

ISO17799:2000

Une présentation générale

Février 2003

Groupe de Travail ISO 17799 : 2000



CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS

30, rue Pierre Semard, 75009 PARIS
Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88
e-mail : clusif@clusif.asso.fr - Web : <http://www.clusif.asso.fr>

Le CLUSIF

Le CLUSIF offre, depuis 1984, un espace d'échange dans lequel les acteurs de la sécurité des systèmes d'information peuvent se rencontrer, travailler et progresser ensemble. A ce jour, le CLUSIF rassemble plus de 600 membres, appartenant à 300 organismes ou sociétés. Sa particularité est d'accueillir les utilisateurs comme les offreurs. De cette complémentarité naît une synergie.

Sa mission

Echanger

La vocation du Clusif est de favoriser le partage des expériences.

Les utilisateurs sont ainsi tenus au courant des nouveautés en matière de sécurité et les offreurs ont accès à une meilleure connaissance des besoins et du marché.

Concevoir

La réalisation de travaux sur la sécurité couvre des domaines très étendus, tels que : l'état de l'art sur des solutions existantes, des méthodes d'analyse de risques, de conception et de développement sécurisés de projets, d'évaluation de la sécurité des systèmes d'information ; des prises de position sur des sujets d'actualité ; des enquêtes, des statistiques ; des guides et des recommandations à caractère didactique.

Promouvoir

Il entre dans les finalités du CLUSIF de sensibiliser et d'influencer un certain nombre d'acteurs de la vie économique et politique, avec le double objectif de promouvoir la sécurité et de faire valoir les besoins et contraintes des utilisateurs auprès des instances dirigeantes. Le CLUSIF s'adresse aux décideurs, utilisateurs, parlementaires, pouvoirs publics, médias, ainsi qu'à d'autres associations.

Eduquer

Le CLUSIF s'implique activement dans le processus d'éducation et de sensibilisation, en matière de sécurité, auprès de ses membres, des professionnels de la sécurité, des enseignants et des étudiants. Il intervient dans les programmes de formation afin que la sécurité des systèmes d'information soit incorporée dans les programmes pédagogiques.

Son fonctionnement

Le fonctionnement du CLUSIF repose principalement sur les commissions et les groupes de travail.

Les commissions, à caractère pérenne, sont au cœur de l'activité.

Les groupes de travail, à vocation temporaire, sont créés pour apporter une réponse à des sujets d'actualité ou aux préoccupations d'utilisateurs et d'offeurs. La contribution peut prendre la forme d'un document, d'une recommandation ou d'une prise de position sur un thème donné.

Commissions

- Espace RSSI
- Evaluation
- Menaces
- Méthodes
- Micro-informatique
- Réseaux et Systèmes Ouverts
- Sécurité des Systèmes d'Information
- Technique de Sécurité Logique
- Technique de Sécurité Physique

Son réseau relationnel

Régional

Le CLUSIF dispose de relais dans les régions : les Clubs de la Sécurité des Systèmes d'Information Régionaux (CLUSIR). Ces associations indépendantes sont agréées par le CLUSIF et s'engagent à respecter le règlement intérieur et le code d'éthique du CLUSIF. Il existe à ce jour six CLUSIR : Est (Strasbourg), Languedoc-Roussillon (Montpellier), Midi-Pyrénées (Toulouse), Nord Pas-de-Calais Picardie (Lille), Provence-Alpes-Côte d'Azur (Marseille), Rhône-Alpes (Lyon).

International

Le CLUSIF entretient des contacts avec des organismes et des associations en Allemagne, Belgique, Canada, Italie, Luxembourg, Suisse.

CLUSIB : Club de la sécurité informatique belge (<http://www.vbo-feb.be>)

CLUSSIL : Club de la sécurité des systèmes d'information Luxembourg (<http://www.clussil.lu>)

CLUSIS : Club de la sécurité informatique suisse (<http://www.clusis.ch>)

CLUSIT : Associazione Italiana per la Sicurezza Informatica (<http://www.clusit.it>)

Associatif

Le CLUSIF entretient des relations avec des organismes qui partagent la même sensibilité sur des thèmes de la Sécurité Informatique. Les principaux sont :

AFAI (Association Française d'Audit et du conseil en informatique)

CIGREF (Club Informatique des Grandes Entreprises Françaises)

Forum des Compétences (club de Responsables de la Sécurité d'organismes bancaires).

Institutionnel

Des liens très étroits sont développés avec les pouvoirs publics afin de promouvoir la sécurité des systèmes d'information. Le CLUSIF participe ainsi à des groupes de travail internationaux sur la cybercriminalité.

