DOSSIER TECHNIQUE

MANAGEMENT DE LA SECURITE DE L'INFORMATION

UNE APPROCHE NORMATIVE : BS7799-2

Décembre 2004

Groupe de Travail BS7799-2/SMSI

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS
30, rue Pierre Semard, 75009 PARIS
Tél. : +33 153 25 08 80 – Fax : +33 1 53 25 08 88
e-mail : clusif@clusif.asso.fr - Web : http://www.clusif.asso.fr

REMERCIEMENTS

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Régis BOURDONNEC	**BNP Paribas - Cardif**
Philippe CHAILLEY	**Ercom**
Anne COAT	**Silicomp – AQL**
Christian GATEAU	**France Telecom – Transpac**
Stéphane GEYRES	**Ernst & Young**
Frédéric HUYNH	**Ernst & Young**
Jean ISNARD	**Euronext**
Laurent MARECHAL	**Silicomp - AQL**
Fred MESSIKA	**Lynx Technologies**
Béatrice RENARD	**France Telecom**
Paul RICHY	**France Telecom**
Hervé SCHAUER	**HSC**
Isabelle WAS	**Deloitte**

Nous remercions aussi les membres ayant participé à la relecture.

TABLE DES MATIÈRES

1. INTRODUCTION

1.1 Objectif de ce document

L'objectif de ce document est de présenter au lecteur, à travers la norme britannique BS 7799-2:2002, une démarche de mise en œuvre d'un système de management de la sécurité de l'information dans les organismes.

1.2 Lectorat

Les documents du CLUSIF sont généralement à destination des RSSI et des DSI. L'élargissement du périmètre à l'ensemble de l'information (et non plus au système d'information) dans le cadre ISO17799 ou BS7799 nous incite à proposer une cible sensiblement plus large :

- comme pour le document ISO 17799, tous les professionnels de la sécurité de l'information,
- mais aussi tous les professionnels d'organismes impliqués dans la sécurité : directeurs sécurité, secrétaires généraux,
- les Directions Générales dans la mesure où l'on parle de certification, ce qui implique une décision et un engagement au plus haut niveau de l'organisme.

1.3 Terminologie

Pour l'ensemble du document, on entend par « organisme » : toute entité (entreprise, administration, organisation, association, etc.) ainsi que tout sous-ensemble de celle-ci (filiale, métier, géographique, etc.).

2. SYSTÈME DE MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION (SMSI)

2.1 Définition d'un SMSI

Un SMSI est un ensemble d'éléments interactifs permettant à un organisme d'établir une politique et des objectifs en matière de sécurité de l'information, d'appliquer la politique, d'atteindre ces objectifs et de contrôler l'atteinte des objectifs.

La politique de sécurité de l'information donne les grandes orientations de l'organisme en matière de sécurité de l'information et fixe des objectifs quantifiés. Elle est officiellement formulée par la Direction, qui s'engage à fournir les moyens nécessaires pour atteindre ces objectifs.

Elle est cohérente avec les objectifs métier de l'organisme, et avec les besoins de ses clients et partenaires. Elle est communiquée au sein de l'organisme, sa compréhension par les intervenants internes et externes est vérifiée, elle est revue de façon périodique (en général annuellement) pour rester en adéquation avec les objectifs globaux de l'entité.

Le SMSI est établi, documenté, mis en œuvre et entretenu. Son efficacité est mesurée par rapport aux objectifs de l'entité, et cette mesure permet d'améliorer en permanence le SMSI.

Le SMSI est cohérent avec les autres systèmes de management de l'entité, notamment avec les systèmes de management de la qualité, de la sécurité des conditions de travail, et de l'environnement.

Le SMSI inclut donc au minimum :

- des éléments documentaires (politique, description des objectifs, cartographie des processus impactés, des activités de sécurité, et des mesures),
- la description de la méthode d'analyse des risques utilisée,
- les processus impliqués dans la mise en œuvre de la sécurité de l'information,
- les responsabilités relatives à la sécurité de l'information,
- les ressources nécessaires à sa mise en œuvre,
- les activités relatives à la sécurité de l'information,
- les enregistrements issus des activités relatives à la sécurité de l'information,
- les (relevés de) mesures prises sur les processus,
- les actions relatives à l'amélioration de la sécurité de l'information.

