

ISO 27001



anne.mur@edelweb.fr

dominique.pourcellie@cnamts.fr

<http://www.club-iso27001.fr>



1. Le Club 27001
2. Systèmes de management
3. Les normes de la série 27001
4. La boucle PDCA
5. Vos questions

Club 27001 Toulousain

Objectif :

Réunir les personnes intéressées par le Système de Management de la Sécurité du SI : norme ISO 27001

Forme :

Groupe de travail, de réflexion et d'échanges.

Au cours des réunions peuvent avoir lieu des présentations, des discussions ouvertes, et des prises de décision.

Qui ?

Groupe ouvert à tous, utilisateurs comme fournisseurs.

Les présentations sont de toutes natures : explications sur les normes, retours d'expérience, solutions commerciales, etc.

Où ?

Chez l'un des participants et sont annoncées par mail

Quand ?

Réunions trimestrielles, le vendredi après midi



Association

Président : Eric Doyen

Vice Président : Emmanuel Garnier

Trésorier : Bertrand Augé

Trésorier adjoint : Bruno Michaud

Sécrétaire : Hervé Schauer

Secrétaire adjointe : Dominique Pourcellié



Club 27001 Toulousain

Comment s'inscrire :

<http://www.club-iso27001.fr/>

Contacts : anne.mur@edelweb.fr
 dominique.pourcellie@cnamts.fr

Prochaines réunions :

Vendredi 24 avril à 14h - CNAMTS, 9 rue Michel Labrousse

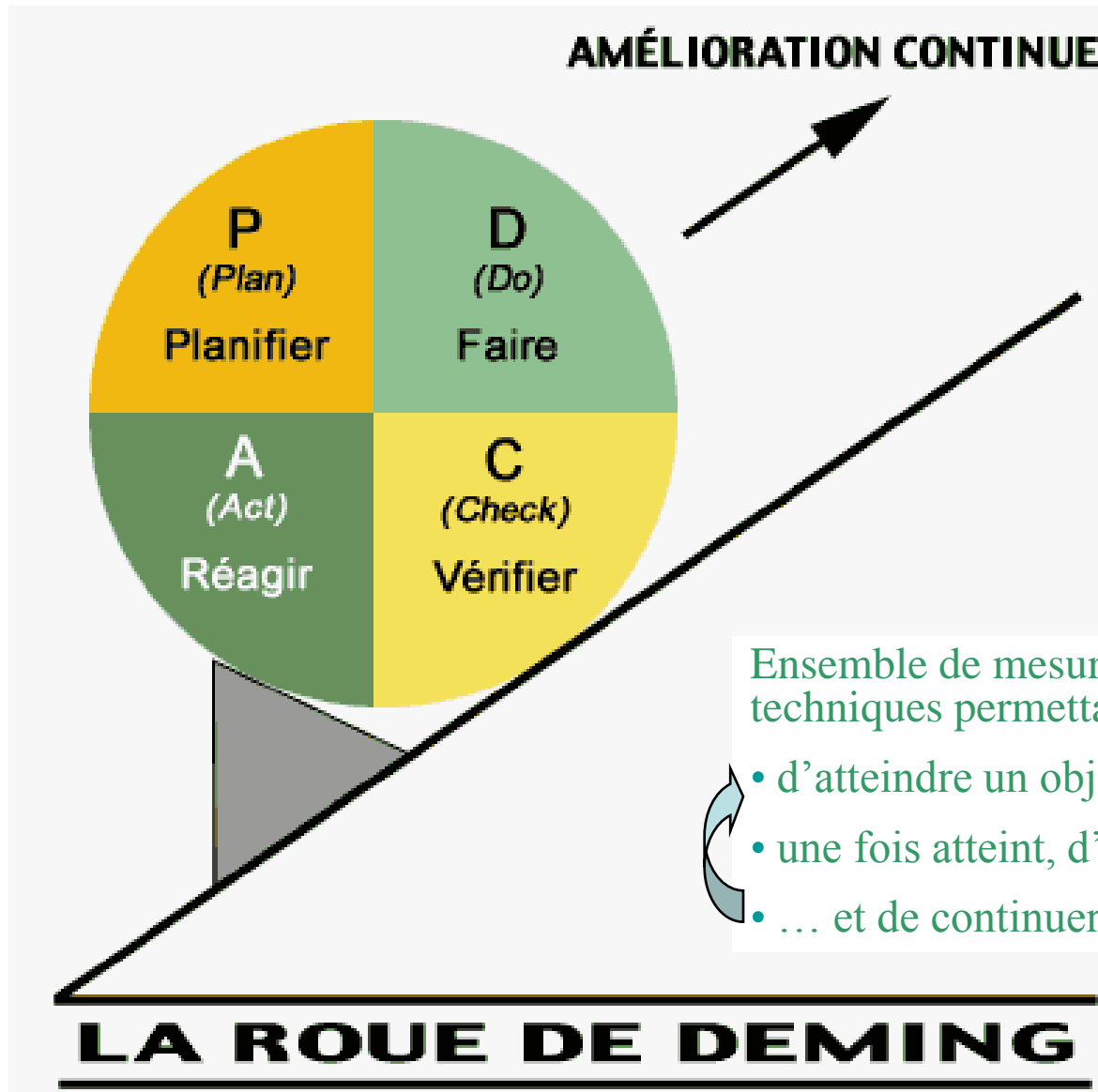
- Retour d'expérience sur les parties sécurité de ISO 20000 et liens avec ISO 9001 et ISO 27000 par Pierre de Thomasson (Hapsis)
- Apports majeurs de la V3 d'Itil (groupe de travail ITIL/27001 animé par Liliane Tonon - Nicole Genotelle)
- Groupe de discussion