Contact

CLUSIF

30 rue Pierre Sémard

75009 PARIS

Tel : 01 53 25 08 80 - Fax : 01 53 25 08 88

Courrier électronique : clusif@clusif.asso.fr

Web : <http://www.clusif.asso.fr>

Remerciements

Nous tenons à souligner la contribution importante des membres du Groupe de Travail à la production de ce document :

Gérard ATTAL	Amacom
Régis BOURDONNEC	Cardif
Frédéric CHAUVOT	GIE Sesam-Vitale
Anne COAT	AQL
Michèle COPITET	Egona Consulting
Jean-François CORNET	Transiciel ISR
Christian GATEAU	France Telecom - Transpac
Stéphane GEYRES	Ernst & Young
Mathieu GRALL	SGDN - DCSSI
Paul GRASSART	XP Conseil
Frédéric HUYNH	Ernst & Young
Bruno MELINE	IBM
Fred MESSIKA	Lynx Technologies
Olivier MEULLEMEESTRE	Barbier Frinault & Associés – Réseau Ernst & Young
Lazaro PEJSACHOWICZ	CNAMTS
Paul RICHY	France Telecom
Jean-Christophe RIVIERE	SchlumbergerSema SGRS
Hervé SCHAUER	HSC Consultants

Table des matières

1. INTRODUCTION	3
1.1. A QUI S'ADRESSE LE PRESENT DOCUMENT ?.....	3
1.2. PERIMETRE DE CE DOCUMENT	3
2. PRESENTATION	5
2.1. LE PERIMETRE DE LA NORME	5
2.2. A QUI S'ADRESSE-T-ELLE ?	5
2.3. HISTORIQUE DE BS7799 ET ISO17799.....	6
3. CONTENU DE LA NORME	7
3.1. ARCHITECTURE	7
3.2. COUVERTURE THEMATIQUE.....	8
4. DIFFERENTS USAGES DE LA NORME	10
4.1. USAGE GENERAL	10
4.2. AVEC UNE ANALYSE DE RISQUES.....	11
4.3. POUR COMMUNIQUER	12
4.4. DANS UNE OPTIQUE DE CERTIFICATION	12
4.5. EN VUE D'UN AUDIT	13
5. CONCLUSION	14
5.1. PROPOSITIONS D'EVOLUTION.....	14
5.2. AMELIORATIONS AUTOUR DE LA NORME.....	14
5.3. SYNTHESE	15
6. BIBLIOGRAPHIE	16

Avertissement

Dans l'ensemble du présent document, le terme « ISO17799 » sera utilisé pour faire référence à la norme « ISO/IEC 17799:2000 ».

Au moment où ce document a été écrit, la norme ISO17799 était en révision auprès des organismes internationaux de normalisation.

Nous ferons donc référence à la dernière version publique datant du 1/12/2000. Une mise à jour de ce document sera réalisée par le CLUSIF si de profonds changements venaient à apparaître dans la norme et qui en affecteraient la nature actuelle.

Tout le long de ce document, on utilisera le terme générique « entité » en lieu et place des termes « entreprise », « organisme d'état », « société », « administration » ou autres synonymes.

1. INTRODUCTION

Les relations entre organisations, entreprises ou administrations rendent nécessaire la définition de référentiels communs. Afin de s'entendre sur les termes et concepts employés, cette question s'applique également au domaine de la sécurité des informations, par exemple concernant les types de mesures de sécurité pouvant être mises en œuvre.

Déjà réel au niveau national, ce besoin est encore plus vivement ressenti dans le cadre d'échanges internationaux. En effet, la prise en compte de cultures et de contextes réglementaires variés est une problématique difficile à gérer pour les grandes entreprises et plus encore pour les PME.

D'autre part, dans un contexte d'économie mondialisée, les entreprises multinationales font aujourd'hui souvent évoluer leur organisation afin de se restructurer par métier et non plus par pays. Cette organisation à l'échelle internationale a un impact fort sur le management de la sécurité de l'information. En effet, la création d'un espace de confiance trans-frontalier nécessite la définition d'une politique de sécurité globale. Avec pour champ d'application une structure internationale, elle devra tenir compte des exigences légales et externes et devra définir des règles, démarches et référentiels utilisables et inter-opérables sur plusieurs pays.

La norme internationale ISO17799, publiée en décembre 2000, est souvent perçue par les spécialistes de la sécurité de l'information comme une réponse à cette attente. Bénéficiant d'une forte médiatisation, elle est de plus en plus fréquemment citée comme référence. Toutefois, le Clusif constate que son contenu, ses objectifs et ses utilisations possibles sont souvent mal connus, ce qui peut parfois entraîner des confusions.

L'objectif du présent document vise précisément à améliorer la connaissance et la perception de la norme par le plus grand nombre.

