HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

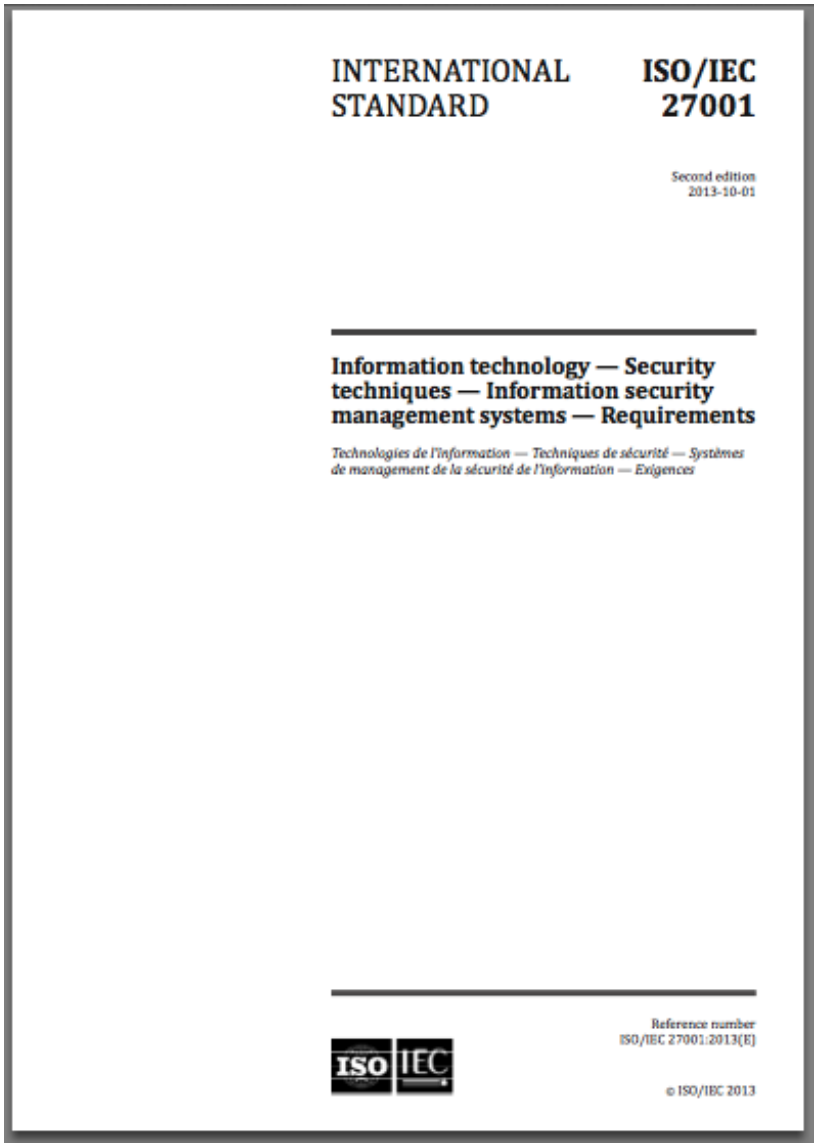
ISO 27001:2013

Béatrice Joucreau
Julien Levrard

Sommaire

- La norme ISO 27001:2013
- Qu'est-ce qu'un SMSI ?
- Pourquoi mettre en place un SMSI ?
- Un SMSI selon la norme ISO 27001:2013
- Pourquoi un SMSI certifié ISO 27001:2013 ?
- Ingrédients du périmètre du SMSI
- Définition du périmètre du SMSI
- Gestion des risques de sécurité
- Lien avec l'ISO 27002:2013

La norme ISO 27001:2013


INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

- ISO CEI 27001: 2013
- Parue le 01/10/2013
- ISO 27001 décrit la mise en œuvre et l'exploitation d'un SMSI
- SMSI : **Système de Management de la Sécurité de l'Information**
  - SM : Système de management
  - SI : Sécurité de l'information

Qu'est-ce qu'un SMSI ?

- Système de management
  - Ensemble de procédures qu'une organisation doit suivre pour réaliser ses objectifs
  - Systématisation, par une organisation, de sa manière d'opérer
- Sécurité de l'information
  - Confidentialité
  - Intégrité
  - Disponibilité
- Gérer la sécurité / gérer les risques de sécurité
  - Mesures de sécurité pour
    - Réduire les vulnérabilités des actifs
    - Réduire les impacts des scénarios d'incidents
    - Éventuellement, dissuader ou anticiper les menaces

Qu'est-ce qu'un SMSI ?

