



Certification ISO 27001

Club ISO 27001

26 octobre 2006

Alexandre Fernandez
Hervé Schauer



Sommaire

- ISO 27001 : PDCA
- Certification d'un système de management
- Processus de certification
- Schéma de certification
- Accréditation
- Autorités d'accréditation
- Certifications
- Certifications en sécurité des systèmes d'information
- Certifications des systèmes de management





Sommaire

- Certification ISO 27001
- Schéma de certification ISO 27001
- Normes utilisées
 - Norme d'audit
 - Normes d'accréditation
- Règlement de certification
- Organismes de certification en France
- Accréditation pour la certification de SMSI
- Auditeurs de certification





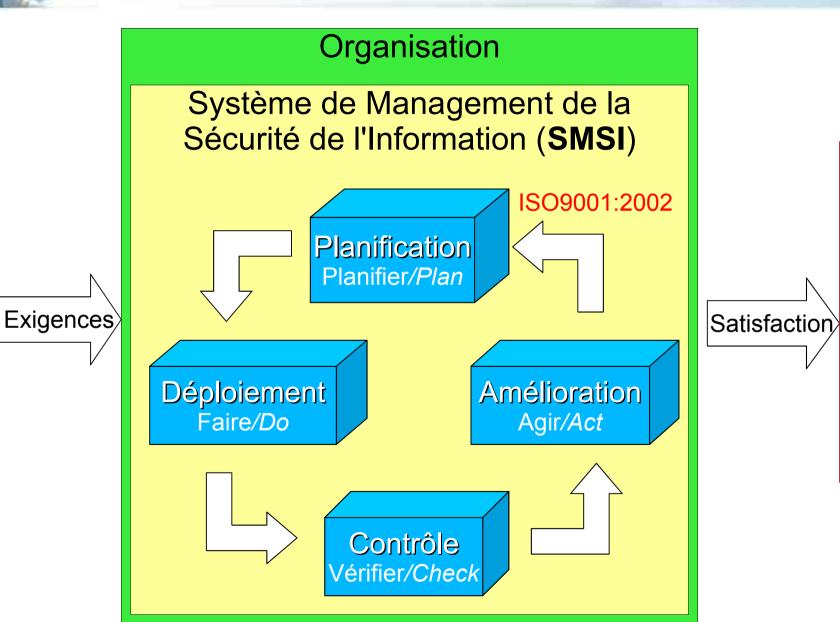
Sommaire

- Processus de certification ISO 27001
- Limites de la certification ISO 27001
- Intérêts de la certification ISO 27001
- Organisations certifiées
- Certificats ISO 27001 publics
- Certification des auditeurs
- Registres d'auditeurs
- Conclusion
- Annexe : acronymes





ISO 27001: PDCA







Parties prenantes



Certification d'un Système de Mgmt

- Assurance par une démonstration indépendante que le système de management est : IS 17021:2006
 - Conforme aux exigences spécifiées
 - Capable de réaliser de manière fiable la politique et les objectifs qu'il a déclarés
 - Mis en oeuvre de manière efficace
- Apporte une plue-value
 - À l'organisme, à ses clients, aux parties interessées
- Certification comprend :
 - Audit du système de management
 - Délivrance d'un certificat