1.1. A QUI S'ADRESSE LE PRESENT DOCUMENT ?

Il s'adresse en premier lieu aux professionnels de la sécurité de l'information qui souhaitent mieux connaître cette norme. Il vise à clarifier les objectifs et le périmètre de la norme internationale ISO17799, à dégager la structure de son contenu, et à en proposer des utilisations possibles. Il n'est donc pas nécessaire d'être un expert de la norme pour le lire.

D'autre part, ce document pourra éventuellement servir de base à un responsable sécurité pour élaborer des synthèses visant à présenter la norme à une Direction générale ou à des Responsables marketing, bien qu'il ne s'adresse pas directement à ces populations.

1.2. PERIMETRE DE CE DOCUMENT

Il n'entre pas dans le cadre de ces travaux de porter un jugement sur la qualité de la norme, que celui-ci soit positif ou négatif. Ce document ne traitera pas non plus les questions relatives au marché potentiel de la norme ISO17799.

Comme tout texte de référence, l'utilité pratique de la norme doit être évaluée en fonction du contexte particulier où l'on souhaite s'y référer.

Les thèmes suivants seront abordés :

- Présentation générale de la norme ISO17799 : thématiques abordées, destinataires théoriques, périmètre, historique ;
- Structure de la norme : logique de construction, « philosophie » de ses sous-chapitres ;
- Utilisations possibles de la norme.

2. PRESENTATION

2.1. LE PERIMETRE DE LA NORME

La norme¹ ISO 17799 est présentée dans un document de 72 pages rédigé en anglais et publié par l'ISO (International Organisation for Standardisation) et l'IEC (International Electrotechnical Commission).

Ce document définit des objectifs et des recommandations concernant « *la sécurité de l'information* ».

Il existe à ce jour des normes de sécurité qui ne s'appliquent qu'à certaines fonctions des entités ou qui ne traitent que de domaines particuliers de la SSI (exemples : ISO14000 ou FIPS140). A la différence de ces normes, la norme ISO 17799 a pour ambition de répondre aux préoccupations globales de sécurisation de l'information des entités pour l'ensemble de leurs activités.

2.2. A QUI S'ADRESSE-T-ELLE ?

Cette norme peut intéresser toutes les entités quel que soit leur secteur d'activité.

Elle a pour objectif de « *donner des recommandations pour gérer la sécurité de l'information à l'intention de ceux qui sont responsables de définir, d'implémenter ou de maintenir la sécurité dans leur organisation. Elle est conçue pour constituer une base commune de développement de standards de sécurité organisationnelle et de pratiques efficaces de gestion de la sécurité et pour introduire un niveau de confiance dans les relations interentreprises.* »

A l'intérieur d'une entité, par sa nature à donner des orientations sécurité sur la base des «bonnes pratiques», cette norme s'adresse avant tout aux responsables sécurité, directions informatiques, risk managers, ou au contrôle interne. Elle concerne aussi tout acteur dès lors que sa fonction contribue à définir, d'implémenter ou de maintenir la sécurité dans son entité. On peut citer par exemple : la Direction Générale, la Direction Juridique, la Direction des Ressources Humaines, la Direction Administrative et Financière.

Cette norme est un vecteur de communication à l'intention de partenaires dès lors que l'entité a besoin de :

- Répondre à des contraintes sur la sécurité de l'information.
- Justifier d'un savoir-faire méthodologique dans la gestion de la sécurité de l'information.
- Se positionner par rapport à un référentiel international.

Le niveau de participation de la Direction Générale à des décisions en matière de sécurité pourra être renforcé par la mise en place d'une démarche de certification.

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

2.3. HISTORIQUE DE BS7799 ET ISO17799

Dans les années 90, des représentants de grandes entreprises comme Shell, British Telecom, Midland Bank, Marks & Spencer se sont réunis et ont défini un « code de bonnes pratiques » à partir de leurs expériences. Ce document a été publié sous forme de document public en 1993 par le British Standard Institute (BSI).

En mars 1995, évolution de ce premier « code », la BS7799:1995 est publiée sous le titre de « Code of practice for information security management ». Une norme nationale complémentaire intitulée « Specifications for security management » est apparue deux ans après sous la dénomination de BS7799-2:1997.

Sur la base de la BS7799-2:1997, le Royaume Uni a mis en place un schéma de certification en 1998, sous le nom de « c:cure », et depuis des certificats ont été émis.

En décembre 1998, la BS7799 est mise à jour pour devenir BS7799:1999. Les modifications apportées concernent principalement :

- le remplacement de « IT » par « Information » (élargissement de la cible),
- la modification d'un certain nombre de chapitres (surtout dans leur libellé),
- l'ajout de quelques sous chapitres (comme la téléinformatique).

