SYSTEME DE MANAGEMENT DE LA SECURITE DE L'INFORMATION (SMSI OU SGSI)

1. Introduction :

1. Définition :

Un **Système de Management (Gestion) de la Sécurité de l'Information** (*Information Security Management System*, (*ISMS*)) est un système documenté et structuré basée sur le concept de l'amélioration continue ou ***roue de Deming (****méthode* ***PDCA)***. Il désigne un ensemble de mesures organisationnelles et techniques pour la gestion de la sécurité de l'information. C'est un système documenté composé des procédures, des politiques, des méthodes de travail et des enregistrements

La suite des normes ISO 27000 (notamment la norme ISO/CEI 27001 et la norme ISO/CEI 27002) définit les mesures et les bonnes pratiques à prendre en considération pour développer, mettre en place, améliorer et certifier un SMSI .

2. Besoin d'un SMSI :

Les experts en matière de sécurité disent que :

1. Les administrateurs de sécurité de la technologie de l'information doivent consacrer un tiers de leur temps à aborder les aspects techniques. Le temps restant doit être consacré notamment : au développement de politiques et de processus, à faire le point sur la sécurité, à analyser les risques associés, à élaborer des plans d'urgence, et à la sensibilisation aux problèmes liés à la sécurité.
2. La sécurité dépend beaucoup plus des personnes que de la technologie.
3. Les employés sont des menaces plus importantes que les personnes extérieures à l'entreprise.
4. La sécurité peut être comparée à une chaîne, elle est aussi résistante que le maillon le plus faible.
5. Le degré de sécurité dépend de trois facteurs : le risque qu'on est prêt à prendre, la fonctionnalité du système et le prix qu'on est prêt à payer.
6. La sécurité n'est pas un statut ou une image mais un processus continu.

Ces faits mènent inévitablement à la conclusion suivante : la gestion de la sécurité n'est pas seulement un problème technique.

L'établissement et le maintien des mises à jour continuelles d'un SMSI indiquent que l'entreprise doit utiliser une approche systématique afin d'identifier, d'évaluer et de gérer les risques.

Les entreprises de taille importante (Banques, Instituts financiers, Opérateurs téléphoniques, Hôpitaux et Instituts publics ou gouvernementaux) ont diverses motivations pour prendre au sérieux la question de la sécurité de l'information. En effet, les exigences légales qui visent la protection des informations personnelles ou sensibles ainsi que les exigences en matière de la protection des citoyens poussent les entreprises à faire de la sécurité de l'information leur priorité.

3. Etapes de développement d'un SMSI :

Compte tenu des circonstances, le développement et la mise en œuvre d'un processus de gestion indépendant est la seule solution. Le processus de développement d'un SMSI selon la norme ISO/IEC 27001:2005 entraîne les six étapes suivantes :

1. Définition de la politique de sécurité.
2. Définition du périmètre du SMSI.
3. Évaluation des risques.
4. Gestion des risques.
5. Sélection des méthodes de vérification appropriées.
6. Application.

4. *Objectifs du SMSI :*

Au-delà de la satisfaction des objectifs de la sécurité de l'information (vus dans le chapitre précédent), le SMSI vise à satisfaire des objectifs à long terme à savoir :

- La continuité de l'activité.
- Minimiser les pertes et les dégâts.
- Une meilleure compétitivité.
- Une meilleure rentabilité et une rentrée des cash-flows.
- Une image de marque respectée par autrui.
- Une conformité légale.

5. *Facteurs clés de réussite pour un SMSI :*

Pour être efficace, un système de gestion de la sécurité informatique doit :

- Avoir le soutien continu, ferme et visible ainsi que l'engagement de la direction générale de l'organisation ;
- Être centralisé sur une stratégie et une politique commune à travers l'organisation entière ;
- Être une partie intégrante du management global de l'organisation et refléter l'approche de l'organisation en termes de gestion des risques, des objectifs de contrôle, des contrôles et du degré d'assurance exigé ;
- Avoir des objectifs de sécurité et des activités qui reposent sur les objectifs et exigences de l'entreprise et qui sont menés par la gestion de l'entreprise ;
- Entreprendre seulement les tâches nécessaires en évitant le sur-contrôle et le gaspillage des ressources de valeur ;
- Être en total conformité avec la philosophie et l'état d'esprit de l'organisation en fournissant un système qui, au lieu d'empêcher les employés de faire ce qu'ils ont à faire, leur permettrait d'exercer leurs activités dans le contrôle et de démontrer l'accomplissement de leurs responsabilités ;
- Être basé sur une formation continue et un savoir du personnel afin d'éviter l'utilisation de mesures disciplinaires ou encore de procédures militaires ;
- Être un processus continu.

6. *Problèmes récurrents :*

Il y a trois grands problèmes qui mènent à l'incertitude en gestion de la sécurité de l'information :

1. **Changements continus des besoins en matière de sécurité :** L'évolution rapide de la technologie entraîne de nouvelles inquiétudes en ce qui concerne la sécurité pour les entreprises. Les mesures de sécurité actuelles et les exigences deviennent obsolètes lorsque de nouvelles vulnérabilités apparaissent avec le perfectionnement de la technologie. Afin de surmonter ces difficultés, le SMSI doit s'adapter avec afin de garder le système à jour.
2. **Externalités provoquées par un système de sécurité :** L'externalité caractérise le fait qu'un agent économique crée par son activité un effet externe en procurant à autrui, sans contrepartie monétaire, une utilité ou un avantage de façon gratuite, ou au contraire une inutilité, ou un dommage sans compensation. Le SMSI utilisé dans une organisation peut provoquer des externalités pour d'autres systèmes en interaction. Ces dernières sont incertaines et ne peuvent être évaluées qu'une fois le système est mis en place.

3. **Évaluation obsolète des inquiétudes :** La méthode d'évaluation des inquiétudes utilisée dans les SMSI devient obsolète lorsque la technologie progresse et de nouvelles menaces font surfaces. Afin de maintenir un système efficace, il est essentiel d'évaluer la sécurité de l'organisation continuellement.

2. Démarche de développement et de mise en place d'un SMSI :

La mise en place d'un SMSI à travers la norme ISO/CEI 27001 apparaît comme une réponse aux besoins de protection des données dans un contexte de démarche qualité (PDCA ou « Roue de Deming ») .

