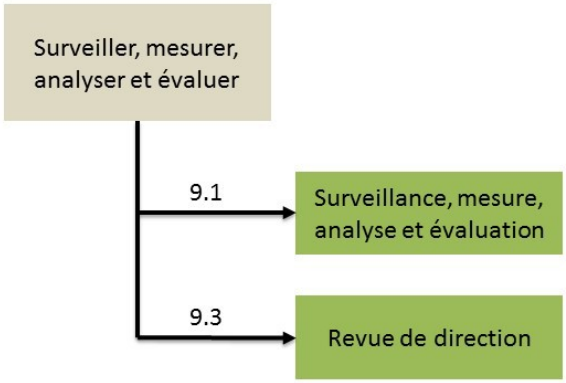
Surveiller, mesurer, analyser et évaluer

Pilote :

L'organisme doit mettre en place des moyens de surveillance, de mesure et d'analyse des performances et de l'efficacité du SI. Les résultats sont conservés.L'organisme fournit les moyens nécessaires (humains et matériels) afin d'entreprendre sans délai la correction et les actions correctives appropriées s'il y a écart. Il est important de réaliser une revue de direction pour s'assurer de l'efficacité et l'adéquation du SMSI est en lien avec la stratégie de l'organisme. Cette revue fournit des décisions et actions sur les opportunités d'amélioration, le besoin de modifier le SMSI et le besoin en ressources.



Retour

1. Acteurs

2. Actions

Responsable : DSI

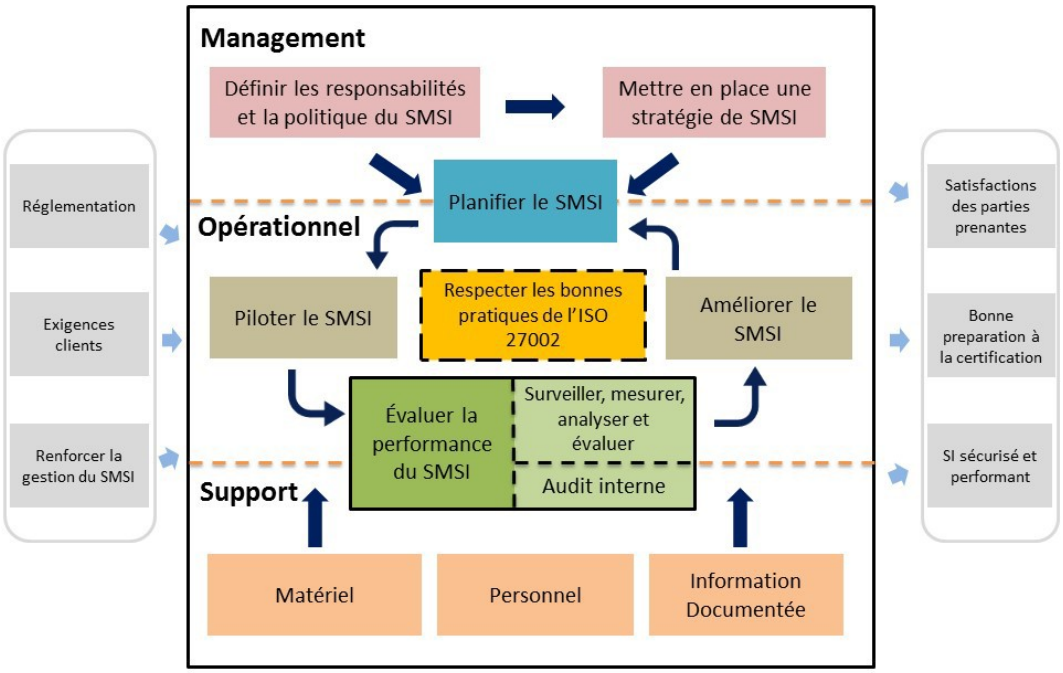
- Évaluer ses performances et l'efficacité de son SMSI
- Surveiller et mesurer ce qui est nécessaire
- Adapter les méthodes de surveillances (résultats comparables et reproductibles)
- Déterminer Qui, Quand pour la surveillance, l'analyse et l'évaluation des résultats
- Conserver sous forme d'informations documentées les éléments de sorties de la revue de direction

