

MANAGEMENT DE LA SECURITE DE L'INFORMATION

FICHE 1 | NORME ISO/IEC 27000

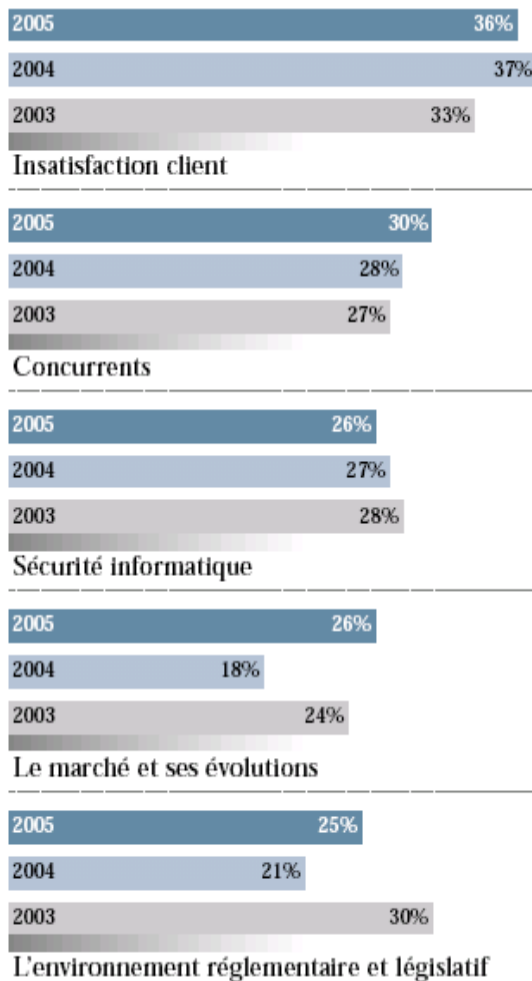


ISO/IEC 27000

CONTEXTE

Depuis quelques années, le volume d'information ne cesse d'augmenter et les systèmes informatiques participent à cette accélération en apportant les bénéfices de la dématérialisation. Les entreprises sont aujourd'hui connectées en interne mais aussi dans le monde entier. De ce fait, leur système d'information est accessible de l'extérieur pour leurs fournisseurs, clients, partenaires et administrations. L'accessibilité par l'extérieur entraîne la vulnérabilité vis à vis d'attaques potentielles – l'attaque de certaines banques par hameçonnage (*phishing*) en est un exemple concret. Des risques

tels que les vols d'informations, l'usurpation d'identité, l'intrusion et l'utilisation de ressources systèmes ou encore la mise hors service des systèmes de ressources informatiques sont donc bien présents aujourd'hui. La sécurité informatique est un des cinq risques majeurs recensés par l'entreprise (cf. étude Protiviti).



L'investissement dans des mesures de protection et de sécurité est donc indispensable et la mise en œuvre d'un plan de sécurité pour garantir la disponibilité, l'intégrité et la confidentialité de l'information s'impose à toutes les entreprises. Ces plans de fiabilité s'appliquent grâce à des normes telles qu'ISO/IEC 27001.

(5 risques majeurs de l'entreprise - Etude Risk Management, Protiviti/TNS Sofres)

À QUI S'ADRESSE CE MANAGEMENT ?

La norme ISO/IEC 27001 peut être mise en œuvre autant dans le cadre d'un grand groupe que celui d'une PME (les TPE sont également concernés).

Pour une PME/PMI, ou un petit organisme, son utilisation supposera de gérer une check-list des thèmes de sécurité à traiter et des contrôles à mettre en œuvre afin de constituer une politique de sécurité. Notons que pour que l'approche soit pertinente, il faut commencer la démarche par une évaluation des risques principaux. L'intérêt de cette norme est multiple. On peut y voir un avantage commercial (appel d'offre exigeant un niveau de sécurité conforme aux normes) : grâce à cette norme, on instaure aussi un climat de confiance vis à vis de ses partenaires extérieurs, actionnaires... Enfin, l'intérêt principal est la fiabilité et la sécurité au sein de son système d'information. Plan de continuité d'activité, maîtrise des dépenses informatiques, responsabilisation des collaborateurs.

POURQUOI UTILISER UNE NORME EN SECURITE DE L'INFORMATION ?

ISO/IEC 27001 ne porte pas sur des techniques d'analyse des risques mais sur la définition d'une politique de sécurité de l'information et sa mise en œuvre. C'est une formalisation en matière d'approche de la sécurité, une prise de conscience des risques et une mise en place de procédures pour la gestion de la sécurité.

