Ecole Nationale Polytechnique Douala

EXPOSE DE NORMES ET BONNES PRATIQUES DE L'INFORMATIQUE

HIGH INSTITUTE OF MANAGEMENT AND ENTREPRENEURSHIP
ime
INSTITUT SUPERIEUR DE MANAGEMENT ET DE L' ENTREPRENEURIAT

INTRODUCTION A ISO 27001

FILIERE : GL et SWE **Niveau : BAC + 3 (En cours)**

EXPOSANT :

NGUEDONG Queline Jodelle
TAYOU SIKAPIN Alan Cédric
KENGNE Rodrigue Martial
Esther ENO EFFIONG
MONTHE Roland
GUIADEM NEUMEGE flavienne

Supervisé par :
Dr. OUAFO Blaise

ANNEE ACADEMIQUE :
2021 / 2022

PLAN DE TRAVAIL

INTRODUCTION
HISTORIQUE ISO 27001
APPLICATION
LES EXIGENCES
MACHINISME DE CERTIFICATION ISO 27001
RELATION ENTRE ISO 27001 ET LES BONNES PRATIQUES

INTRODUCTION

La norme internationale ISO 27001 décrit les exigences nécessaires à la mise en place d'un système de management de la sécurité des systèmes d'information (SMSSI).

Cette norme est destinée à définir les mesures de sécurité afin d'assurer la protection des biens sensibles du système d'information d'un organisme. Les exigences en matière de sécurité sont propres à chaque organisme en fonction du périmètre défini et de son activité.

I. HISTORIQUE ISO 27001

La norme ISO/CEI 27001 porte sur le management de la sécurité et de l'information. Elle tire ses origines de la norme britannique BS 7799-2:2002 dont la première version a été publiée en 1999. En 2005, l'ISO adopte et améliore cette norme pour donner naissance à la norme ISO/CEI 27001. Cette norme vise à la mise en place d'un système de management de la sécurité de l'information efficace. En 2013, celle-ci sera révisée, se rapprochant d'une structure similaire aux autres normes de systèmes de management (ISO 9001, ISO 14001…). La norme est actuellement en cours de révision depuis le 19/05/2017.