Responsable : DSI

- Réaliser la revue du SMSI à des intervalles planifiés pour s'assurer de son efficacité globale ainsi que de ses objectifs
- Passer en revue tous les éléments du Système de management (retours de performances, retours d'informations, modifications des enjeux...)
- Fournir des décisions et actions sur les opportunités d'amélioration, le besoin de modifier le SMSI et le besoin en ressources
- Conserver sous forme d'informations documentées les éléments de sorties de la revue de direction

ISO27001 : version 2013

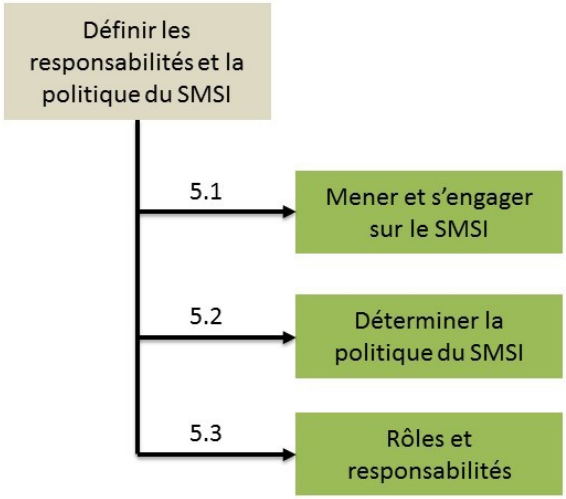
Différents éléments peuvent inciter une entreprise à sécuriser son système d'information autour de trois axes (sécurité de l'information, disponibilité de l'information et intégrité de l'information). Cette décision peut provenir d'une réglementation (Règlement Général sur la Protection des Données), d'un choix interne ou d'une exigence cliente (avec exigence d'audit ou de certification). Le macro-processus réalisé à partir des exigences de l'ISO 27001 permet d'établir, mettre en oeuvre évaluer et améliorer le SMSI d'un organisme pour obtenir la satisfaction des parties prenantes avec un SI sécurisé et performant,et ainsi le préparer à la certification.



Définir les responsabilités et la politique du SMSI

Pilote :

La direction communique et met à disposition sa politique qualité qu'elle applique et met à jour par la suite. La direction attribue les responsabilités et les autorités au sein de l'organisme afin d'appliquer sa politique de sécurité du système d'information.



Retour

1. Acteurs

2. Actions

Responsable : Direction général/Directeur des systèmes d'information/Responsable Qualité

Assure:

- la compatibilité entre le SMSI et la politique du SMSI
- que le SMSI est intégré aux pratiques de l'organisme
- que le résultat du SMSI correspondent aux résultats attendus

Communique:

- sur l'importance du SMSI et de son amélioration continue

Soutient les personnes impliquées

Responsable : Direction général/Directeur des systèmes d'information/Responsable Qualité

Définit une politique:

- adaptée à l'entreprise
- avec des objectifs et des engagements pour satisfaire les exigences et les amélioration continue
- disponible (informations documentées)
- communiquée (entreprise et partie prenante)