L'existence d'un SMSI dans l'organisme permet de renforcer la confiance dans le mode de gestion de la sécurité de l'information.

2.2 Comment mettre en place un SMSI ?

L'adoption d'un SMSI est une décision stratégique pour un organisme. Sa conception, son implémentation, et son organisation dépendent des besoins de sécurité de l'organisme. Ces besoins sont eux-mêmes fonction du métier de l'organisme, des exigences de sécurité (client/interne) qui en résultent, des processus mis en place, de sa taille et de sa structure.

Pour initialiser une démarche de SMSI, l'organisme doit :

- déterminer le périmètre (fonctionnel, géographique, organisationnel, etc.) concerné,
- identifier parmi les processus de ce périmètre, ceux qui sont concernés par la sécurité de l'information, et leurs risques associés,
- déterminer les exigences (objectifs, référentiels, méthodes, etc.) nécessaires pour assurer la sécurité des processus,
- définir les mesures de sécurité nécessaires pour se conformer aux exigences exprimées.

Les processus nécessaires au SMSI comprennent ceux relatifs :

- aux activités de management,
- à la mise à disposition de ressources,
- à la réalisation des produits/services,
- aux mesures et à l'amélioration.

Si l'organisme décide d'externaliser un processus ayant une incidence sur la sécurité, il doit en assurer la maîtrise et mentionner dans le SMSI les moyens de cette maîtrise.

3. LA NORME BS7799-2:2002

3.1 Historique

Au début des années 1990 de grands groupes britanniques (BT, Shell, Marks & Spencer, Nationwide Building Society, etc.) se sont rencontrés au sujet de l'assurance des échanges commerciaux en ligne. L'objectif était alors de proposer un nombre réduit de mesures clés, liées à la sécurisation de l'information, que toute entreprise serait à même de mettre en œuvre. Le Département des Transports et de l'Industrie britannique (DTI) tenait à ce que ces dix mesures clés soient identifiées et présentées dans une norme de gestion de la sécurité de l'information, il parraine donc la rédaction d'une première version de ce document - dans le respect des normes et standards du BSI (British Standards Institute).

En 1991 un projet de « Code de bonnes pratiques » a été réalisé. Il recommandait en particulier la formalisation d'une politique de sécurité de l'information. Cette dernière devait intégrer au minimum 8 conditions (au niveau stratégique et opérationnel) ainsi qu'une condition de "conformité" – et être maintenue à jour. Ceci se traduit par l'augmentation du nombre de responsables de la sécurité de l'information chargés de s'assurer de la conformité en accord avec la politique de l'entreprise.

En 1995, la BS 7799 présente 10 mesures clés intégrant 100 mesures détaillées potentiellement applicables.

En 1998, il est adjoint une partie 2 à la BS 7799 dans laquelle plus de 100 mesures de sécurité sont détaillées selon le principe du management de la sécurité du système d'information (Information Security Management System - ISMS) et fondée sur une approche de maîtrise des risques. La motivation de la partie 2 a été de mettre à disposition les fondements d'un schéma de certification permettant d'attester la conformité à ce qui est devenu la partie 1.

La priorité a été donnée à l'intégration des problématiques d'e-business en les structurant dans la partie 1 de la BS 7799, pour que cette norme puisse être présentée à l'ISO. Le nombre de mesures passe alors à 127.

La BS7799-1:1999 est reconnue après une réflexion au niveau international et devient alors la norme internationale ISO / IEC 17799 en 2000.

La BS 7799-2:2002 remplace la version de 1998 de la BS7799-2 pour mieux s'inspirer des autres systèmes de management déjà existants tels que BS EN ISO 9001:2000 et BS EN ISO 14001:1996 afin de permettre une implémentation intégrée des différents systèmes de management.