- Applicable à tout organisme
  - Petit ou grand, quel que soit le produit ou le service fourni, dans tout secteur d'activité
- Applicable à tout l'organisme
  - Tout le monde est concerné au sein du périmètre
- Se fonde sur des référentiels précis
  - Importance du document écrit
- Auditable
  - Quelqu'un peut venir vérifier qu'il n'y a pas d'écart entre l'exigence et la pratique
  - Système documenté : passage de la tradition orale à la tradition écrite

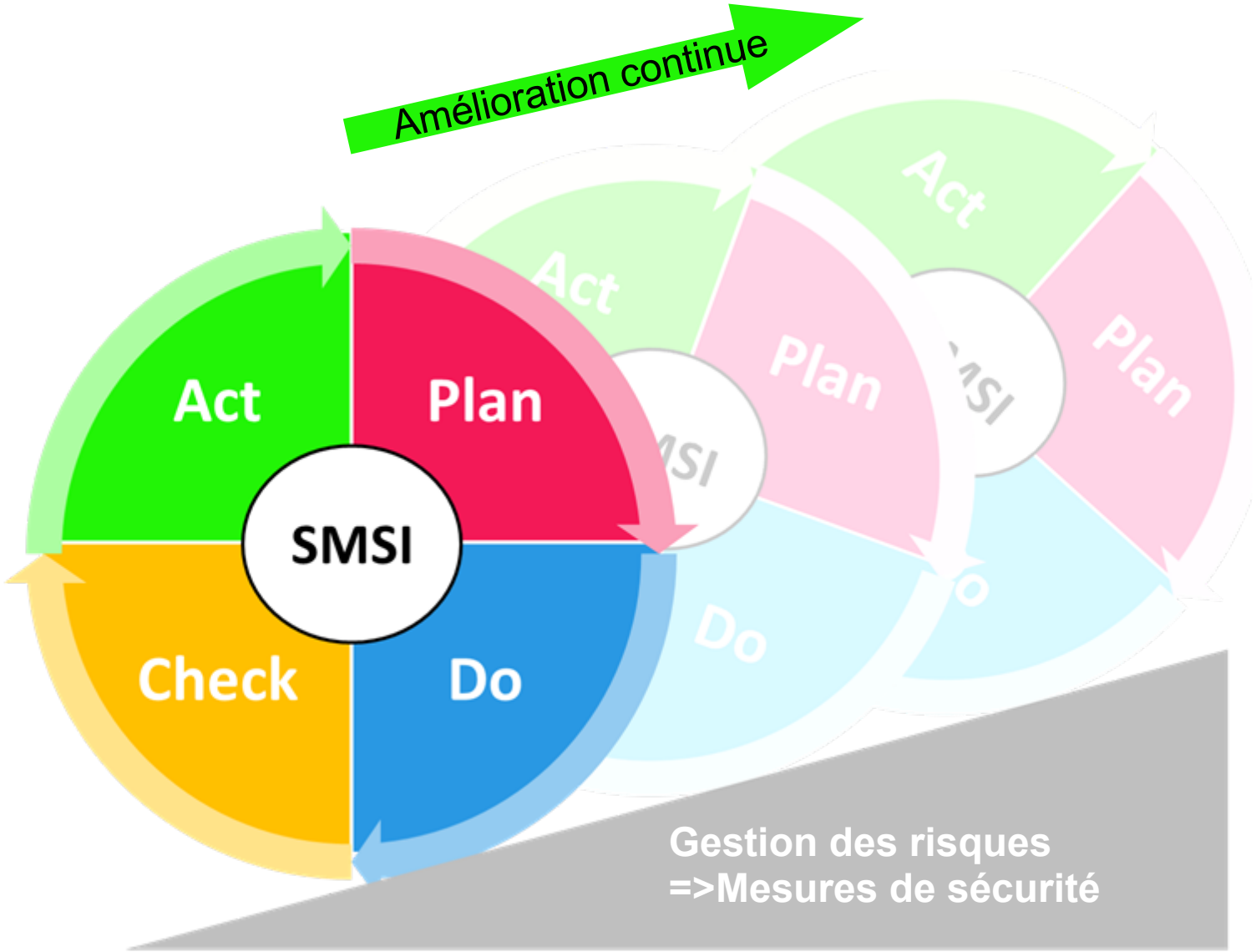
Pourquoi mettre en place un SMSI ?