La BS7799 a été reprise comme norme par quelques pays (Pays-Bas, l'Australie...). Elle a été traduite par le BSI en plusieurs langues (français, allemand, ...).

La première partie de la BS7799 a été soumise deux fois à l'ISO en utilisant la procédure « fast track » (procédure rapide permettant l'adoption d'une norme nationale au niveau international). Après avoir été rejetée une première fois en 1996, elle a été acceptée suite à un nouveau vote intervenu en 2000 et publiée sous le numéro ISO17799:2000. Pour tenir compte des différents commentaires faits par les instituts nationaux de normalisation ayant pris part au vote, elle est entrée en phase de « révision » en 2001.

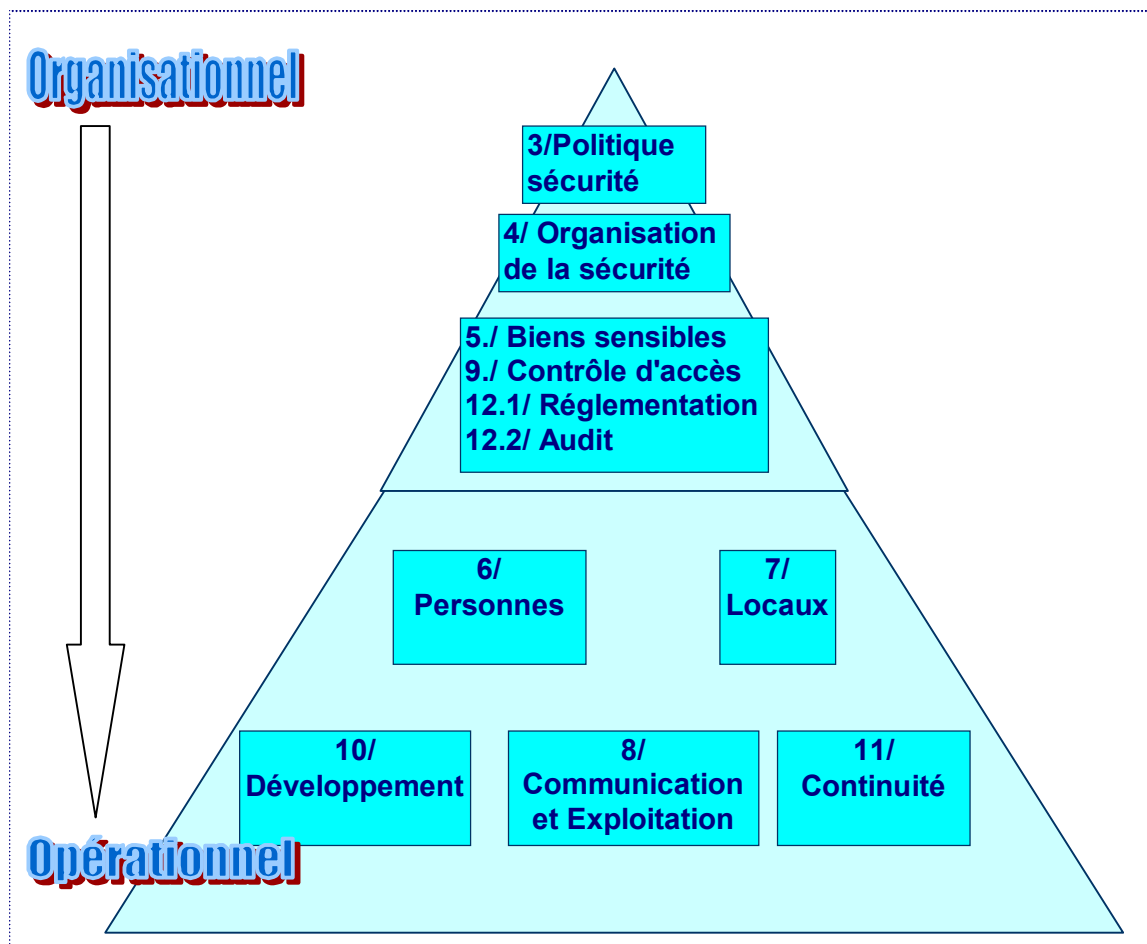
3. CONTENU DE LA NORME

3.1. ARCHITECTURE

La norme ISO17799 présente tout à la fois un ensemble d'objectifs de sécurité très généraux et d'ordre théorique, et des bonnes pratiques concrètes à mettre en œuvre pour les atteindre, le tout organisé en un ensemble de chapitres d'objectifs différents :

- des chapitres de management, globaux à l'entité : politique, organisation,
- des chapitres sur l'environnement : personnels et locaux,
- des chapitres opérationnels sur le développement et l'exploitation des S.I.

