Gouvernance de la sécurité des SI

Dominique Bergerot, membre du comité directeur ADELI

Philippe Junière, consultant en sécurité SI depuis 15 ans a été notre conférencier d'Autour d'un verre le 3 février 2009. Le thème de cette conférence étant très large, et la sécurité des SI un sujet souvent traité sur des aspects techniques, il nous a proposé de retracer l'historique en terme de démarche de la gouvernance de la sécurité des SI de l'entreprise au travers des normes et référentiels de bonnes pratiques depuis l'Orange Book (DoD5200.28-STD) en 1985 jusqu'à la famille de normes ISO 27000 publiée à partir de 2005.

Introduction

Lors de son expérience professionnelle, Philippe Junière est intervenu pour des grandes entreprises et a observé que parfois une politique sécurité avait bien été définie et initiée, que le document existait, mais que cette politique n'était pas mise en œuvre de manière réelle. Par contre, il arrive que des entreprises sensibilisées au sujet appliquent de fait le processus d'amélioration continue, sans que cela soit formalisé.

Selon lui, les deux domaines sécurité et qualité qui étaient séparés et l'affaire de spécialistes de cultures assez différentes, convergent de plus en plus.
Les principaux thèmes abordés ont été:

- l'historique des principaux standards en sécurité logique et visant la certification des logiciels ;
- la famille des normes ISO 27000 ;
- Qualité et SMSI (système de management de la sécurité des SI) et outils d'aide à la gouvernance.

Principaux standards en sécurité logique

Normes et référentiels fondés sur des critères d'évaluation de certification

En 1985, le DoD (Department of Defense) américain a publié la norme DoD 5200.28-STD (**TCSEC** ou Trusted Computer System Evaluation Criteria) connue également sous le nom d'Orange Book utilisée pour **certifier** des systèmes d'exploitation d'ordinateurs. Une extension, le Red Book spécifie les exigences au niveau réseau, ce qui a permis de certifier certaines solutions de réseau local. L'Orange Book spécifie quatre niveaux de sécurité de A (la plus stricte) à D en passant par les systèmes de niveau B dits "multiniveau" fondés sur le contrôle d'accès obligatoire et les systèmes de niveau C pour des fonctions de contrôle d'accès discrétionnaires renforcées.

En 1991, l'**ITSEC** (Information Technology Security Evaluation Criteria) publie un standard européen qui distingue fonctionnalités exigées et niveau d'assurance procuré par l'évaluation. Les critères d'assurance se décomposent en critères de conformité (correctness) et d'efficacité (effectivness). Le périmètre de certification de l'ITSEC concerne toujours le matériel et le logiciel qui implémentent des fonctions de sécurité (calculateur et réseau).

De 1996 à 1999, la norme ISO 15408, fruit de la mise en commun des travaux des USA, du Canada et des pays européens (ITSEC), ce qui lui vaudra le nom de Critères Communs, est élaborée et devient une norme reconnue au niveau mondial. Le document est structuré en trois parties : introduction et modèle général, exigences fonctionnelles de sécurité et exigences d'assurance de sécurité.
Les principaux concepts introduits sont :

- les profils de protection (PP ou Protection Profile) qui correspondent à un exemple type de fonctions et d'exigences de sécurité pour une catégorie de produits ;
- les cibles à évaluer (TOE ou Target of Evaluation) décrivent l'objet à certifier ;
- les ST (Security Target) définissent le niveau de sécurité ;
- les composants qui représentent les ensembles élémentaires d'exigences de sécurité.

Les documents sont disponibles sur le site de la DCSSI, organisme officiel français rattaché au Premier Ministre.

