



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

Forum Alger IT-Sécurité solutions

18 Janvier 2004

Usage des normes ISO17799 / BS7799-2

Hervé Schauer

<Herve.Schauer@hsc.fr>

- x Objectifs de ces normes
- x Présentation synthétique des normes
 - x ISO17799 / BS7799-1 : *Code of practice for information security management*
 - x BS7799-2 : *Information Security Management systems – Specification with guidance for use*
- x Historique, contenu, couverture thématique, SMSI
- x La certification
 - x Le schéma de certification
 - x Les registres
 - x Le processus d'audit BS7799 en vue d'être certifié
- x La société de service en sécurité dans la démarche BS7799

- x Usage des normes
 - x Général
 - x Avec une analyse de risques, pour communiquer, en vue d'un audit, pour obtenir une certification
- x Le modèle PDCA
- x La mise en place d'un SMSI
- x Autre norme utile : ISO19011 :
 - x Lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental
- x Conclusion
- x Références et remerciements

- x HSC est un cabinet de conseil et d'expertise en sécurité depuis 1989
 - x Indépendant
 - x Audit, tests d'intrusion, conseil, formation, études
 - x Formations à Alger chaque année

- x Objectif : donner un aperçu de ce que recouvrent les normes ISO17799 et BS7799-2, et leur usage

- x Deux documents payants, en anglais
 - x ISO17799 : *Code of practice for information security management*
 - x BS7799-2 : *Information Security Management systems – Specification with guidance for use*
- x Une spécification pour le **management de la sécurité de l'information**
- x ISO 17799 = ISO 17799:2000 = BS 7799-1:1999
 - x Code des bonnes pratiques pour les systèmes de management de la sécurité de l'information
- x BS 7799-2 = BS 7799-2:2002, qui n'est pas normalisée à l'ISO
 - x Spécification articulée autour de *clauses* et de *controls*
 - x *Clause* : Obligatoire, management de la sécurité de l'information
 - x *Controls* : Obligatoires si applicables (*statement of applicability*)
 - x La présence de la politique de sécurité est toujours applicable

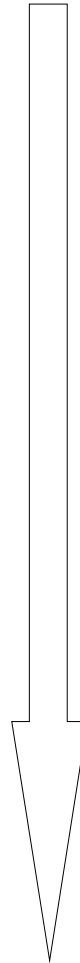
Ce que ces normes ne sont pas

- x Une norme strictement informatique
 - x Cela concerne l'information
- x Une checklist de sécurité
- x Une assurance d'un certain niveau de sécurité
- x Une méthodologie d'audit
- x Une méthode d'analyse de risques