Vendredi 26 juin à 14h



1. Le Club 27001
- ➔ 2. **Systemes de management**
3. Les normes de la série 27001
4. La boucle PDCA
5. Vos questions

Systeme de Management



ISO 27001

Mais aussi

ISO 9001 (Qualité)


ISO 20000 (Itil)

ISO 14000 (Env.)

.....

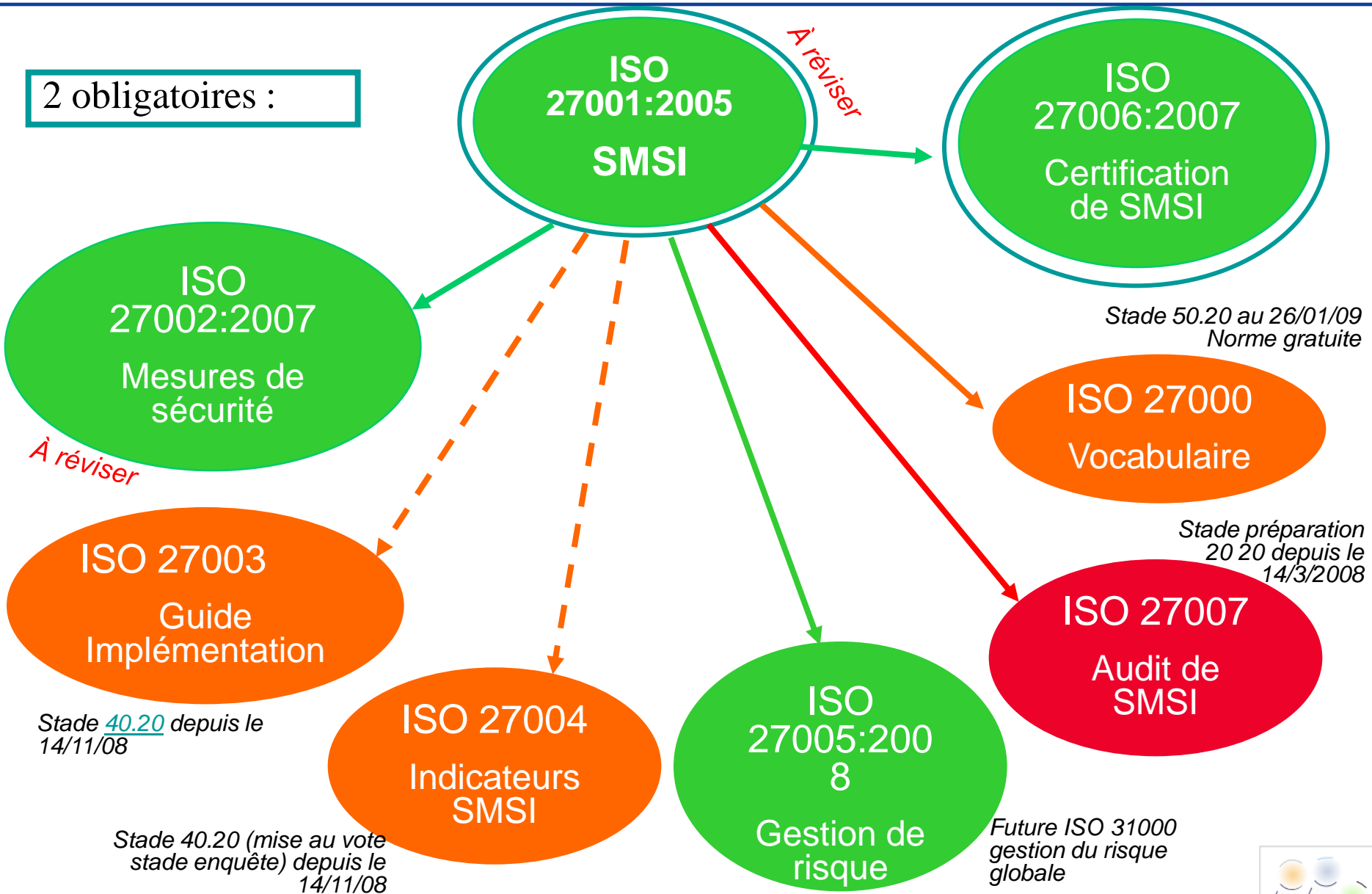
Ensemble de mesures organisationnelles et techniques permettant