Octobre 2005 : Première Publication de ISO 27001

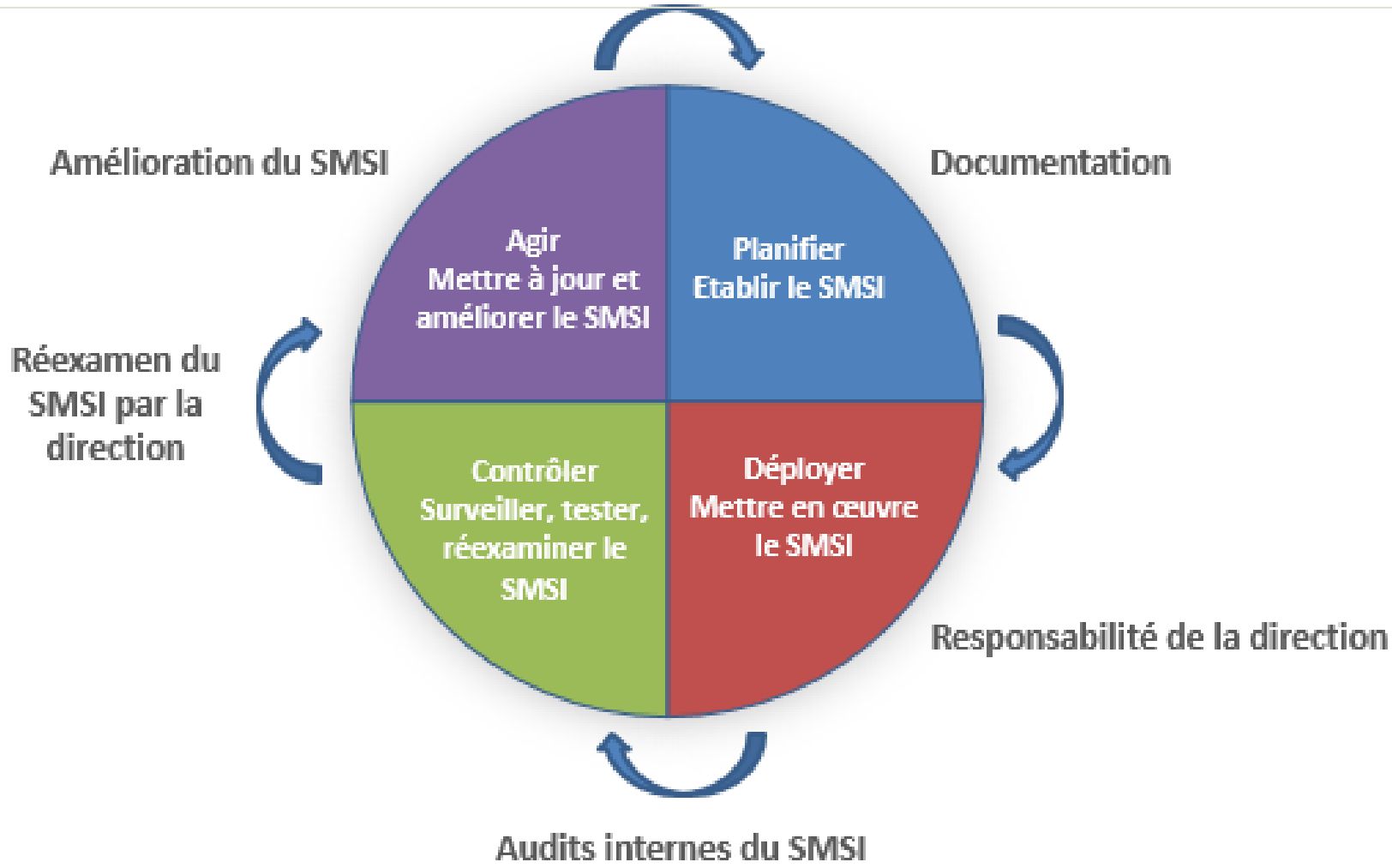


Figure de représentation de ISO 27001 versions 2005

Octobre 2013 : Révision et adoption de la norme afin de mieux répondre aux défis changeants de la sécurité de l'information