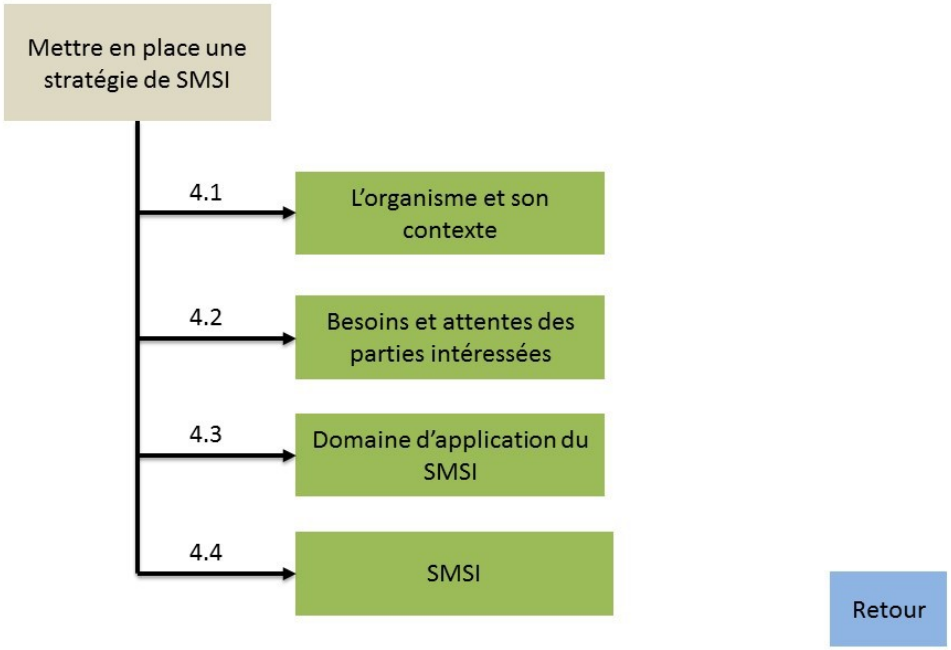
Responsable : Direction Général

- Désigne le responsable (autorité) de la conformité

Mettre en place une stratégie de SMSI

Pilote :

L'organisme détermine les enjeux externes et internes liés au contexte socio-économique dans lequel il se situe. De plus, les parties intéressées sont identifiées ainsi que leurs attentes et exigences. Ces dernières sont listées et revus périodiquement. Les champs d'application du système de management de la qualité (SMSI) sont fixés, ainsi que l'ensemble des processus nécessaires à la mise en oeuvre de ce système.



1. Acteurs

2. Actions

Responsable : Direction Général

- Déterminer les enjeux internes et externes ainsi que la finalité et l'orientation stratégique de l'organisme
- Identifier les facteurs d'influence sur l'efficacité du SMSI

Responsable : Responsbale Qualité

- Identifier les parties intéressées prenantes dans le cadre du SMSI
- Prendre en considération les exigences des parties intéressées ainsi que celles légales et réglementaires

Responsable : Directeur des systèmes d'information/Responsable Qualité

- Etablir le domaine d'application du SMSI ainsi que les limites de son applicabilité en prenant en compte les interfaces et les dépendances existant entre les activités réalisées par l'organisation et celles réalisées par d'autres organisations

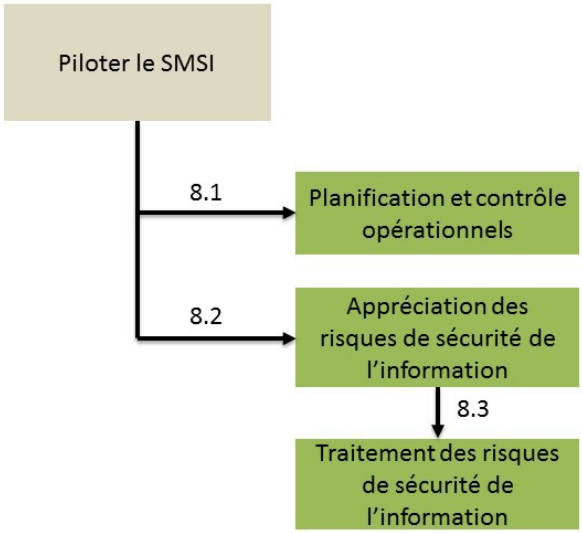
Responsable : Directeur des systèmes d'information

- Etablir, mettre en oeuvre, tenir à jour et améliorer en continu le SMSI

Piloter le SMSI

Pilote :

L'organisme planifie, met en œuvre et maîtrise les processus, y compris externalisés, nécessaires à la réalisation des activités opérationnelles, après avoir recensé les objectifs en terme de sécurité de l'information et recueilli les informations documentées explicitant ces besoins. Elle vérifie de façon continue, principalement après la mise à jour des processus, les informations relatives aux actions menées qui doivent être documentées et conservées.