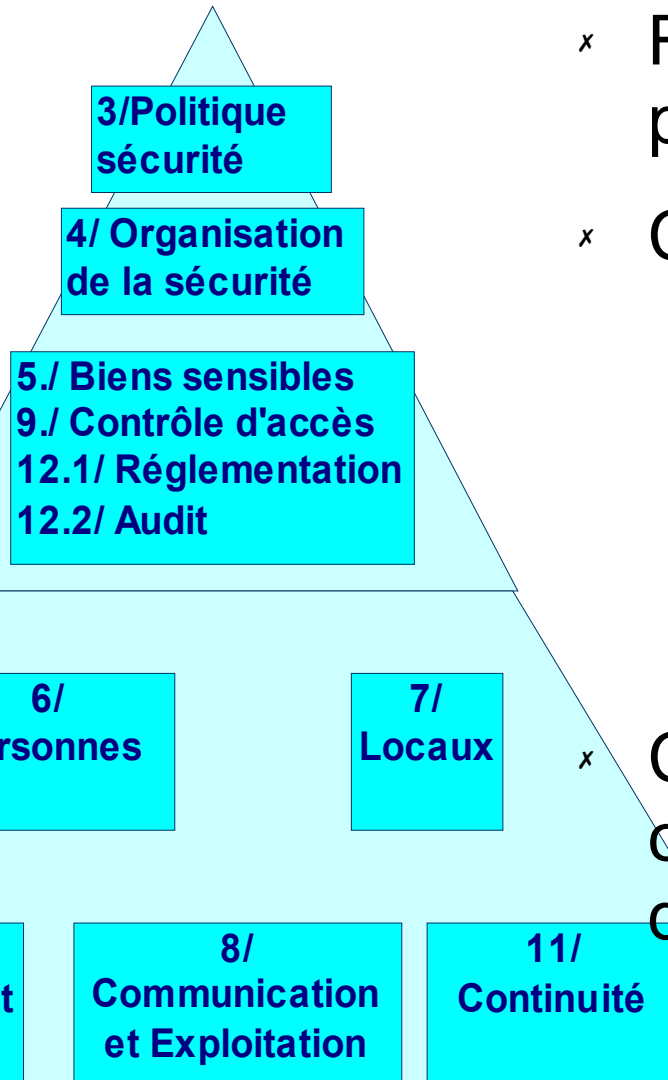
- x ISO17799:2000
 - x Défini des objectifs et des recommandations concernant la sécurité de l'information
 - x Norme globale applicable à tout type d'organisme
- x Est complétée par BS7799-2, qui n'est pas prévue à l'ISO
- x Historique ISO17799
 - x Groupe britannique ayant produit BS7799:1995, puis BS7799-1:1999
 - x Soumis 2 fois en procédure *fast track* à l'ISO
 - x Adopté en Décembre 2000 dans des conditions particulières
 - x Actuellement en phase de révision depuis 2001

- x Norme anglaise
 - x Reprise par plusieurs pays comme norme
 - x Pas de norme concurrente significative
 - x S'adresse à tout organisme qui souhaite améliorer sa sécurité
- x Défini les exigences d'un système de management de la sécurité de l'information
 - x Règles de bonnes pratiques à suivre
 - x Déclinables pour toutes les technologies et environnements
 - x Auditables et donc le suivi est contrôlable
 - x Permet d'attester que le niveau de sécurité du périmètre de la politique de sécurité est satisfaisant
- x Utilise le modèle PDCA : *Plan-Do-Check-Act*