La DCSSI a par ailleurs défini un spectre de caractéristiques d'évaluation nommé niveau standard qui est un EAL2+ (on parle de EAL2 augmenté), et un niveau dit renforcé EAL4+. Un troisième niveau, dit niveau élevé est défini en fonction du type de dispositif. Le *niveau* d'assurance *EAL (Evaluation Assurance Level)* défini de 1 à 7, 7 pour le plus strict, représente le *niveau* de confiance que l'on peut accorder à la mise en œuvre des objectifs de *sécurité.*

Les certifications EAL consistent en un niveau d'assurance concernant la qualité et les conditions de développement d'une solution à travers différents

processus de test et de surveillance, elles ne constituent cependant pas une garantie de sécurité absolue dans laquelle on peut avoir une confiance aveugle.
Actuellement, les produits et solutions certifiés jusqu'au niveau EAL4 commencent à être nombreux, mais il est important de préciser sur quelle cible d'évaluation, ou en référence à quel profil de protection.

Méthodes d'Analyse de Risque (ou d'appréciation des risques)

La méthode MARION (Méthode d'Analyse de Risques Informatiques Orientée par Niveau)
Cette méthode a été lancée dans le cadre du CLUSIF dans les années 80, avec parmi ses initiateurs des spécialistes Sécurité du monde des Assurances.

La méthode MEHARI (MEthode Harmonisée d'Analyse de RIsques).
En 1996, le CLUSIF donne naissance à la méthode MEHARI et invite les utilisateurs de MARION à migrer vers MEHARI. MEHARI se place dans un cadre plus global "Système d'Information". MEHARI veut fournir aux organisations une gamme d'outils adaptés au management de la sécurité : plans de sécurité, schémas directeurs, mise en place de règles ou politiques de sécurité, conduite de diagnostics, rapides ou approfondis sur l'état de la sécurité, évaluation et le management des risques, gestion de la sécurité dans la conduite de projets de développement, sensibilisation et formation à la sécurité, pilotage de la sécurité et le contrôle des actions décidées.

MELISA (Méthode d'Evaluation de la Vulnérabilité Résiduelle des Systèmes d'Information)
MELISA, contemporaine de MARION est née à la DGA (Délégation Générale pour l'Armement). Elle a longtemps été promue et supportée par la société CF6, puis abandonnée après le rachat de CF6 par TELINDUS. MELISA a la réputation d'être une méthode assez lourde plutôt adaptée aux très grosses entités. Historiquement, certaines entités militaires, comme le CELAR (Centre Electronique de l'Armement), se sont intéressées parallèlement à d'autres méthodes.

La Méthode EBIOS publiée par la DCSSI
Créée en 1995, EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est la méthode retenue actuellement par l'état français. C'est une méthode abordable, pouvant être déclinée suivant des modalités souples, depuis un simple guide de démarche jusqu'à une méthode plus contraignante. Elle s'adresse au niveau de la DSI plus qu'au niveau de l'entreprise.
Elle permet de produire différents types de livrable :

- FEROS (Fiche d'Expression Rationnelle des Objectifs de Sécurité)
- Profil de Protection
- Cahier des Charges SSI
- Synthèse d'Etude de sécurité
- Politique de Sécurité

De nombreuses informations et d'outils gratuits (logiciel, questionnaires) sont disponibles sur le site de la DCSSI (www.ssi.gouv.fr).

Sécurité dans TCP/IP
Philippe Junière a ensuite rapidement évoqué la sécurité du protocole TCP/IP, qui concerne les normes techniques liées à Internet, standards de fait et donc incontournables.
Le modèle sur lequel repose la standardisation de ces protocoles et technologies est original et particulièrement ouvert. Il a fait ses preuves. Il repose essentiellement sur deux familles d'organismes : l'IETF (IESG, IAB, ISOC…) et le W3C. Un certain nombre de sous comités de ISO-IEC/JTC1 travaillent sur des mécanismes de TCP/IP ; l'évolution de TCP/IP ne se fait donc pas sans lien de coordination avec l'ISO.
Les RFC (Request for Comment) existent depuis 1969 et celle sur TCP/IP depuis 1975.
Le protocole Internet, IP, était caractérisé initialement par une recherche de disponibilité et d'autoadaptation, la sécurité n'était pas une préoccupation majeure.