Retour

1. Acteurs

2. Actions

Responsable : DSI

- Planifier, mettre en oeuvre et contrôler les processus du SMSI
- Identifier et contrôler les processus externalisés
- Conserver les informations documentées
- Gérer les modifications:

1.Contrôler les prévues

2.Analyser les conséquences des imprévues

3.Limiter les effets négatifs

Responsable : Directeur des systèmes d'information/Responsable Qualité

- Planifier et réaliser à intervalles réguliers
- Réaliser lors de changements significatifs
- Conserver les résultats (ID)

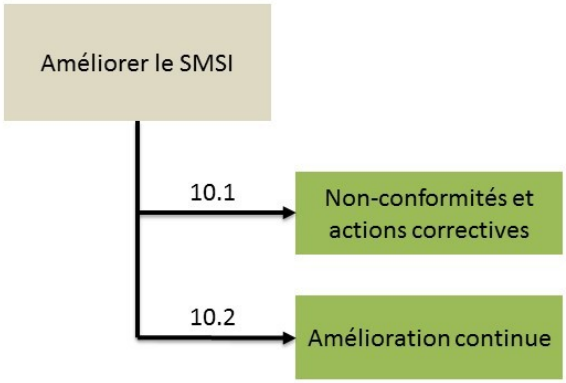
Responsable : DSI

- Mise en oeuvre des plans
- Conserver les résultats (ID)

Améliorer le SMSI

Pilote :

L'organisme améliore en continu la sécurité de son système d'information. Cela passe par la correction des anomalies et des non conformités , mais aussi par les actions préventives suite à l'étude et l'analyse des résultats d'évaluation de la performance du SMSI. L'organisme sera donc constamment dans une optique d'amélioration continue.



Retour

1. Acteurs

2. Actions

Responsable : DSI

- Faire face à la non-conformité et agir pour la maîtriser et la corriger en atténuants les conséquences
- Effectuer la revue de la non-conformité en analysant ses causes et en cherchant des non-conformités similaires

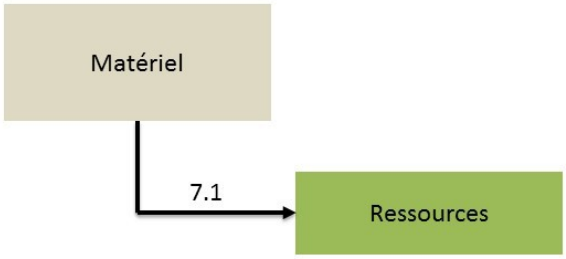
Responsable : DSI

- S'engagent à améliorer en continu la pertinence, l'adéquation et la performance du SMSI

Support Matériel

Pilote :

Les ressources matérielles nécessaires sont mises à disposition pour la réalisation des processus du SMSI.