- d'atteindre un objectif
- une fois atteint, d'y rester dans la durée
- ... et de continuer à s'améliorer

1. Le Club 27001
2. Systèmes de management
-  3. **Les normes de la série 27001**
4. La boucle PDCA
5. Vos questions

ISO 2700x : une famille de normes

2 obligatoires :



ISO 2700x : une famille de normes

27008	Guide pour audits (complément à ISO 27007)	Draft
27009	Gouvernance sécurité	Draft
27010	Communications intersectorielles	Draft
27011	Guide pour le secteur des télécommunications	50.60 30/05/08
27012	Administration électronique	10.99 11/08/08
27013	Financier et assurances	Draft
27031	Continuité d'activité	Draft
27032	Cybersécurité (Internet)	10.99 04/10/07
27033-x	Sécurité des réseaux x=(1,7)	10.99 à 40.20
27034	Guide pour la sécurité applicative	10.99 03/04/08
27035	Gestion des incidents de sécurité	30.20 19/01/09
27799	Déclinaison de l'ISO 27002 pour le secteur de la santé	2008

Objectif : Disposer d'un SMSI documenté → Exigences pour mettre en place, exploiter, améliorer la sécurité du SI

Pourquoi y aller ?

- Apporter la confiance
- Maîtriser les risques opérationnels des processus métier
- Avantages concurrentiels
- Rester dans un référentiel international

Comment y aller ?

- Travail transversal : tout le monde est concerné
- Passage de l'oral à l'écrit

Points clé

- Impliquer tous les acteurs
- Ne pas oublier l'aspect humain
- S'approprier la démarche
Ne pas suivre « aveuglement »
les experts
- Fixer les priorités
- Prendre en compte l'existant les
retours d'expérience (ITIL,
9001, 20000)

Résultats

- Politique
- Objectifs de sécurité
- Bonnes pratiques
- Recommandations
- Tableaux de Bord