1. Principe de la roue de Deming (PDCA) :

La notion de "***roue de Deming***" a été popularisée par ***William Edwards Deming***, promoteur de la qualité « *Made In Japan* ». Cette méthode présente les quatre phases à enchainer successivement afin de s'inscrire assurément dans une logique d'amélioration continue. Ces phases doivent être répétées tant que le niveau attendu n'est pas atteint :

- ***Plan :*** Planifier et préparer le travail à effectuer, établir les objectifs, définir les tâches à exécuter.
- ***Do :*** Faire, réaliser, et exécuter les tâches prévues. Il peut être intéressant de limiter l'ampleur et la portée des tâches à exécuter afin de disposer d'un meilleur contrôle (processus répétitif).

La Roue de Deming et l'amélioration permanente…

- ***Check :*** Vérifier les résultats, mesurer et comparer avec les prévisions.
- ***Act :*** Agir, corriger, prendre les décisions qui s'imposent. Identifier les causes des dérives entre le réalisé et l'attendu. Identifier les nouveaux points d'intervention, redéfinir les processus si nécessaire. Boucler, c'est une roue.

2. Les étapes de la mise en place d'un SMSI :

Le SMSI s'appuie sur un modèle d'amélioration continue (appelé PDCA ou « Roue de Deming ») qui conduit dans un premier temps à fixer les objectifs du SMSI (Plan), à le déployer (Do), puis à vérifier les écarts éventuels entre ce qui a été défini et ce qui est mis en œuvre (Check), enfin à mettre en place les actions qui permettront de corriger ces écarts et améliorer le SMSI (Act).

a) Etape de Planification « Plan » (Planifier) :

Dans cette étape on doit définir le périmètre que l'on va gérer dans le SMSI : périmètre géographique mais surtout périmètre en termes d'activités [2].

Il faut choisir et mettre en place une méthode d'analyse de risques pour déterminer, évaluer et couvrir les principaux risques qui peuvent peser sur le SI. Cette méthode prendra en compte les étapes suivantes :

- La définition de la politique et le périmètre du SMSI ;

- L'identification des menaces, l'analyse des vulnérabilités ;
- L'identification et l'évaluation des risques liés à la sécurité, leur classification, et l'élaboration d'une PSSI.
- Le traitement des risques retenus et l'identification des risques résiduels par un plan de gestion : établir la liste des risques couverts et non-couverts et le choix des solutions pour couvrir les risques (*Prévention (Evitement), Réduction, Transfert ou Acceptation*).
- Choisir les mesures de sécurité à mettre en place (la norme ISO 27001 propose une liste de 114 mesures (bonnes pratiques), et la définition des coûts, bénéfices, et impacts des solutions retenues.
- L'acceptation des risques résiduels par la direction.

Les mesures choisies sont recensées dans un document particulier exigé par la norme appelée « ***Déclaration d'Applicabilité(DdA).*** »

Pour une structure déjà en place cette étape passe nécessairement, par un **état des lieux de l'existant** et surtout par un **recensement des mesures** qui sont déjà en place (on part en effet rarement de rien) : inventaire des documents existants et des mesures déjà appliquées. A quel degré sont-elles déjà conformes avec le SMSI ? Existe-t-il déjà une appréciation des risques ?

Il est nécessaire aussi de prendre en compte les ressources (financières, matérielles, humaines…) réellement disponibles, les freins psychologiques et surtout les réels enjeux métiers de la recherche.

b) Etape du déploiement « Do » (Faire):

Après l'analyse de risques, il est nécessaire de déployer les mesures de sécurité décidées dans un plan nommé **le plan de traitement des risques** et retenues dans la **DdA**.

Il est également nécessaire de former et sensibiliser les personnels. En effet rien ne sert de mettre en place des mesures si les personnels n'en sont pas informés et ne sont pas sensibilisés aux bonnes pratiques de sécurité. De même il ne sert à rien d'installer des outils de sécurité si ceux qui doivent les utiliser ne sont pas formés.

Enfin, il faut gérer **le risque au quotidien** par la génération des **indicateurs de performance** pour savoir si les mesures de sécurité sont efficaces, ainsi que des indicateurs de conformité permettant de savoir si le SMSI est conforme à ses spécifications. Ces indicateurs aident à la détection et la réaction rapide aux incidents.

c) Étape de vérification « Check » (Vérifier) :

C'est une étape fondamentale dans un SMSI puisqu'il s'agit de vérifier en permanence :

- Qu'il n'existe pas d'écarts majeurs entre ce que le SMSI définit et ce qui est mis en œuvre en pratique ;
- Que les mesures de sécurité qui couvrent les risques les plus critiques sont adaptées, efficaces et suffisantes.

Les indicateurs et les outils permettant ces contrôles sont multiples (liste des incidents de sécurité, des indicateurs de contrôle, des tableaux de bord de sécurité, etc). Parmi ces outils trois sont très importants :

- Le **contrôle interne** qui consiste à s'assurer en permanence que les processus fonctionnent normalement.
- Les **audits internes** qui vérifient la conformité et l'efficacité du système de management. Ces audits sont ponctuels et planifiés.
- **Les revues** (ou réexamens) qui garantissent périodiquement l'adéquation du SMSI avec son environnement.

Il faut garder à l'esprit, lors de cette étape, que les contrôles ne sont pas mis en place pour mesurer l'efficacité « théorique » du SMSI (celle décrite sur le papier), mais surtout l'efficacité des mesures appliquées.

En effet cette phase permet de réexaminer à intervalles planifiés l'appréciation du risque ; et de s'adapter aux changements d'organisation, de techniques, d'objectifs, de menaces de mesures de sécurité, de règlementation ...

d) Étape d'ajustement « Act » (Réagir) :

Il s'agit de définir, lors de cette étape, les actions qui permettront de réaliser les corrections et les améliorations du SMSI, mises en évidence par les indicateurs lors de l'étape précédente.

Les actions résultantes sont classées en trois catégories :

- **Actions correctives (sur incident ou écart constaté) :** agir sur les effets pour corriger les écarts puis sur les causes pour éviter que les incidents ne se reproduisent
- **Actions préventives (sur une anomalie potentielle) :** agir sur les causes avant que l'incident ne se produise.
- **Actions d'amélioration (amélioration de la performance du processus existant) :** améliorer la performance d'un processus du SMSI.

3. *Certification ISO 27001 :*

Pour exprimer auprès de ses partenaires clients et fournisseurs la conformité de son SMSI aux exigences de la spécification, ou pour profiter des avantages directs que procurent les meilleures pratiques, il est tout à fait possible de procéder à une démarche de certification. Celle-ci sera délivrée par un organisme habilité après une série d'audits successifs.

La certification ISO/IEC 27001 est une possibilité, mais pas une obligation. Elle se déroule sur un cycle de trois ans jalonné par **l'audit initial**, les **audits de surveillance** et **l'audit de renouvellement**.