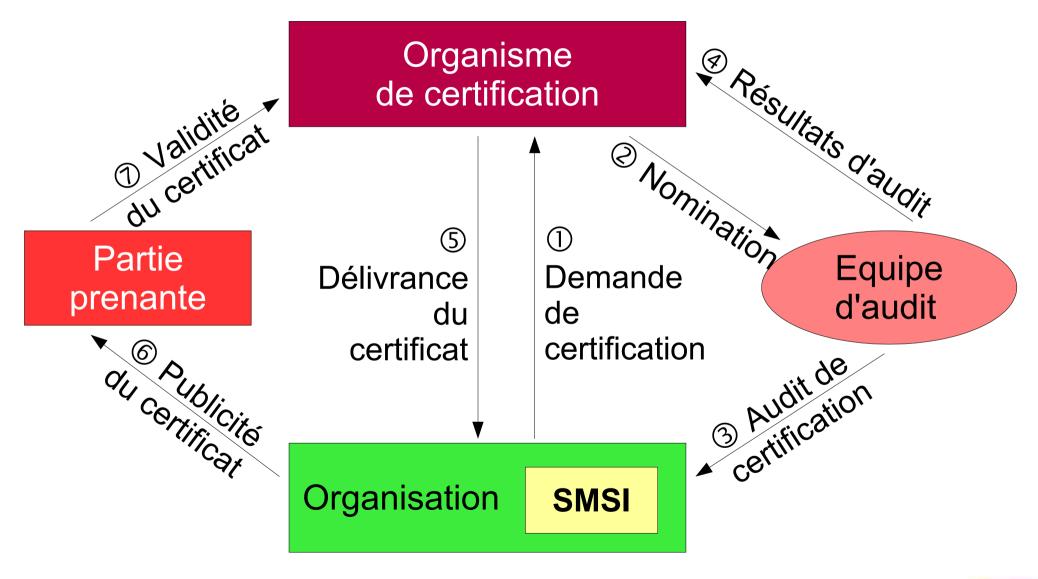






Schéma de certification

Autorité d'accréditation



Organisme de certification



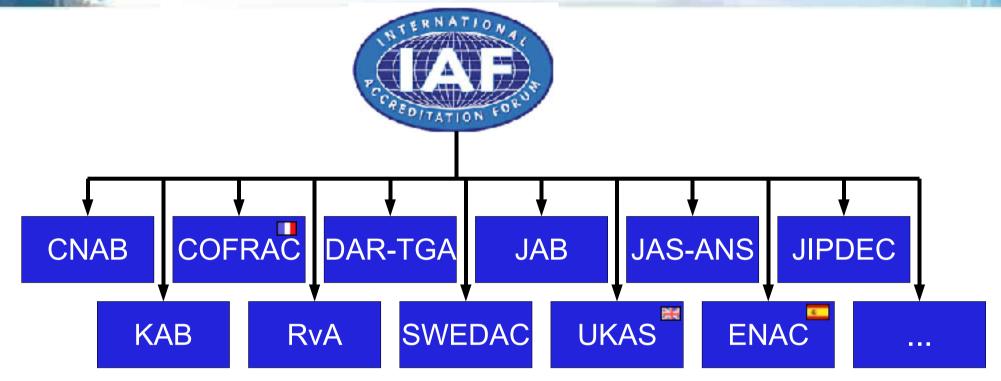
Organisation souhaitant être certifiée

- Schéma commun à toutes les certifications
- Autorité d'accréditation
 - Une seule par pays
 - Organisme d'état
- Organisme de certification (ISO17021 1)
 - Nombreux
 - Généralement des sociétés privées
 - Peut être un organisme gouvernemental
 - Avec ou sans pouvoir règlementaire





Accréditation



- Reconnaissance mutuelle internationale des organismes de certifications accrédités
 - MoU: Memorandum of Understanding
- Même valeur des certificats dans tous les pays
 - Certificat indien même valeur qu'un certificat français





Autorités d'accréditation

- France : COFRAC (Comité Français d'Accréditation)
 - Registre des organismes accrédités :



- LSTI pour les SMSI (ISO 27001) et les PSC/PSCe
- Grande-Bretagne: UKAS (United Kingdom Accreditation Service)
 - Registre des organismes accrédités :

http://www.ukas.com/about_accreditation/accredited_bodies/certification_body_schedules

- BSI, Veritas, KPMG Audit, JACO-IS, JQAO, etc pour les SMSI
- Espagne : ENAC (Entidad Nacional de Acreditación)
- Luxembourg : OLAS (Office Luxembourgeois d'Accréditation et de Surveillance)
- Suisse : SAS (Service d'Accréditation Suisse)







Certifications

- Quatres types de certification :
- ① Certification des produits
- Certification des organisations
 - ② Certification des services
 - ③ Certification des systèmes de management
 - ISO 17021
 - Norme pour toutes les certifications de systèmes de management
- 4 Certification de personnels
 - ISO 17024
 - Norme pour toutes les certifications de personnels





Certifications en sécurité des SI

- ① Certification des produits
 - En sécurité des SI : ISO 15408 : Critères d'évaluation pour la sécurité des technologies de l'information
- Certification des organisations
 - ② Certification des services
 - Ex. en sécurité des SI en France : PRIS v2 par LSTI : Politique de Référencement Intersectorielle de Sécurité (DCSSI/DGME)
 - Pour prestataires de services de confiance : signature électronique, authentification, horodatage électronique, ...
 - ③ Certification des systèmes de management
 - En sécurité des SI : ISO 27001
- 4 Certification de personnels
 - En sécurité des SI :
 - CISSP par ISC2
 - En France: ISO 27001 Lead Auditor par LSTI (accréditation en cours)





Certifications des systèmes de mgmt

- Certification des systèmes de management :
 - de la qualité (SMQ) : ISO 9001:2002
 - environnemental (SME): ISO 14001:2004
 - de la santé et la sécurité au travail (SMSST) : OHSAS 18001:1999
 - n'est pas devenu une norme ISO comme prévu
 - de la sécurité de l'information (SMSI) : ISO/IEC 27001:2005
 - de la sécurité alimentaire (SMSA) : ISO 22000:2005
 - des services informatiques des organismes : ISO 20000:2005 (ITIL, BS15000)
 - de la sureté pour la chaîne d'approvisionnement : ISO 28000:2005
 - **.** . . .