Ne garantit pas un bon niveau de sécurité

Maturité des entreprises

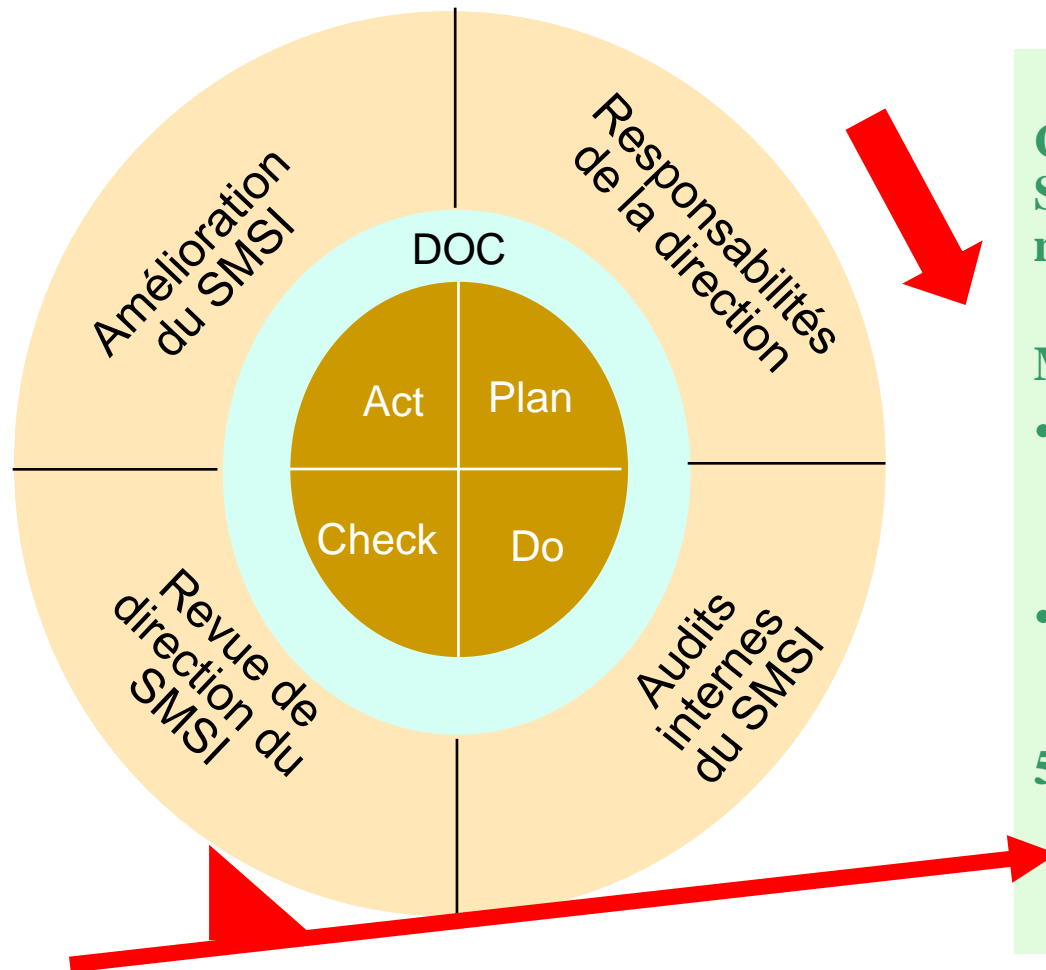
- Au niveau international : plus de **4000** entreprises sont certifiées (www.iso27001certificates.com).
- En France, seules une dizaine d'entreprises sont référencées :

Sur un panel de 50 grands comptes :
 - 33 % ont fait une analyse des écarts
 - 12 % ont défini un SMSI sans objectif de certification
 - 9 % ont un projet de certification lancé

*Source: Solucom Group
Septembre 2008*

1. Le Club 27001
2. Systèmes de management
3. Les normes de la série 27001
-  4. **La boucle PDCA**
5. Vos questions

Système de Management de la Sécurité de l'Information



Conçu pour aligner et intégrer le SMSI aux autres systèmes de management.

Marque le passage:

- De la protection du système d'information à la protection de l'information
- de l'oral à l'écrit

5 chapitres obligatoires

La phase PLAN (4.2.1)

Norme	Résultats
<p>Périmètre du SMSI</p> <p><i>(pour activités qui exigent de la confiance)</i></p>	<p>Description de(s) activité(s):</p> <ul style="list-style-type: none">• Enjeux métier, caractéristiques• Actifs primordiaux et secondaires• Architecture fonctionnelle et technique
<p>Politique de sécurité et/ou politique du SMSI</p> <p><i>(pour préciser le niveau de sécurité que l'entreprise s'engage à atteindre en disponibilité, intégrité, confidentialité)</i></p>	<p>Cadre de référence :</p> <ul style="list-style-type: none">• Périmètre du SMSI• Grandes orientations de sécurité (objectifs)• Contraintes légales, réglementaires et contractuelles,• Critères d'évaluation future du risque

La phase PLAN (4.2.1)