L'audit initial porte sur l'ensemble du SMSI et dure une période déterminée dans l'annexe C de la norme ISO 27006. L'auditeur ne donne pas la certification, il donne juste un avis qui sera étudié par un comité de validation technique, puis par un comité de certification.

Ce n'est qu'après cela que le **certificat initial** est délivré pour une durée de **trois ans**. Dans le cas contraire, il y a un **audit complémentaire** dans le délai maximum de **trois mois**. L'organisme devra, durant ce délai, **corriger les problèmes** décelés lors de l'audit initial pour obtenir le certificat.

L'audit de surveillance, annuel, aura lieu pendant la période de validité du certificat (3 ans) afin de s'assurer que le SMSI est toujours valable. L'audit porte notamment sur les écarts ou non-conformités relevés lors de l'audit initial ainsi que sur d'autres points :

- Le traitement des plaintes ;
- L'état d'avancement des activités planifiées ;
- La viabilité du SMSI ;
- L'utilisation de la marque de l'organisation certificatrice ;
- Différentes clauses choisies par l'auditeur.

Si l'auditeur relève des non-conformités, le certificat sera suspendu, voire annulé. L'organisme doit donc être perpétuellement mobilisé.

L'audit de renouvellement se déroule à l'échéance du certificat. Il porte sur les non-conformités du dernier audit de surveillance ainsi que sur la revue des rapports des audits de surveillance précédents et la revue des performances du SMSI sur la période.

4. *Documentation du SMSI :*

La documentation SMSI doit se conformer aux recommandations de la clause 4.3 de l'ISO 27001.

La documentation doit :

- Refléter le cycle de vie de toutes les étapes du SMSI,

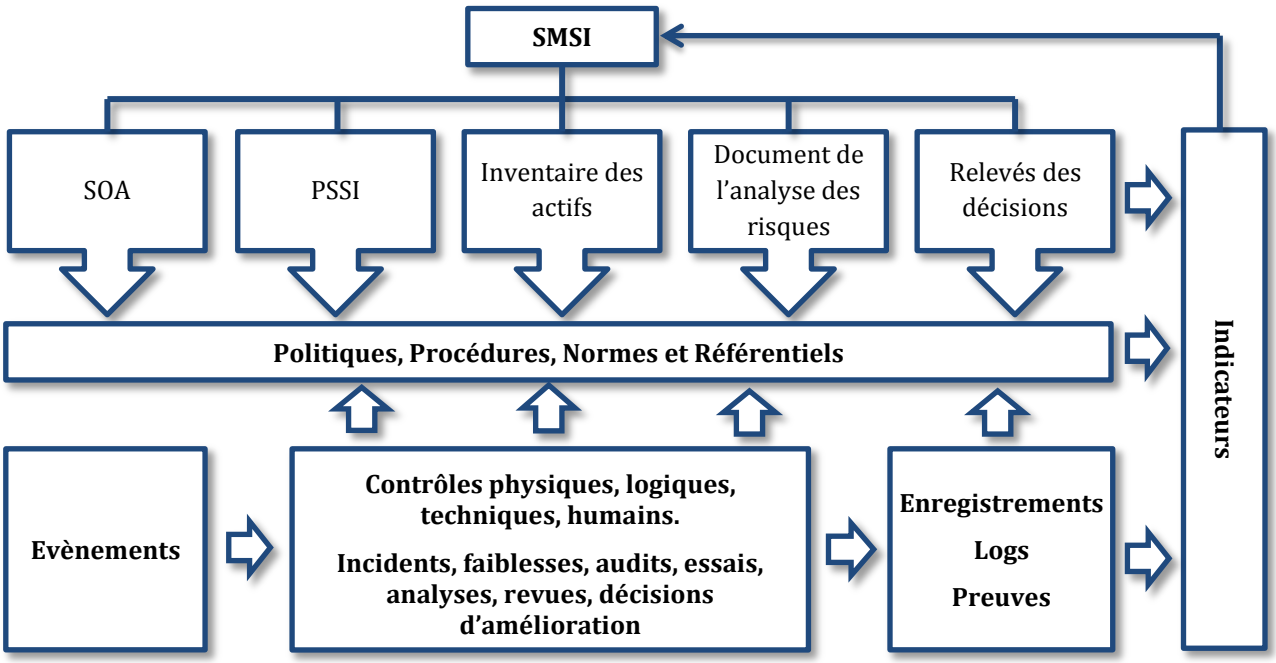
- Enregistrer les décisions de management et leur traçabilité,
- Faire le lien entre solutions de sécurité et analyse de risques.

Elle doit inclure :

- La documentation de la politique de sécurité du SMSI.
- Le périmètre du SMSI,
- Les procédures de contrôle et de maintenance du SMSI,
- La méthodologie d'évaluation des risques,
- Le résultat de l'analyse des risques,
- Le Plan d'action sécurité résultant,
- L'ensemble de la documentation relative aux mesures de sécurité, à leur mise en œuvre et à leur processus de contrôle,
- L'ensemble des "preuves" et outils d'enregistrement (physiques ou logiques) des événements de sécurité,
- Le SOA (***Statement Of Applicability***) ou document décrivant les choix d'application ou non des mesures de sécurité de l'ISO 27001/27002.

La documentation elle-même doit être contrôlée, et elle doit comporter :

a. Un processus d'approbation avant diffusion ;
b. Un processus de revue et d'amélioration ;
c. Une trace des changements et approbations des révisions ;
d. Un système d'identification clair ;
e. Un système de publication et de classification (système documentaire) la rendant disponible à qui de droit ;
f. Une identification claire des documents externes ;
g. Un système de contrôle de la diffusion ;
h. Un système de gestion des archives et d'identification des documents devenus obsolètes ;
i. Un système de trace des emprunteurs ou lecteurs.



En résumé : Écrire pour toutes les mesures du SOA ce que l'on fait, faire ce qui est écrit, contrôler (audit interne) qu'on le fait réellement et régulièrement, et qu'on l'améliore de façon continue en gardant comme preuve les traces de toutes les observations et décisions prises.

Le rôle de l'audit sera de vérifier que l'on fait bien ce que l'on a dit en comparant l'aspect opérationnel de la documentation avec les faits observés et les relevés d'enregistrement du SMSI.

Attention : au-delà de cette sémantique, il vérifiera aussi que le SMSI est bien aligné sur les objectifs de l'entreprise et que les mesures de sécurité sont adaptées aux enjeux.