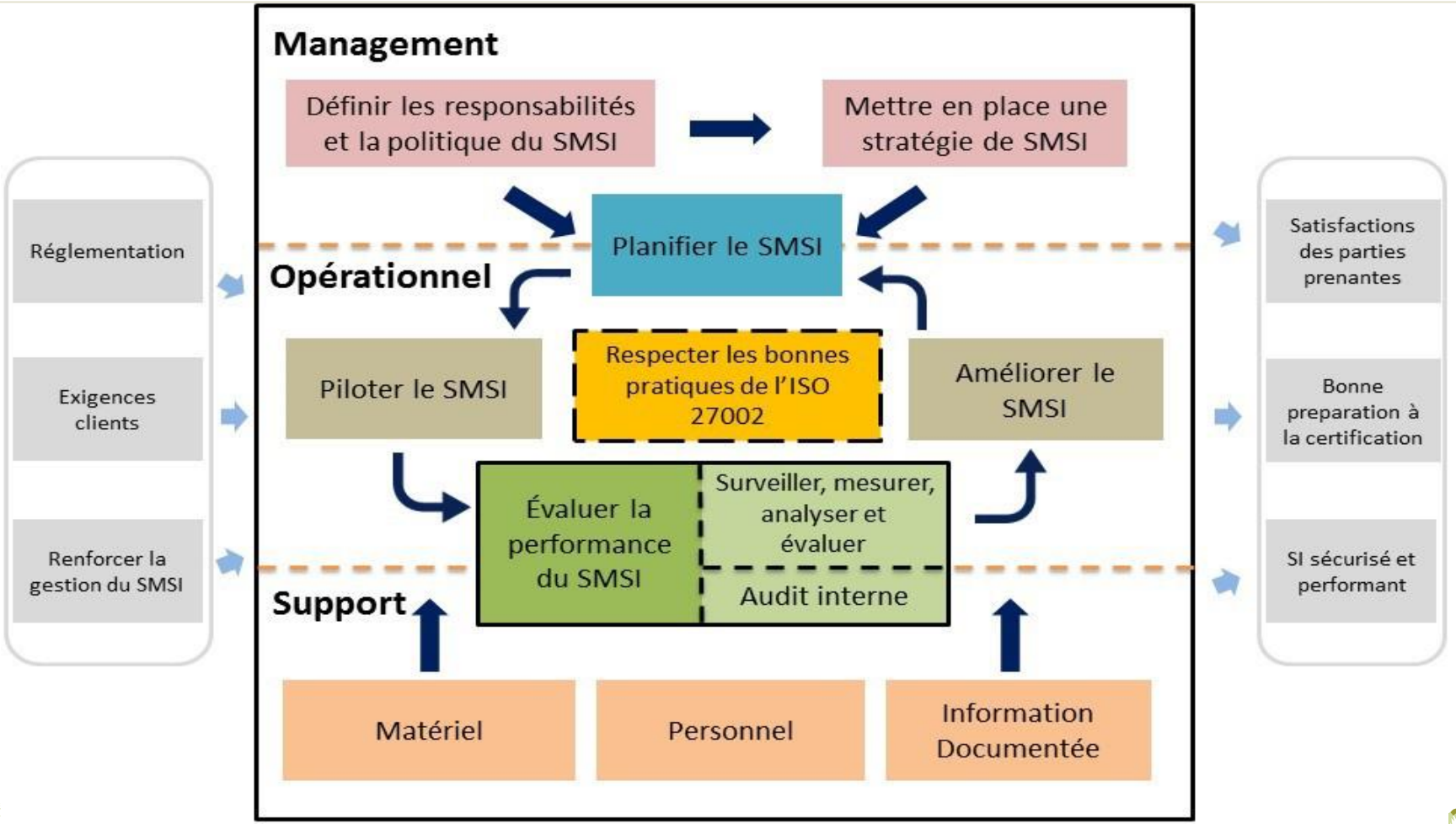


Figure de représentation de ISO 27001 versions 2013

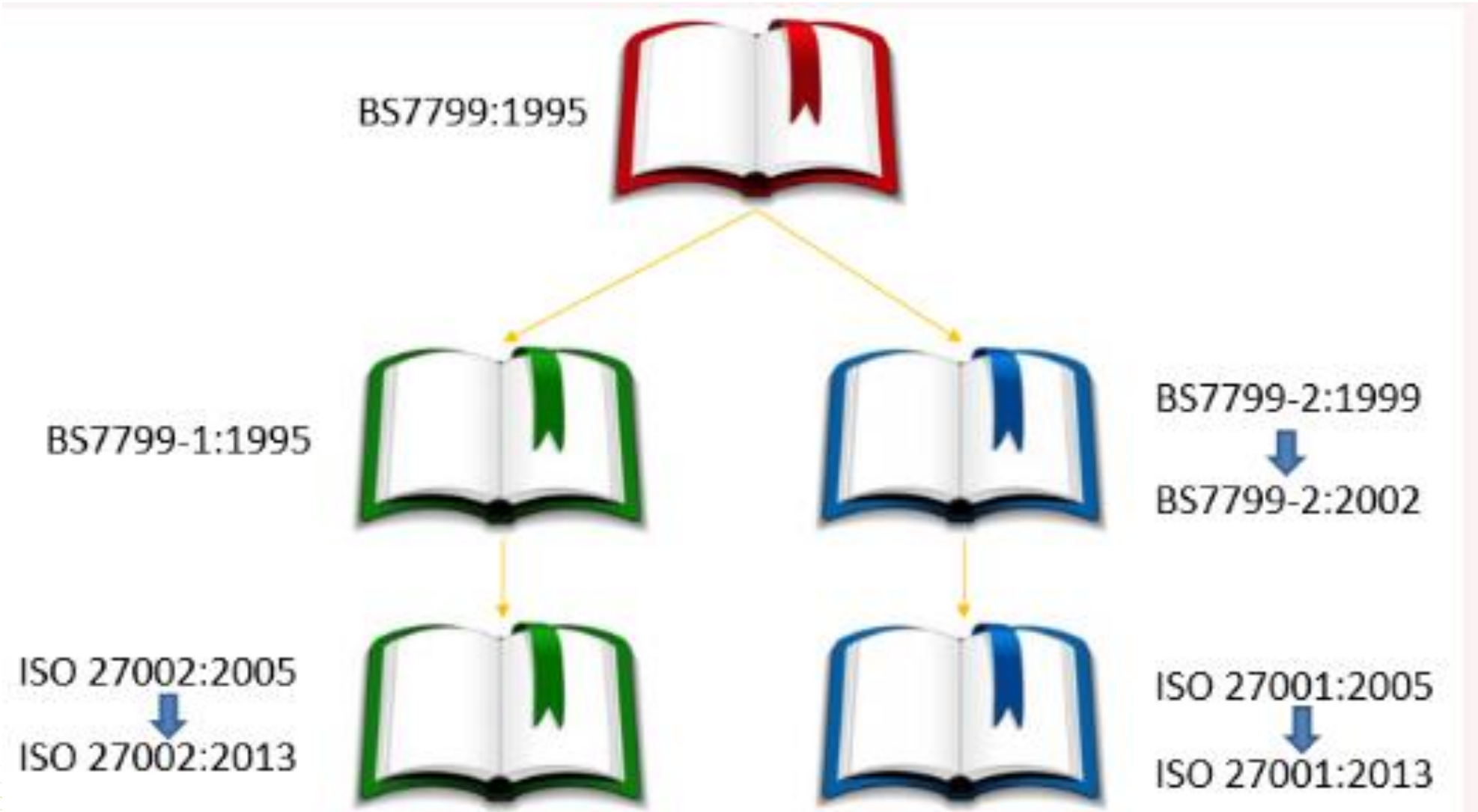


Figure 2 Historique de la norme ISO/CEI 27001

II. APPLICATIONS DE LA NORME ISO 27001

ISO 27001 aides les entreprises à définir les règles en matière de gestion des risques liés aux informations.

ISO 27001 s'applique à tous les types et à toutes les tailles d'organisations, y compris les entreprises publiques et privées, les entités gouvernementales et les organisations à but non lucratif.

Le domaine d'application de notre système de management de la sécurité de l'information s'applique à tous les produits et services proposés par notre organisation incluant la conception, la production et les activités après livraison. Les enjeux externes et internes pertinents pour le SMSI et les actions face aux risques identifiés et opportunités d'améliorations trouvées sont pris en compte.