- Liste des étapes
- Établissement d'un climat de confiance
- Sécurisation les partenariats
- Préférence pour les échanges électroniques
- Meilleure gestion du risque
- Réductions des coûts
- Économies d'échelle
- Diminution des primes d'assurances
- Appels d'offres exigeant la conformité à la norme (Europe)
- Image de marque vis à vis de la sécurité
- Conformité (SOX, C198, HIPPA)

ORIGINE DE LA NORME ISO/IEC 27000

Cette norme définit les exigences pour le management de la sécurité de l'information. À la base même de celle-ci, la norme britannique BS 7799 créée en 1995 puis révisée et divisée en 2 parties en 1999, BS 7799-1 et BS 7799-2.

La BS 7799-1 (*Code of Practice for Information Security Management*), adoptée par l'ISO, est devenu l'ISO 17799 en 2000. La BS 7799-2 (*Information Security Management systems – Specification with Guidance for Use*) a été révisée en 2002.

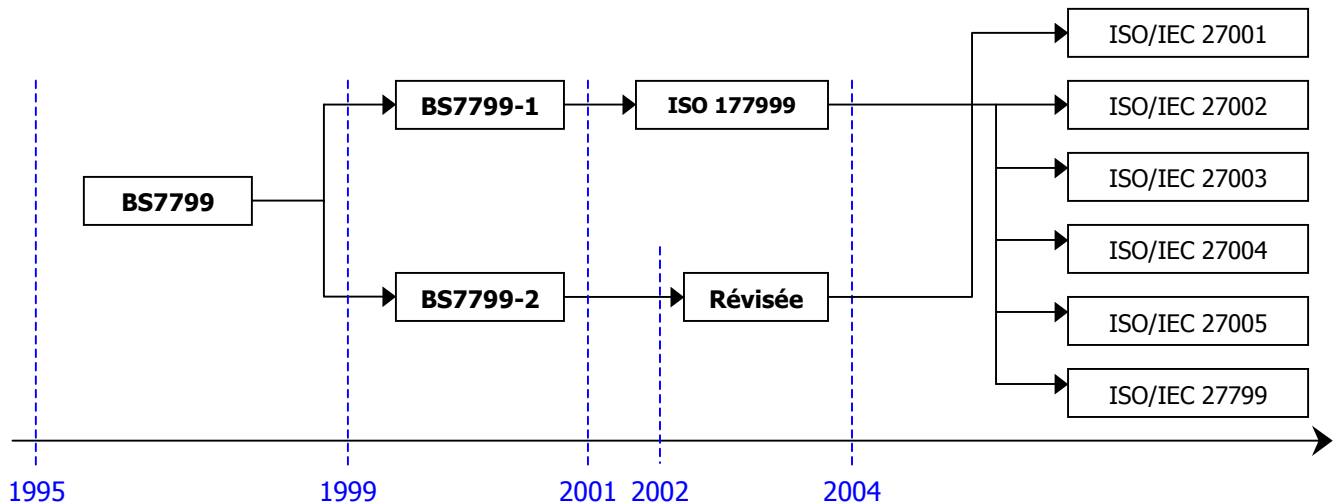
Depuis 2001, la norme ISO 17799 est en vigueur qui comprend la politique de sécurité, l'organisation de la sécurité, la sécurité du personnel, le contrôle d'accès, le développement, la maintenance etc.

Une version contenant des évolutions significatives a été publiée en 2005 contenant entre autres un chapitre sur l'analyse de risques.

En 2005 est créée une nouvelle famille de norme ISO/IEC 27000 comprenant :

- ISO/IEC 27001 : Système de management de la sécurité de l'information (SMSI) (en vigueur)
- ISO/IEC 27002 : Renumérotation de l'ISO 17799 (2007)
- ISO/IEC 27003 : Implémentation (en développement)
- ISO/IEC 27004 : Métriques et mesures (en développement)
- ISO/IEC 27005 : Management du risque (ISO 13335-2)
- ISO/IEC 27799 : ISO 17799 pour la santé (en développement)
-

ISO/IEC 27002 est donc un cadre général de bonnes pratiques et d'audit qui nécessite d'être accompagné d'un référentiel d'évaluation pour être directement exploitable au plan opérationnel.



MISE EN ŒUVRE

ISO/IEC 27001 permet aux entreprises et aux administrations d'obtenir une certification qui atteste de la mise en place effective d'un système de management de la sécurité de l'information (SMSI). Cette norme garantit aux parties prenantes (clients, actionnaires, partenaires, etc.) que la sécurité des systèmes d'information a été sérieusement prise en compte et que l'entreprise s'est engagée dans une démarche d'amélioration constante.