Organisationnel



Opérationnel



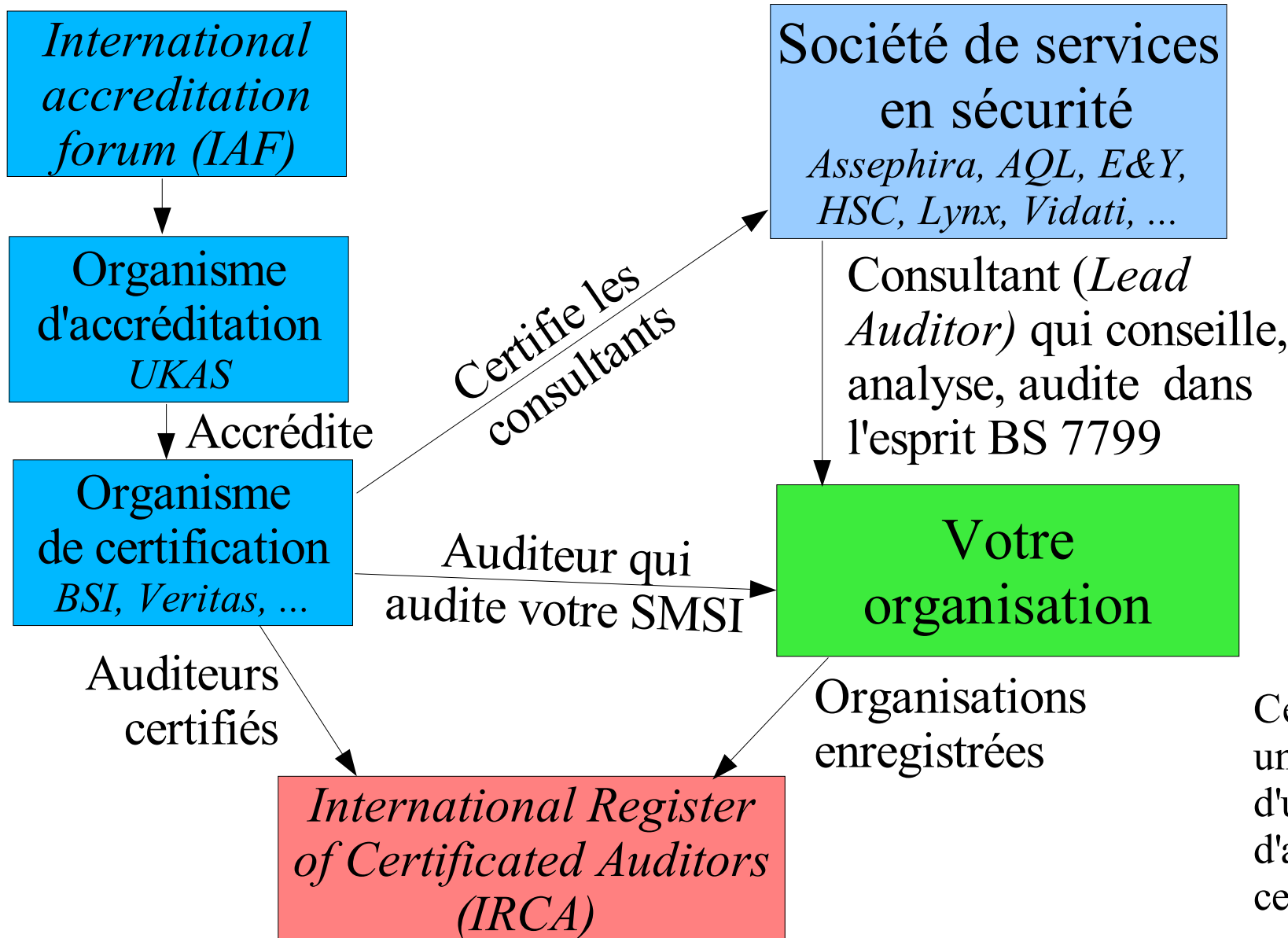
- x Référence de bonnes pratiques
- x Chaque chapitre inclu des
 - x Objectifs de sécurité
 - x Mesures à mettre en œuvre
 - x Contrôles à effectuer
- x Chaque chapitre peut être consulté indépendamment des autres

Numéros = chapitres de la norme

- x Couvre toutes les thématiques
 - x Politique de sécurité
 - x Organisation de la sécurité
 - x Classification et contrôle du patrimoine informationnel
 - x L'insécurité issue des défaillances humaines
 - x La sécurité physique
 - x La gestion des opérations et des communications
 - x N'ignore pas Internet
 - x Ignore les réseaux sans fil : c'est à l'auditeur de compléter (*controls*)
 - x Le contrôle d'accès
 - x Le développement
 - x La continuité d'activité
 - x La conformité à la réglementation

- x Système de Management de la Sécurité de l'Information (SMSI)
 - x Définir une politique de sécurité et des objectifs en sécurité
 - x Appliquer la politique
 - x Atteindre les objectifs
 - x Contrôler que les objectifs ont été atteints
- x Permet une certification de l'organisme
 - x Certification dite "ISO17799" impossible : abus de marketing
 - x Certification des auditeurs par le BSI : *BS7799 Lead Auditor*
 - x Abilités à mener un audit conformément aux principes de la BS7799
 - x Certification BS7799 de l'organisation par un organisme accrédité

- x Annexe A
 - x Normative
 - x Contient les objectifs associés à chaque recommandation de sécurité listée dans ISO17799, et pour chaque objectif les mesures à mettre en place
 - x Proche de ce que les experts en sécurité font souvent
 - x Reste très général et indépendant des technologies
 - x Exemples :
 - x 8.5.1 : *A range of controls shall be implemented to achieve and maintain security in networks*
 - x 9.4.1 : *Users shall only have direct access to the services that they have been specifically authorized to use*
 - x 9.4.8 : *Shared networks shall have routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications*