3.2 Description de la norme

3.2.1 Périmètre de la norme

La norme BS7799-2:2002 définit des exigences pour planifier, implémenter, contrôler et améliorer un SMSI. Elle s'applique à tout organisme, mais aussi à toute unité opérationnelle, tout département au sein d'une entreprise ou tout site géographique, dès lors que celui-ci a la responsabilité de la protection de son information et donc dispose d'un responsable identifié.

Au sein de l'organisme la norme concerne, aussi bien le système informatique, que les aspects humains et physiques, les processus, etc.

3.2.2 Structure de la norme

La norme[1] est constituée de 2 parties distinctes :

- le corps du document rappelle et définit les concepts de SMSI, le modèle de « Plan, Do, Check, Act » (PDCA, cf. 3.4) et insiste sur les tâches et l'implication du management,
- les annexes (A, B, C et D) du document.

En dehors des chapitres introductifs de toute norme ISO (§1 Champs d'application, §2 Références, §3 Définitions), la norme aborde les thèmes suivants :

- la notion de SMSI au travers de l'approche « processus » et du modèle PDCA (§0) ainsi que le parallèle entre SMSI et les autres systèmes de management (qualité, environnement) (§0),
- les jalons et tâches clés de la dynamique d'un SMSI (§4),
- les implications et les responsabilités du management associées à un SMSI (§5 et 6),
- l'amélioration continue du SMSI (§7).

L'annexe A (normative) établit les objectifs de maîtrise de la sécurité en reprenant les thèmes directeurs de toutes les sections du document ISO17799. Le terme « normatif » signifie que cette annexe est d'application obligatoire pour conformité à la norme BS7799-2.

L'annexe B (informative) présente de manière générique les actions à mettre en œuvre à chaque étape du cycle PDCA.

Enfin, les annexes C et D, également informatives, précisent respectivement les similitudes entre les différents systèmes de management (ISO 9001:2000, ISO 14001:1996 et BS7799-2:2002) et les modifications survenues sur les versions antérieures de la norme dans BS7799-2:2002.

3.3 Reconnaissance internationale

Comme le précise le tableau ci-après, à la date de rédaction de ce document, la norme BS7799-2:2002 est soit :

- utilisée directement dans sa version britannique par les organismes, sans avoir été adoptée formellement par les instances de normalisation nationales,
- reprise à l'identique, i.e. avec un numéro de norme national, comme par exemple en Australie, en Nouvelle-Zélande ou en Afrique du Sud,
- reprise au niveau national, avec adaptation, comme par exemple en Espagne, au Danemark ou en Suède.

[1] Au-delà de la définition issue d'un dictionnaire, nous pouvons définir une norme comme étant un document de référence issu d'un consensus d'acteurs du marché et reconnu au niveau local, régional, national ou international.

Pays[2]	Norme
Asie	
Japon	JIS X 5080:2002: “Information technology – Code of practice for information security management” (ISO17799) JIS Q 2001:2001 Guidelines for Development and Implementation of Risk Management System (qui joue le role de la BS7799-2) JIPDEC Certification (Schéma de certification réglementaire)
Océanie	
Australie Nlle Zélande	AS/NZS 7799.2:2003: Information security management - Specification for information security management systems
Europe	
Danemark	DS484-2
Espagne	UNE 71502: "Requisitos para la gestión de la seguridad de TI" Norme basée sur la BS7799-2:2002 comprenant des éléments contextuels supplémentaires, traitant de la protection des données personnelles. Il existe un schéma de certification.
Suède	SS 627799.2:2003 Information security management - Specification for information security management systems Il existe un schéma de certification.
Afrique	
Afrique du Sud	SABS7799-2

A décembre 2004, plus de 1000 certificats BS7799-2 ont été recensés à travers le monde. Ce nombre représente une augmentation de plus de 100% par rapport à début 2003.

Leur répartition géographique est de 47% au Japon, environ 18% en Royaume Uni, 14% dans le reste de l’Europe, 17% en Asie (hors Japon), 2% pour les Amériques et 2% Pour le reste du monde. Aucun certificat n’a été délivré en France.