III. LES EXIGENCES DE LA NORME ISO 27001

La norme ISO 27001 est une norme internationale sur le management de la sécurité de l'information. Elle définie un système de management de la sécurité de l'information (SMSI) à mettre en place dans l'entreprise.

Cette norme présente les exigences en matière d'organisation (système de management). Elle s'assure que la sécurité de l'information est bien maîtrisée :

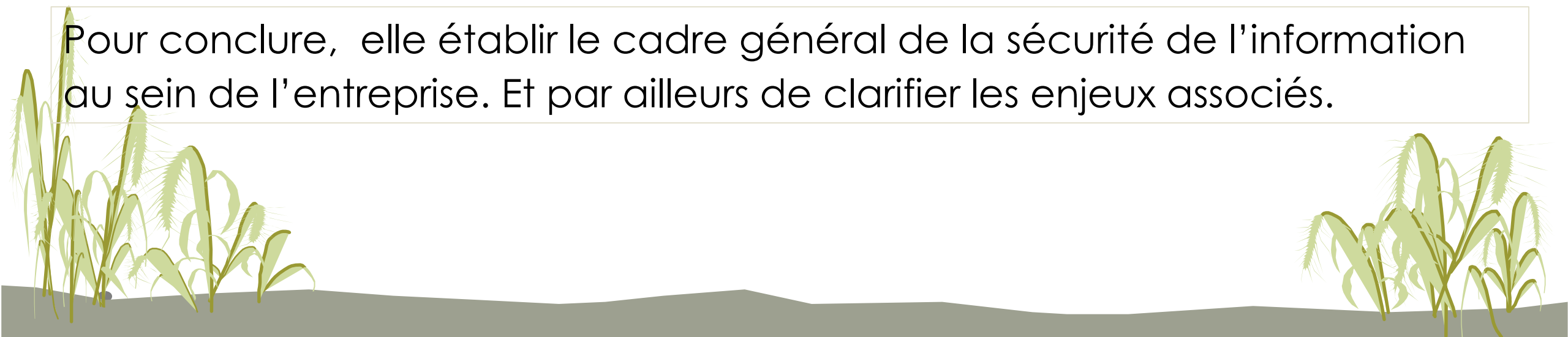
* La gouvernance liée à la sécurité de l'information et la stratégie.
* Les processus nécessaires à la maîtrise de la sécurité de l'information.
* Différentes méthodes pour ainsi analyser les risques et en rendre compte.
* Les processus de mesure, de suivi et d'amélioration de la sécurité.
* Les responsabilités liées à la sécurité de l'information.

1. Exigences contexte de l'organisation

L'entreprise doit :

- Déterminer les enjeux externes et internes pertinents qui ont un impact sur la sécurité de l'information.
- Déterminer les parties intéressées et leurs exigences en matière de sécurité
- Déterminer précisément le domaine d'application du SMSI

Pour conclure, elle établir le cadre général de la sécurité de l'information au sein de l'entreprise. Et par ailleurs de clarifier les enjeux associés.



2. Exigences Leadership

En pratique la direction doit s'assurer :

* qu'une politique et des objectifs sont établis en matière de sécurité de l'information.
* ainsi que les exigences liées au SMSI sont mis en place dans les processus métiers.

La direction doit également :

* Communiquer sur l'importance de disposer d'un SMSI efficace et d'être conforme aux exigences.
* Orienter et soutenir les personnes pour qu'elles contribuent à l'efficacité du SMSI.

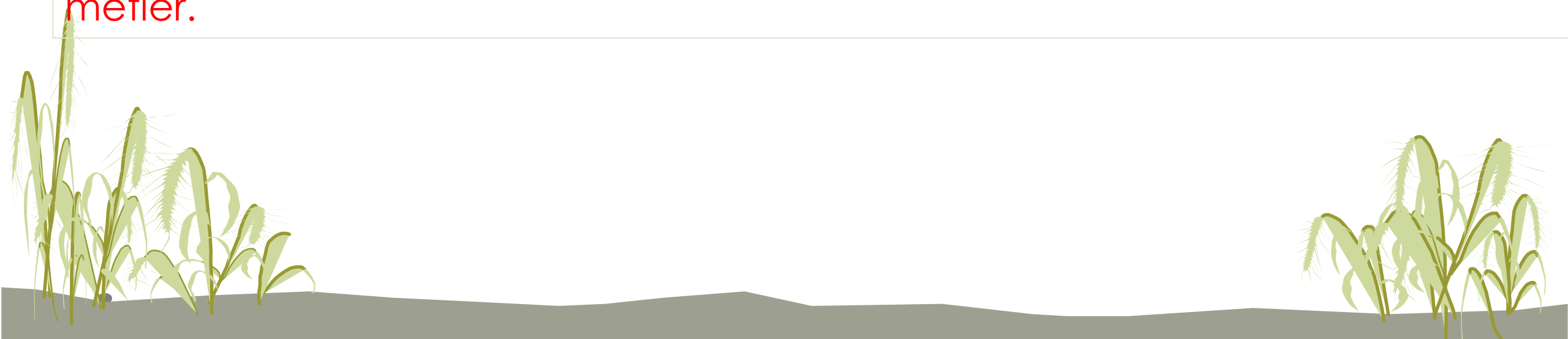
- La direction doit définir une politique en matière de sécurité de l'information

Ces responsabilités couvrent différents périmètre de la sécurité :

le management du SMSI : Responsable du SMSI.