Avec le développement du e-commerce, la sécurisation des échanges sur internet (protocoles SSL puis TLS (Transport Layer Security) normalisé en 1999) a permis d'utiliser « https » avec des applications sécurisées pour le paiement en ligne ainsi que l'utilisation de systèmes d'authentification forts (tels que les PKI). Tous ces outils logiciels sont fondés sur la cryptographie et les certificats.

Famille des normes ISO 27000

Standards britanniques BS 77999

À partir de 1995, l'organisme britannique de normalisation - British Standard Institute - a publié successivement deux standards :

- Le standard BS 7999-1 qui est un Guide de bonnes pratiques de Sécurité déclinées en 10 thèmes principaux : existence d'une politique de sécurité dans l'entreprise, organisation de la sécurité, classification des informations et procédures de traitement, risques créés par le personnel et mesures de sécurité, risques liés à l'environnement (locaux, accès, risques physiques, .), administration de la sécurité, contrôle de l'accès aux informations, développement, exploitation et maintenance des systèmes, plan de continuité, audit de contrôle et légalité des dispositifs ;
- Le standard BS 7999-2 qui contient des recommandations pour définir un cadre de gestion de la sécurité de l'information efficace. Ce standard permet d'établir un système de gestion de sécurité de l'information (SGSI).

Depuis l'an 2000, on a observé en France une tendance à l'évolution vers l'analyse des risques résiduels, après application des mesures de l'état de l'art, comme le font les britanniques, connus pour leur pragmatisme.

Courant 2000, les standards BS évoluent en normes ISO :

- rapidement (Décembre 2000) une norme ISO/IEC est dérivée de BS 7999-1 – sous le nom ISO/IEC 17799:2000, Technologies de l'information -- Code de pratique pour la gestion de sécurité d'information ;
- dans un premier temps, il n'y a pas de notion de certification ;
- le standard BS 7999-2 continue à évoluer, pour arriver à l'adoption comme norme ISO 27001, Technologies de l'information -- Techniques de sécurité -- Systèmes de gestion de la sécurité de l'information -- Exigences ;
- un peu plus tard, BS 7999-1 donne la norme ISO 27002, Technologies de l'information -- Techniques de sécurité -- Code de bonnes pratiques pour la gestion de la sécurité de l'information.

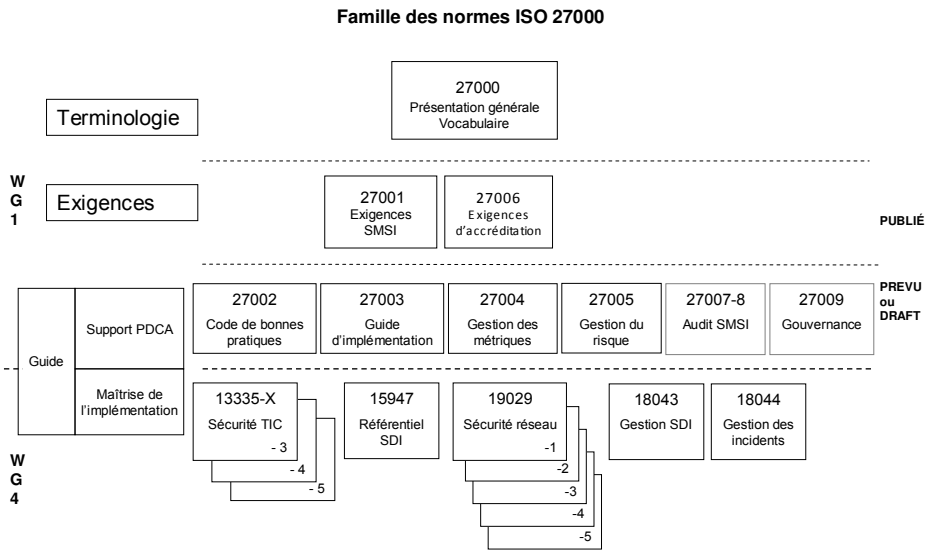
Au final, les suffixes –1 et –2 sont permutés entre les normes BS et les normes ISO 27001 et 27002, ce qui d'une certaine manière matérialise la primauté du SMSI et de la démarche d'amélioration permanente, par rapport au détail des thèmes de mesures de sécurité.