Listes des Documents du SMSI produits par étape :

Phases	Etapes	Documentation principale
Plan	*Obtenir le support du management.*	*Enregistrement des décisions de management.*
	Définir le champ du système de management.	*Périmètre du SMSI.*
	Définir la politique du SMSI.	*Politique du SMSI.*
	Définir une méthodologie de gestion des risques.	*Méthode d'analyse des risques.*
	Evaluer et traiter les risques.	*Rapport d'analyse des risques.*
	Choisir les mesures de sécurité réduisant les risques.	*Plan de traitement de risques.*
	*Produire le SOA (**Statement of Applicability**) qui énumère les mesures de sécurité à appliquer.*	*SOA.*
	Définir une stratégie de gestion documentaire.	*Procédure de gestion des documents du SMSI.*
Do	*Ecrire et implémenter le plan de réduction des risques.*	*Plan Projet SMSI.*
	Affecter les ressources nécessaires.	*Plan Projet SMSI.*
	Rédiger la documentation.	*Procédures SMSI.* *PSSI.* *Procédure de mesures (**Controls**).*
	Former le personnel.	*Plan de formation/communication.*
	Appliquer les mesures décidées.	*Plan Projet (suivi).*
	Identifier les risques résiduels.	*RTP (Plan de Traitement des Risques).*
	Mettre en place les mesures de détection et de traitement des incidents de sécurité.	*Procédure de gestion des évènements de sécurité.*
Check	*Mettre en place les indicateurs et tableaux de bord.*	*Métriques/indicateurs.*
	Revue des risques résiduels.	*Rapport de revue de risques.*
	Revue des risques acceptés.	*Rapport de revue de risques.*
	Audit et revue périodiques du SMSI.	*Rapport d'audit interne.*
	Procédures d'actions correctives et d'amélioration.	*Rapport d'actions correctives et amélioratrices.*
Act	*Prendre les mesures qui permettent de réaliser les corrections et amélioration du SMSI.*	*Revue de mesures du SMSI.*
	Communication.	*Enregistrement de traces.*
	Préparer une nouvelle itération de la phase Plan.	*RTP.*

Références bibliographiques :

- L. Bloch & C. Wolfhugel "Sécurité informatique : Principes et méthodes à l'usage des DSI, RSSI et administrateurs" Eyrolles 2ème édition 2013.
- S. Ghernaouti « Cybersécurité Analyser les risques Mettre en œuvre les solutions » DUNOD 6ème édition 2019.
- A. Fernandez Toro "Sécurité opérationnelle –Conseils pratiques pour sécuriser le SI" EYROLLES 2015.
- G. Billois & T. Savalle « L'ISO 27000, nouveau nirvana de la sécurité ? » Livre blanc rédigé sous le pilotage de L. Bellefin ISBN : 2-9525584-2-6
- Le blog du manager du système d'information http://www.ismanager.fr/le-smsi-en-bref/
- Wikipedia https://fr.wikipedia.org/
- Suivons la roue de Deming : La méthode PDCA https://blog-gestion-de-projet.com/
- https://www.accordance.fr/prestations/conseil/certification-iso27001/
-

ANNEXES

Exemple d'étapes de certification chez « ACCORDANCE Consulting » :

ACCORDANCE Consulting accompagne les entreprises (les organisations) pour la mise en place de leurs systèmes de Management de la Sécurité de l'Information (SMSI), en vue d'une certification ISO27001.

La démarche ACCORDANCE s'articule en 9 phases :

Phase 1 : Diagnostic préalable et préconisations :

Objectifs : réaliser un audit initial sur l'ensemble du périmètre de la norme ISO 27001 et la norme 27002 et mettre en place un plan d'action en discussion avec la Direction.

Phase 2 : Documentation du SMSI :

Objectifs : mettre à niveau l'ensemble des documents exigés par le Norme ISO27001 (documentation des exigences de sécurité de l'information et de la politique et des objectifs de sécurité, création ou actualisation des documents et procédures obligatoires, documentation du système d'audit et de contrôle opérationnel).

Phase 3 : Création ou complémentation du répertoire de risques :

Objectifs : créer ou mettre à niveau la documentation des risques en cohérence avec le SMSI.

Phase 4 : Sensibilisation et formation des personnels :

Objectifs : sensibiliser les acteurs du SMSI afin de s'assurer de la bonne compréhension du projet ISO27001 et ses implications, mettre à niveau la formation des auditeurs et contrôleurs.

Phase 5 : Audit système préalable à certification :

Objectifs : vérifier la bonne mise en œuvre du SMSI et sa conformité au référentiel ISO27001.

Phase 6 : Revue de Direction :

Objectifs : faire le bilan de fonctionnement du SMSI, assurer son pilotage et décider d'actions d'amélioration.

Phase 7 : Assistance à certification :

Objectifs : accompagner l'entreprise durant l'audit de certification et le bon déroulement de celui-ci.