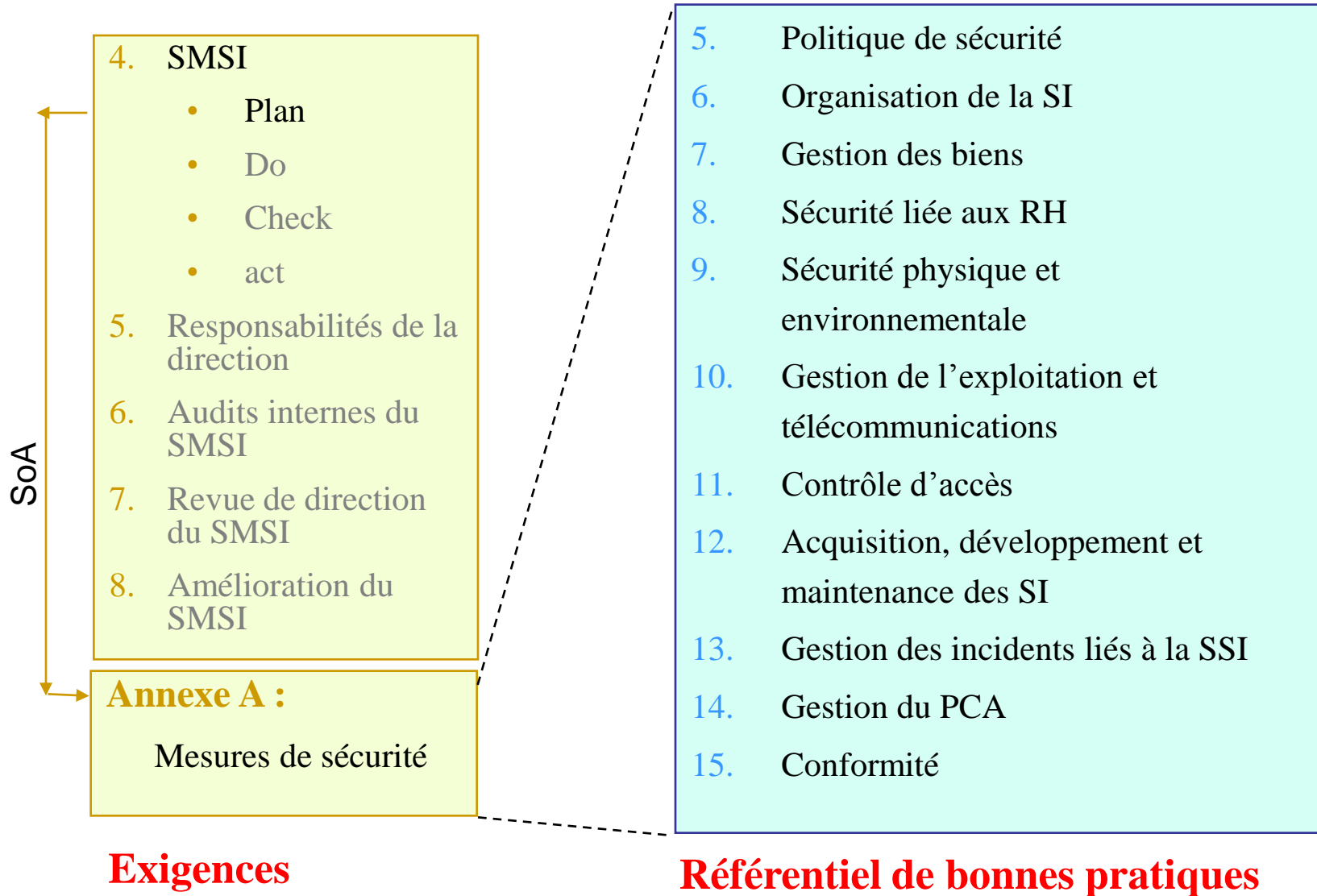
Norme	Ecueils - Points remarquables
<ul style="list-style-type: none">Périmètre du SMSI <i>(pour activités qui exigent de la confiance)</i>	<p>Définition primordiale</p> <ul style="list-style-type: none">Le périmètre doit être maîtrisableLes domaines d'application exclus devront être expliqués <p>Formaliser plan d'action et calendrier</p> <p>Doit être Validé par la direction</p>
<ul style="list-style-type: none">Politique de sécurité et/ou politique du SMSI <i>(pour préciser le niveau de sécurité que l'entreprise s'engage à atteindre en disponibilité, intégrité, confidentialité)</i>	<p>Doit être ajustée après une analyse de risque</p> <p>Doit être validée par la direction</p> <p>La politique SMSI couvre la politique de sécurité du SI</p>