Le schéma ci-dessous résume une vision possible de l'architecture de la norme (les nombres mentionnés indiquent les chapitres de la norme) :



Chaque chapitre du document présente une thématique de sécurité détaillée en sous-chapitres, qui peuvent être structurés autour :

- d'activités :
 - exemple pour le personnel : recrutement, formation, gestion des incidents
 - exemple pour le contrôle d'accès aux réseaux : authentification des utilisateurs et des nœuds, diagnostic des ports, Isolement des réseaux, contrôle des connexions et des routages
- d'objets :
 - exemple pour la sécurité physique : périmètre de sécurité, équipement,
- ou un mélange des deux (le plus souvent) :
 - exemple pour l'exploitation : Validation de Système, Virus, Sauvegarde, Gestion des Réseaux, Support, Echanges

Chaque chapitre ou sous-chapitre présente des objectifs de sécurité (encadrés en début de sous-chapitre), des recommandations :

- sur les mesures de sécurité à mettre en oeuvre,
- et des contrôles à effectuer.

La structure de la norme n'est pas sans rappeler les thèmes et facteurs de sécurité proposés par le questionnaire de la méthode MARION.

3.2. COUVERTURE THEMATIQUE

La norme identifie des objectifs visant à assurer la sécurité de l'information selon trois critères: la confidentialité, l'intégrité et la disponibilité. Ces objectifs sont regroupés au travers des dix grandes thématiques suivantes :

- La politique de sécurité : pour exprimer l'orientation et l'engagement de la direction à la sécurité de l'information.
- L'organisation de la sécurité : pour définir les responsabilités de management de la sécurité de l'information au sein de l'entité, y compris lorsque des tiers accèdent à l'information ou sont responsables du traitement de l'information.
- La classification et le contrôle du « patrimoine informationnel » : pour maintenir un niveau de protection approprié au patrimoine informationnel de l'entité.²
- La sécurité et les ressources humaines : pour réduire les risques d'origine humaine, de vol, de fraude ou d'utilisation abusive des infrastructures, notamment par la formation des utilisateurs et la gestion des incidents.
- La sécurité physique : pour prévenir les accès non autorisés aux locaux, au patrimoine informationnel, aux informations de l'entité ainsi que les dommages, les perturbations, et la compromission de ces locaux.

² Le terme « patrimoine informationnel » traduit le terme anglais « information assets ».

- La gestion des opérations et des communications : pour assurer le fonctionnement correct et sûr des infrastructures de traitement de l'information, et minimiser les risques portant sur les communications.
- Les contrôles d'accès : pour maîtriser les accès au patrimoine informationnel.
- Le développement et la maintenance des systèmes : pour que la sécurité soit une part intégrante du développement et de la maintenance des systèmes d'information, ceci dès les phases de spécification et de conception.
- La gestion de la continuité d'activité : pour parer aux interruptions des activités de l'entité et permettre aux processus cruciaux de l'entité de continuer malgré des défaillances majeures ou des sinistres impactant le système d'information.
- La conformité à la réglementation interne et externe : pour éviter les infractions de nature légale, réglementaire ou contractuelle ; pour vérifier la bonne application de la politique de sécurité

A chacune de ces thématiques correspond un chapitre qui peut être consulté indépendamment des autres.