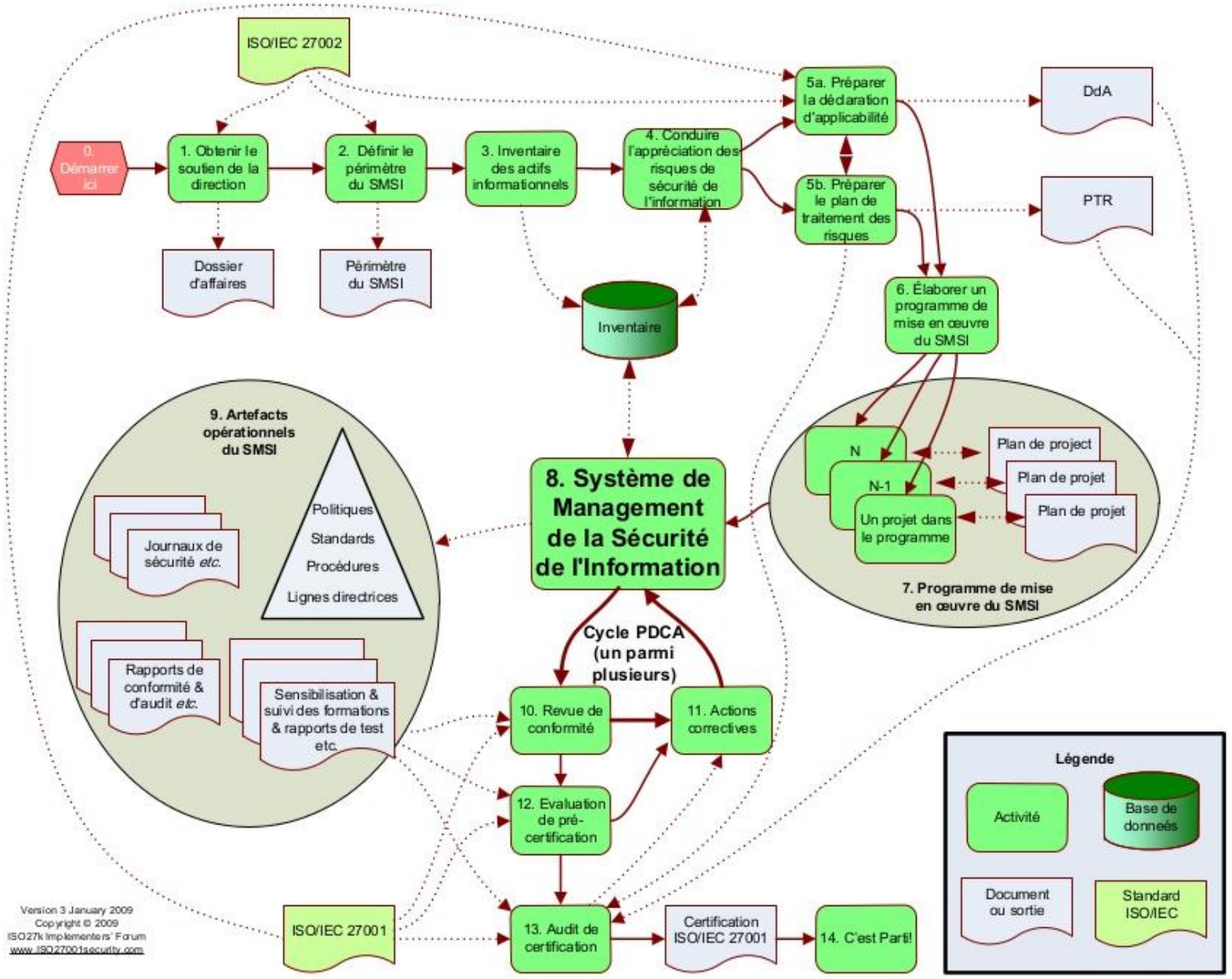
Phase 8 : Pilotage et Reporting de projet :

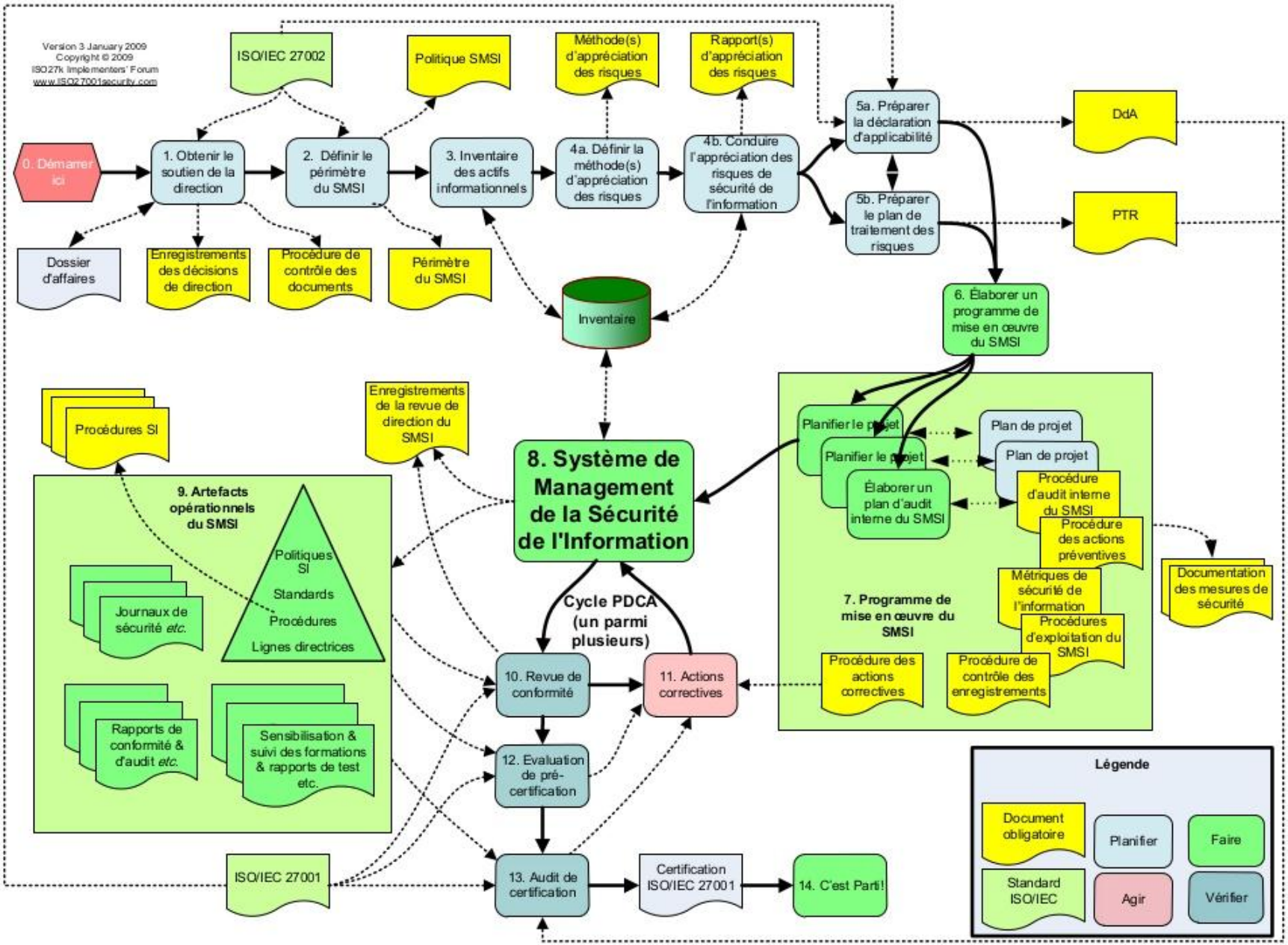
Objectifs : suivre le projet, assurer sa coordination et délivrer des informations sur l'état d'avancement à la Direction.

