

Historique de la norme / suite

- 2000 : Grand succès de BS7799 ! => L'ISO décide de l'intégrer dans ses normes.
  - ça devient l'ISO-17799 (quelques mesures supplémentaires : enrichissement du catalogue)
  - pas de notion de SMSI
- 2002 : BSI fait la deuxième version de BS7799-2 (version 2002)
- 2005 (juin) : ISO : enrichissement de ISO-17799.
- 2005 (octobre) : ISO : ISO-27001 = adaptation de la BS7799-2:2002
- 2007 : Cohérence des nomenclatures : 17799 devient 27002

Composition de la norme

- document de 34 pages, 8 chapitres.
- 3 premiers chapitres = généralités
- Chapitres intéressants : de 4 à 8 = 10 pages !
  130 € (vendu sur le site de l'AFNOR)
- 3 annexes : A, B et C

Les chapitres

- Chapitre 4 : chapeau (rappel du modèle PDCA et de ce que signifie SMSI)
- Chapitre 5 : Responsabilité du management
- Chapitre 6 : Audit interne du SMSI
- Chapitre 7 : revue du SMSI
- Chapitre 8 : amélioration du SMSI

Les annexes

- Annexe A : Liste d'objectifs de sécurité et de mesures
  - Cette liste est extraite du catalogue de bonnes pratiques (ISO-27002).
- Annexe B et C : Correspondances avec d'autres normes

Contenu de la phase « Plan »

- Étape n°1 : définir le périmètre et la politique
- Étape n°2 : apprécier les risques
- Étape n°3 : traiter le risque et identifier le risque résiduel
- Étape n°4 : sélectionner les mesures de sécurité

PLAN / Étape n°1 : définir le périmètre et la politique

- **Périmètre** : sur quoi s'applique mon SMSI (de très petit à très vaste)
  - Inclure en priorité les composantes de l'entreprise dont les parties prenantes exigent le plus de confiance
- **Politique** : la politique décrit le niveau de sécurité qui s'appliquera sur le périmètre
  - quel niveau doit-on atteindre en terme de disponibilité, intégrité, confidentialité
- **On est libre de choisir** le périmètre que l'on veut et la politique que l'on veut et de se faire certifier.

PLAN / Étape n°2 : apprécier les risques

- Voir la norme 27005 ou méthode EBIOS
  - Identifier les risques
  - Estimer les risques
  - Évaluer les risques
- La norme 27001 n'impose pas de méthode particulière. Une conformité à 27005 est conseillée.

PLAN / Étape n°3 : traiter le risque et identifier le risque résiduel

- Traiter le risque
  - Prendre le risque
  - Refuser le risque
  - Réduire le risque
  - Transférer le risque
- Calculer le risque résiduel
- Accepter les risques résiduels

PLAN / Étape n°4 : sélectionner les mesures de sécurité

- pour chaque risque choisir les mesures dans le catalogue
  - C'est la liste des mesures applicables
  - Rédaction d'un tableau avec la liste de toutes les mesures du catalogue
  - pour chaque mesure : oui / non – justification (tout exclusion doit être bien fondée)
  - C'est une déclaration d'applicabilité (SoA : Statement of Applicability)
- On ne dit pas encore comment on va faire.

Contenu de la phase « Do »

- La phase Do consiste à mettre en oeuvre les objectifs fixés dans « Plan ».
  - On entre ici dans le domaine de la gestion de projet => chef de projet + équipe + argent
  - Activité n°1 : Rédiger un plan de traitement des risques
  - Activité n°2 : Déployer les mesures de sécurité
  - Activité n°3 : Générer des indicateurs
  - Activité n°4 : Sensibiliser et former le personnel
  - Activité n°5 : Détecter et réagir rapidement aux incidents

DO / Activité n°1 : Rédiger un plan de traitement des risques

- Listes des actions à entreprendre
- Les moyens nécessaires
- La définition des responsabilités et des priorités en matière de gestion des risques de sécurité de l'information.