- Un système de management
  - Oblige à adopter de bonnes pratiques
  - Augmente donc la fiabilité de l'organisme dans la durée
  - Comme un système de management est auditable
    - Il apporte la confiance aux parties intéressées

- Un SMSI permet
  - D'adopter de bonnes pratiques de sécurité
  - D'adapter les mesures de sécurité aux risques encourus

SMSI selon la norme ISO 27001:2013

Parties intéressées



Parties intéressées

Pourquoi un SMSI certifié ISO 27001:2013 ?

- Un système de management selon une norme ISO est un système de management
  - Qui reprend un consensus d'experts mondiaux sur les bonnes pratiques à mettre en œuvre
  - Adapté au contexte, à la culture, à l'environnement et à la taille de l'organisme
- Un SMSI selon la norme ISO 27001:2013
  - S'améliore dans la durée (PDCA)
    - Organisation
    - Gestion des risques
    - Niveau de sécurité

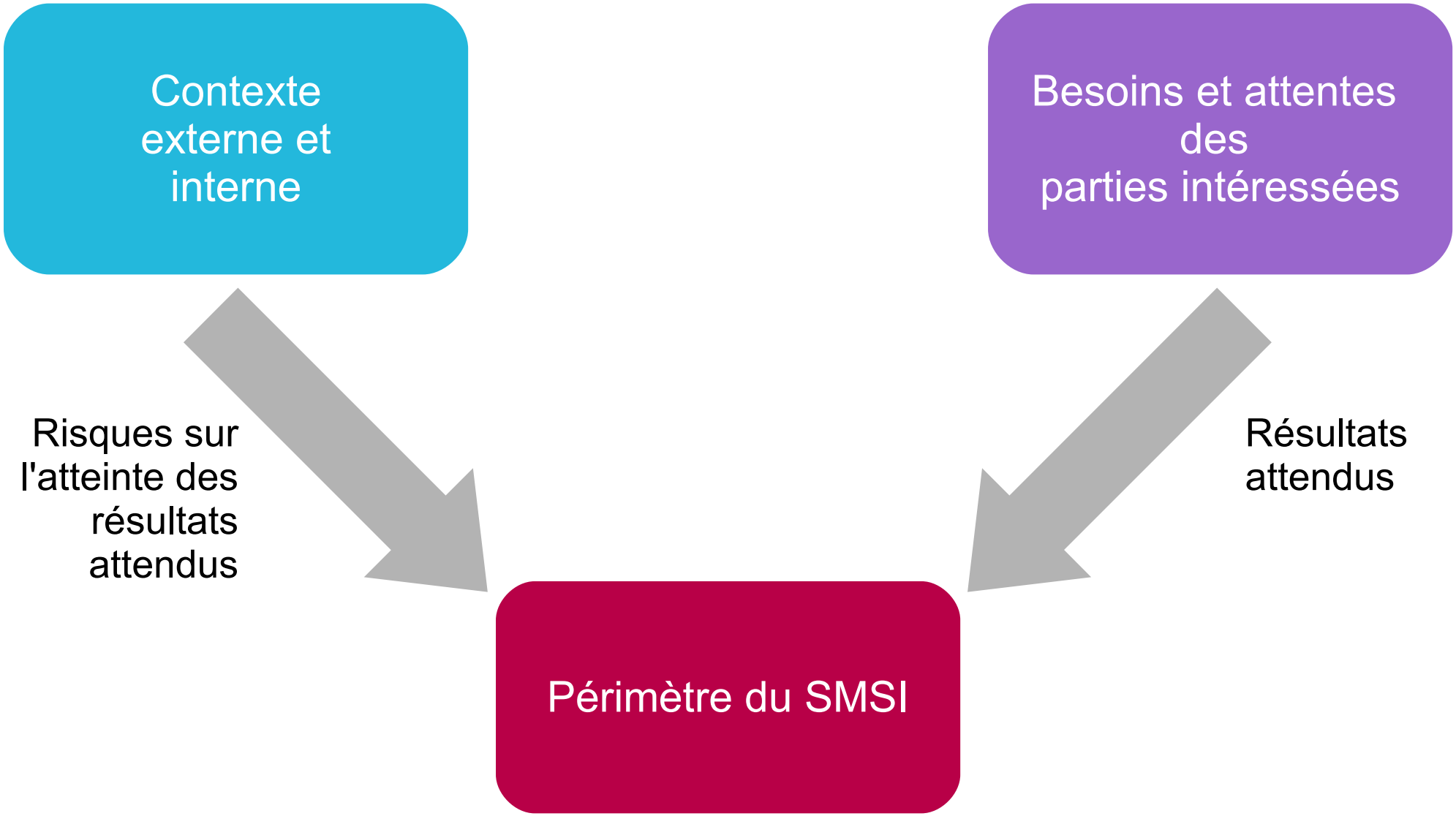
Pourquoi un SMSI certifié ISO 27001:2013 ?