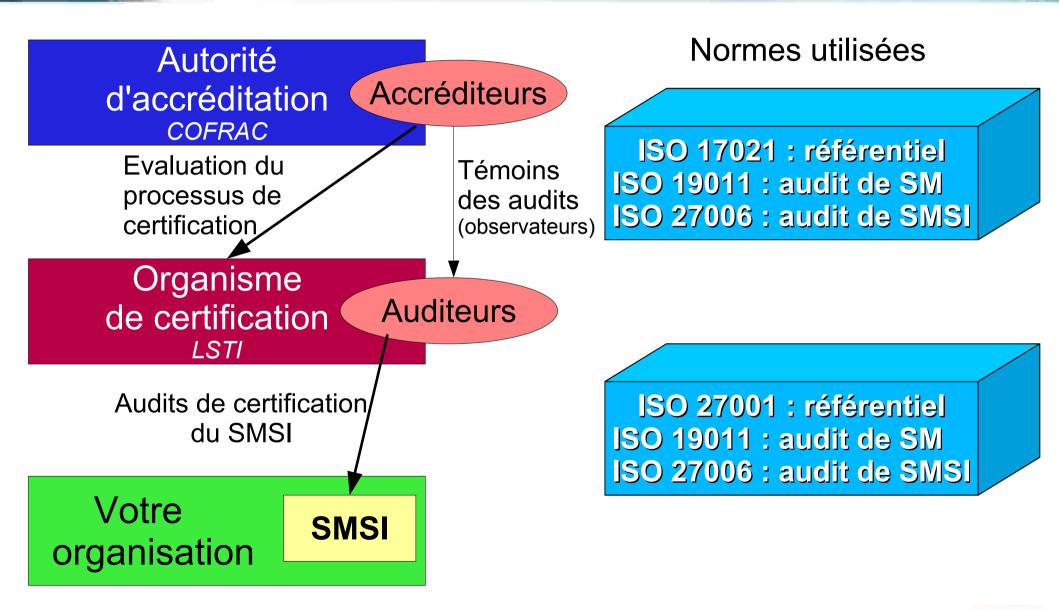
Certification ISO 27001

- Certification des Systèmes de Management de la Sécurité de l'Information
- Schéma de certification commun à toute la certification
 - Autorité d'accrédiation
 - Se déclare compétante pour le domaine : certification des SMSI
 - Evalue, puis accrédite des organismes de certification
 - Accréditeurs (Assessors) ou auditeurs d'accréditation
 - Organismes de certification accrédités
 - Aucun, un ou plusieurs par pays
 - Evalue puis certifie votre organisation suivant l'ISO27001
 - Auditeurs (Auditors)
 - Organisations certifiées
 - Peuvent rendre public leur certificat





Schéma de certification ISO 27001







Normes utilisées

- Norme d'audit de système de management
 - ISO 19011
 - Lignes directrices pour l'audit des systèmes de management
- Normes d'accréditation
 - ISO 17021 qui était auparavant EN 45012 / ISO Guide 62
 - Conformity assessment requirements for bodies providing audit and certification of management systems
 - EA 7/01
 - Guidelines on the application of EN 45012 / ISO Guide 62
 - ISO 27006 qui remplacera EA 7/03
 - Guidelines for the accreditation of bodies operating certification of Information Security Management Systems





Norme d'audit

- ISO 19011
 - Spécifie les règles que doit suivre un auditeur de système de management
 - Bonnes pratiques d'audit
 - Audit interne ou externe
 - Principes de l'audit
 - Etablissement, mise en oeuvre et revue des programmes d'audit
 - Programme d'audit : revue de documents, audit sur site, rapport
 - Réunions d'ouverture et de cloture
 - Compétences des auditeurs
 - Qualités personnelles, connaissances, aptitude, formation initiale, formation d'auditeur





Normes d'accréditation

ISO 17021

- ISO Guide 62:1996 est devenu EN 45012:1998 (norme européenne) puis IS 17021:2006
- Spécifie les exigences
 - Qu'un organisme de certification doit satisfaire
 - Dans le domaine des systèmes de management
 - Pour être reconnu compétent et fiable
- Objectif
 - Rendre homogènes les certifications délivrées par les différents organismes dans le monde