Comme pour les normes ISO9000, ces certificats portent le plus souvent sur un sous-ensemble des différents organismes. De ce fait, certains organismes peuvent détenir plusieurs certificats. Ces différents points sont développés au chapitre 4.

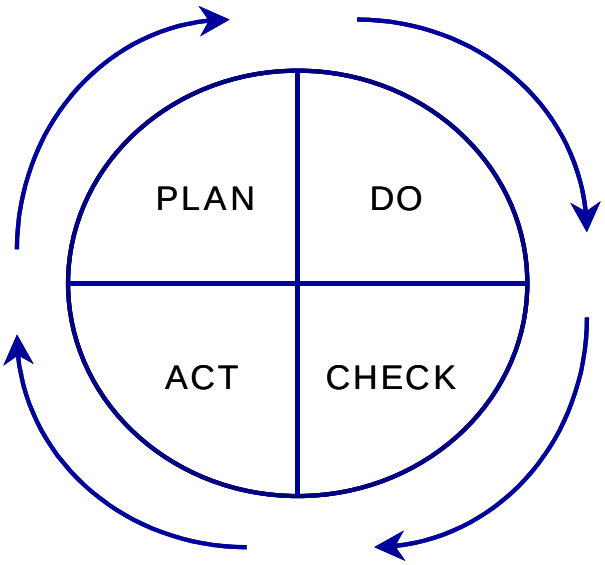
3.4 BS7799-2 et SMSI

La BS 7799-2 a été établie pour des managers et leurs équipes afin de fournir un modèle pour mettre en place et gérer un Système de Management de la Sécurité de l’Information efficace.

[2] Hors Royaume-Uni.

La BS 7799-2 s'appuie sur une approche processus pour définir, implémenter, mettre en fonction, maîtriser et améliorer l'efficacité de l'organisation d'un SMSI.

La démarche du British Standard suit le « Modèle PDCA » (Plan-Do-Check-Act), connu également sous le nom de « Roue de Deming » (cf. ISO9001:2000) qui s'applique ainsi à tout SMSI. L'approche processus met l'accent sur l'importance des points suivants :



- P (compréhension) : Une bonne compréhension des besoins en matière de sécurité de l'information au regard du business, et la nécessité d'élaborer une politique et des objectifs en matière de sécurité de l'information – Etablissement du SMSI
- D (politique) : Les contrôles en phase d'implémentation et de fonctionnement dans un contexte de management de l'ensemble des risques de l'organisation – Mise en œuvre des processus,
- C (surveillance) : La surveillance et la révision des performances et de l'efficacité du SMSI,
- A (amélioration) : L'amélioration permanente du système de management, basée sur des mesures objectives.

3.5 BS7799-2 et la gestion de la sécurité

Différents acteurs sont concernés par la BS 7799-2:2002. Chacun d'eux trouvera dans la lecture de ce document les informations sur son rôle en fonction des étapes de mise en œuvre d'un SMSI :

- analyse des risques,
- management du risque,
- processus d'amélioration continu.

3.5.1 Qui est concerné par la norme elle-même ?

Toute personne concernée par une démarche de SMSI et/ou certification sont directement concernés par cette norme.

3.5.2 Qui est concerné par le SMSI ?

Acteur	Rôle / Intérêt	Etape
Propriétaires des informations, Responsables métiers	Définissent les exigences de sécurité des informations dont ils sont les propriétaires.	P
Responsable de l'analyse de risques	Identifie de manière exhaustive les actifs sensibles de l'entreprise, les menaces pesant sur ces actifs et les vulnérabilités qu'elles pourraient exploiter.	P / C
RSSI	Propose des mesures de sécurité	P
Tous	Mettent en œuvre des mesures de sécurité Participent à l'amélioration du SMSI	D A
Direction Générale	Lance la démarche PDCA Valide le traitement du risque	P
Contrôle Interne	Audite la démarche, les mesures mises en place	C

3.5.3 Analyse des risques

Les exigences de sécurité (Disponibilité, Intégrité, Confidentialité, Preuve) sont définies par les propriétaires des informations.

Le responsable de l'analyse des risques à partir de l'identification exhaustive des actifs sensibles de l'entreprise, des menaces pesant sur ces derniers et des vulnérabilités qu'elles pourraient exploiter, évalue les risques.