La sécurité opérationnelle : Responsable de la sécurité du Système d'Information (RSSI).

Les managers métier qui auront des responsabilités en sécurité liées à leur métier.



3. Exigences Planification

Cette partie porte sur l'analyse des risques, l'évaluation des risques ainsi que l'établissement du plan de traitement des risques.

* Garantir l'atteinte des objectifs.
* Réduire les risques.
* Améliorer en continue la sécurité.

une fois les risques déterminés l'entreprise planifie les actions associées et s'assurer qu'elles sont efficaces.

Appréciation des risques de sécurité de l'information

Traitement des risques

Objectifs de sécurité de l'information et plans pour les atteindre

Les sous-étapes suivantes sont très importantes dans l'appréciation des risques:

1. • Identifier les actifs
2. • *Identifier les personnes responsables*
3. • *Identifier les vulnérabilités*
4. • *Identifier les menaces*
5. • *Identifier les impacts*
6. • *Evaluer la vraisemblance*
7. • *Estimer les niveaux de risque*

4. Exigences Support

Elle porte sur la définition des activités supports en soutien au SMSI. Il porte sur l'attribution des ressources nécessaires, les ressources humaines, la formation, la communication et la gestion documentaire.

5. Exigences Fonctionnement

Elle porte sur la vie de votre SMSI et le maintien des dispositifs décrits plus haut.

6. Exigences Evaluation des performances

Elle porte sur l'évaluation des résultats en matière de sécurité de l'information par le recueil d'indicateurs et la réalisation d'audits.

7. Exigences Amélioration

L'entreprise doit aussi améliorer en continue son SMSI.

Cette exigence globale porte sur l'ensemble du SMSI :

Utiliser l'analyse des risques comme moyen d'apprentissage de votre système et comme voie d'amélioration

Les mesures de sécurité sont revue pour renforcer en continue la sécurité

STRUCTURE OF ISO 27001 2013 INFORMATION SECURITY MANAGEMENT STANDARD

- **4. CONTEXT**
  - 4.1 Understand your organization's context
  - 4.2 Define the expectations of interested parties
  - 4.3 Clarify scope of infosec management system
  - 4.4 Develop an infosec management system
- **5. LEADERSHIP**
  - 5.1 Provide leadership and show that you support ISMS
  - 5.2 Establish an appropriate information security policy
  - 5.3 Assign ISMS roles, responsibilities, and authorities
- **6. PLANNING**
  - 6.1 Formulate actions to address risks and opportunities
    - 6.1.1 Consider risks and opportunities when you plan your ISMS
    - 6.1.2 Establish an information security risk assessment process
    - 6.1.3 Develop an information security risk treatment process
  - 6.2 Set ISMS objectives and make plans to achieve them
- **7. SUPPORT**
  - 7.1 Support ISMS by providing resources
  - 7.2 Support ISMS by promoting competence
  - 7.3 Support ISMS by making people aware of duties
  - 7.4 Support ISMS by controlling ISMS communications
  - 7.5 Support ISMS by managing related information
    - 7.5.1 Include information and documents that the ISMS needs
    - 7.5.2 Manage the creation and modification of ISMS documents
    - 7.5.3 Control your organization's ISMS documents and records
- **8. OPERATIONS**
  - 8.1 Carry out planning and control your ISMS processes
  - 8.2 Conduct suitable information security risk assessments
  - 8.3 Implement information security risk treatment plans
- **9. EVALUATION**
  - 9.1 Monitor, measure, and analyze information security
  - 9.2 Set up audit program and use it to evaluate your ISMS
  - 9.3 Review your organization's ISMS at planned intervals
- **10. IMPROVEMENT**
  - 10.1 Identify nonconformities and take corrective action
  - 10.2 Improve information security management system

ISMS stands for Information Security Management System.

www.praxiom.com/iso-27001-outline.htm

IV. MECHANISME DE CERTIFICATION ISO 27001

ISO/IEC **27001 est** la **norme** la plus connue de cette famille qui n'en compte pas moins d'une douzaine. Elle spécifie les exigences relatives aux systèmes de management de la sécurité des informations (SMSI).

Ainsi, grâce à la **certification** ISO **27001**, une entreprise obtient un système fonctionnel, cadré, sécurisé et évolutif. Au-delà de fournir un cadre d'exploitation, le respect de cette norme permet de réduire ses coûts de sécurité, puisqu'elle permet la mise en place d'actions parfaitement adaptées aux besoins.