La phase PLAN ^(4.2.1) : Plan de gestion des risques

Norme	Résultats
<p>Méthodologie d'appréciation des risques</p> <ul style="list-style-type: none"> • Choix de la méthode • Critères d'acceptation du risque et niv. acceptables 	<p>Choix et adaptation de la méthode</p> <ul style="list-style-type: none"> • Méthode : 27005, EBIOS, Méhari, CRAAM, méthode empirique • Métriques : impacts , risques • Référentiels : objectifs, menaces, vulnérabilités
<p>Identification et évaluation des risques</p>	<p>Rapport d'analyse des risques</p> <ul style="list-style-type: none"> • Liste des risques identifiés (niveau , priorité, acceptabilité, refus, transfert) • Objectifs de sécurité (Organisationnels et techniques) (Prévention, protection)
<p>Traitement des risques</p> <ul style="list-style-type: none"> • Réduction des risques à un niveau acceptable • Acceptation des risques résiduels (par DG) • Refus ou évitement des risques • Transfert 	<p>Choix du traitement du risque</p> <ul style="list-style-type: none"> • Objectifs de sécurité retenus • Mesures de sécurité (• Objectifs et mesures non retenus avec argumentaire • Risques résiduels acceptés • Déclaration d'applicabilité (DdA / SoA)

La phase PLAN ^(4.2.1) : Plan de gestion des risques

Norme	Ecueils - Points remarquables
<p>Méthodologie d'appréciation des risques</p> <ul style="list-style-type: none">• Choix de la méthode• Critères d'acceptation du risque et niv. acceptables <p>Identification et évaluation des risques</p> <p>Traitement des risques</p> <ul style="list-style-type: none">• Réduction des risques à un niveau acceptable• Acceptation des risques résiduels (par DG)• Refus ou évitement des risques• Transfert	<p>S'appuyer sur l'existant</p> <ul style="list-style-type: none">• Autre système de management existant• Organisation• Procédures <p>Rester toujours au plus près du métier</p> <p>Tous les objectifs de l'annexe A doivent y figurer</p> <ul style="list-style-type: none">• Intégrer les mesures existantes• Argumenter les choix et les exclusions <p>Spécifier tous les éléments permettant de prouver que le risque a été accepté</p>



Exemple du lien entre 27001 et 27002

27002

27001

- **A.7.1.3 :**
utilisation correcte des actifs
- **Mesure :**
Des règles permettant l'utilisation correcte de l'information et des actifs associés aux moyens de traitement de l'information **doivent** être identifiées, documentées et mises en œuvre

- **Mesure :**
Il convient d'identifier, de documenter, de mettre en œuvre des règles permettant l'utilisation correcte de l'information et des biens associés aux moyens de traitement de l'information.
- **Préconisations de mise en œuvre**
Il convient que tous les assurés, contractants et utilisateurs suivent les règles relatives à l'utilisation correcte de l'information et des biens associés aux moyens de traitement de l'information, à savoir :
 - Règles utilisations de la messagerie (voir 10.8)
 - Lignes directrices relatives à l'utilisation d'appareils mobiles, notamment à leur utilisation hors locaux de l'organisme (voir 11.7.1)...

La phase *DO* (4.2.2)

Norme	Résultats
Elaborer un plan de traitement du risque	Plan de traitement du risque présentant : <ul style="list-style-type: none">• actions à engager,• ressources,• responsabilités,• priorités
Mettre en œuvre le plan de traitement pour atteindre les objectifs fixés	Plan d'action formalisé Calendrier précis
Mettre en œuvre les mesures de sécurité sélectionnées	Spécifications (exigences) fonctionnelles et techniques déclinées des objectifs de sécurité. Choix de solutions et d'outils. Formalisation des procédures. Matrice de couverture des objectifs de sécurité.
Définir le mode d'évaluation des mesures sélectionnées	Modes internes, externes Autoévaluations... Indicateurs stratégiques, tactiques et opérationnels

La phase *DO* (4.2.2)