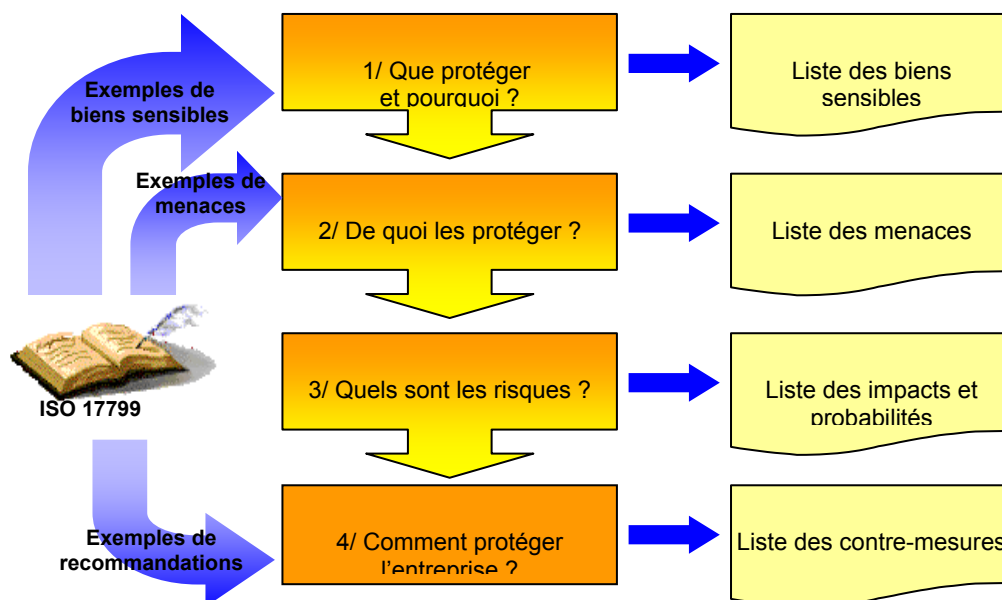
4. DIFFERENTS USAGES DE LA NORME

4.1. USAGE GENERAL

Ainsi qu'il l'est indiqué dans son titre, la norme ISO17799 est un « guide de bonnes pratiques » en matière de sécurité de l'information. Son usage est donc laissé à l'appréciation de l'entité.

La norme ISO17799 présentant à la fois un ensemble d'objectifs globaux de sécurité et des bonnes pratiques concrètes à mettre en œuvre pour les atteindre, l'entité pourra chercher à mettre en œuvre une partie plus ou moins étendue des dispositions proposées, selon la criticité des processus concernés, et l'impact de leur dysfonctionnement sur sa pérennité.

L'application de cette norme peut donc être le résultat d'une série d'étapes, décrites rapidement dans l'introduction de la norme, et qui peuvent être schématisées ainsi :



Pour mettre en œuvre cette norme, il appartient aux entités de mener les trois premières étapes, en utilisant la méthodologie de leur choix.

Le corps de la norme ISO17799 décrit la quatrième étape de cette démarche en indiquant « quoi faire » (checklist) sans pour autant préciser « comment le faire ».

Il est ainsi nécessaire :

- d'identifier les exigences légales et réglementaires (En France entre autres, les lois « Informatique et Liberté », « Godfrain », « sur la société de l'information », « sur la sécurité quotidienne », Code du Travail, Règlements sectoriels...) ;
- d'identifier les enjeux de l'entité et les attentes qui en découlent ;
- de définir le périmètre de mise en application de la norme :
 - périmètre organisationnel (groupe d'activités, processus complet, département, ensemble du groupe...),

- périmètre physique (atelier automatisé, salle serveur, réseau d'une usine...),
- périmètre au sein de la norme (paragraphes retenus ou non).

Toutefois, d'autres approches peuvent être utilisées en se basant sur les recommandations de la norme. A titre d'exemple, le lecteur pourrait :

- s'approprier tel quel le contenu de la norme en tant que standards de sécurité pour l'entité ;
- sélectionner des sous-ensembles de la norme pour les intégrer dans les standards de sécurité de l'entité ;
- se servir des règles et standards présentés dans la norme pour conduire des audits internes de sécurité ;
- se servir de la norme pour vérifier les standards de l'entité et éventuellement les mettre à jour ou les compléter ;
- s'en servir comme guide ou de base de travail pour la structuration de documents présentant des standards techniques plus détaillés.

La norme peut donc être abordée aussi bien de manière globale pour une mise en œuvre directe que ponctuellement comme « check-list » sur un sujet particulier d'organisation ou de mesure technique.

Elle constitue un élément de référence pour aider l'entité à établir sa propre cible en matière de sécurité et construire une démarche de mise en œuvre adaptée.

4.2. AVEC UNE ANALYSE DE RISQUES

ISO17799 recense un certain nombre de modalités et de règles pouvant être prises en compte par l'entité pour traiter ses risques de sécurité (réduire, transférer, prendre ou refuser les risques). La norme recommande en complément qu'une analyse des risques soit entreprise de manière méthodique. Les résultats d'une telle analyse servent essentiellement à déterminer les besoins de sécurité et à choisir les mesures de sécurité à mettre en œuvre. Les mesures contenues dans la norme peuvent être utilisées à cette fin.

ISO17799 ne précise aucune obligation quant à la méthode d'analyse de risques, chaque organisation ayant ses besoins et spécificités propres. Indépendamment de la norme, il existe différentes méthodes reconnues dont le choix dépendra du contexte d'utilisation (application, type de résultat attendu, spécificité du domaine, compatibilité avec le référentiel de l'entité...). Les plus connues en France sont notamment MARION (CLUSIF), MEHARI (CLUSIF) et EBIOS (DCSSI).

Chacune de ces méthodes possède ses propres référentiels qui – en particulier pour des raisons historiques – ne couvrent pas toujours strictement le spectre de l'ISO17799. Il peut ainsi être nécessaire de retravailler les bases de connaissances et prendre en compte certains aspects de l'ISO17799 pour obtenir une couverture complète de la sécurité par rapport à ce référentiel.