Normes d'accréditation

- EA-7/01
 - Précise des informations utiles à l'application de l'EN45012:1998
 - Nombre de jours d'audit en fonction du nombre d'employés
 - Qui sera remplacé par ISO 27006
- Documents EA (European co-operation for Accreditation) disponibles en ligne sur le site de l'EA
 - www.european-accreditation.org





Normes d'accréditation

- ISO 27006
 - EA-7/03 deviendra IS 27006:2006 ou IS 27006:2007
 - Référentiel d'application de l'ISO 17021, ISO 27001 et ISO 19011
 - À l'accrédidation d'un organisme de certification de SMSI
 - sans ajouter de réelles nouvelles exigences
 - À l'audit de certification d'un SMSI
 - Compétence des auditeurs et experts techniques
 - Programme d'audit appliqué aux SMSI
 - Appréciation de la complexité du SMSI à auditer
 - Calcul de la durée des audits
 - Harmonisation de l'audit des mesures de sécurité de la déclaration d'applicabilité (DDA ou SOA)
 - Qualification : organisationelle et/ou technique
 - Vérification visuelle
 - Test sur le système possible, recommandé, obligatoire

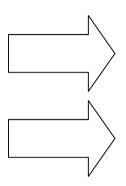




1/5

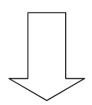






Guides EA-7/01 et EA-7/03 Référentiels ISO 17021 et ISO 27006





Organisme de certification



Référentiel ISO 27001



Organisation demandant la certification

SMSI









- Règlement de certification annexé au contrat de certification (IS 17021:2006 5.1.2)
 - Formalise des exigences complémentaires au référentiel ISO 27001
 - Entre l'organisme de certification et l'organisation à certifier
- Exigences complémentaires exigées dans ISO 17021
 - Confidentialité (8.5)
 - Informations à échanger (8.6)
 - Programme d'audit ^(9.1)
 - Plan d'audit initial (9.2) et d'audit de surveillance (9.3)
 - Renouvellement du certificat (9.4)
 - Exemple : changement de contexte législatif





- Exigences complémentaires exigées dans ISO 17021
 - Usage de la marque (8.4)
 - Traitement des plaintes des clients (4.7) (9.8)
 - Suspension du certificat (9.6)
 - Demande du certifié : force majeure, déménagement, ...
 - Suspension publique
 - Publication du motif de la suspension à la discrétion de l'organisation certifiée
 - Organisme de certification doit vérifier que l'organisation certifiée ne continue pas la publicité de son certificat (8.4.3) (9.6.3)
 - Processus d'appel (9.7)





- Exigences complémentaires exigées dans ISO 27006
 - Production par l'analyse de risques de résultats comparables et reproductibles (G.9.2.3 (2) a)
 - Analyse de la sécurité par rapport aux menaces pertinente (G.9.2.3 (3) a)
 - Procédures d'identification, d'examen et d'évaluation reliant les menaces aux actifs, vulnérabilités et impacts cohérentes avec la politique, les objectifs et les cibles de sécurité (G.9.2.3 (3) b)
 - Temps passé par les auditeurs sur la revue documentaire, l'évaluation de l'analyse de risque, l'audit d'application et le rapport d'audit (G.9.2.4 (1) a.iii)





- Durée des audits précisée dans ISO 27006 (actuellement encore dans EA-7/01)
 - Audit du SMSI (A.3.2)
 - Au minimim 1 jour de revue documentaire et 1 jour de revue sur site
 - Audit des mesures de sécurité → + 2 jours
 - Audit des autres sites géographiques → + ½
 journée par site
 - Facteurs de complexité du SI : moyen → + ¼
 journée, élevé → + ½ journée (A.1.1)
 - Nombre de clients (ex: service en ligne)
 - Taille du SI: nombre de serveurs, postes de travail et applications
 - Personnel des fournisseurs dans le SMSI
 - Technologies : Usage de chiffrement ou d'ICP

Number of employees	Auditor time for initial audit (auditor days)
1-10	2
11-25	3
26-45	4
46-65	5
66-85	6
86-125	7
126-175	8
176-275	9
276-425	10
426-625	11
626-875	12
876-1175	13
1176-1550	14
1551-2025	15
2026-2675	16
2676-3450	17
3451-4350	18
4351-5450	19
5451-6800	20





Organismes de certification en France

- Accrédité par le COFRAC pour la certification des SMSI
 - LSTI : La Sécurité des Technologies de l'Information
 - www.lsti.fr



- Dossier n° 04-063
- Accréditation délivrée en juin 2006
- Peut-être en cours d'accréditation au COFRAC
 - AFAQ-AFNOR, BSI, BVQI, DNV, SGS
- En projet :
 - AQL, OPPIDA, VISION IT
 - Peut-être d'autres qui ne se sont pas déclarés auprès d'HSC