Ce schéma n'est pas un schéma officiel d'un organisme d'accréditation ou de certification

- x **Registre des organismes accrédités:**
http://www.ukas.com/about_accreditation/accredited_bodies/certification_body_schedules.asp
 - x BSI, Veritas, KPMG Audit, JACO-IS, JQAO, etc
 - x Système développé principalement au Royaume-Uni et au Japon
- x **Registre des organisations certifiées par des organismes accrédités :** <http://www.xisec.com/register.htm>
 - x Beaucoup de sociétés ayant mené une démarche de quasi-certification n'apparaissent pas
 - x Pas d'accréditation dans leur pays & ne souhaitent pas passer par un organisme anglais, cas d'entreprises françaises
- x **Registre des auditeurs certifiés et travaillant dans des organisations accréditées :** <http://www.irca.org/>
 - x La majorité des auditeurs titulaires d'une certification étant dans les sociétés de conseil, ils n'apparaissent pas dans ce registre

- x Une organisation qui se lance dans un processus de certification BS7799 s'engage dans un processus de trois ans
 - x Un audit BS7799 par un organisme de certification par an
 - x Chaque année les auditeurs sélectionnent avec l'organisme un échantillon de processus à auditer
 - x Les processus sélectionnés sont audités
 - x Si des disconformités graves sont constatées, la certification BS7799 est immédiatement supprimée
 - x Si des disconformités moins graves sont constatées, elles sont rapportées dans le rapport d'audit
 - x Le client est tenu dans un délai rapide de présenter un plan des actions correctives
 - x Au plus tard l'année suivante les auditeurs vérifient que ces actions ont bien été menées à terme
- x Le processus est continu, au bout de 3 ans, tout est à refaire

- x La société de service en sécurité pourra proposer
 - x Validation de la politique de sécurité et de son périmètre
 - x Aide à la rédaction des éléments documentaires du SMSI
 - x Description des objectifs, cartographie des processus impactés, ...
 - x Conseil sur l'organisation à mettre en place dans votre organisme
 - x Analyse du travail restant à faire pour atteindre la BS7799
 - x Notamment au travers d'audits de sécurité
 - x Organisationnels et techniques
 - x Conseil sur les actions correctives
 - x Pré-audit BS7799 à blanc
 - x Afin d'être sûr que l'audit par l'organisme de certification officiel se déroulera bien
 - x Avec ou sans engagement de résultat
- x La méthode de travail demeure pragmatique

Exemples de biens sensibles

Exemples de menaces

1/ Que protéger et pourquoi ?

Liste des biens sensibles

Permet de sélectionner ses mesures de sécurité sur la base d'une analyse de risques

- * Analyse de risque selon tout types de méthode y compris la sienne

2/ De quoi les protéger ?

Liste des menaces

Propose un référentiel commun international

- * Positionnement de son organisme vis-à-vis des autres

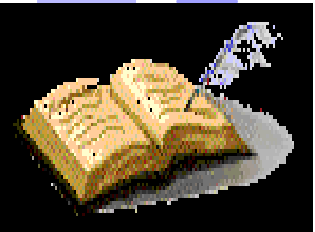
3/ Quels sont les risques ?

Liste des impacts et probabilités

Permet une utilisation partielle comme règle ou guide interne

4/ Comment protéger l'entreprise ?

Liste des contre-mesures



ISO17799

Exemples de recommandations

- x Avec une analyse de risque
 - x BS7799 ne précise pas d'obligation quand à la méthode d'analyse de risque
 - x MEHARI (Clusif) & EBIOS (DCSSI) sont compatibles ISO17799
 - x Beaucoup de sociétés de conseil utilisent une approche pragmatique qui n'impose pas l'usage d'une méthode d'analyse de risque
- x Pour communiquer
 - x En interne : du RSSI à la direction ou à l'ensemble de l'organisation
 - x A l'extérieur
 - x à vos clients, prospects, partenaires
 - x pour montrer que vous êtes au même niveau que les autres entreprises
- x Lors d'audits
 - x BS7799 est un référentiel
- x Pour acquérir la certification