3.5.4 Gestion du risque

Le RSSI est le principal acteur à qui s'adresse ce document. Il devra :

- définir la démarche à suivre (description des étapes nécessaires) pour établir son SMSI,
- proposer les mesures de sécurité à mettre en place « a priori » (issus de la BS ou non).

La Direction Générale a pour attribution principale :

- d'affecter les ressources humaines et financières nécessaires à la mise en œuvre des mesures et éventuellement d'accepter certains risques pour l'entreprise,
- de valider et s'engager sur les objectifs de la politique de sécurité.

Les différentes structures de l'entreprise devront mettre en place les mesures validées par la Direction Générale.

3.5.5 Processus d'amélioration continue

Le Contrôle Interne ou Audit a en charge la conduite de missions d'audit interne de la gestion de la politique de sécurité déployée. Le document précise les modalités (la périodicité, les objets et la qualité) de ces audits du SMSI.

3.6 BS7799-2 et qualité

La norme dispose d'un « héritage » affiché, exposé dès le paragraphe d'introduction, avec l'approche qualité. Cette problématique est omniprésente dans tout le document.

Ce fort lien est illustré notamment par les deux points suivants :

- alignement de la BS 7799-2:2002 avec la norme ISO 9001:2000 pour être compatible avec d'autres systèmes de management,
- utilisation de l'approche processus, élément fondamental de management de la qualité dans l'ISO 900n:2000, et du modèle dit « PDCA ».

Par ailleurs, le contenu du texte de la BS 7799-2:2002 est, en ce qui concerne la protection de l'information, en grande partie une déclinaison de l'ISO 9001:2000.

Enfin, l'annexe C fournit les correspondances, chapitre par chapitre de BS7799-2:2002 avec l'ISO 9001:2000, ainsi que l'ISO 14001:1996 pour les thématiques communes.

Il faut néanmoins noter que ces deux premières normes sont structurées différemment :

- la structure de la BS 7799-2:2002 est basée sur le modèle de Deming (PDCA) et de l'analyse des risques,
- la structure de l'ISO 9001:2000 est une description plus complète de l'ensemble des processus impactant la qualité du produit.

Si certains thèmes de l'ISO 9001 sont repris dans la BS 7799-2, d'autres sont :

- traités de manière très succincte, comme le paragraphe sur les audits internes, la revue de direction, etc.
- traités de manière indirecte. Par exemple, le paragraphe 6.2 (« Management des ressources humaines ») de l'ISO 9001:2000 est rapproché du paragraphe 5.2.2 de la BS 7799-2:2002 (« Training, awareness and competency ») quoique plus réducteur,
- non cités, comme le contenu du chapitre 7 de l'ISO 9001:2000 (« Réalisation du produit »), à peine évoqué par le biais des "actions" dans le paragraphe sur l'analyse des risques ou le paragraphe 6.3 de l'ISO 9001:2000 (« Infrastructure »).

3.7 BS7799-2 et analyse de risques

L'analyse de risques joue un rôle essentiel tout au long de la vie du SMSI, aussi bien lors de sa définition (le *plan* du modèle PDCA), que lors de sa maintenance et de son amélioration (le *check* du PDCA). En effet, la norme stipule qu'une analyse de risques doit être intégrée dans le processus d'établissement du SMSI. Idéalement cela peut être réalisé dès la phase de démarrage, afin de lui fournir de la matière première à l'établissement des besoins et des mesures de sécurité à mettre en œuvre. Une approche méthodique est recommandée, toute mesure devant avoir un justificatif formel (i.e., écrit et argumenté) à partir des risques identifiés.

Les objectifs du SMSI sont alors fixés en vue de ramener les risques identifiés à un niveau acceptable pour l'organisme.