Accréditation pour la certif. de SMSI

- Dans chaque pays
 - Une et une seule autorité d'accréditation
 - Zéro, un ou plusieurs organismes de certifications accrédités pour la certification des SMSI
- Si pas d'organisme de certification accrédité dans un pays
 - Alors tout organisme de certification accrédité dans un autre pays peut certifier
- Si au moins un organisme de certification accrédité dans un pays
 - Alors l'usage veut que les organismes de certifications étrangers se fassent accréditer dans le pays
 - Légalement pas obligatoire







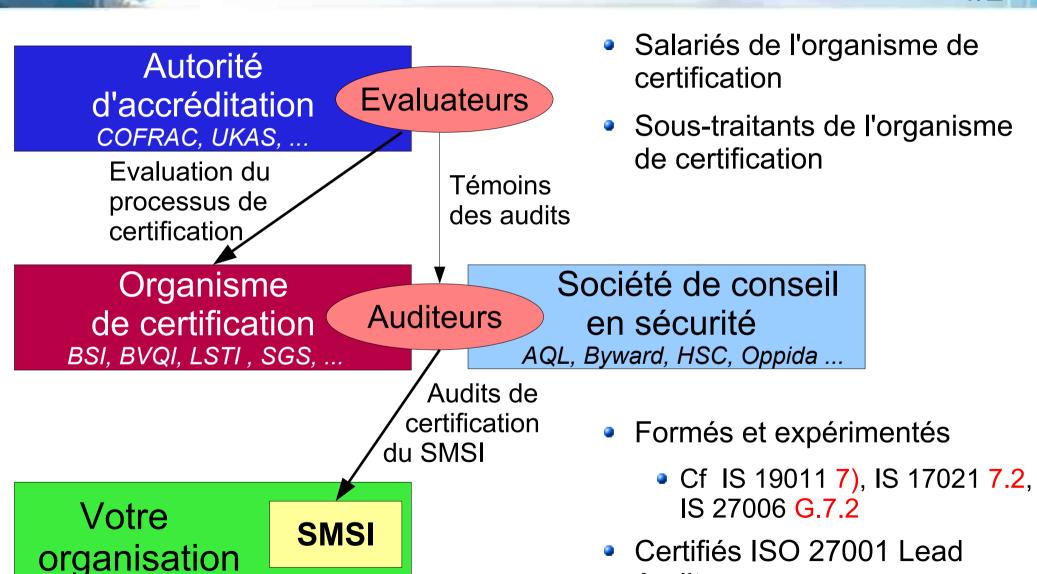
Accréditation pour la certif. de SMSI

- Si l'autorité d'accréditation se déclare incompétante pour l'audit de SMSI
 - Alors un organisme de certification peut se faire accréditer par n'importe quel organisme d'accréditation dans le monde
 - Exemple : premier organisme de certification des SMSI en Inde accrédité aux Pays-Bas





Auditeurs de certification





Auditor



Auditeurs de certification

- Organismes de certification font souvent appel à des tiers pour effectuer les audits de certification
 - Des sociétés de service ou des indépendants en sécurité qui ne seraient pas intervenus en conseil auparavant
 - Une même entité juridique ne peut pas être organisme de certification et de conseil
 - Un auditeur doit demeurer indépendant
 - Organismes de certification n'ont pas toujours le personnel compétant dans le domaine de la sécurité de l'information
 - Souvent plus des qualiticiens





1/4



départ **→**

Audit initial

+ 6 mois

+ 12 mois -

+ 18 mois

+ 24 mois

+ 30 mois

3 ans

Audits de surveillance ou de contrôle

- Généralement tous les 6 mois
- Si plus de 12 mois entre deux audits la certification est perdue (IS 17021 9.3.2.2)
- Audit de renouvellement de la certification
 - Tous les 3 ans
 - Permet de remettre en concurrence les organismes de certification





2/4

- Audit initial
 - Couvre l'ensemble des clauses 4 à 8 de l'ISO 27001
 - Ne couvre pas nécessairement tous les processus inclus dans le périmètre du SMSI
- Audit de surveillance
 - Reprise de tous les écarts constatés lors de l'audit précédent
 - Echantillonage
 - Par rapport aux clauses 4 à 8 de l'ISO 27001
 - Par rapport aux processus inclus dans le périmètre du SMSI
- Audit de recertification ou de renouvellement de la certification
 - Comme l'audit initial