- Un SMSI selon la norme ISO 27001:2013
  - Est régulièrement audité
    - Audits internes
  - Prend en compte les attentes des parties intéressées
- Un SMSI **certifié** ISO 27001:2013
  - Est régulièrement audité par un organisme indépendant
    - Audits de certification
  - Fournit la certitude aux parties intéressées
    - que leurs attentes sont prises en compte
    - que le SMSI est conforme à la norme
    - que le niveau de sécurité et sa gestion s'améliorent dans le temps

Ingrédients du périmètre du SMSI

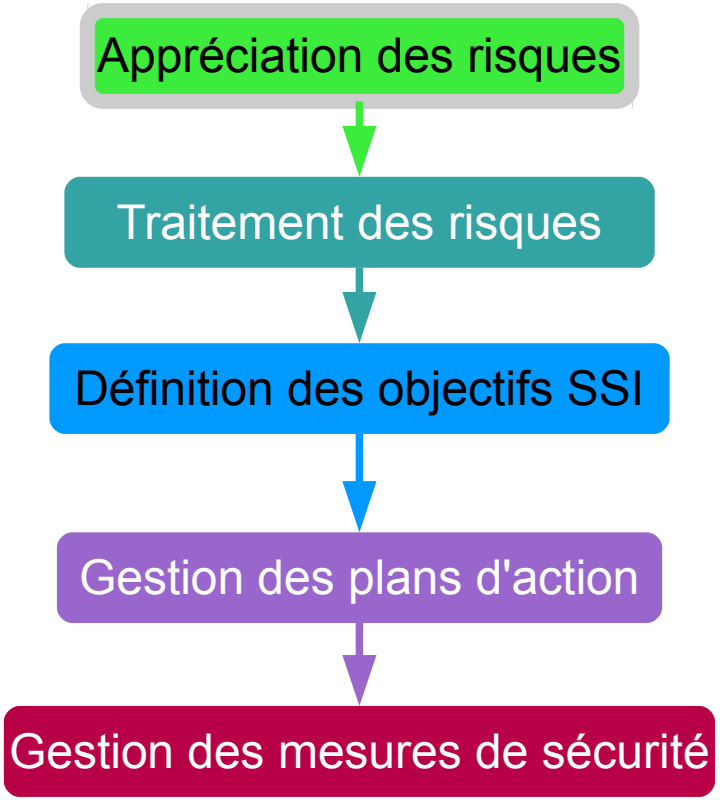
- Contexte externe (opportunités et menaces) (ISO 31 000 5.3.2)
  - Environnement social et culturel, politique, légal, réglementaire, financier, technologique, économique, naturel et concurrentiel
  - Facteurs et tendances ayant un impact déterminant sur les objectifs de l'organisme
  - Relations avec les parties prenantes externes, leurs perceptions et leurs valeurs
- Contexte interne (atouts et faiblesses)
  - Culture, processus, structure, stratégie de l'organisme (ISO 31 000 5.3.3)
  - Comment fonctionnons-nous ?
  - Quels sont nos atouts et nos faiblesses ?
  - Comment le SMSI devra fonctionner pour s'intégrer à ce contexte ?
- Besoins et attentes des parties intéressées

