Avertissements :
Le contenu de ce document est sous licence GPL. Le document est librement diffusable dans le contexte de cette licence. Toute modification est encouragée et doit être signalée à olivier[chez]thebaud.com
Les documents ou applications diffusées sur thebaud.com sont en l'état et sans aucune garantie ; l'auteur ne peut être tenu pour responsable d'une mauvaise utilisation (au sens légal comme au sens fonctionnel). Il appartient à l'utilisateur de prendre toutes les précautions d'usage avant tout test ou mise en exploitation des technologies présentées.

Objet :	**ISO 27001 // ISO 27002 (versions 2005)**	Date :	**28/10/2008**
		Version :	**1.0**

Pourquoi ce document ?
Faire une synthèse la plus abordable possible sur les normes ISO 27001/ISO 27002, leur utilité et leur approche.

Qu'est ce que la norme ISO 27001 (version 2005) ?

Cette norme récente, décrit les exigences pour la mise en place d'un système de management de la sécurité de l'information (SMSI).
Il existe notamment des systèmes de management de la qualité (ISO 9001 :2002), environnemental (ISO 14001 :2004), de la sécurité des denrées alimentaires (ISO 22000 :2005) et de l'informatique (ISO 27001 :2005).
Cela permet à une entreprise de choisir les mesures de sécurité afin d'assurer la protection des biens sensibles d'une entreprise, sur un périmètre défini.
La norme ISO27001 s'appuie sur les 11 chapitres (soit 133 points de mesure de l'annexe A) de la norme ISO27002 pour s'assurer de la pertinence des engagements de sécurité définis par le management.
Cette norme s'adapte à tout type d'entreprise, quelque soit le secteur d'activité, sa structure, sa taille et la complexité de son système d'information. L'application de cette norme passe par une démarche qualiticienne classique : la roue de Deming (Plan, Do, Check, Act = Plannifier, Mettre en oeuvre, Vérifier, Améliorer).
L'application de la norme ISO 27001, voire sa certification ne garantie pas un niveau de sécurité mais qu'un système de gestion de la sécurité informatique est en place et fonctionne (analyse des risques, pertinences des solutions, …).
C'est devenu un standard international, reconnu, concret, facilement applicable et utilisé par l'ensemble des entreprises ayant souhaité une sécurisation de leur systèmes d'information.
A savoir, le process « gestion de la sécurité » d'ITIL v3 est une mise en œuvre opérationnelle d'un chapitre de l'ISO 27001.

La certification ISO 27001

La certification est donc possible pour une entreprise quelle qu'elle soit : là aussi, la certification d'une entreprise ISO 27001 est encadré par des normes et des organismes accrédités. Les quelques avantages d'une certification : réduction des audits intermédiaire du SI (SOX, BALE, IOSA,….), accès aux appels d'offre internationaux,….

Qu'est ce que ISO 27002 (version 2005) ?

C'est un code de bonnes pratiques pour la gestion de la sécurité de l'information.
Anciennement ISO 17799 :2005, la référence ISO 27002 :2005 va devenir la référence normative.
Dans cette norme, les chapitres 4 à 15 listent les domaines qui peuvent être appliqués à l'entreprise : en fonction de ses contraintes légales, son domaine d'activité, sa structure,… Tous les points de mesure ou recommandations ne sont pas à appliquer nécessairement : cela dépend du contexte de l'entreprise.
Ces **11 chapitres** sont décrits dans le code de bonnes pratiques 27002 (version 2005) mais sont repris dans l'annexe A de la 27001 :2005 et font l'objet de points de 133 mesures.

Chap 4 : Appréciation et traitement des risques informatiques

Chap 5 : Politique de sécurité

Chap 6 : organisation interne et avec les tiers de la sécurité de l'information

Chap 7 : Gestion des biens

- Responsabilités relatives aux biens
- Classification des informations

Chap 8 : Sécurité liée aux ressources humaines

- Le recrutement
- Pendant le contrat
- La fin ou la modification du contrat

Chap 9 : Sécurité Physique et environnementale

- Zones sécurisées
- Sécurité du matériel

Chap 10 : Gestion de l'exploitation et des télécommunications

- Procédures et responsabilités liées à l'exploitation

- Gestion de la prestation de service par un tiers
- Planification et acceptation du système
- Protection contre les codes malveillants et mobiles
- Sauvegarde
- Gestion de la sécurité des réseaux
- Manipulation des supports
- Echange des informations
- Services de commerce électronique
- Surveillance

Chap 11 : Contrôle d'accès

- Exigences métiers relatives au contrôle d'accès
- Gestion de l'accès utilisateur
- Responsabilités utilisateurs
- Contrôle d'accès réseau
- Contrôle d'accès au système d'exploitation
- Contrôle d'accès aux applications et à l'information
- Informatique mobile et télétravail

Chap 12 : Acquisition, développement et maintenance des systèmes d'information

- Exigences de sécurité applicables aux SI
- Bon fonctionnement des applications
- Mesures cryptographiques
- Sécurité des fichiers systèmes
- Sécurité en matière de développement et d'assistance technique
- Gestion des vulnérabilités techniques

Chap 13 : Gestion des incidents liés à la sécurité de l'information

- Signalement des événements et des failles
- Gestion des améliorations et incidents

Chap 14 : Gestion du plan de continuité de l'activité

Chap 15 : Conformité

- Conformité avec les exigences légales
- Conformité avec les politiques et normes de sécurité, conformité technique
- Prises en compte de l'audit du SI

Dans la pratique ISO27002 ou ISO 27001 ?

Ces deux normes font l'objet d'améliorations continues, notamment grâce à l'activité de spécialistes Français reconnus dans le domaine de la sécurité informatique,. Ce sont des normes concrètes et applicables.

Améliorer la sécurité de son système d'information suppose de suivre la norme ISO 27001 :2005 et donc d'impliquer en tout premier lieu la Direction Générale de l'entreprise. Dans la pratique, la démarche vient du management de haut niveau pour s'appliquer sur tous les niveaux de la pyramide, la perception globale des enjeux et des risques pour l'exploitation de l'entreprise permet d'adapter les démarches de sécurisation du SI, ni trop, ni trop peu.

La norme ISO27002 :2005 est généralement suivie par les directions informatiques ou par des équipes techniques autonomes lorsque l'engagement de la direction générale n'est pas au rendez-vous. Dans la pratique, le périmètre couvert est inadapté dans la mesure où il est vu du point de vue la DSI et non en fonction des biens identifiés et nécessaires à l'exploitation de l'entreprise.

ISO 27005

Publiée en juin 2008, cette norme propose une approche dans l'appréciation des risques informatiques d'une entreprise.
Les notions basiques Confidentialité / Disponibilité / Intégrité sont confrontées aux menaces afin d'en hiérarchiser l'importance, de décider du traitement du risque en fonction des impacts, de leur probabilité d'occurrence.
Autrement dit la norme propose, à partir du contexte de l'entreprise, une appréciation des risques (identification, estimation) et une évaluation avec quatre traitements possibles de ces risques : refuser le risque, réduire le risque, transférer le risque, conserver le risque.
Cette norme peut être un sous-ensemble de la norme ISO 27001, spécifique à la gestion des risques mais est applicable de manière concrète et autonome.
De nombreuses méthodes permettent d'effectuer cette démarche d'appréciation des risques : eBios, Méhari,…

Evolutions à venir sur ce document :
Imbrication avec ITIL
Questionnaire XL