L'annexe A de la norme ISO 27001 est normative. Elle liste les points à contrôler pour la certification. En France, la société LSTI est habilitée pour accréditer des « lead-auditor » ISO 27001.

Normes et guides ISO 2700x

La famille s'enrichit de guides qui complètent la norme, certains ayant valeur de norme, d'autres ayant un rôle de simple guide plutôt qu'une valeur normative. Certains sont déjà publiés ou les travaux de normalisation sont en cours. Il s'agit de :

- ISO/IEC 27000 **–** Technologies de l'information -- Techniques de sécurité -- Systèmes de gestion de la sécurité des informations -- Vue d'ensemble et vocabulaire : présentation de la famille de normes et du vocabulaire. Ce document est gratuit, ce qui mérite d'être signalé pour une norme ISO (publication prévue en 2009) ;
- ISO/IEC 27003 **–** Technologies de l'information -- Techniques de sécurité -- Guidage d'implémentation de système de gestion de sécurité de l'information : Guide d'implémentation d'un SMSI (travaux en cours en 2009) ;
- ISO/IEC 27004 **–** Technologies de l'information -- Techniques de sécurité -- Gestion de la sécurité de l'information – Mesurage : Standard de mesures de management d'un SMSI, il précise également les métriques (travaux en cours en 2009) ;
- ISO/IEC 27005 – Technologies de l'information -- Techniques de sécurité -- Gestion du risque en sécurité de l'information : Standard de gestion de risques liés à la sécurité de l'information (publié en 2009) ;
- ISO/IEC 27006 – Technologies de l'information -- Techniques de sécurité -- Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information : Standard qui décrit les exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information (publié en 2007) ;
- ISO 27007 – Guide d'audit de système de management de sécurité de l'information (titre encore officieux) ; c'est un standard qui proposera des instructions pour les audits accrédités en cas d'audit ISO 27001 d'un SMSI. (publication prévue en 2010).



Sigles du schéma : SDI = Système de Détection d'Intrusion; TIC = Technologies de l'Information et de la Communication
PDCA = Plan Do Check Act ; SMSI = Système de Management de la Sécurité du SI
27007-8 signifie ISO 27007 et ISO 27008 ; WG1 et WG4 signifient groupes de travaux 1 et 4 ISO
Source Alain de Greve – membre belge du groupe d'experts ISO/IEC JTC1/SC27 – conférence du 28/11/2008

Schéma 1 – Famille des normes ISO 27000

Le tableau suivant présente les termes anglais du schéma initial ainsi que leur traduction en français.

Texte anglais (d'origine)	**Traduction en français**
Accreditation requirements	Exigences d'accréditation
Code of Practise	Code de bonnes pratiques
Control of implementation	Maîtrise de l'implémentation
Guideline	Guide
ICT Security	Sécurité TIC
IDS Management	Gestion SDI
IDS Framework	Référentiel SDI
Implementation Guidance	Guide d'implémentation
Incident Management	Gestion des incidents
ISMS audit	Audit SMSI
ISMS requirements	Exigences SMSI
Management measurement	Gestion des métriques
Overview & Vocabulary	Présentation générale - Vocabulaire
Requirements	Exigences

Appréciation du risque et ISO 27005

Pour la partie appréciation du risque (Traduction de l'anglais – Risk Assessment), ISO 27005 constitue un apport important et traite globalement de cette tâche.
Initialement, la démarche d'appréciation du risque qui s'articule dans la plupart des cas autour d'une analyse de risques (Risk Analysis) était traitée au sein de ISO 27001- sur à peine plus d'une page – laissant libre le type de méthode d'analyse utilisée.
Avec l'apparition de l'ISO 27005, cette partie fait l'objet d'une norme à part entière, avec une description et des exigences beaucoup plus développées sur ce thème. ISO 27005 contient 64 pages : 28 pages normatives et 36 pages d'annexe. Les méthodes et démarches d'analyse et d'évaluation sont toujours libres, mais elles doivent satisfaire aux critères ISO 27005.