Définition du périmètre du SMSI



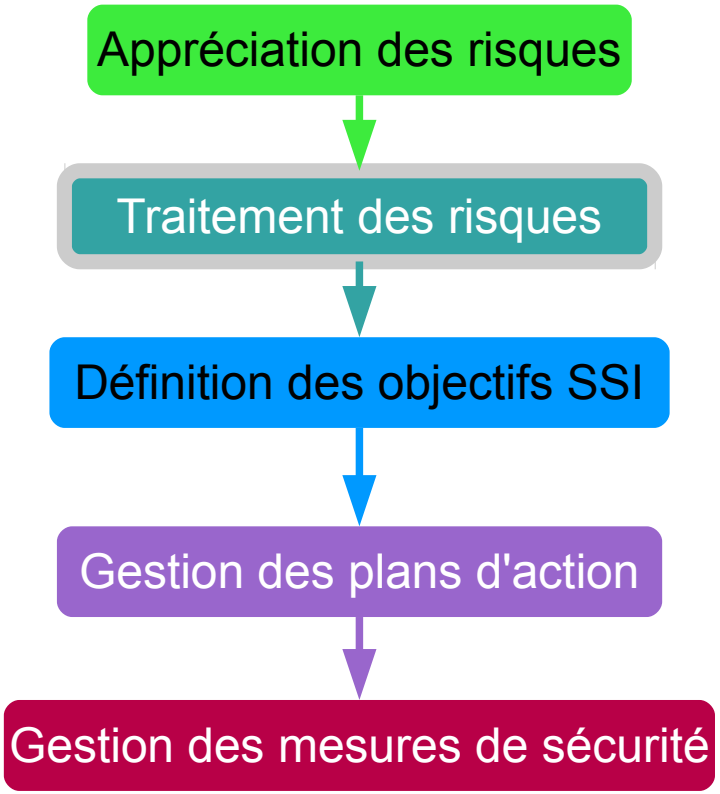
Gestion des risques de sécurité

- Appréciation des risques
  - Processus documenté
    - Critères d'acceptation et d'appréciation des risques
    - Résultats cohérents, valides et comparables
  - Identifier les risques de sécurité de l'information et leur propriétaire
  - Analyser les risques
    - Niveau de risque = f(Conséquences : Vraisemblance)
  - Évaluer les risques par rapport aux critères définis et les prioriser pour le traitement



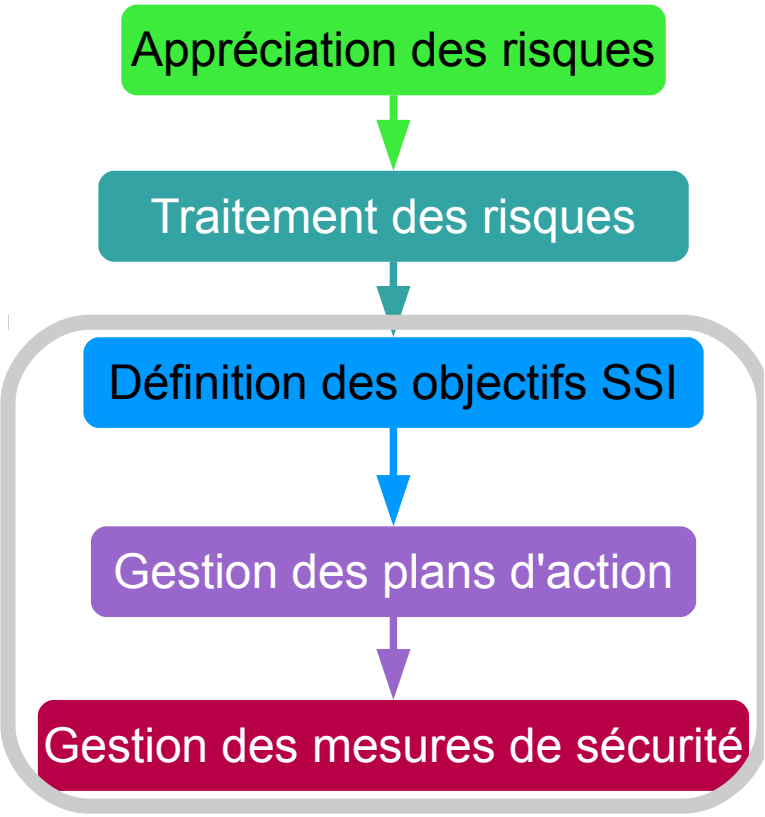
Gestion des risques de sécurité

- Traitement des risques
  - Processus documenté
  - Choisir les options de traitement des risques
  - Déterminer les mesures de sécurité nécessaires
  - Rédiger le plan de traitement des risques
  - Obtenir l'approbation du plan de traitement des risques et des risques résiduels par les propriétaires des risques



Gestion des risques de sécurité

- Définir les objectifs de sécurité
  - Prenant en compte les exigences de sécurité, l'appréciation des risques et le plan de traitement des risques
  - Cohérents avec la politique de sécurité
  - Mesurables
  - Communiqués
  - Mis à jour de manière adéquate
  - Documentés
- Et les plans pour les atteindre
  - Déclinaison des objectifs en actions opérationnelles = mesures de sécurité
  - Quoi, qui, quand, avec quelles ressources, comment sont-ils évalués



Lien avec l'ISO 27002:2013

- SMSI dans l'ISO 27001
  - Gestion de la sécurité
  - Les clauses sécurité ont disparu de l'ISO 27001
  - Approche par les risques

- Mesures de sécurité dans l'ISO 27002
  - Utilisées lorsqu'on met en place un SMSI
    - Vérifier que tous les points importants sont traités
  - Peuvent être utilisées telles quelles
    - Approche conformité

Merci

Questions ?