DO / Activité n°2 : Déployer les mesures de sécurité

- Importance d'une bonne gestion de projet

DO / Activité n°3 : Générer des indicateurs

- A chaque objectif de sécurité est associé un indicateur
- Liberté dans le choix des indicateurs
- Très difficile à mettre en oeuvre
- ISO-27004 (norme concernant la mise en oeuvre des indicateurs)

DO / Activité n°4 : Sensibiliser et former le personnel

- Pédagogie
- Charte de sécurité
- Importance de l'implication

DO / Activité n°5 : Détecter et réagir rapidement aux incidents

- Toute attaque prend un certain temps à l'agresseur
- Toute attaque prend un certain temps à être détectée par le défenseur
- Les actions entreprises par le défenseur pour contrecarrer l'attaque prennent un certain temps

Contenu de la phase « Check »

- Est-ce que tout fonctionne comme prévu ?
- La norme impose la mise en place de moyen de contrôle pour vérifier
  - L'efficacité du SMSI
  - Sa conformité par rapport aux spécifications
- 3 familles d'outils existent pour effectuer ces contrôles
  - Les audits internes (on prévient)
  - Le contrôle interne (contrôle d'un point précis sans prévenir)
  - Les revues

CHECK / Audit Interne

- Planifié longtemps à l'avance. On a le temps de s'y préparer.
- l'auditeur étudie les documents écrits (politique, procédure, relevé de décisions), il vérifie sur le terrain ce qui est fait réellement. Il interroge les responsables, les employés => recoupement d'informations.
- Permet de vérifier la conformité du SMSI aux spécifications et son efficacité.
- Doit être réalisé par des personnes n'ayant pas participé à l'élaboration du SMSI.
- On essaye d'être exhaustif sur 3 ans avec plusieurs audits.

CHECK / Le contrôle interne

- contrôle d'un point précis sans prévenir
- Effet de surprise
- L'idée ne doit pas être de piéger

CHECK / Les revues

- Une par an
- Bilan des audits internes de l'année
- retour des parties prenantes
- État des lieux sur les actions en cours
- Interprétation des indicateurs
- Grand changement survenus dans l'entreprise (réorganisation, fusion)

Contenu de la phase « Act »

- Le constat de la phase CHECK génère:
  - des actions correctives (on agit sur les effets puis sur les causes)
  - des actions préventives
  - des actions d'amélioration

La norme ISO-27002

- Il s'agit d'un catalogue de bonnes pratiques
  - 133 mesures
  - Réparties dans 11 chapitres
- 110 pages
- Attention : Il ne faut mettre en place que les mesures nécessaires couvrant des risques identifiés et nécessitant un traitement.

Mesure de sécurité

- Pour chaque mesure on trouve :
  - Un numéro de référence
  - Brève description de la mesure
  - Préconisation de mise en oeuvre (comment)
  - Précisions utiles

Classification des mesures

- Les mesures sont classées par type dans les 11 chapitres suivants :

1) Politique de sécurité (rédaction d'une politique de sécurité)
2) Organisation de la sécurité de l'information (gouvernance de la sécurité)
3) Gestion des biens (un responsable par actif)
4) sécurité liée aux ressources humaines (avant embauche, pendant le contrat, au départ)
5) Sécurité physique et environnementale (locaux, matériel)
6) Gestion de l'exploitation et des télécommunications (chapitre très gros)
7) Contrôle d'accès
8) Acquisition, développement et maintenance des systèmes d'informations
9) Gestion des incidents liés à la sécurité de l'information (signalement et gestion)
10) Gestion du plan de continuité de l'activité
11) Conformité (réglementation)

Comparaison 27001 / 27002

ISO 27001	ISO27002
SMSI	Pas de SMSI
PDCA	Pas de PDCA
Clause obligatoire	Rien d'obligatoire
Certification possible	Pas de certification possible

avantages principaux 27001

- La confiance des clients
- Diminuer le coûts des audits (utilisation d'un tiers neutre = factorisation) de type clients
- Diminution des primes d'assurance (transfert du risque)
- Valorisation

avantages principaux 27002

- Tableaux de bord
- Consolidation tableau de bord (fournit un cadre)
- Consolidation audit (fournit un cadre si on sous-traite l'audit)
- Politique de sécurité

Autres normes dans la série 27000

- 27003 : Implémentation d'un SMSI
- 27004 : Indicateurs
- 27006 : certification de SMSI
- 27007 : audit de SMSI (2010)