

*NOUVEL ISO  
LISO NOUVEAU*

L' ISO/IEC 17799 poursuit lentement mais sûrement son évolution afin d'être plus opérationnel dans les organismes et surtout s'adapter aux nouveaux contextes technologiques et organisationnels dans lesquels les systèmes d'information évoluent aujourd'hui.

La version « officielle » adoptée comme standard international sous une procédure spéciale dite de « fast track » en décembre 2000 (adoptée avant d'être révisée par les commissions nationales de l'ISO) connaît sa troisième évolution :

- Juin 2003 : première version (CD : Committee Draft) de l'ISO/IEC 17799 CD (2<sup>nd</sup> édition) proposée aux groupes de travail nationaux pour approbation le 9 septembre. 22 votes d'approbation - 4 votes contre.
- Février 2004 : après une réunion de tous les groupes internationaux , organisée à Paris en octobre par la Commission Normative de la Sécurité des Systèmes d'Information de l'AFNOR , une seconde version de ce document a été proposée en deuxième lecture. Cette nouvelle mouture a été adoptée par 19 pays. 3 ont désapprouvé cette version et 2 pays se sont abstenus.
- Le 17 juin 2004 : Le secrétariat du JTC1/SC27 (Comité technique qui gère les normes et standards de l'ISO concernant les techniques de sécurité informatique) a proposé une nouvelle version « Final Committee Draft » ISO/IEC FCD 17799 de cette deuxième édition du standard.

Cette ébauche finale est proposée pour amélioration et vote, aux membres des commissions nationales pour la prochaine réunion du JTC1/SC27 qui aura lieu à Fortaleza (Brésil) en octobre 2004.

Un an après sa première modification, ce document reste donc toujours pour étude et est sujet à modifications. Néanmoins, pour les clients d'Asséphira Consulting qui nous font confiance pour mettre en oeuvre ces recommandations ou qui ont simplement suivi ses formations, voici les principales évolutions et améliorations.

La première constatation est que le standard s'enrichit d'une quarantaine de pages écrites en plus petit ... on peut donc s'attendre soit à de grands bouleversements ou à beaucoup d'enrichissement ☺

Plus sérieusement, les deux principaux manques (constatés par l'auteur) dans la première version de l'ISO 17799:2000 sont enfin abordés :

- L'évaluation des risques en préalable à la mise en oeuvre des recommandations (contrôles) spécifiés dans ce guide de bonnes pratiques.
- Le traitement des incidents.

Bien sûr, d'autres standards traitent plus dans le détail ces deux aspects. L'ISO guide 73 :2002 et l'ISO/IEC TR 13335 pour la gestion des risques et la nouvelle version de l'ISO/IEC TR 18044:2004 pour le traitement des incidents (comme quoi les groupes de travail du JTC/SC27 de l'ISO sont très actifs).

Cette deuxième édition de l'ISO 17799 fait aujourd'hui référence et se rapporte à ces autres standards dans son chapitre « Termes et Définitions ».

Aussi, une page entière est consacrée à l'évaluation des risques et au traitement des risques. (pour ceux qui connaissent la numérotation de l'ISO 17799, ceci devient le chapitre 4 du standard).

Sinon dans l'introduction (chapitre 1) quelques modifications ont été apportées. Sur la forme, un effort certain de vulgarisation des concepts de la sécurité auxquels s'ajoute une internationalisation de l'anglais permettent une lecture plus aisée et plus fluide du document.

Par contre sur le fond, on peut constater qu'il sera difficile de trouver un consensus sur la sélection des contrôles et les points de départ pour implémenter la sécurité de l'information. En effet, ces deux sous-chapitres changent à chaque version, sans logique apparente - « débats d'experts ».

Les « facteurs critiques de succès » s'enrichissent de nouvelles propositions intéressantes, comme la gestion des incidents.

Le principal changement de cette 2<sup>nd</sup> édition de l'ISO 17799 est la structure même du document :

- - **11 Chapitres de contrôles** de sécurité (*précédemment 10 domaines de sécurité*)
- - **39 Catégories principales** de sécurité (*précédemment 36 objectifs de sécurité*)

Le terme « Chapitre » ne doit pas être considéré acquis - En effet après avoir été « Domaine » dans la version 2000 et « Aire - Areas » dans la première ébauche de la 2<sup>nd</sup> édition, « chapitre » devient « Clauses » deux ligne plus loin dans le document ...

Donc, les 11 clauses ou chapitre de la future version de l'ISO/IEC 17799 sont :

Numéro	Clause (*)	Nombre de catégories	Nombre de Contrôles
5	Politique de sécurité de l'information	1	2
6	Organisation de la sécurité de l'information	2	11
7	Gestion des Actifs	2	5
8	Sécurité Ressources Humaines	3	9
9	Sécurité physique et environnementale	2	13
10	Gestion opérationnelle et communications	10	30
11	Contrôle d'accès	7	25
12	Acquisition des systèmes d'information, développement et maintenance	6	16
13	Gestion des incidents de sécurité de l'information	2	5
14	Gestion de la continuité d'affaires	1	5
15	Conformité	3	10
		<b>39</b>	<b>131</b>

(\*) = traduction littérale - A interpréter pour un français correcte

Pour ceux qui en feront la demande à l'adresse suivante ( [information@assephira.com](mailto:information@assephira.com) ), un tableau comparatif entre les domaines, objectifs et points de contrôles leur sera fourni.

Toutefois, avant de s'enthousiasmer rapidement sur la gestion des incidents de sécurité de l'information ( = le nouveau chapitre ), ce sujet est traité seulement sur quatre pages qui correspondent à surtout un regroupement de contrôles éparpillés dans la version 2000 de l'ISO (ex 6.3 ou 8.1.3 par exemple).

Alors, pour ceux qui se préoccupent plus particulièrement de cet aspect, il reste donc préférable de se reporter plutôt aux 60 pages de l'ISO/IEC TR 18044:2004 (Information security incident management).

Asséphira Consulting compte mettre à profit la période estivale pour s'investir particulièrement dans cette proposition de standard et participer activement à son amélioration.