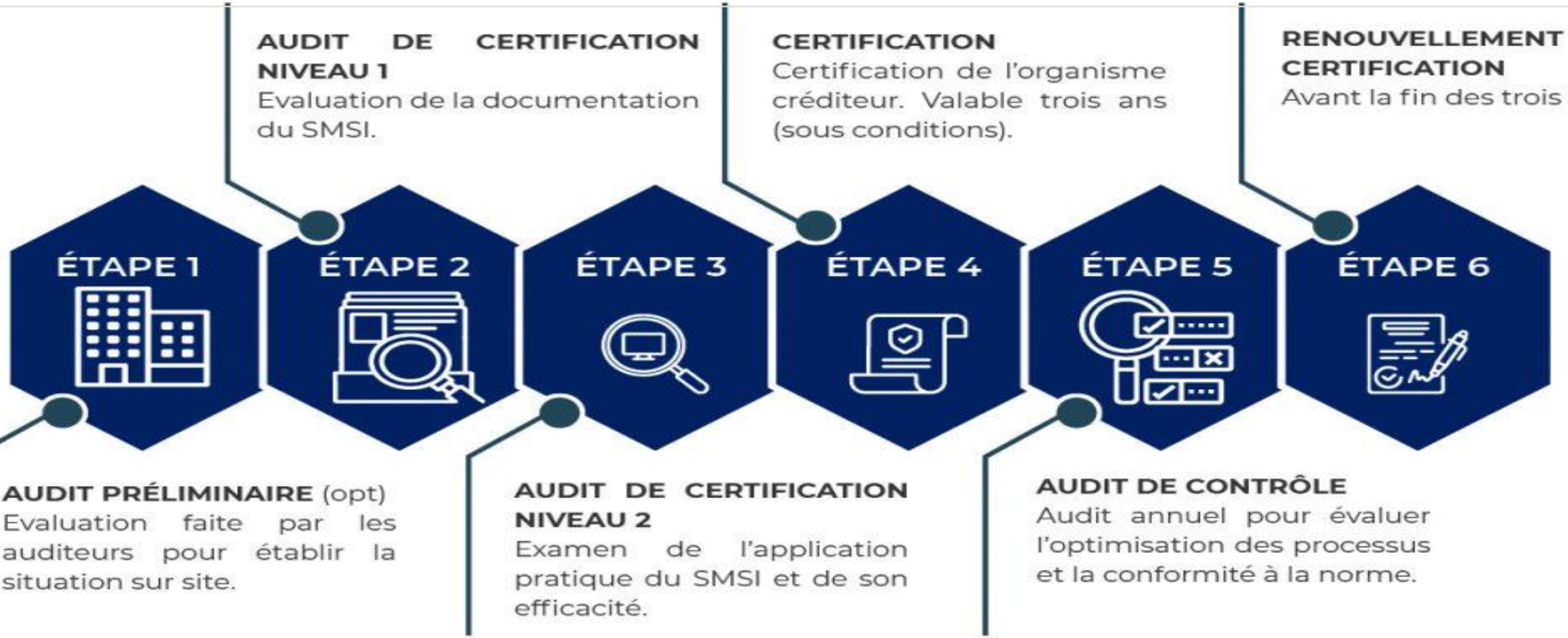
Les Normes **ISO** aident les entreprises de toutes tailles et de tous secteurs à réduire leurs coûts, accroître leur productivité et accéder à de nouveaux marchés.

L'International Organization for Standardization définit la **certification ISO** comme une « Procédure par laquelle une tierce partie donne une assurance écrite qu'un produit, un processus ou un service **est** conforme aux exigences spécifiées dans un référentiel. »

Le **SMSI** désigne un ensemble de politiques et de processus visant à gérer la sécurité et à atténuer les risques, particulièrement pour la sécurité de l'information.

Rôle de l'ISO 9001

ISO 9001 définit les critères applicables à un système de management de la qualité. Il s'agit de la seule norme de la famille **ISO** 9000 à pouvoir être utilisée pour la **certification** (mais ce n'**est** pas une obligation). Toute organisation, grande ou petite, **quel** que soit son domaine d'activité, peut l'utiliser.



LES 9 ETAPES DE MISE EN PLACE DE LA NORME ISO 27001

1. Contenu de la mission : Le projet de mise en place doit commencer par la désignation d'un leader de projet, qui travaillera avec d'autres membres du personnel.

2. Initiation du projet : Les organisations doivent utiliser leur contenu de mission afin de construire une structure plus définie et plus détaillée concernant les objectifs liés à la sécurité de l'information et l'équipe gérant le projet, la planification et les risques.

3. Initiation du ISMS : La prochaine étape est d'adopter une méthodologie de mise en place d'un ISMS. La norme ISO 27001 reconnait que la démarche d'amélioration continue suivant une approche par processus est le modèle le plus efficace pour la gestion de la sécurité de l'information.

4. Cadre de gestion : Cela comprend l'identification de la portée du système, qui dépendra du contexte. La portée doit également prendre en compte les appareils mobiles et les télétravailleurs.