ISO 27005 n'a pas pour finalité de remplacer les méthodes d'évaluation du risque, qui s'appuient toutes sur les mêmes étapes principales telles que le recensement des actifs sensibles, l'identification des menaces, l'analyse des vulnérabilités, les mesures à proposer en fonction de scénarios d'attaque, une analyse finale des risques résiduels et une aide à la prise de décisions sur les risques acceptables. Au contraire, il est souhaitable qu'elles continuent à s'enrichir, mais elles doivent être présentées en conformité à ISO 27005, avec la même démarche itérative d'amélioration continue.
Les méthodes MEHARI et EBIOS évoluent, le CLUSIF et la DCSSI font les adaptations nécessaires.

Remarques sur la traduction des normes ISO 27000
Hervé Schauer Consultants qui a participé à des travaux sur la traduction, précise que les bonnes équivalences de vocabulaire sont :

Risk Analysis	Analyse du risque
Risk Estimation	Estimation du risque
Risk Evaluation	Évaluation du risque
Risk Assessment	Appréciation du risque

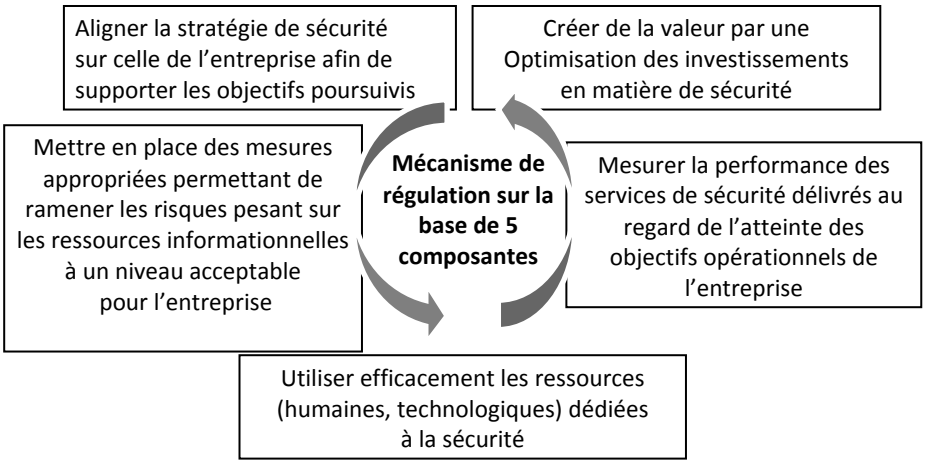
Une rigueur dans la traduction des termes s'impose. Dans le langage courant on dit presque toujours Analyse de Risque pour le grand bloc qui correspond à Risk Assessment dans ISO 27005. Or les méthodes dites d'analyse de risque bien connues (MEHARI, EBIOS …) couvrent plus que la phase analyse au sens ISO 27005, mais bien le bloc « Risk Assessment », il faut donc prendre l'habitude de parler d'appréciation du risque.

Qualité et SMSI – Outils d'aide à la gouvernance

Le domaine de la sécurité a un grand intérêt à se rapprocher des expériences et des outils d'aide à la gouvernance, cela pour bénéficier de l'expérience acquise en qualité, et des référentiels orientés gouvernance, au premier rang desquels CobiT, et ITIL pour la production des services informatiques de l'entreprise.
Le modèle de niveaux de maturité CMMI qui traite des études et développement du système d'information intègre la gestion de la sécurité, et CobiT s'appuie sur ce modèle pour adresser les niveaux de maturité.