Retour

1. Acteurs

- DSI

2. Actions

Responsable : Direction Général

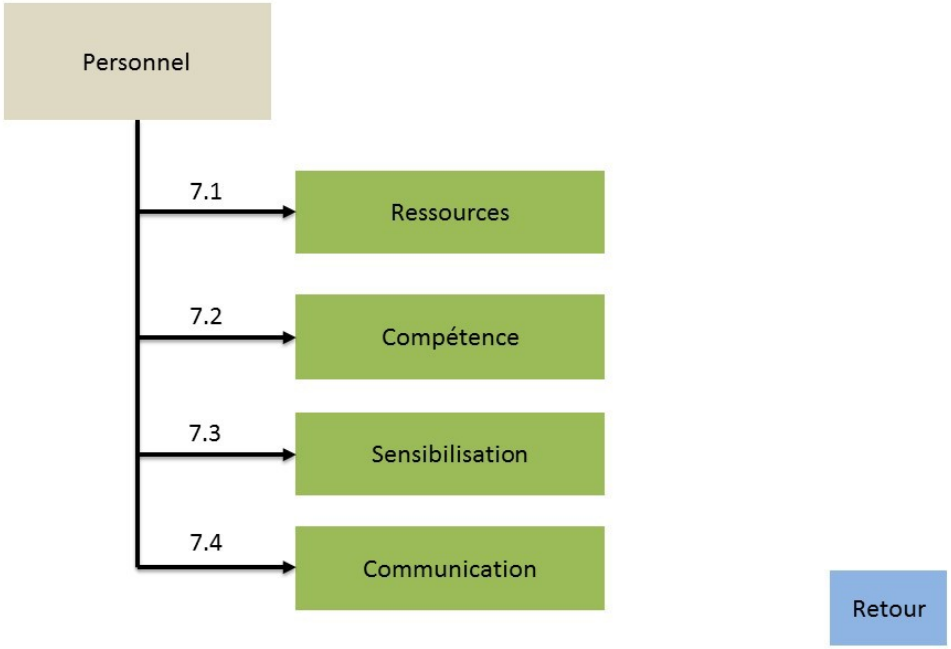
Contributeurs : DSI

- Identifier et fournir les ressources nécessaires

Support personnel

Pilote :

Les ressources humaines nécessaires sont mises à disposition pour la réalisation des processus du SMSI. Les compétences des personnes qui ont un impact direct sur la sécurité du système d'information sont contrôlées. L'organisme sensibilise sur la sécurité de l'informations auprès des parties prenantes.



1. Acteurs

- DSI
- les parties prenantes impliquées

2. Actions

Responsable : Direction Général

Contributeurs : DSI, les parties prenantes impliquées

- Identifier et fournir les ressources nécessaires

Responsable : Direction Général

Contributeurs : DSI, les parties prenantes impliquées

- Sensibiliser le personnel(effet des non-conformités, rôle de leur contribution)

Responsable : Direction Général

Contributeurs : DSI, les parties prenantes impliquées

- Communiquer de manière pertinente

Responsable : Direction Général

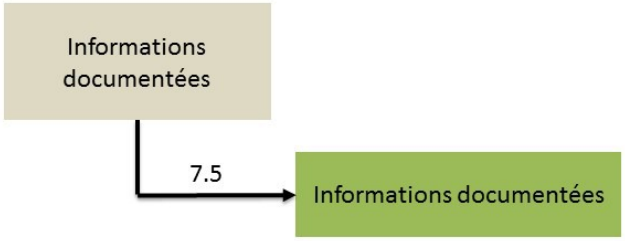
Contributeurs : DSI, les parties prenantes impliquées

- Identifier et assurer les compétences nécessaires

Support informations documentées

Pilote :

Des réunions périodiques et des entretiens avec l'ensemble des pilotes de processus sont planifiées, ceci pour vérifier l'existence, la conformité et l'application sur le terrain des dispositions demandées. Les informations documentées sont créées, mises à jour, diffusées et utilisées par l'ensemble des parties prenantes.