L'analyse de risques intervient de nouveau en phase de supervision et de révision du SMSI (la phase *check*). Cette étape est nécessaire pour garantir la pérennité du SMSI et son adéquation face aux évolutions de l'organisme, aux changements d'ordres réglementaires, légaux et techniques, et à

des nouvelles menaces identifiées. Cette étape, planifiée, est l'occasion d'adapter les procédures qui ont été mises en place dans le SMSI en fonction des risques, qu'ils soient initiaux ou nouveaux, et de leur niveau d'acceptation.

Aucune méthode d'analyse de risques n'est préconisée dans la BS7799-2. Toute méthode, suffisamment éprouvée, peut être utilisée à condition qu'elle soit bien adaptée au SMSI en cours de définition, à l'organisme et au contexte d'utilisation (application, type de résultat attendu, spécificité du domaine, compatibilité avec le référentiel de l'entité, etc.).

Les méthodes les plus connues en France sont EBIOS (DCSSI) et MEHARI (Clusif).

Chacune possède sa propre base de connaissance (vulnérabilités, méthodes d'attaques, exigences de sécurité, etc.), qui peut ne pas traiter tous les thèmes cités dans la BS7799-2.

4. BS7799-2 ET CERTIFICATION

4.1 La certification BS7799-2 des organismes

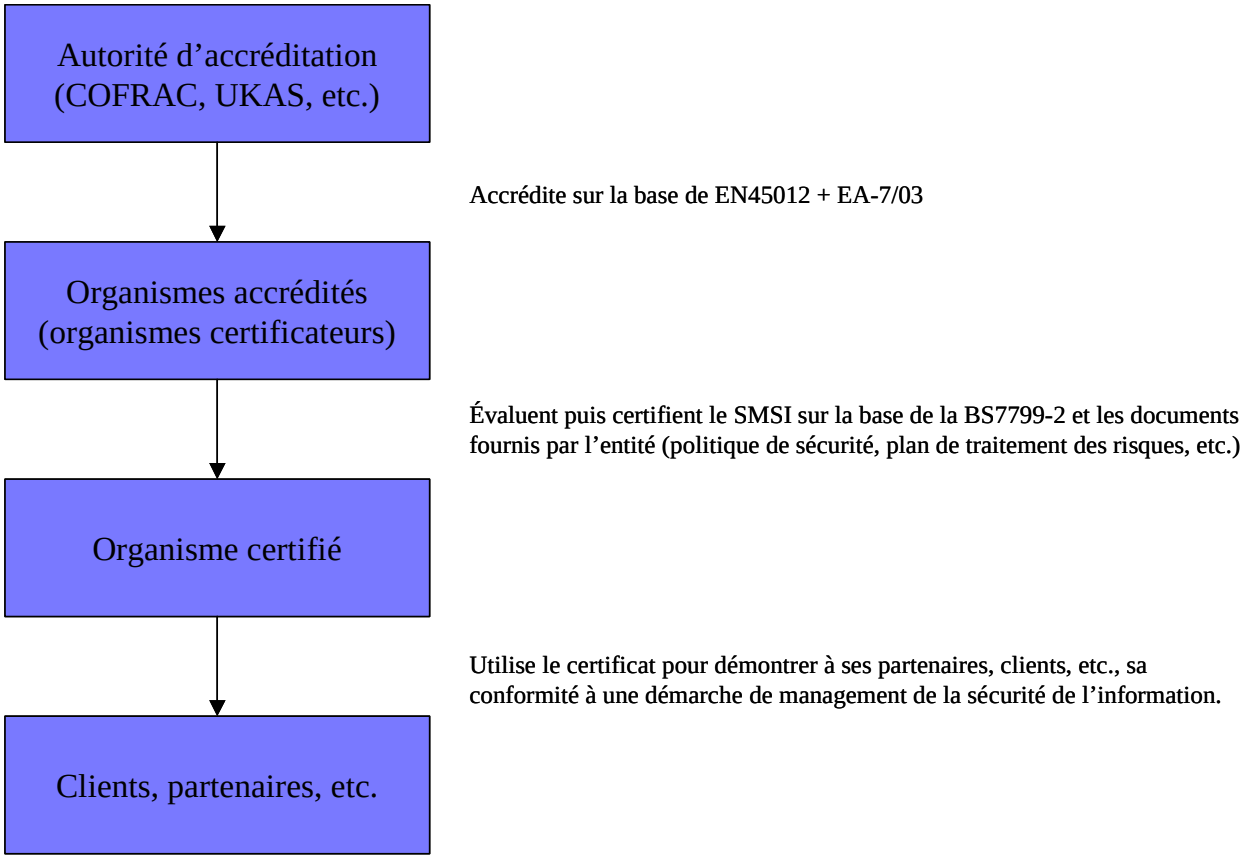
Une des motivations des utilisateurs de la BS7799-2 est d'obtenir une certification sur une organisation, un service ou une entité, afin de pouvoir notamment en faire état. La certification ne garantit pas un niveau de sécurité, elle atteste de l'application d'une démarche de management de la sécurité de l'information selon la norme BS7799-2.