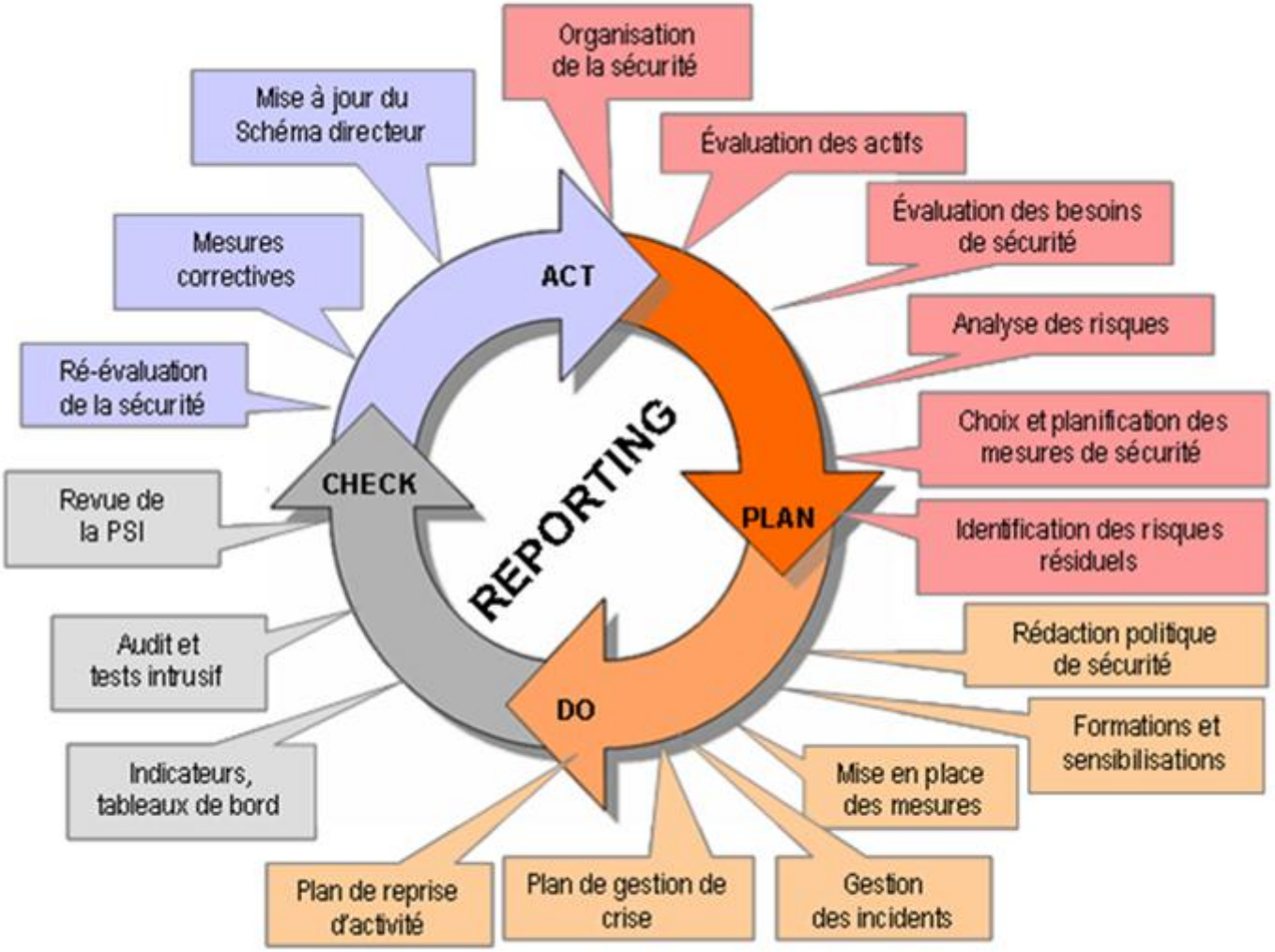
Phase 9 : Mise en place de l'outil de gestion de la performance « Performance en Ligne » :

Objectifs : en cas d'utilisation, paramétrer l'application, former les administrateurs et utilisateurs, répondre aux questions liées à l'utilisation du logiciel.

Organigramme de la mise en œuvre du SMSI et processus de certification ISO 27001 v3




Version 3 January 2009
Copyright © 2009
ISO27k Implementers' Forum
www.ISO27001security.com
ISO/IEC 27002
Politique SMSI
Méthode(s) d'appréciation des risques
Rapport(s) d'appréciation des risques
0. Démarrer ici
1. Obtenir le soutien de la direction
2. Définir le périmètre du SMSI
3. Inventaire des actifs informationnels
4a. Définir la méthode(s) d'appréciation des risques
4b. Conduire l'appréciation des risques de sécurité de l'information
5a. Préparer la déclaration d'applicabilité
5b. Préparer le plan de traitement des risques
DdA
PTR
Dossier d'affaires
Enregistrements des décisions de direction
Procédure de contrôle des documents
Périmètre du SMSI
Inventaire
6. Élaborer un programme de mise en œuvre du SMSI
Procédures SI
Enregistrements de la revue de direction du SMSI
8. Système de Management de la Sécurité de l'Information
9. Artefacts opérationnels du SMSI
Politiques SI
Standards
Procédures
Lignes directrices
Journaux de sécurité etc.
Rapports de conformité & d'audit etc.
Sensibilisation & suivi des formations & rapports de test etc.
Cycle PDCA (un parmi plusieurs)
10. Revue de conformité
11. Actions correctives
12. Evaluation de pré-certification
13. Audit de certification
ISO/IEC 27001
Certification ISO/IEC 27001
14. C'est Parti!
7. Programme de mise en œuvre du SMSI
Planifier le projet
Plan de projet
Élaborer un plan d'audit interne du SMSI
Procédure d'audit interne du SMSI
Procédure des actions préventives
Métriques de sécurité de l'information
Procédures d'exploitation du SMSI
Procédure de contrôle des enregistrements
Procédure des actions correctives
Documentation des mesures de sécurité
Légende
Document obligatoire
Standard ISO/IEC
Planifier
Faire
Agir
Vérifier



DEMARCHE DE CONSTRUCTION D'UN SMSI ISO 27001

Terminologie :

- **Cash-flow** (**flux de liquidités**) : indicator allowing to know the aptitude of the company to finance its investments from its exploitation or its capacity to distribute dividends to its shareholders.

- **التدفق النقدي :** مؤشر على قدرة الشركة على تمويل استثماراتها من عملياتها أو قدرتها على توزيع أرباح على مساهميها.

- **Return on investment (ROI) :** is a financial ratio used to calculate the benefit an investor will receive in relation to their investment cost.

- **عائد الاستثمار (ROI) :** نسبة مالية تُستخدم لحساب المنفعة التي سيحصل عليها المستثمر فيما يتعلق بتكلفة الاستثمار.

What Is Return on Investment (ROI)?