En ce qui concerne la méthode MEHARI, publiée par le CLUSIF, celle-ci regroupe :

- une méthode d'analyse avec quantification des risques,
- une démarche d'audit des services de sécurité (ensemble de mesures de sécurité regroupés en sous-services de sécurité),
- un cadre de gestion de la sécurité avec définition d'un plan d'action et élaboration de tableaux de bord avec indicateurs.

L'analyse des risques de la méthode MEHARI permet de choisir des mesures de sécurité appropriées à l'entité. Ces mesures peuvent être issues de l'ISO17799. C'est la raison pour laquelle la Commission Méthodes du CLUSIF a entrepris de corrélérer les bases de connaissances de la méthode afin de couvrir l'ensemble des mesures de la norme.

4.3. POUR COMMUNIQUER

La norme ISO17799 est de nature à faciliter la communication de la politique sécurité de l'entité en interne comme en externe

En effet, ISO17799 peut servir de référentiel pour communiquer avec une Direction Générale, des clients, ou des partenaires. Ce cadre commun permet de formaliser la prise en compte de mesures de sécurité par rapport à une norme reconnue. Néanmoins, cette communication peut se faire quels que soient les méthodologies, outils ou produits spécifiques utilisés.

On peut schématiser ces aspects sous la forme du tableau ci-dessous :

De	A	Sur quoi communiquer
Responsable sécurité	Direction Générale	Le besoin d'établir une politique de sécurité inspirée de l'ISO17799.
	Toute l'entité	La sensibilisation des services et des personnels sur les « meilleures pratiques de sécurité ».
	Toute l'entité	Le bien-fondé des mesures de sécurité à mettre en place.
	Direction Générale	La conformité des mesures de sécurité par rapport au cadre de la norme.
L'entité	Aux clients, prospects et partenaires	La cohérence de la démarche sécurité de l'entité avec la norme ISO17799.
	Aux partenaires et fournisseurs	Le bien-fondé d'imposer des exigences de sécurité cohérentes avec ISO17799.

4.4. DANS UNE OPTIQUE DE CERTIFICATION

Une certification est délivrée par un organisme indépendant et permet d'attester la conformité d'un produit, d'un système ou d'un service à des exigences bien définies comme, par exemple, celles de l'ISO 9001 (exigences pour les systèmes de management de la qualité) ou de l'ISO 14001 (exigences pour les systèmes de management de l'environnement).

Une certification s'appuie sur un audit « tierce partie », c'est à dire un audit réalisé par un organisme externe indépendant de toute partie ayant un intérêt dans l'entité auditée.

En tant que code de bonnes pratiques pour le management de la sécurité de l'information, l'ISO17799 ne définit aucune exigence en matière de produit, de système ou de service. Une certification par rapport à cette norme n'est donc pas possible.

En conséquence, le terme « certification ISO17799 » est un abus de langage.

Le British Standard Institute (BSI) a d'ailleurs rédigé une seconde partie à la norme BS7799 (cf. ci-dessus, chapitre sur l'historique de BS7799 et de l'ISO17799). La BS7799-2 définit ainsi les exigences d'un « ISMS » (Information Security Management System – système de management de la sécurité de l'information) et peut donc, à ce titre, être utilisée pour auditer et certifier un tel système de management.

L'ISO9000:2000 définit un système de management de la façon suivante : *ensemble d'éléments corrélés ou interactifs permettant d'établir une politique et des objectifs et d'atteindre ces objectifs.*

L'ISO9000:2000 précise également que le système de management d'une entité peut inclure différents systèmes de management, tels qu'un système de management de la qualité (cf. norme ISO9001:2000), un système de management financier ou un système de management environnemental (cf. norme ISO14001:1996).

Donc, un système de management de la sécurité de l'information peut être défini comme un *ensemble d'éléments corrélés ou interactifs permettant d'établir une politique et des objectifs, en matière de sécurité de l'information, et d'atteindre ces objectifs.*

De plus, l'ISMS se rapproche d'une démarche qualité (système de management de la qualité), ce qui favorise la synergie entre ces deux systèmes.

Un ISMS prévoit une analyse de risques qui peut exploiter ISO17799 pour couvrir les risques identifiés, par l'intermédiaire des dispositions proposées dans ses bonnes pratiques.

Des schémas de certification ISMS ont été définis dans de nombreux pays (sur la base de la norme BS7799-2). Sur cette même base, la définition d'une norme d'exigences sur les ISMS et du schéma de certification correspondant est à l'étude en France.

4.5. EN VUE D'UN AUDIT

On prend ici le terme « auditer » pour signifier qu'on cherche à comparer « la réalité du terrain » (ressources, procédures, usages...) avec un référentiel choisi en vue d'apprécier les écarts et de définir les axes d'amélioration.