Norme	Résultats
Mettre en œuvre un programme de formation et sensibilisation	Tous les collaborateurs doivent être sensibilisés <ul style="list-style-type: none">• Aux enjeux et aux risques• aux problématiques de sécurité• à leurs responsabilités• aux bons réflexes
Gérer les opérations et les ressources du SMSI	Procédures de gestion et de suivi intégrant les rôles et responsabilités Tableaux de bord
Gérer les incidents	Procédure de gestion et de traitement des incidents de sécurité

La phase *DO* (4.2.2)

Norme [Rappel]	Ecueils - Points remarquables
<ul style="list-style-type: none">• Elaborer un plan de traitement du risque• Mettre en œuvre le plan de traitement et les mesures de sécurité sélectionnées• Définir le mode d'évaluation des mesures sélectionnées• Mettre en œuvre un programme de formation et sensibilisation• Gérer les opérations du SMSI• Gérer les ressources du SMSI• Mettre en œuvre les procédures et mesures de gestion des incidents	<p>Bien définir les niveaux de responsabilités → Toute action doit avoir un responsable</p> <p>Le plan de traitement du risque doit être validé par la hiérarchie (avec coûts, délais et responsabilités)</p> <p>Respecter les délais</p> <p>Disposer d'éléments de preuve</p> <p>Sensibiliser tous les acteurs</p>

La phase *CHECK* (4.2.3)

Norme	Résultat
Surveiller en permanence l'efficacité du SMSI	Procédure de surveillance Rapport concernant la réalisation du plan d'action
Réaliser des réexamens réguliers de l'efficacité du SMSI	Plan d'action et procédure de réexamen Calendrier
Évaluer l'efficacité des mesures	Cahiers de tests et de recette Matrice de couverture des exigences
Réexaminer les appréciations du risque à intervalles planifiés <ul style="list-style-type: none">• Audits internes• Revue de direction	Rapports d'audit (Cf 6) Document de revue <ul style="list-style-type: none">• Plan de traitement du risque actualisé• Plan d'action actualisé

La phase *CHECK* (4.2.3)

Norme	Résultat
<p>Mener des audits internes à intervalles fixés sur la base de</p> <ul style="list-style-type: none">• Documents• Analyse de traces ou enregistrements• Tests techniques	<p>Rapport d'audit présentant :</p> <ul style="list-style-type: none">• Écarts / exigences• Ecarts de mise en œuvre du plan d'action• Ecarts /exécution des procédures
<p>Effectuer une revue de direction du SMSI de manière régulière (Cf 5)</p> <ul style="list-style-type: none">• Implication de la direction (preuves)• Management des ressources	<p>Eléments de preuve:</p> <ul style="list-style-type: none">• Politique de SMSI• Mise à disposition des ressources nécessaires• Validation des documents• Validation des risques• Réalisation des revues de SMSI
<p>Mettre à jour les plans de sécurité</p>	<p>Plan de sécurité</p>
<p>Consigner les actions et les évènements qui pourraient avoir un impact sur efficacité et performance du SMSI</p>	

La phase *ACT* (4.2.4)

Norme	Résultat
<p>Mise à jour et amélioration du SMSI</p> <ul style="list-style-type: none">• Mettre en œuvre les améliorations identifiées• Entreprendre les actions correctives et préventives . Leçons tirées des expériences...• Informer toutes les parties prenantes des actions et améliorations• S'assurer des améliorations permettent d'atteindre les objectifs prévus	<ul style="list-style-type: none">• Plan d'action• Tableau de suivi des actions• Moyens d'information

Alimente la phase PLAN

La documentation (4.3)

Norme	Résultats
<p>Documentation doit permettre de démontrer que les objectifs du SMSI sont pris en compte.</p> <p>Les documents doivent être protégés et maîtrisés</p> <p>Les enregistrements doivent être protégés et maîtrisés pour apporter la preuve de la conformité aux exigences</p> <ul style="list-style-type: none">• Légales, réglementaires et contractuelles• Lisibilité et accessibilité des enregistrements• Durée de conservation	<p>Ensemble des documents présentés précédemment</p> <p>Procédures de gestion de la documentation</p> <ul style="list-style-type: none">• Approbation et mise à jour• Identification• Gestion des versions• Disponibilité, diffusion et protection• Retrait et archivage des documents <p>Procédures de gestion des enregistrements et des traces</p>

Passage d'une culture de tradition orale à une culture de tradition écrite