Return on Investment (ROI) is a performance measure used to evaluate the efficiency of an investment or compare the efficiency of a number of different investments. ROI tries to directly measure the amount of return on a particular investment, relative to the investment's cost. To calculate ROI, the benefit (or return) of an investment is divided by the cost of the investment. The result is expressed as a percentage or a ratio.

How to Calculate ROI

The return on investment formula is as follows:

$$\text{ROI} = \frac{\text{Current Value of Investment} - \text{Cost of Investment}}{\text{Cost of Investment}}$$

"Current Value of Investment" refers to the proceeds obtained from the sale of the investment of interest. Because ROI is measured as a percentage, it can be easily compared with returns from other investments, allowing one to measure a variety of types of investments against one another.

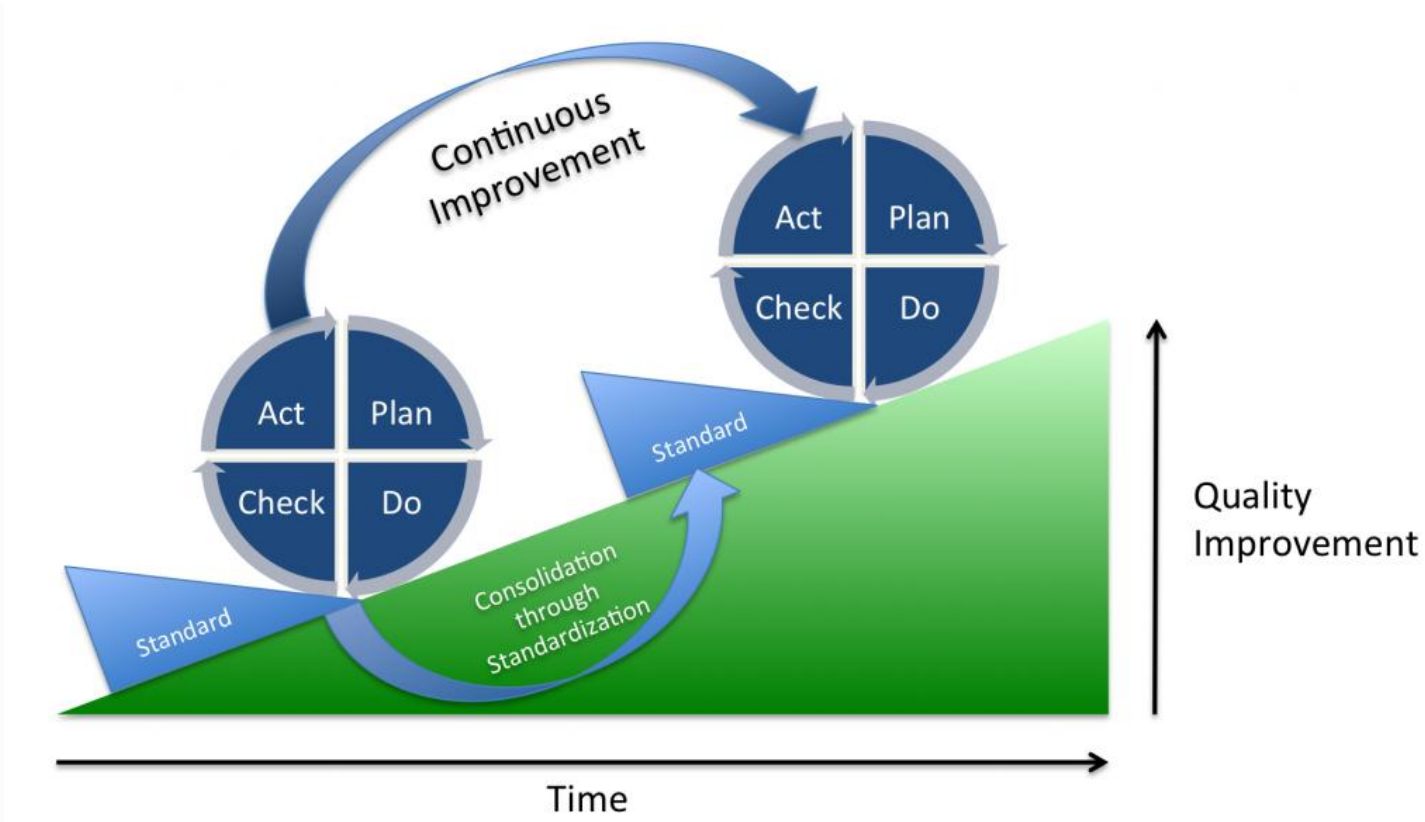
On attend par SMSI le système de management de la sécurité de l'information basé sur la norme ISO 27001. Un Système de Management est un système documenté et structuré basée sur le concept de l'amélioration continue ou roue de Deming. On dit que c'est un système documenté car, il est composé par des procédures, politiques, méthodes de travail et des enregistrements.

Sommaire [masquer]

Concept d'amélioration continue

Le concept d'amélioration continue a été conçu par Edwards Deming qui a pensé que pour atteindre et améliorer de façon continue les objectifs d'une organisation, il faut les évaluer par rapports aux retours venants des clients et des processus. Ce concept a été exploité par les japonais dans leur méthode appelé Kaizen qui a contribué au développent exponentiel de l'empire Toyota. Par ailleurs, la vulgarisation du système de management a été propulsé par l'arrivé de la norme ISO 9001. Dans le concept d'amélioration continue, il y a quatre phases :

- La phase Plan (planification) : Planifier ce que l'on va faire
- La phase Do (faire) : Faire ce que l'on a planifié
- La phase Check (Vérifier) : Vérifier s'il y a des écarts entre la planification et l'implémentation
- La phase Act (Réagir) : Apporter des actions correctives pour rectifier les écarts trouvés dans la phase Check.



Qu'est ce qu'un SMSI ?

Un SMSI ou Système de Management de la Sécurité de l'information est un système qui applique le concept de l'amélioration continue sur la sécurité de l'information. Il a été conçu pour établir, mettre en œuvre, exploiter, surveiller, revoir, maintenir et améliorer la sécurité de l'information. Un SMSI certifie que :

- Les actifs informationnels ou les biens essentiels de votre entreprise sont bien définis et sécurisés
- Les risques liées à la sécurité sont bien gérés et atténuées
- Des politiques et des procédures sont en place
- Les mesures de sécurités sont respectées et vérifiées régulièrement

Le SMSI et les normes ISO

De nos jours, l'information et le système d'information jouent un rôle très important au sein de chaque organisation. Par conséquent, il faut les protéger contre les attaques et les catastrophes. Pour ce faire, il faut bien gérer la sécurité de l'information dans les entreprises, mais cela nécessite une approche systématique et complexe. Face à ce problème; ISO a mis en place les séries de normes ISO 27000 pour faciliter la gestion de la sécurité de votre système d'information.