- x Approche similaire à tout système de management
- x Méthode classique, recommandée par l'OCDE
- x Processus cyclique continu
- x Démontre que les bonnes pratiques sont documentées, appliquées et améliorées dans le temps
- x *Plan-Do*
 - x Investissement initial : formalisation de la gestion de risque, documentation des règles de sécurité applicables, etc
- x *Check-Act*
 - x Vérification que les mesures de sécurité prises sont appliquées, les solutions de sécurité utilisées, et l'ensemble régulièrement amélioré
 - x Audits périodiques de chaque composant du système d'information

- x Approche processus
- x Par le modèle PDCA : *Plan-Do-Check-Act*
- x Pour définir, implémenter, mettre en fonction, maîtriser et améliorer l'efficacité de l'organisation de son SMSI
 - x Bonne compréhension des besoins en matière de sécurité
 - x Politique de sécurité et objectifs clairs par rapport à son métier
 - x Contrôles lors de l'implémentation et la production
 - x Surveillance et révision de l'efficacité du SMSI
 - x Amélioration permanente du système à base des mesures objectives

ISO19011 : Audit des systèmes de management de la qualité (1/2)

- x Norme d'audit, Octobre 2002, remplace ISO14010/14011/14012:1996
 - x Basé sur les concepts et le vocabulaire ISO9000:2000
 - x Conçue pour l'audit des systèmes de management de la **qualité** ou de management **environnemental**
 - x S'applique parfaitement aux audits de gestion de la **sécurité**, notamment aux audits de réseau et de sécurité réseaux, plates-formes, applications, etc
 - x Les normes ISO17799 et BS7799-2 s'adressent en priorité à l'organisme, la norme ISO19011 s'adresse en priorité aux auditeurs
 - x Les auditeurs BS7799 utilisent généralement leur propre méthode
 - x Garantie la qualité de l'audit

- x La norme ISO19011 défini en détail le processus d'audit
 - x Les principes de l'audit
 - x La gestion du processus de l'audit dans le temps
 - x Etablissement, mise en œuvre et revue du programme d'audit
 - x Le programme d'audit :
 - x Objectifs, Étendue, Responsabilités et ressources, Procédures
 - x L'organisation de l'audit
 - x Les qualités et connaissances requises

- x Les normes elles-mêmes
- x ISO17799:2000 : présentation générale, Groupe ISO17799, Clusif, 03/2003
 - x <http://www.hsc.fr/presse/publications.html.fr#ouvrages>
 - x <http://www.hsc.fr/~schauer/clusif/Presentation-ISO17799.pdf>
- x BS7799-2 : presentation générale, Groupe ISO17799, Clusif, à paraître courant 2004

- x Je vous invite vivement à prendre connaissance de ces normes
- x Une bonne opportunité d'améliorer sa sécurité dans un cadre de référence international

Questions ?

www.hsc.fr

Herve.Schauer@hsc.fr

- x Plusieurs centaines de présentations et de documents sont disponibles sur <http://www.hsc.fr/ressources/>
- x Pour mieux me connaître :
 - x Biographies : http://www.hsc.fr/societe/herve_schauer.html.fr
http://www.solutionslinux.fr/fr/conferencier_detail.php?id_conferencier=68
 - x HSC : <http://www.hsc.fr/societe/>
 - x Associations : AFUL, AFUP, CLUSIF, IEEE, FNTC, IALTA, IETF, ISACA, ISOC, ISSA, CES, OSSIR, SAGE, SANS, SEE, USENIX,
<http://www.hsc.fr/societe/associations.html>

- x Alexandre Fernandez et Nicolas Jombart (certifiés *Lead Auditor* BS7799 chez HSC) pour leur relecture et corrections
- x Marie-Agnès Couwez et Pascal Lointier pour l'usage des 2 schémas du document du Clusif
- x Amor Zebar et son équipe pour leur accueil à Alger