Politique de sécurité et ISO 27001/27002

1. Politique de sécurité : quelle référence ?

Le document le plus important lors de l' élaboration d'une politique de sécurité est celui définit dans l'**ISO 27001** comme **Politique du SMSI**, car dans la majorité des cas, la politique de sécurité de l'information au sien d'une entité correspond bien à la politique du SMSI.

2. Définition de la politique de sécurité d'après la norme ISO 27001/27002

Si on parcourt les normes ISO 2700x on trouvera que : tout d'abord le mot **Politique d'après** ISO 27000:2009 :

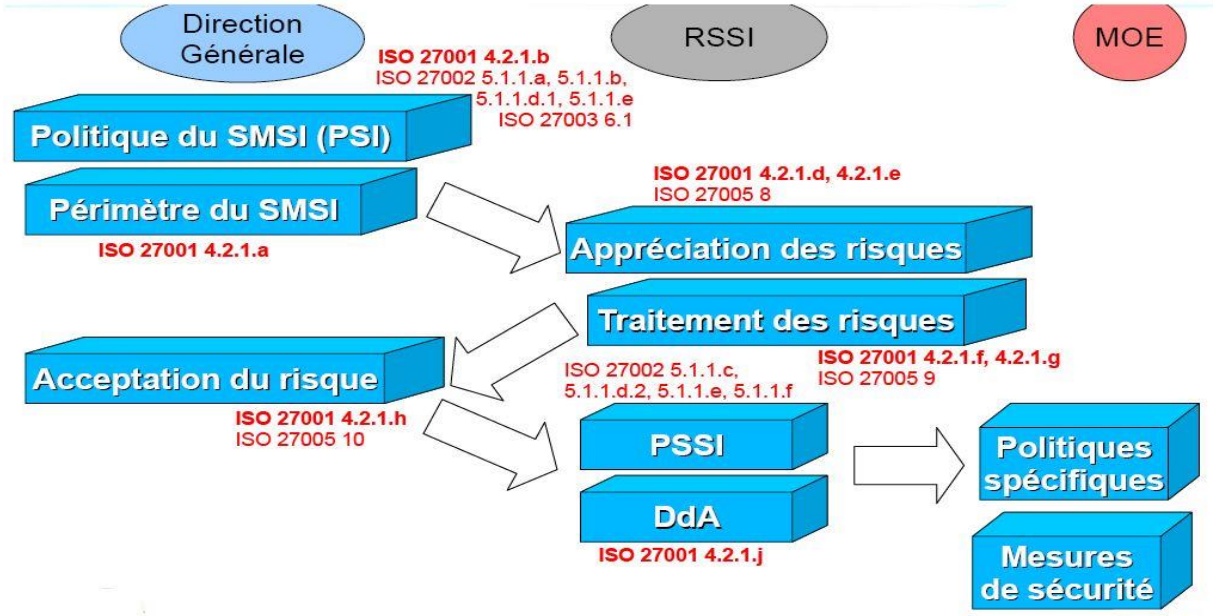
- **Policy** (ISO27000 **2.28**) : Overall intention and direction as formally expressed by management.

Alors que le mot **sécurité** de l'information signifie :

- **Information Security** (ISO27000 **2.19**) : "Preservation of Confidentiality, Integrity and Availability of Information … In addition, other properties such as authenticity, accountability, non repudiation and reliability can also be involved".

3. Pré requises relatifs à l'ISO 27001 et 27002 liés à la politique de sécurité

Le schéma suivant résume les différents paragraphes de l'ISO 27001 et 27001 pour la mise en place d'une politique de sécurité :



On remarque donc qu'on a plusieurs politiques de sécurité validées à des niveaux hiérarchiques différents :

a) PSI : **politique de du SMSI** (ISO 27001 **4.2.1.b**) ou politique de sécurité de l'information, et qui est validée au niveau de la direction générale, et qui doit être lisible et compréhensible par tous les membres du comité de direction, et par suite par toute l'entreprise. Et ne doit changer sur le fond que lorsque la stratégie de l'organisme.

Elle doit aussi inclure les critères d'acceptation des risques (ISO 27001 **4.2.1.c.2**) et doir permettre aussi de déterminer les critères d'évaluation des risques manquent régulièrement. Elle est encore aval de la direction permet d'acquérir la légitimité pour agir et faire la PSSI. Et enfin il se peut qu'elle soir revalidée ou mise à jour lors chaque revue de direction.

b) PSSI : **politique de sécurité des systèmes d'information** (ISO 27001 **4.2.1.b**), validés au niveau de la RSSI.

c) Les politiques spécifiques validées au niveau de la MOE.

Exemples :

- Politique de contrôle d'accès (ISO 27002 11.1.1)
- Politique de conservation des données nominatives (ISO 27002 15.1.4)
- Politique de gestion des enregistrements (ISO 27002 15.1.3)
- Politique d'échange d'information avec les tiers (ISO 27002 6.2.3)
- Politique d'accès pour les télémaintenances (ISO 27002 11.4.4)
- Politique de maniement des clés-mémoire USB (ISO 27002 10.7.1) … etc.

4. Communication de la politique de sécurité :

Une fois établie, la politique de sécurité de l'information doit être communiquée à tous (ISO27001 5.1 d). Elle doit être courte et synthétique donc affichable.

Les politiques spécifiques ne sont communiquées qu'aux destinataires ayant besoin de les connaître.