Les plus importants de ces séries de normes sont la norme ISO 27001 et la norme ISO 27002. La première fournie les exigences pour la mise en place d'un SMSI et la seconde est un outil de référence pour sélectionner les mesures de sécurité nécessaires pour sa mise en œuvre. L'ISO 27001 parle de la façon pour mettre en œuvre, surveiller, maintenir et améliorer en permanence un SMSI. ISO 27001 est également la norme qui régit la certification du SMSI. La dernière version de l'ISO 27001 est la version 2013.

Comment le SMSI perçoit-elle la sécurité de l'information ?

En se référant sur la norme ISO 27001, la sécurité de l'information est la protection de l'information pour assurer ce qui suit :

- **La confidentialité :** La confidentialité garantie que l'information est accessible aux personnes ou aux systèmes autorisées à y accéder seulement.

- **L'intégrité :** L'intégrité signifie que l'information est exacte et complète et que l'information ne soit pas modifiée sans autorisation.
- **La disponibilité :** La disponibilité signifie que l'information est accessible aux utilisateurs ou systèmes autorisés en cas de besoin.

Les avantages qu'un SMSI peut apporter

La mise en place d'un SMSI nécessite du temps et de budget et parfois le top management des entreprises pense que c'est de la dépense pour rien car il ne génère pas directement des profits pour l'organisation. Cependant, il peut apporter des nombreux avantages:

- Si l'information est l'atout majeur ou la base de votre entreprise, le SMSI permet alors de protéger et de rentabiliser votre activité
- La direction de l'entreprise est toujours impliquée dans la sécurité
- Votre fiabilité et crédibilité vis à vis de vos partenaires s'améliorent
- La certification de votre SMSI ouvre d'autres opportunités d'affaires
- Les sources d'informations et les données sont utilisées de manière plus efficace
- L'adoption des bonnes pratiques
- Le SMSI rend votre investissement dans la sécurité de l'information plus efficace
- Le SMSI change la culture de votre entreprise

En somme, le SMSI est non seulement un système qui améliore la sécurité de vos données et vos informations, elle conduit aussi à une utilisation plus efficace de vos informations et une meilleure position concurrentielle sur le marché.

Est- ce que le SMSI est fait pour les petites entreprises ?

Quelque soit la taille de votre organisation, que ce soit un multinationale ou une entreprise familiale avec 10 salariés, vous pouvez toujours mettre en place un SMSI. ISO l'a précisé dans la norme ISO 27001.

Certification ISO 27001

Pour exprimer auprès de ses partenaires clients et fournisseurs la conformité de son SMSI aux exigences de la spécification, il est tout à fait possible de procéder à une démarche de certification. Celle-ci sera délivrée par un organisme habilité après une série d'audits successifs. Cette démarche, souvent plus contraignante qu'il n'y paraît, reste encore assez rare, en France en tout cas.

Iso 27000

Les principales normes du standard ISO 27000

- 27000 Présentation, glossaire
- 27001 La norme internationale SMSI
- 27002 Sécurité de l'information, les 133 bonnes pratiques
- 27004 Les indicateurs de sécurité, la mesure et la métrique pour le suivi du SMSI
- 27005 La gestion des risques

Normes ISO : 27000 - 27999 / Sécurité de l'information[modifier | modifier le code]

- ISO 27000 : Série de normes dédiées à la sécurité de l'information
  - ISO/CEI 27000 : Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire (2018)
  - ISO/CEI 27001 : Système de Gestion de la Sécurité de l'Information (ISMS) — Exigences
  - ISO/CEI 27002 : Code de bonnes pratiques pour la gestion de la sécurité de l'information (anciennement ISO/CEI 17799)
  - ISO/CEI 27003 : Système de Gestion de la Sécurité de l'Information (ISMS) — Guide d'implémentation
  - ISO/CEI 27004 : Mesure de la sécurité de l'information
  - ISO/CEI 27005 : Gestion du risque en sécurité de l'information
  - ISO/CEI 27006 : Exigences pour les organismes réalisant l'audit et la certification de Systèmes de Gestion de la Sécurité de l'Information (ISMS)
  - ISO/CEI 27007 : Guide pour l'audit de Systèmes de Gestion de la Sécurité de l'Information (ISMS), *en préparation*
  - ISO/CEI 27008 : Lignes directrices de vérification en matière de mesures de sécurité, *en préparation*
  - ISO/CEI 27011 : Guide pour l'implémentation de ISO/CEI 27002 dans l'industrie des télécommunications (publié le 15 décembre 2008)
  - ISO/CEI 27013 : Guide sur la mise en œuvre intégrée de l'ISO/CEI 27001 et de l'ISO/CEI 20000-1
  - ISO/CEI 27017 : Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/CEI 27002 pour les services du nuage (autre nom UIT-T X.1631, révision courante 2015)[5]
  - ISO/CEI 27018 : Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII
  - ISO/CEI 27031 : Code de bonnes pratiques en matière de Technologies de l'information – Techniques de sécurité – Lignes directrices pour mise en état des technologies de la communication et de l'information pour continuité des affaires (publié le 1er décembre 2012)
  - ISO/IEC 27032 : Technologies de l'information - Techniques de sécurité - Lignes directrices pour la cybersécurité

- ISO/CEI 27034 : Sécurité des applications
- ISO/CEI 27035 : Gestion des incidents
- ISO/CEI 27036 : Sécurité d'information pour la relation avec le fournisseur
- ISO/CEI 27037 : Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques (publié le 15 octobre 2012)
- ISO/CEI 27038 : Spécifications pour la rédaction numérique
- ISO/CEI 27039 : Sélection, déploiement et opérations des systèmes de détection d'intrusion (publié le 11 février 2015)
- ISO/CEI 27799 : Informatique de santé - Gestion de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002

CERTIFICATION À ISO/IEC 27001

Comme toutes les autres normes de systèmes de management de l'ISO, la certification selon ISO/IEC 27001 est une possibilité, mais pas une obligation. Certains utilisateurs décident de mettre en œuvre la norme simplement pour les avantages directs que procurent les meilleures pratiques. D'autres font le choix de la certification pour prouver à leurs clients qu'ils suivent les recommandations de la norme. L'ISO ne fournit pas de services de certification.

En savoir plus sur la certification selon les normes de systèmes de management.

De nombreuses organisations dans le monde sont certifiées à ISO/IEC . Pour en savoir plus, consultez l'Étude ISO.