5. Critères de sécurité : Il s'agit des exigences et mesures correspondantes ou des contrôles nécessaires pour gérer l'entreprise.

6. Gestion des risques : La norme ISO 27001 permet aux organisations de définir de manière plus large leurs propres processus de gestion des risques.

7. Plan de traitement des risques : Il s'agit du processus de construction des contrôles de sécurité ayant pour but de protéger les informations de votre organisation.

8. Mesurer, contrôler et réviser : ça implique l'identification de métriques ou d'autres méthodes permettant de juger l'efficacité et la mise en place des contrôles.

9. Certification : Le processus de certification implique la révision des documentations des systèmes de gestion de l'organisation afin de vérifier que les contrôles appropriés ont été mis en place.

V. CERTIFICATION ISO 27001

La **certification ISO 27001** permet une gestion optimale des risques liés à la sécurité de l'information.

Les entreprises surveillent, révisent, entretiennent et améliorent la gestion de la sécurité des informations en mettant en place un Système de Management de Sécurité de l'Information (SMSI).

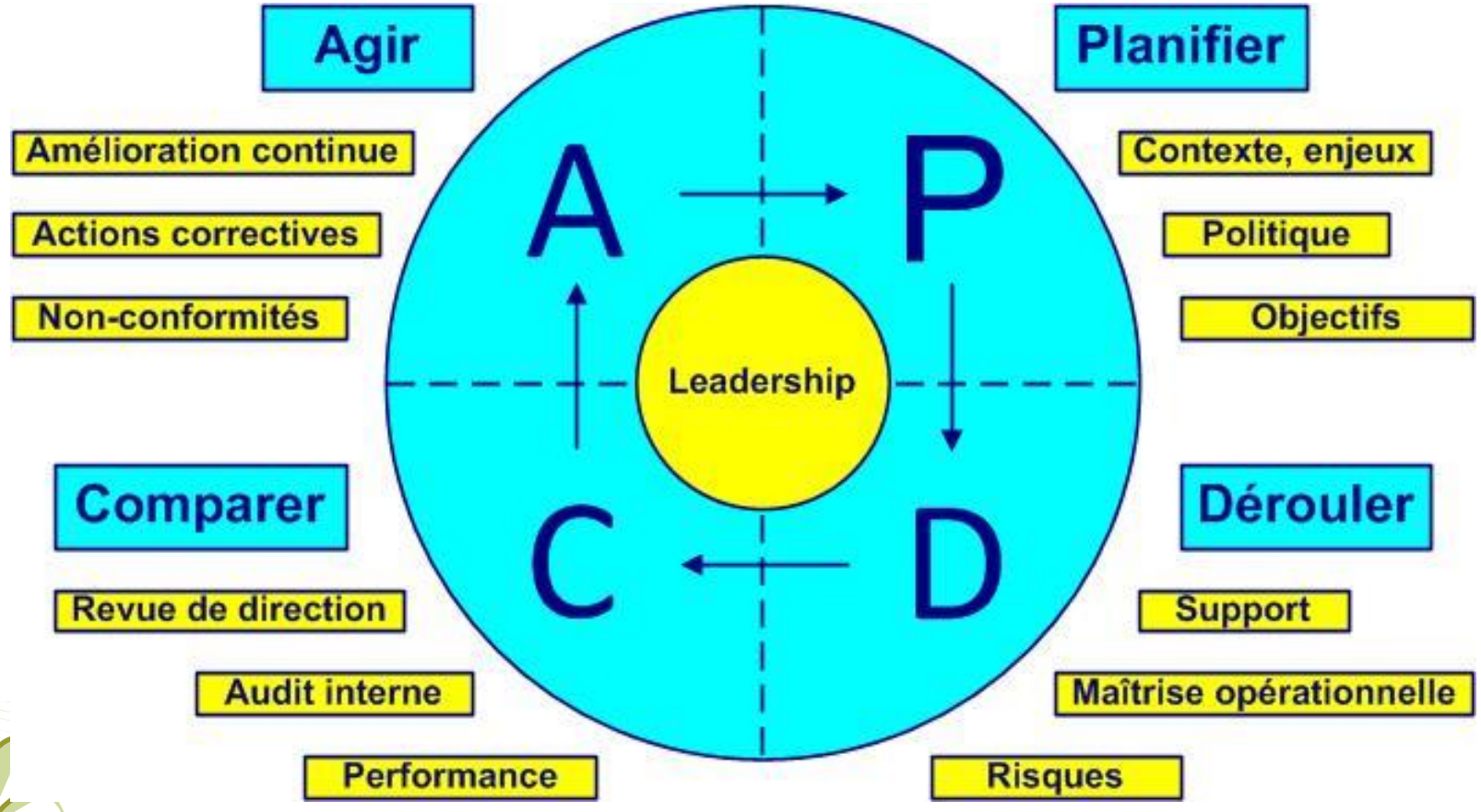
a) Rendre la norme ISO 27001 opérationnelle : construire efficacement son SMSI

La **mise en place** d'un **SMSI** doit s'appuyer sur une stratégie solidement établie définie lors d'une étude d'opportunité préalable.

