Politique de sécurité, ISO 2700x et EBIOS 2010

1. Politique de sécurité : quelle référence ?

Les documentsutileslors de l'élaboration d'une politique de sécurité ou d'une **Politique du SMSI** sont les standards **ISO 27001**et **ISO 27002** ainsi que **EBIOS.** Dans la majorité des cas, la politique de sécurité de l'information au sein d'une entité correspond bien à la politique du SMSI.

2. Définition de la politique de sécurité

2.1 Définition de la PSSI 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".

2.2 Définition de la PSSI d'après EBIOS :

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme.

Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel réglementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

Le guide PSSI édité par la DCSSI a pour objectif majeur l'accompagnement des responsables de sécurité dans l'élaboration d'une politique de sécurité d'un ou des systèmes d'information au sein de leur organisme.

3. Thèmes relatifs à l'ISO 2700x pour la rédaction d'une politique de sécurité

La norme **ISO 27001** offre **un modèle général** (un cadre) pour la détermination, la mise en œuvre, l'exécution, le contrôle, l'évaluation, le maintien et l'amélioration d'un système de gestion documenté en matière de sécurité de l'information (ISMS - information security management system). Alors que l'**ISO 27002** contient un **aperçu détaillé** des mesures de gestion possibles.

Le tableau suivant présente, sans entrer dans les détails, les principales mesures et politiques de gestion cadrant avec l'ISMS de l'institution. Sur base des thèmes mentionnés ici, des **documents de politique spécifiques** (« policies ») peuvent être rédigés.

Thème	Objective de la politique
Organisation de la sécurité de l'information	La **politique** d'organisation de la sécurité de l'information a pour objectif de gérer la protection de l'information au sein de l'institution.

Gestion des ressources	La **politique** de gestion des ressources a pour objet le maintien d'une protection adéquate de ces ressources.
Sécurité liée aux collaborateurs tant interne, qu'externe	Cette **politique** vise à mettre à profit l'expérience des collaborateurs et à maintenir à niveau leurs connaissances dans le but de promouvoir la sécurité de l'information.
Sécurité physique et protection de l'environnement	Cette **politique** a pour but : • de prévenir l'accès physique non autorisé ou inutile à l'information et aux systèmes d'information afin de limiter la prise de connaissance non autorisée, l'altération ou le vol d'informations ; • de prévenir les dommages aux systèmes d'information ou leur perturbation.
Gestion opérationnelle	Cette **politique** vise à garantir une manipulation et un fonctionnement corrects et sûrs des équipements des systèmes d'informations.
Sécurité d'accès logique	L'objectif de cette **politique** est la maîtrise de l'accès aux informations et aux processus d'entreprise conformément aux besoins fonctionnels et aux exigences en matière de sécurité.
Développement et maintenance de systèmes	L'objectif de cette **politique** est d'assurer la protection adéquate des systèmes utilisés et ce tout au cours de leur vie.
Gestion d'incidents relatifs à la sécurité de l'information	L'incident response team (IRT) a pour mission de réagir de façon appropriée aux incidents de sécurité. Cette équipe est chargée de réduire au maximum les dommages résultant d'incidents de sécurité et de perturbations, d'effectuer le monitoring de

	tels incidents et de proposer des améliorations sur la base de l'expérience acquise.
Gestion de la continuité	La **politique** de gestion de la continuité a pour but de pouvoir réagir à la perturbation des activités d'entreprise et de protéger les processus critiques d'entreprise en cas d'incidents importants. Une perturbation importante des activités opérationnelles de l'institution aurait un impact négatif sur le fonctionnement de la sécurité sociale en Belgique.
Respect	L'institution respectera les exigences légales et contractuelles en matière de sécurité auxquelles sont soumis les systèmes d'information utilisés.

On trouve donc deux types de politiques de sécurité validées à des niveaux hiérarchiques différents :

- **Politique de sécurité des systèmes d'information générale (**cf. ISO 27001 **4.2.1.b**) validés au niveau de la RSSI.