CobiT

CobiT est un référentiel orienté processus qui traite de gouvernance au niveau de l'entreprise. Il a été développé entre 1994 et 1996 et publié à cette date par l'ISACA. L'AFAI est le chapitre français de l'ISACA.
CobiT est le référentiel par excellence de la gouvernance du SI. Ce référentiel initialement destiné au niveau de l'entreprise pour l'aspect finance a détaillé la partie système d'information. Il en est à la version 4.1.
Il comporte 34 processus regroupés en 4 domaines, chaque processus comporte un objectif de haut niveau ainsi que les métriques et est décomposé en activités.
Certains processus traitent spécifiquement de Sécurité (processus DS5 – « Ensure Systems Security » du domaine « Delivery and Support »), mais certains services de sécurité sont évoqués en différents processus.
Un manuel intitulé « CobiT Security Baseline : An information survival kit » est disponible sur le site de l'ISACA.
La Commission européenne a sélectionné CobiT en 2005 comme norme de sécurité pour les systèmes d'information de ses organismes payeurs.
Enfin, un autre aspect important de CobiT est la présentation d'indicateurs de performance et la production de tableaux de bord qui sont de véritables outils d'aide destinés aux directions générales. Certains spécialistes de l'utilisation de CobiT proposent des outils d'aide à la décision qui s'appuient sur la méthode BSC - « Balanced Scorecards » de Robert Kaplan et David Norton.
Le schéma suivant présente les principes de la gouvernance de la sécurité SI de l'entreprise et le principe de l'amélioration continue.



Source du schéma – société HAPSIS (2009)

Schéma 2 – Principes de gouvernance de la sécurité du SI
*(*source: Information security governance
« guidance for board of directors and executive management », 2nd edition ITGI)

ITIL – « Information Technology Infrastructure Library »

Le référentiel de bonnes pratiques ITIL défini par l'OGC – « Office of Government Commerce » fait référence pour améliorer la qualité du service offert par la DSI à l'ensemble de l'entreprise ou par une entité externe fournisseur de services en technologie de l'information.
ITIL est suivi et promu par l'itSMF (IT Service Management Forum) qui a un chapitre français. ITIL permet de certifier des personnes. ITIL intègre l'assurance de l'intégrité, de la disponibilité et de la confidentialité de l'information dans le processus gestion de la disponibilité.
ITIL a une approche orientée processus, très concrète et facile à appréhender, qui a le mérite d'aider à bien séparer les rôles et missions des différents processus (par exemple la distinction bien établie entre gestion des incidents, gestion des problèmes et gestion des changements).
La version la plus utilisée aujourd'hui est la version ITIL V2, bien que la version V3, publiée en 2007 soit mise en œuvre. Elle se distingue par une approche qui vise à donner des outils plus stratégiques offrant des services à la stratégie business. Elle intègre explicitement le concept d'amélioration permanente (PDCA, roue de Deming), comme ISO 27001. ITIL évolue bien vers l'aide à la gouvernance de la sécurité.

ISO 20000 - Reprise des concepts ITIL dans un cadre normatif ISO

En 2005, le pas a été franchi afin de donner un caractère normatif au référentiel ITIL, repris en tant que norme ISO 20000. Dorénavant les normes ISO 27001 et ISO 20000 forment un duo complémentaire, et il n'est pas rare que des entités, notamment des entités de service, grosses ou parfois de taille modeste, mènent en parallèle les certifications ISO 27001 et ISO 20000.
Au cours des deux dernières journées organisées par le club 27001 dans le cadre du salon INFOSEC (2007 et 2008), des présentations très claires ont été données sur les articulations entre ces différentes normes.

Les présentations faites au cours de ces 2 dernières éditions font clairement ressortir que la démarche 27001 menée jusqu'à la certification se passe beaucoup plus aisément quand l'entité a préalablement mené des démarches Qualité, ceci étant bien évidemment vrai également pour ISO 20000.
Une autre évolution intéressante à observer est que de petites entités se lancent avec succès dans ce type de certification, ce qui illustre l'adaptabilité de ce type de démarche.

