

# LA JUNGLE DES FORMATIONS ET DES CERTIFICATIONS ISO 27001 ET 27005

Auto-certifications, certifications inventées de toutes pièces : tout existe à côté des certifications réelles. Pourtant leur conformité à la norme ISO 17024 est essentielle. Nous avons cherché à en savoir plus en interrogeant HSC, Accenture et Altran.



Hervé Schauer,  
fondateur de la  
société HSC  
Consultants.

## > HSC : ACTEUR ENGAGÉ ET SANS LANGUE DE BOIS

Il nous a paru intéressant de demander à Hervé Schauer, fondateur du cabinet HSC, de nous expliquer pourquoi il s'est engagé depuis plusieurs années dans une activité de formation sur ces sujets et de nous décrire le panorama français.

**Mag Securs :** *Hervé Schauer, vous vous êtes lancé depuis quelques années dans la mise en œuvre des systèmes de management et, notamment, des formations qui y sont associées, pourquoi ?*

**Hervé Schauer :** La norme ISO 27001 permet de construire une organisation de la sécurité de l'information accessible à tout organisme, afin de lui permettre de progresser. Le principe est le même que celui de la norme ISO 20000-1 s'inspirant d'ITIL. Le pragmatisme et le réalisme des principes simples qui gouvernent ces systèmes de management nous ont séduits.

Pour partager notre enthousiasme, nous avons décidé de créer des formations sur ce sujet, puis, nous avons été amenés à proposer la certification ISO 27001 Lead Auditor ou responsable d'équipe d'audit ISO 27001, et maintenant ISO 20000-1 Lead Auditor.

**MS :** *La certification des personnes sur l'ISO 27001 est devenue un véritable business, et HSC est reconnu comme un acteur significatif. Pouvez-vous nous indiquer qui sont vos confrères ?*

**Hervé Schauer :** Il y a plus d'une quinzaine de sociétés en France proposant des formations ISO 27001. Plus si on inclut les sociétés étrangères qui cherchent à vendre des formations en France. Un formateur n'a pas la possibilité de délivrer lui-même un certificat, car il ne peut pas être juge et partie. Pour cette raison, les sociétés de formation travaillent avec des organismes de

certification qui font passer les examens aux candidats formés. Il existe une certification des implémenteurs et des auditeurs des SMSI et, depuis peu, une certification des gestionnaires de risque qui se réfère à la nouvelle norme ISO 27005. A ma connaissance, il existe quatre organismes de certification actifs en France. C'est un marché qui intéresse beaucoup de monde !

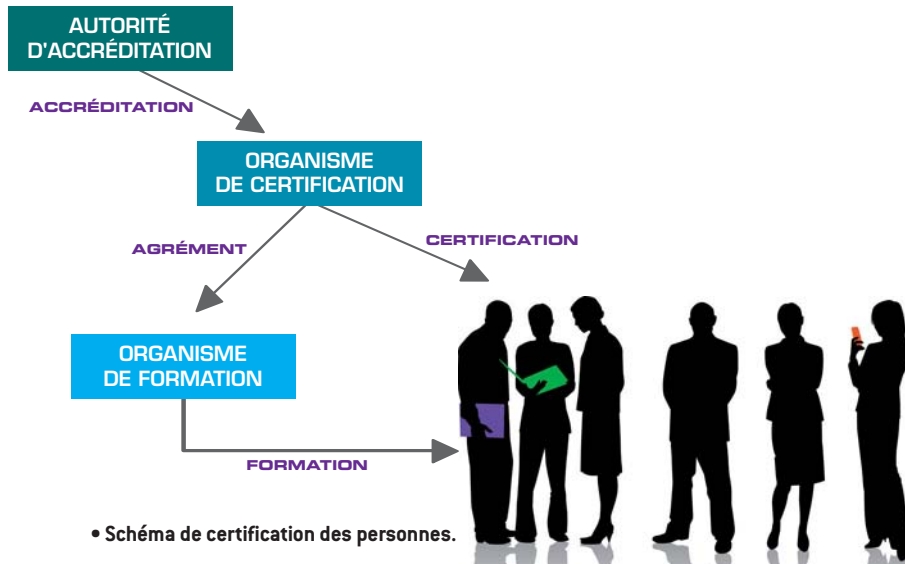
Les référentiels à la base de ces certifications sont des normes. Ces certifications ont l'avantage d'être ouvertes à tous. C'est très différent du CISSP pour lequel une seule société, à savoir ISC2, est propriétaire exclusif de la certification et utilise son propre référentiel, non publié et sans processus d'élaboration ouvert. Cette société commerciale n'hésite cependant pas à utiliser un nom de domaine en « .org ».