La validité d'un certificat BS7799-2 est de trois ans, sous réserves d'une surveillance au minimum annuelle effectuée par l'organisme certificateur sur un échantillon de processus.

Si des non-conformités majeures par rapport à la démarche BS7799-2 sont constatées, la certification BS7799-2 n'est pas accordée (ou immédiatement supprimée, dans le cas d'un audit de surveillance). Si des non-conformités mineures sont constatées, elles sont rapportées dans le rapport d'audit. L'entité est tenue dans un délai rapide de présenter un plan des actions correctives, dont l'exécution sera vérifiée lors du prochain audit de surveillance.

De notre compréhension, un organisme de certification ne peut pas assister l'entité dans sa démarche de préparation à la certification.

Dans le cadre de la certification BS7799-2, le schéma de certification est le suivant :



A ce jour, il n'existe pas de certificateur français. Néanmoins, il est possible pour un organisme français de se faire certifier par un certificateur (français ou étranger) accrédité lui-même par une autorité d'un autre pays européen.

Des organismes français ont envisagé d'entamer une démarche en vue d'une certification, mais la plupart se sont interrompus, notamment faute d'un certificateur français.

4.2 La certification « Lead Auditor » des personnes

Dans le cadre de ses activités para-normatives, le BSI organise depuis plusieurs années, différents cycles de formation autour de la norme BS7799-2. Un de ces cycles de formation appelé « BS7799 Lead Auditor » permet aux participants, majoritairement des auditeurs internes ou externes, d'aborder les notions de base des principes d'audit général de sécurité, de l'analyse et du management des risques et de l'approche de la certification BS7799-2. Elle permet de participer à un examen final des connaissances, dont la réussite est sanctionnée par l'attribution de la certification « BS7799 Lead Auditor ».

Il n'existe pas de liste exhaustive de personnes certifiées « BS7799 Lead Auditor ». Des organismes proposent des listes d'individus certifiés construites à partir de critères supplémentaires (diplômes académiques, années d'expériences professionnelles, audits réalisés, cotisation, etc.).

Selon notre compréhension :

- la certification « BS7799 Lead Auditor » apporte la garantie que l'auditeur a suivi et compris la formation et a réussi l'examen,
- il n'est pas nécessaire (ni suffisant) d'être qualifié « BS7799 Lead Auditor » pour pouvoir participer à l'équipe de certification d'un SMSI selon la BS7799-2. En effet, il n'est fait mention d'aucune obligation de qualification « officielle » du personnel de certification dans les normes EA7/03.

A la date de rédaction de ce document, d'autres sociétés que le BSI sont habilitées à dispenser le cours et l'examen du « BS7799 Lead Auditor ».

4.3 Autres pratiques et normes de certification

4.3.1 ISO9001

Il faut distinguer la certification d'organisations (ex. ISO 9001, ISO 14001, OHSAS 18001[3]), de la certification de produits ou systèmes (ex. ISO 15408). Pour rester dans la perspective globale de ce document, nous parlerons dans ce paragraphe, à titre d'exemple, de l'audit de certification ISO 9001:2000 des Systèmes de Management de la Qualité.