Retour

1. Acteurs

- les parties prenantes impliquées

2. Actions

Responsable : DSI

Contributeurs : les parties prenantes impliquées

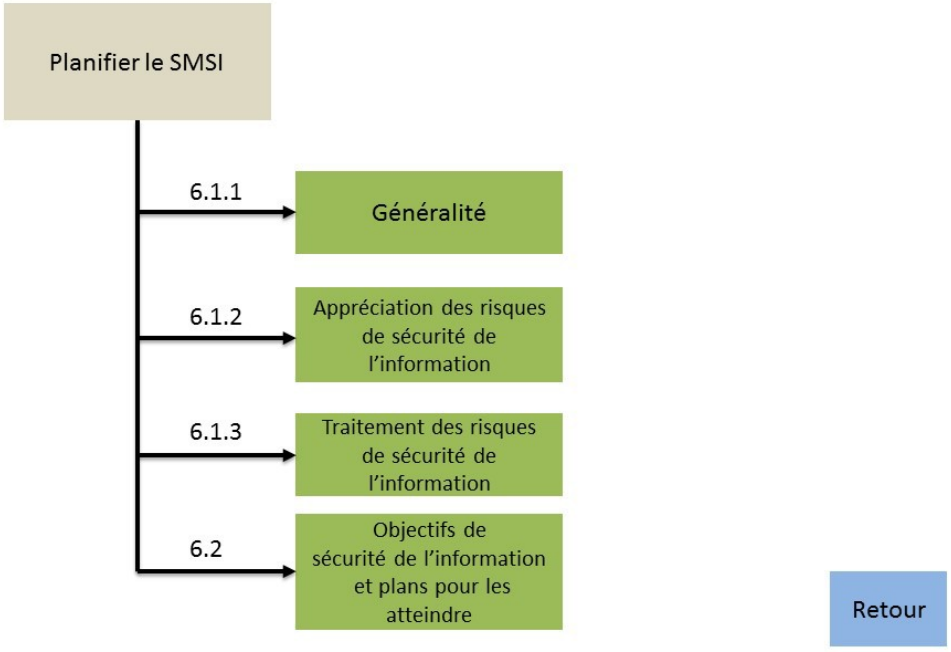
- Créer et mettre à jour de manière approprié (identification, description, format, support, approbation) les informations documentées
- Maîtriser la disponibilité, l'utilisabilité et la protection des informations documentées externes et internes
- Contrôler la distribution, la préservation, l'accès, les modifications, la conservation et la suppression des informations documentées

Planifier le SMSI

Pilote :

Les risques liés aux enjeux de l'organisme sont identifiées et les mesures nécessaires pour y remédier (l'annexe A) mises en application.

Des objectifs pertinents et cohérents avec la politique de sécurité de l'information de l'organisme sont fixés et sont documentés, communiqués à l'ensemble des acteurs et mesurables afin de pouvoir évaluer la performance dans l'atteinte de ces objectifs.



1. Acteurs

2. Actions

Responsable : DSI

Assurer que les objectifs sont réalisables: s'attaquer aux effets indésirables

Responsable : DSI

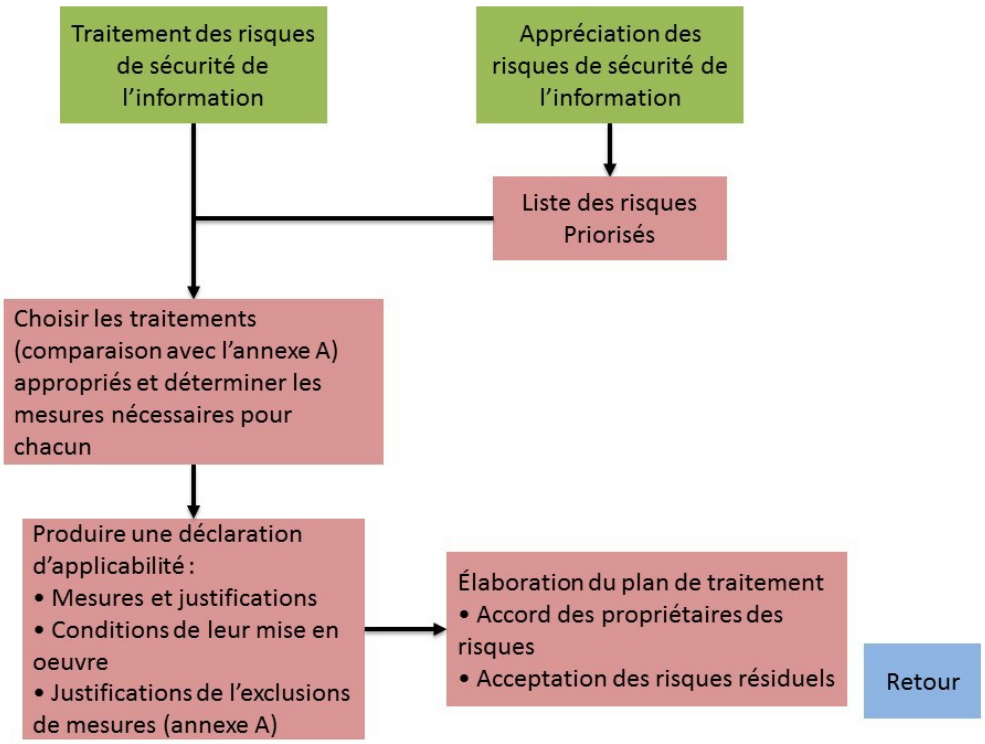
Déterminer:

- les ressources nécessaires
- les responsabilités

- les échéances
- Le moyen de les évaluer

Traitement des risques de sécurité de l'information

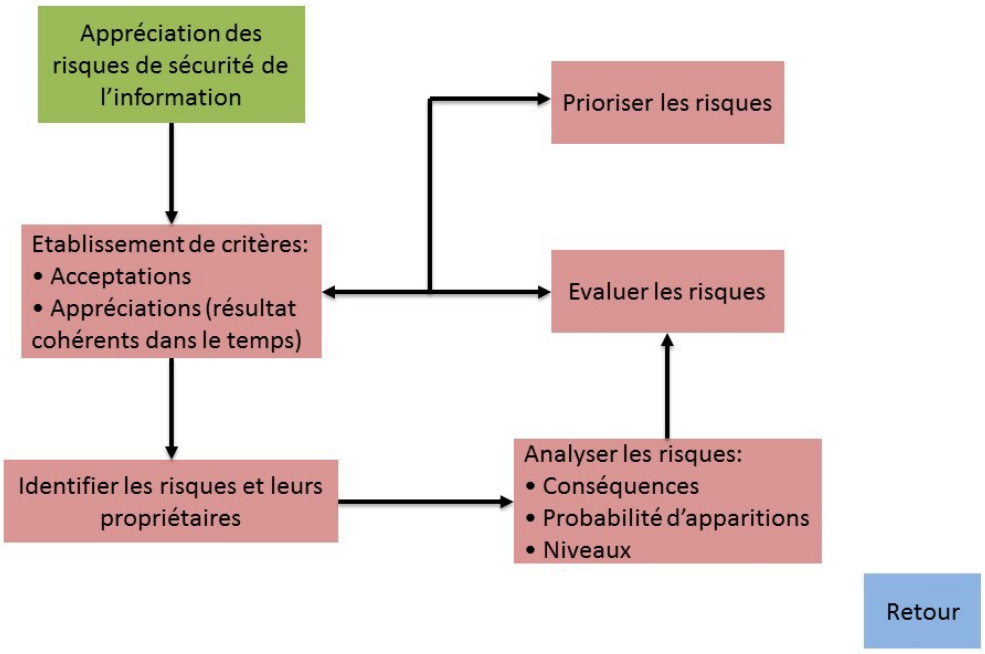
Pilote :



1. Acteurs

Appréciation des risques de sécurité de l'information

Pilote :

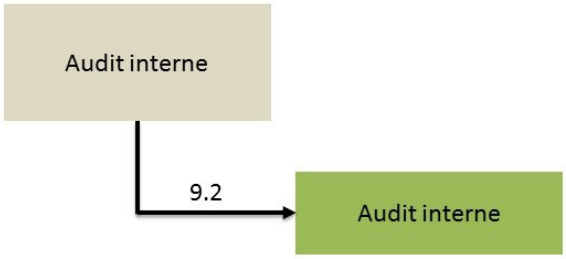


1. Acteurs

Audit interne

Pilote :

L'organisme a met en place des audits internes de façon périodique et de communiquer les résultats à la direction.