En matière d'audit de la sécurité de l'information, la norme ISO17799 peut être utilisée principalement Comme base de construction du référentiel d'audit sécurité de l'entité (cf. chapitre 4.1).

Lors de la construction du référentiel d'audit, il est pertinent de sélectionner et d'adapter les différentes mesures de l'ISO17799 au contexte propre à chaque entité en particulier, en fonction de son activité et de son environnement.

Par ailleurs, l'ISO17799 ne propose aucune métrique qui pourrait être utilisée pour évaluer la sécurité de l'entité.

Enfin, il existe des outils se référant à l'ISO17799, il appartient à chaque entité d'apprécier leur utilité dans son contexte.

5. CONCLUSION

5.1. PROPOSITIONS D'EVOLUTION

L'ISO17799 se positionne comme un ensemble de bonnes pratiques opérationnelles à laquelle on pourrait souhaiter voir adosser une norme d'exigences, ce qui pourrait servir de base à des modalités de certification et à la mise en place de système de management de la sécurité.

L'hétérogénéité de structure de ISO17799, pourrait faire l'objet d'une restructuration en profondeur. En effet la norme actuelle est composée d'une imbrication de principes théoriques et de conseil pratiques hétérogènes qui peuvent nuire à sa compréhension et à son exploitation.

Un axe d'amélioration pourrait consister à viser deux documents séparés (ou non) et homogènes traitant pour l'un des principes théoriques, d'ordre managérial (exemple : éléments d'organisation et de réglementation...) et pour l'autre des conseils pratiques, d'ordre opérationnel (exemples : procédures de contrôles techniques, administration de l'infrastructure, etc.).

S'agissant des conseils pratiques, on pourrait approfondir certains points techniques dans des annexes, par exemple sur les thèmes suivants :

- Check-list de sécurité pour les environnements d'exploitation.
- Utilisation sécurisée des technologies réseaux et Internet en particulier.
- Sécurité des accès pour les fournisseurs et prestataires de services.
- Utilisation de la cryptographie, de la signature électronique, et de la messagerie sécurisée.
- Sécurité des postes nomades.

Cette structure permettrait des modalités d'évolution et de révision régulière (à préciser) permettant à la norme de rester en phase avec l'état de l'art et l'évolution des techniques.

5.2. AMELIORATIONS AUTOUR DE LA NORME

De manière plus pratique et immédiate, par rapport au contenu actuel de l'ISO 17799, un Guide de mise en œuvre précisant « Comment s'en servir ? Par quoi commencer ? Que contrôler? », ou tout du moins les éléments suivants seraient utiles :

- **Un document expliquant les principes de la mise en place d'un Système de Management de la Sécurité Informatique basée sur la BS7799-2** : qui est en charge du processus sécurité ? quels sont les outils disponibles et à mettre en place ? quelle démarche adopter ? quel périmètre et comment le définir ? comment le déployer dans l'entité ?
- **Un guide proposant des critères de définition de « niveaux de sécurité »**. La définition de « niveaux de sécurité » permettrait au RSSI de situer son entité vis-à-vis de la norme, de se fixer des objectifs par rapport à celle-ci, et d'évaluer les sujets prioritaires à traiter compte tenu des paramètres internes de l'entité.

5.3. SYNTHÈSE

Pour établir un parallèle avec la famille de norme ISO900x:2000, l'ISO17799 serait aujourd'hui comparable à l'ISO9004 (norme « outil »), et il lui manquerait son ISO9001 (norme d'exigences), avec les concepts suivants :

- notion de processus,
- notion de système de management de la sécurité de l'information (ISMS),
- notion d'amélioration continue.

La version 2002 de la BS 7799-2 (éditée par le BSI), en présentant les notions d'ISMS et d'amélioration continue, approche de ce qu'on pourrait attendre d'une norme d'exigences, et vient assez bien compléter l'ISO17799.

6. BIBLIOGRAPHIE

- ISO TR-13335 (Guidelines for the Management of Information Technology Security).
- ISO 15408 (Evaluation Criteria for Information Technology Security - Critères Communs).
- BS7799-2:2002 (Specification for security management).
- ITSEC (Information Technology Security Evaluation Criteria)
- TCSEC (Trusted Computer System Evaluation Criteria), plus connu sous le nom de "Livre Orange".
- ISO WD 18044 (Security incident management).
- Un document publié sous l'égide de la Commission Européenne Un document conçu aux Etats-Unis, les TCSEC (Trusted Computer System Evaluation Criteria), plus connu sous le nom de "Livre Orange", version de décembre 1985., les ITSEC (Information Technology Security Evaluation Criteria), V1.2 de juin 1991.