Conclusion

Le conférencier a conclu en mentionnant que les référentiels, normes et outils structurants, destinés à aider à la Gouvernance de la Sécurité de Système d'Information dans l'entreprise ne manquent pas. Pour embrasser globalement le problème de la Gouvernance du SI, englobant nécessairement la Sécurité, compte tenu de l'exposition croissante de SI induite par le développement des téléservices et de la réalité de la Cybercriminalité, il paraît souhaitable dans le cas général, de partir de la démarche Gouvernance du SI et de prendre en compte en son sein la démarche Sécurité. Un référentiel comme CobiT n'a pas vocation à exclure les autres, les référentiels sont complémentaires, en terme de qualité. Début 2007, lors d'une conférence organisée par l'ANDSI, Jean Pierre Delvaux avait mis l'accent sur la complémentarité de CobiT, CMMI et ITIL. Philippe Junière ajoute que 27001 s'adresse au RSSI soutenu par le DSI et la Direction Générale car il importe de bien positionner le standard au bon niveau de responsabilité! Et les positionnements sont différents!

Au cours de la séance de questions, il a été mentionné un document publié en novembre 2008 sur le site de l'ISACA décrivant la correspondance entre CobiT 4.1, CMMI et ITIL V3.▲

dominique.bergerot@adeli.org
et pour contacter le conférencier ……
philippe.juniere@orange.fr

Sigles

AFAI	Association Française de l'Audit et du conseil Informatique
ANDSI	Association Nationale des Directeurs de Systèmes d'Information
CobiT	Control OBjectives for Information and related Technology
CMMI	Capability Maturity Model Integration
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information (www.ssi.gouv.fr)
EAL	Evaluation Assurance Level
IAB	Internet Architecture Board (www.iab.org – organisme intervenant en conseil au sein de l'ISOC)
IESG	Internet Engineering Steering Group (www.ietf.org/iesg.html - dépend de l'ISOC, supervise les activités techniques de l'IETF ainsi que le processus de définition des normes de l'Internet)
IETF	Internet Engineering Task Force (www.ietf.org – organisation à l'origine des principaux standards de l'Internet)
ISACA	Information Systems Audit and Control Association (www.isaca.org)
ISOC	Internet Society (www.isoc.org – association pilotant l'IETF et l'IAB)
ITIL	Information Technology Infrastructure Library (www.itsmf.fr)
ITSEC	Information Technology Security Evaluation Criteria
SSL	Secure Socket Layer (protocole de la couche réseau transport)
TCSEC	TCSEC Trusted Computer System Evaluation Criteria
TLS	Transport Layer Security (protocole de la couche réseau transport, évolution de SSL)
W3C	World Wide Web Consortium (www.w3.org – organisme de standardisation dans le domaine du Web

Références

- Management de la Sécurité de l'Information – Implémentation ISO 27001; Alexandre Fernandez Toro – EYROLLES
- Stratégie appliquée à l'audit des systèmes d'information - Ossad, Merise, Axial, MDA, UML, Idef0, Mehari, Melisa, Marion ; Alphonse Carlier – Hermès-Lavoisier
- CobiT – Pour une meilleure gouvernance des systèmes d'information; Dominique Moisand, Fabrice Garnier de Labareyre - EYROLLES
- MEHARI 2007 est téléchargeable gratuitement sur le site du CLUSIF : www.clusif.fr
  Manuel de Référence - fichier pdf de 250 pages + tableaux Excel.
- L'ensemble de la documentation EBIOS est disponible en ligne sur le site de la DCSSI (www.ssi.gouv.fr)
  Les outils peuvent être obtenus sur demande.

Clubs, forums ou associations concentrant des informations en Sécurité des SI

- **CIGREF** www.cigref.fr
- **CLUSIF** www.clusif.fr
- **OSSIR** - 2 groupes de travail d'accès libre – Sécurité Windows et SUR (Unix) - www.ossir.org
- **Club 27001** www.club-27001.fr
  Ce club est co-animé par Hervé Schauer (HSC) et Éric Doyen (Crédit Immobilier). C'est un groupe de travail qui organise des réunions mensuelles ouvertes à tous sur les thèmes ISO 270001 et ISO 20000. Un sous-groupe s'est créé sous l'impulsion d'Alexandre Fernandez Toro pour travailler sur une mutualisation possible des tâches entre les démarches ISO 27001 et ISO 20000.
- **AFAI** – www.afai.org
- **itSMF** – www.itsmf.fr