Retour

1. Acteurs

2. Actions

Responsable : DSI

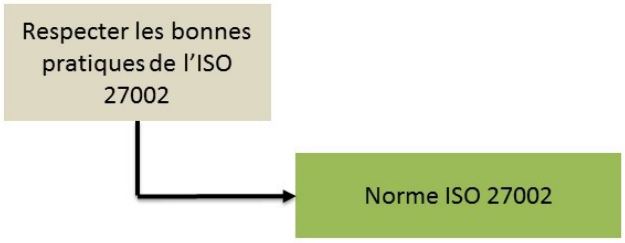
Mener des audits internes du SMSI à intervalles planifiés

Déroulement:

- Planifier le programme d'audit
- Définir les champs, les critères la méthode et la fréquence d'audits
- Choisir un auditeur impartial (ne peut auditer ses activités,...)
- Documenter la procédure d'audit
- Entreprendre les actions sans délais pour corriger les écarts
- Inclure le suivi et la vérification des actions dans les comptes rendus
- Conserver les résultats dans des ID

Respecter les bonnes pratiques de l'ISO 27002

Pilote :



Retour

1. Acteurs

- Direction Général
- les parties prenantes impliquées

2. Actions

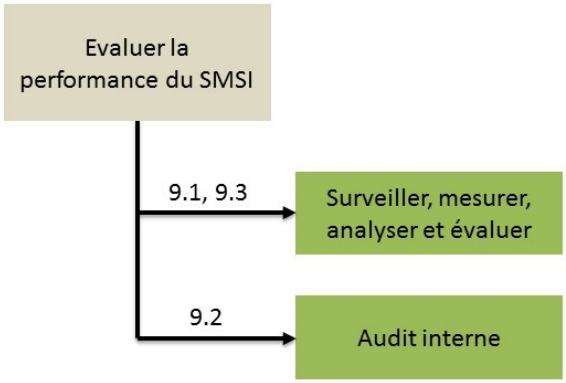
Responsable : DSI

Contributeurs : Direction Général, les parties prenantes impliquées

La norme ISO/CEI 27002 est un guide de bonne pratique qui donne des indications pour:

- Définir des exigences en matière de sécurité
- Apprécier le risque lié à la sécurité
- Définir le plan d'action

Pilote :



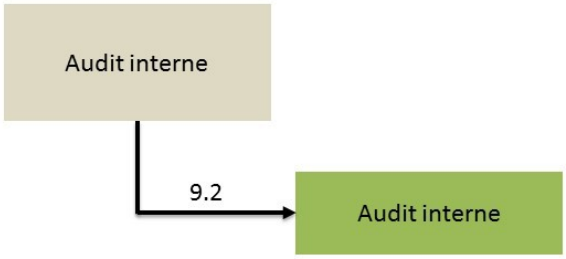
Retour

1. Acteurs

Audit interne

Pilote :

L'organisme a met en place des audits internes de façon périodique et de communiquer les résultats à la direction.



Retour

1. Acteurs

2. Actions

Responsable : DSI

Mener des audits internes du SMSI à intervalles planifiés

Déroulement:

- Planifier le programme d'audit
- Définir les champs, les critères la méthode et la fréquence d'audits
- Choisir un auditeur impartial (ne peut auditer ses activités,...)
- Documenter la procédure d'audit
- Entreprendre les actions sans délais pour corriger les écarts
- Inclure le suivi et la vérification des actions dans les comptes rendus
- Conserver les résultats dans des ID