- Auditeurs constatent des écarts, typiquement :
 - Non-conformité majeure, ou écart majeur
 - Non-conformité mineure, ou écart mineur
 - Remarque
- Audités proposent des actions correctives
- Formalisé dans des fiches d'écart
- Évolution de la classification des écarts qui n'ont pas été corrigés d'un audit à l'autre
 - Non-conformité mineure
- → Non-conformité majeure

Remarque

→ Non-conformité mineure





4/4

- Audit de certification
 - Si des non-conformités majeures sont constatées, la certification ISO27001 n'est pas accordée (audit initial) ou supprimée (audit de surveillance)
 - Si des non-conformités mineures et/ou des remarques sont constatées, elles sont rapportées dans le rapport d'audit
 - Avec les actions correctives proposées par l'audité
 - Au plus tard lors de l'audit suivant les auditeurs vérifient que ces actions correctives ont bien été menées à terme





Limites de la certification ISO 27001

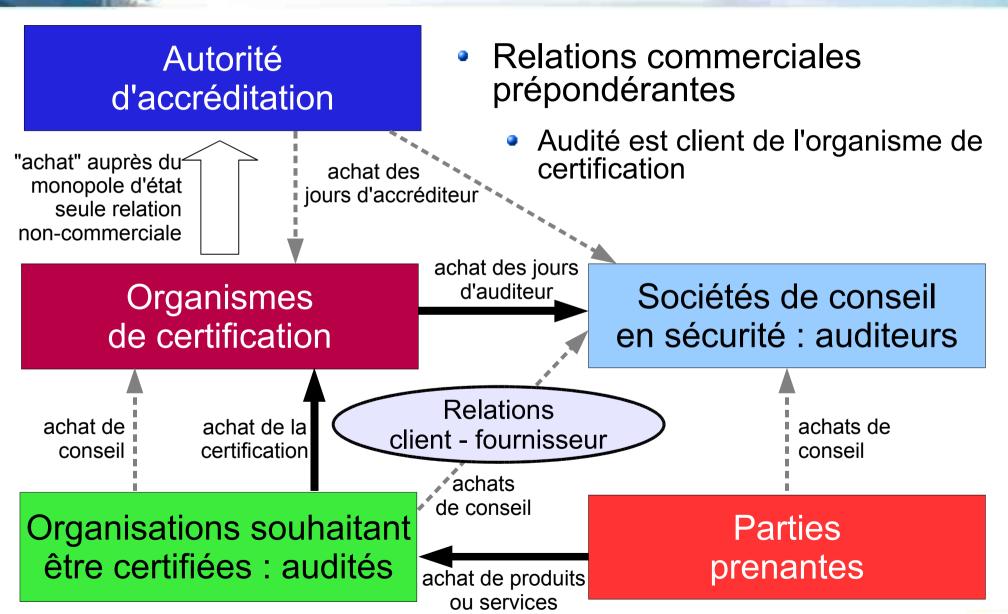
- Inhérentes à un processus en phase d'amorçage
 - Volonté commerciale du BSI d'amorcer la pompe quitte à dévaloriser les processus
 - Faible expérience des organismes d'accréditation par rapport aux spécificités des enjeux en sécurité des systèmes d'information
 - Activité nouvelle pour les organismes de certification
 - Inexpérience des auditeurs face à des audités plus aguerris
 - Manque de responsables d'audit (lead auditor)
 - Auditeurs avec compétence sécurité et sans compétence qualité et audit de certification
 - Auditeurs avec compétence qualité sans compétence en sécurité des systèmes d'information
 - Manque de formalisation de la profondeur des vérifications à effectuer