La démarche, connue sous l'abréviation **PDCA**, ou **principe de la roue de Deming**, vise une amélioration continue du système par le déploiement de 4 phases :

- **Planifier** (*Plan*) : **collecte des informations** Il s'agit de définir un ensemble de politiques et de processus tout en établissant des méthodes assurant l'optimisation continue du SMSI.
- **Faire** (*Do*) : **permet d'appliquer les politiques** déterminées en suivant la norme ISO 27001 et les ressources d'une entreprise cible.

- **Vérifier** (*Check*) : permet de **mener une veille de l'efficacité** des processus et évaluez les résultats.
- **Agir** (*Act*) : permet **d'améliorer les processus existants**, en éliminant ou en construisant de nouveaux grâce aux actions correctives.



Les avantages de la certification iso 27001

- **Gagner en crédibilité** sur votre marché. Les clients ont confiance en vous et vous restent fidèles.
- **Réduire vos coûts** en matière de sécurité. Cette certification vous permet d'identifier le bon SMSI à mettre en place et de supprimer toute autre mesure de sécurité inutile
- **Faciliter les échanges à l'international** avec une certification reconnue par-delà les frontières.
- **Gagner en sécurité.** Vous améliorez continuellement vos pratiques pour sécuriser les données.
- **Être conforme à la réglementation** en matière de gestion des risques et de la sécurité.

VI. LES NORMES DE LA FAMILLE ISO/CEI 27001

a. L'ISO/CEI 27000

L'ISO/CEI 27000 est structurée en trois parties.

La première, définit 46 termes tels que, la confidentialité, l'intégrité, la disponibilité, l'authenticité, tous principalement axés sur l'appréciation et l'analyse des risques, des menaces, de la vulnérabilité.

La deuxième partie développe la notion de processus avec le modèle PDCA et présente les concepts propres aux SMSI comme par exemple, l'importance de l'engagement de la direction.

La troisième partie, est une présentation de l'ensemble des normes de la famille ISO/CEI 2700x.

b. L'ISO/CEI 27002

l'ISO/CEI 27002 est un guide de bonnes pratiques, une série de préconisations concrètes, abordant les aspects tant organisationnels que techniques, qui permettent de mener à bien les différentes actions dans la mise en place d'un SMSI

c. L'ISO/CEI 27003

Elle est utilisée en complément de la norme ISO 27001. L'ISO 27003 propose cinq étapes(qui concernent l'initialisation du projet) pour implémenter le SMSI.

- Un résumé de l'activité (explication de l'étape en question),
- Les entrées (tous les documents à utiliser au cours de l'étape),
- Les recommandations (détail des points à aborder),
- Les sorties (liste des livrables à produire).

d. L'ISO/CEI 27004

En utilisant les mesures des indicateurs l'objectif est d'identifier les points du SMSI qui nécessitent une amélioration ou une correction.

e. L'ISO/CEI 27005

L'objectif n'est pas de remplacer ou rendre obsolètes les méthodes existantes mais d'harmoniser le vocabulaire employé

	ITIL	CobiT	ISO/CEI 27001
Domaine d'application	Production informatique	Contrôle et audit des SI	Sécurité des systèmes d'information
Propriétaire du référentiel	OGC	ISACA	ISO/CEI
Diffusion du référentiel	OGC	En France, AFAJ	En France, AFNOR
Secteur économique de l'entreprise	Tous secteurs	Tous secteurs	Tous secteurs
Objet de la reconnaissance	Personne physique pour son expérience et ses connaissances en fourniture et en support de services	Personne physique pour ses compétences en audit informatique en sécurité des SI ou en gouvernance des SI	Personne morale pour le système de management de la sécurité
Type de reconnaissance	Certification	Certification	Certification
Portée	Internationale	Internationale	Internationale
Durée de validité	Non spécifiée	3 ans avec confirmation annuelle	3 ans avec audits de suivi
Type d'évaluation	Examen en français pour le niveau fondamental, sinon	Examen CISA : en français CISM : en français	Audit tierce partie

CONCLUSION GENERALE

Face aux nombreuses malveillances que peut connaître une organisation, l'une des plus critiques concerne certainement l'atteinte à la sécurité de l'information. Cette atteinte peut remettre en cause la pérennité de l'organisme en s'en prenant à sa « mémoire interne », à sa source première de valeur ajoutée.

L'application d'une telle norme dans l'organisme permettra de protéger l'information de l'entreprise par la formalisation de processus, la mise en œuvre d'actions de sécurisation et de gestion du risque IT (et des risques découlant de ce type de risque opérationnel) mais aussi de formation et de sensibilisation, de traçabilité du risque par une documentation et une formalisation/remontée des éléments de preuve.


MERCI !