Deux problématiques se posent alors :

- Comment mettre en place un système de management de la sécurité de l'information (SMSI) conforme à la norme ISO/IEC 27001 ?

- *Définir un responsable projet*
- *Définir les budgets*
- *Analyse de risques*
- *Implication de la direction*
- *Politique de sécurité*
- *Construction du système de management*
- *Sensibilisation ou formation des collaborateurs*
- *Audits internes*
- *Mise en œuvre du PDCA*

- Comment auditer un SMSI selon les critères de l'ISO/IEC 27001 ?

Un organisme de certification vient vérifier la conformité du système de management au référentiel ISO/IEC 27001. À l'issue de cet audit, et si l'entreprise répond aux exigences de la norme, l'organisme de certification délivre un certificat valable pour une durée de trois ans.

Principes équivalents à tout audit :

- Analyse du SMSI selon un plan d'audit pré-établi
- Analyse des pratiques de l'entreprise en fonction des procédures et des exigences du référentiel
- Détection des écarts significatifs (Non conformité ou remarque)
- 2 Audits de suivis durant la période de 3 ans

CERTIFICATION

- Qui sont les corps accrédités de certification pour la norme ?

Il y a un nombre de plus en plus important d'organisme, parmi lesquels : LSTI, BSI, Certification Europe etc. Tous les organismes accrédités sont répertoriés sur ce site : www.xisec.com

QUELQUES EXEMPLES DE METHODES D'ANALYSE DE RISQUES

Les standards sont des normes non entérinées par un organisme officiel de normalisation, mais qui se sont imposés par la force des choses parce qu'ils font consensus auprès des utilisateurs qui les adoptent. Toutefois, la méthode d'analyse des risques doit être reproductible (aspect normatif).

- **E**BIOS : **E**xpression des **B**esoins et **I**dentification des **O**bjectifs de **S**écurité, est une méthode publiée par la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) en version 1.02 de février 1997. Cette méthode permet, lors de la phase de spécification de besoins d'un système, d'identifier les besoins de sécurité de ce système (autre méthode du DCSSI : PSSI, TDBSSI, PC² etc.).
- **R**SSI pilote : Management des risques des systèmes d'information, outil de management et de communication, spécialement conçu pour favoriser les développements de bonnes pratiques de sécurité dans la perspective de la certification ISO 27001.
- **M**éhari (CLUSIF) : **M**éthode **H**armonisée d'**A**nalyse de **R**isques, c'est une base méthodologique et un ensemble d'outils permettant de s'adapter au contexte.

Méthode de scoring : Le scoring est un outil qui peut être utilisé dans une analyse de risques.

Toutes les méthodes : COBIT, CRAMM, EBIOS, IPAK, MARION, MEHARI, MELISA, MG3, MG9, MV3, OCTAVE

DEGRE D'APPLICABILITÉ

Normes - Standards sécurité de l'information : où en êtes-vous ?

Nom et version	Description	Applicabilité/portée	Spécification	Evolution
<u>BS 7799</u>				
7799-1	Code of practice for information security management	Immédiate/nationale	Certifié ISO 17799 en 2000	Aucune
7799-2	Information Security Management systems – Specification with guidance for use	Immédiate/nationale	Révisée en 2002	Aucune
<u>ISO 17799</u>				
17799	Code de bonne pratique pour la gestion de la sécurité de l'information	Immédiate/internationale	publiée le 6 octobre 2005	Profils sectoriels tels que la santé etc. ¹
<u>ISO 27000</u>				
27001	systèmes de gestion de sécurité de l'information	Immédiate/internationale	Publiée le 14 octobre 2005	Stable
27002	Renumérotation de l'ISO 17799	Immédiate/internationale	2006	Stable
<u>METHODES D'ANALYSE DES RISQUES</u>				
EBIOS	Expression des B esoins et I dentification des O bjectifs de S écurité (DCSSI)	Non normalisée	Version 2	
RSSI Pilote	Management des risques des systèmes d'information (RSSI Pilote)	Non normalisée	En vu de la certification ISO 27001	
Méhari	ME thode H armonisée d' A nalyse de R isques (clusif)	Non normalisée « évolution envisagée pour certification ISO 27001 »	Version 3	

¹ Profils sectoriels :

- santé (développement de l'ISO 27799)
- automobile
- aéronautique