Limites de la certification ISO 27001

2/8





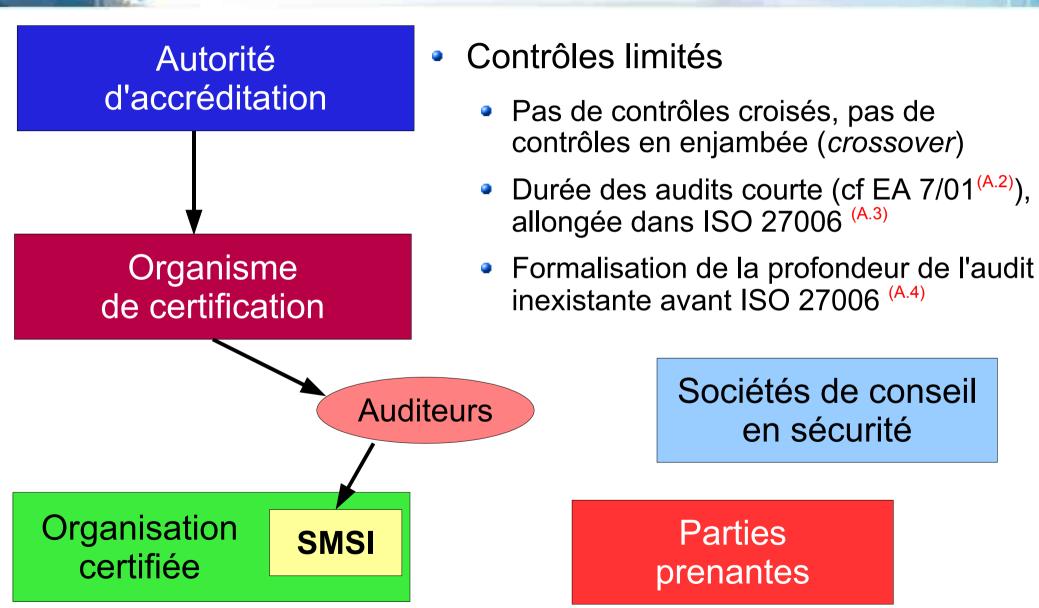


- Relations commerciales prépondérantes
 - Concurrence sur les prix entre organismes de certification
 - - Trouver un prétexte pour demander à l'organisme de certification le remplacement de l'auditeur (IS 19011 6.2.4) (IS 17021 9.1.7)
 - Demander à son organisme de certification un autre auditeur pour le prochain audit
 - Changer d'organisme de certification
 - Tendance à la minimisation des écarts





4/8







- Pré-audit
 - Organismes de certifications ont tous inventé le "pré-audit" ("preassessment")
 - Audit de conseil qui précède l'audit de certification
 - Fait pas les auditeurs de certification
 - Concurrence avec les sociétés de conseil
 - Pas normalisé
 - Non-conforme avec l'ISO 17021





- Pas de norme pour qualifier formellement les écarts
 - Non-conformité majeure, non-conformité mineure, remarque

- Possible de certifier un SMSI qui n'a pas encore réellement tourné
 - Sans révision du SMSI
 - Sans enregistrements dans la durée
 - Pourrait être changé avec ISO 27006





- Mélanges des genres
 - Société de conseil en même temps organisme de certification
 - Organisme de certification en même temps société de conseil
 - Monopole de la production et traduction des normes reconnu d'intérêt public et en partie financé par l'état, en même temps organisme de certification à but lucratif

•





- Rappel : certification d'un processus
- Pas certification d'un état ou d'un résultat
 - Certification du fait que le système de management fonctionne, pas du niveau de sécurité
 - Et auditeur de certification ne doit pas apporter de conseil
 - Obligation d'accepter lors d'un audit de certification certaines aberrations
 - Ne protège pas d'un incident ayant un retentissement médiatique
 - Peut donner une fausse idée d'être en sécurité





Intérêts de la certification ISO 27001

Sécurité

- Processus d'amélioration continue, donc le niveau de sécurité a plutôt tendance à croître
- Meilleure maîtrises des risques
- Diminution de l'usage des mesures de sécurité qui ne servent pas
- Homogénéisation
 - Référentiel universel, international
 - Facilite les échanges d'expérience
 - Fera le lien avec les autres métiers





Intérêts de la certification ISO 27001

- Communication aux parties prenantes
 - Savoir-faire de la profession, pratiques éprouvées
 - Référentiel qui améliore la confiance
- Communication aux auditeurs hors SSI
 - SoX et SAS70, LSF et LCEN, Bâle 2, Commission bancaire, Cours des comptes, ITIL/ISO20000, ...
- Communication interne
 - Même référentiel international





Intérêts de la certification ISO 27001

- Mutualisation des audits
 - Moins d'audits de sécurité à mandater pour les parties prenantes
 - Moins d'audits de sécurité à supporter pour l'organisation certifiée
- Réduction des coûts
 - Par la diminution d'usage de mesures de sécurité inutiles
 - Par la mutualisation des audits
- Simplicité
 - Processus simple et peu couteux
 - Par la certification du processus qui s'améliore





Organisations certifiées

- Registre des organisations certifiées par des organismes accrédités
 - Qui souhaitent publier leur certificat
 - http://www.ISO27001certificates.com/
- Publication des certificats optionnelle
 - Un certificat peut concerner un sous-ensemble d'une organisation donc une organisation peut en avoir plusieurs
- Trois certificats publiés en France (juillet 2006)
 - Donc une seule société française
- 57 en Allemagne, 42 en Italie, ...
- 1 au Maroc





Certificats ISO 27001 publics

- Juillet 2006 : 2746 certificats ont étés publiés
- Forte croissance en Inde
- Bon démarrage aux USA