L'audit de certification selon l'ISO 9001 se déroule en plusieurs étapes, qui sont :

- La définition du périmètre de l'audit et sa planification,

[3] OHSAS 18001 : Certification Santé et Sécurité au Travail

- La phase d'audit proprement dite, avec l'examen du système de management de la qualité, et les différents entretiens, dont les entretiens avec la direction. Cette phase se déroule généralement sur quelques jours, mais la durée et le nombre d'auditeurs et d'intervenants internes peuvent varier selon la taille de l'organisation, et le périmètre de l'audit. Elle se conclut par une première réunion de restitution "à chaud" avec la direction, qui permet d'éclaircir des ambiguïtés ou des remarques issues des entretiens.
- Elle se termine par l'émission, dans des délais brefs (une à deux semaines), du rapport d'audit, qui récapitule les conformités et les atouts de l'organisation par rapport à ses objectifs et à la norme, mais aussi les remarques, voire les non-conformités, qui justifient la conclusion :
  - d'attribution ou non du certificat lors de l'audit initial,
  - de renouvellement ou de retrait du certificat, dans le cadre d'un audit de renouvellement.

Les audits se déroulent conformément aux recommandations de la norme ISO 19011 *Lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental*. Elle requiert notamment l'indépendance entre l'organisme effectuant l'audit de certification de l'organisation et l'organisation, donc, éventuellement, l'entreprise accompagnant l'organisation dans sa démarche de certification.

Le certificat est valide pour une durée maximale de 3 ans, et fait l'objet d'audits annuels de suivi, puis, au bout de 3 ans, d'un audit de renouvellement.

Durant cette période, l'organisme ayant attribué le certificat surveille l'emploi qui en est fait par l'organisation, et peut sanctionner, par exemple, des annonces abusives sur des extensions de périmètre imaginaires, sanctions pouvant aller jusqu'au retrait immédiat du certificat hors audit.

L'organisme certificateur doit avoir été accrédité par le COFRAC pour la norme considérée.

4.3.2 ISO15408

La certification selon les « Critères Communs » (« CC » ou encore « ISO15408 ») concerne les produits et systèmes informatiques (pas nécessairement des produits et systèmes de *sécurité informatique*).

A la différence des autres certifications, un produit est certifié ISO15408 par rapport à un *niveau d'assurance* (à tort aussi appelé « niveau de sécurité ») de EAL1 (le plus faible) à EAL7 (le plus élevé). Ces différents niveaux impliquent une étude plus ou moins approfondie de la cible d'évaluation (Target Of Evaluation, TOE) qui délimite le périmètre du produit qui est évalué.

Le schéma de certification ISO15408 diffère des certifications traditionnelles puisqu'il n'existe qu'un seul organisme de certification gouvernemental : la DCSSI, en France. De même, les laboratoires d'évaluation (CESTI) sont accrédités par le COFRAC, et doivent être aussi agréés par la DCSSI.

Ainsi, un organisme souhaitant faire évaluer un produit (ou système) doit :

- déterminer sa cible d'évaluation (TOE), qui inclut le niveau d'assurance,
- la faire valider par la DCSSI,
- choisir un laboratoire d'évaluation agréé,
- faire évaluer son produit.

A l'issue de l'évaluation, le dossier d'évaluation est transmis à la DCSSI, qui émettra le cas échéant le certificat correspondant.

La certification d'un produit ou d'un système est un investissement à long terme puisque le processus d'évaluation peut prendre plusieurs mois.

De même, tout changement significatif de la cible d'évaluation nécessite une ré-évaluation de l'ensemble.

5. CONCLUSION

La norme BS7799-2 a rencontré une large audience et adhésion dans différents pays. Il est vraisemblable qu'elle servira de base de travail à une prochaine norme internationale de type ISO.

Jusqu'à présent il manquait une démarche structurée de mise en œuvre d'une politique de sécurité au quotidien. La BS7799-2 comble ce vide et permet à des organismes de structurer la gestion de leur sécurité.

Si on se réfère aux données publiques, il apparaît à l'évidence une très forte croissance en termes de nombre de certificats délivrés sur un an. Toutefois on constate que l'Europe continentale et l'Amérique du Nord sont en retard par rapport à la Grande Bretagne et à l'Asie sur ce point.