- **Les politiques spécifiques** validées au niveau de la MOE. Par exemple :
    - 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. Thèmes relatifs à EBIOS 2010 pour la rédaction d'une politique de sécurité

Chez EBIOS, les mesures de sécurité proviennent à la fois du [RGS] et de l'Annexe A de l'ISO 27001 (ou de l'ISO 27002). Sur base des thèmes mentionnés ici, on peut encore rédigés des **documents de politique spécifiques**.

4.1. Mesures de sécurité issues du [RGS]

Les mesures de sécurité suivantes proviennent des mesures de l'Annexe A de l'ISO 27001 (ou de l'ISO 27002). Les lignes de défense auxquelles elles contribuent ont été déterminées.

Thème	Description
Politique de sécurité	Il convient qu'un document de **politique** de sécurité de l'information soit approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés. Pour garantir la pertinence, l'adéquation et l'efficacité de la politique de sécurité de l'information, il convient de réexaminer la politique à intervalles fixés préalablement ou en cas de changements majeurs.
Organisation de la sécurité de l'information	Il convient que la direction soutienne activement la **politique** de sécurité au sein de l'organisme au moyen de directives claires, d'un engagement franc, d'attribution de fonctions explicites et d'une reconnaissance des responsabilités liées à la sécurité de l'information.
Gestion des biens	Il convient d'identifier, de documenter et de mettre en œuvre une **politique** permettant l'utilisation correcte de l'information et des biens associés aux moyens de traitement de

	l'information.
Sécurité liée aux ressources humaines	Il convient de définir et de documenter les rôles et responsabilités en matière de sécurité des salariés, contractants et utilisateurs tiers, conformément à la **politique** de sécurité de l'information de l'organisme.
Sécurité physique et environnementale	Cette **politique** a pour but de protéger les zones contenant des informations et des moyens de traitement de l'information par des périmètres de sécurité. Cette politique vise aussi la protection du matériel de manière à réduire les risques de menaces et de dangers environnementaux et les possibilités d'accès non autorisé.
Contrôle d'accès	Il convient d'établir, de documenter et de réexaminer une **politique** de contrôle d'accès sur la base des exigences d'exploitation et de sécurité.
Conformité	Il convient que les responsables s'assurent de l'exécution correcte de l'ensemble des procédures de sécurité placées sous leur responsabilité en vue de garantir leur conformité avec les **politiques** et normes de sécurité.

5. EBIOS vs ISO 2700x

5.1. Différence entre l'ISO 27001/27002 et le document base de connaissance d'EBIOS :

Les mesures de sécurité citées dans le document base de connaissance d'EBIOS n'est qu'une reprise de l'Annexe A de l'ISO 27001 et des chapitres de l'ISO 27002, il contient aussi de

mesures provenant des chapitres du RGS intégrant des clauses qui peuvent être interprétées comme des mesures de sécurité. Les lignes de défense auxquelles elles contribuent ont été déterminées.

5.2. Différence entre l'ISO 27005 et du guide méthodologique d'EBIOS :

Dans l'ISO 27005 on trouve des lignes directrices relatives à la gestion de risque. Mais on remarque l'absence de méthodologie spécifique, mais il dérive très fortement de la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité : Méthode de gestion des risques de l'ANSSI.) grâce à une importante implication de l'ANSSI dans sa définition.

6. Références :

- Guide méthodologique EBIOS 2010 : http://www.ssi.gouv.fr/IMG/pdf/EBIOS-1-GuideMethodologique-2010-01-25.pdf
- Bases de connaissances EBIOS 2010 : http://www.ssi.gouv.fr/IMG/pdf/EBIOS-2-BasesDeConnaissances-2010-01-25.pdf
- ISO 27001 Information technology – Security Techniques – Information security management systems – Requirements, International Organization for Standardization – ISO (2005).
- ISO 27002 Information technology – Code of practice for information security management systems – Requirements, International Organization for Standardization – ISO (2005).
- Présentation du Livre Blanc 2013 : (EBIOS vs ISO 27K) http://www.defense.gouv.fr/content/download/210592/2337422/file/Pr%C3%A9sentation%20du%20Livre%20Blanc%202013.ppt