Royaume-uni: 9 %

• Europe: 11 %

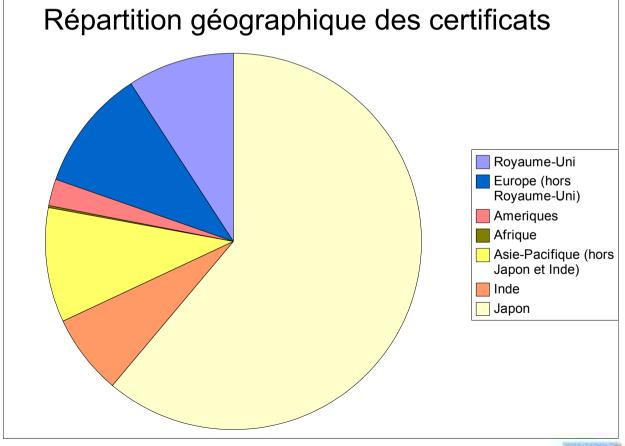
Amériques : 2 %

• Afrique : 0 %

Asie-Pacifique : 10 %

• Inde: 7 %

Japon : 61 %







Certification des auditeurs

- ISO27001 Lead Auditor ou responsable d'audit ISO27001
 - ISMS Lead Auditor ou responsable d'audit de SMSI
 - Anciennement BS7799 Lead Auditor

- Proposé en français sous deux formes
 - Formation et examen liés
 - Formation et examen organisés par des entités distinctes





Certification des auditeurs

- Formation et examen liés :
 - AFNOR/Auditware, BSI/Byward, BVQI, Netexpert/SGS
 - Formateur délivre la certification au stagiaires

- Formation et examen organisés par des entités distinctes :
 - Conformément à la norme ISO 17024
 - Possibilité d'accréditation > reconnaissance nationale et internationale
 - LSTI pour l'examen et la certification
 - Double correction manuelle
 - Fidens ou HSC pour la formation





Certification des auditeurs

- ISO27001 Lead Auditor : certification d'auditeur
 - Pas certification en sécurité
 - Audit de certification, pas audit de conseil
 - Difficile pour les consultants en sécurité habitués à l'audit de conseil
 - Double compétence sera indispensable avec l'ISO 27006
- Nombreuses autres certifications des individus en sécurité
 - CISM (www.afai.asso.fr)
 - CISSP (www.isc2.org)
 - ProCSSI (www.inseca.fr)
 - etc





Registres d'auditeurs

- Service d'enregistrement et de publication des auditeurs de certification
 - Sociétés à but lucratif >> service payant
 - Aucune reconnaissance officielle ni accréditation
 - Confiance auprès de ces registres par certains organismes de certification → sous-traitance de l'obligation de contrôle des compétences des auditeurs
 - Registres revendent également tous eux-mêmes de la formation et de la certification
 - Enregistrent tous les types d'auditeurs dont ceux de SMSI
- IRCA (IQA): International Register of Certificated Auditors (www.irca.org)
- RABQSA (www.rabqsa.com)
- ICA (AFAQ-AFNOR): Institut de Certification des Auditeurs (www.afaqcompetences.org)
 - Pas encore d'enregistrement d'auditeurs de SMSI en France





Conclusion

- Certification ISO 27001 identique aux autres certifications de systèmes de management
- Démonstration universelle et formelle
 - De sa volonté de s'améliorer en sécurité
 - De sa volonté de respecter un minimum en sécurité
- Simple, pragmatique et peu couteux
- Accessible à tous
- Démonstration aisée de sa sécurité et de sa volonté pour établir la confiance
 - Ne dispense pas les parties prenantes de faire preuve de discernement





Prochains rendez-vous

- Formation ISO27001 Lead Auditor :
- HSC
- Certification ISO27001 Lead Auditor par LSTI
- http://www.hsc.fr/services/formations/

Lyon: 27 nov -1 déc

Paris: 4 - 8 décembre

Genève: 22-26 janvier

Toulouse: 5-9 février

Sécurité VoIP & Enquêtes post-incident

Tutoriels les 22 et 23 novembre 2006

http://www.infosecurity.com.fr/?Jpto=116&IdNode=11



- Surveillance et détection sous Linux
 - Tutoriel en deux parties le 1er février 2007
 - http://www.solutionslinux.fr/



Questions?

Herve.Schauer@hsc.fr www.hsc.fr





Annexe: acronymes

- EA: European co-operation for Accreditation
 - www.european-accreditation.org
- EN : European Norm
- IAF : International Accreditation Forum
 - www.iaf.nu
- IRCA: International Register of Certificated Auditors
 - www.irca.org
- ISO
 - Pas un acronyme, vient du grec isos : égal
 - Organisation Internationale de Normalisation
 - International Organisation for Standardization
 - www.iso.ch