**MS :** *Cela signifie-t-il que tous les examens ont la même valeur ?*

**Hervé Schauer :** Non, justement ! Certains déclarent « Mon examen est facile, vous l'aurez tous ! » pour attirer les candidats. Mais s'il n'y avait que cela. Les malhonnêtetés vont bien plus loin

**MS :** *Que voulez-vous dire ?*

**Hervé Schauer :** La certification des personnes autour des systèmes de management comprend deux types d'acteurs : deux géants que sont IRCA et RABQSA, et des acteurs régionaux en grand nombre. Ces derniers sont souvent spécialisés : évaluation de biens immobiliers



pour HypZert en Allemagne, ou évaluation des auditeurs et implémenteurs en informatique et en sécurité de l'information pour LSTI en France. La première malhonnêteté est que tous les organismes de certification régionaux doivent respecter la norme ISO 17024. Celle-ci précise les conditions d'organisation des formations et des examens pour une certification. Les organismes conformes à cette norme peuvent être accrédités. Les organismes d'accréditation sont, pour leur part, contrôlés et financés par les États. Or, les deux mastodontes, IRCA et RABQSA, n'ont que faire de la norme ISO 17024 et du système d'accréditation sous contrôle des États ! Ils disposent bien d'une certification conforme à la norme ISO 17024 sur un sujet particulier, une certification prétexte en quelque sorte, dont ils se servent pour les autres sujets. Leurs schémas de certification sur les auditeurs et implémenteurs ISO 27001 et ISO 20000-1 ne sont pas conformes.

S'ils ont l'avantage de ne pas être onéreux, les examens sont toutefois sans valeur. Le formateur joue le rôle de l'examineur et donne le « certificat ». La norme ISO 17024 impose une séparation stricte entre ces rôles : on n'est pas juge et partie en même temps.

**MS. :** *Il faut donc éviter les certifications IRCA et RABQSA. Vous avez dit « la première malhonnêteté », y a-t-il quelque chose de pire encore ?*

**Hervé Schauer :** Oui. Plusieurs organismes de formation en France ont carrément inventé leur propre certification, à mes yeux en « carton-pâte » et sans valeur. Et ce ne sont les moindres. Par exemple, Afnor Compétences. Cette société commerciale exploite, à merveille, son nom

historique particulièrement ambigu pour prétendre délivrer une certification ISO 27001. Une autre filiale du groupe Afnor, qui s'appelle Afnor Certification, vend, quant à elle, une certification ISO 27001 Lead Auditor indépendante. Cette dernière a cependant disparu cet été de leur catalogue, alors qu'Afnor Certification annonçait il y a 3 mois sur son site Web son accréditation prochaine. Afnor Certification propose toujours une certification réellement nouvelle, mais pour laquelle elle est accréditée, à savoir l'ISO 20000-1 Lead Auditor. Vous voyez, nous nageons en plein délire. On mélange tout. Et l'ingénieur qui veut se former est complètement démuni pour y voir clair, son responsable encore plus.

**MS. :** *C'est « règlements de comptes à Ok Corral » !*

*N'exagérez-vous pas un peu ?*

**Hervé Schauer :** Pas du tout ! Les entourloupes et les mensonges sont malheureusement le quotidien des formations certifiantes. Vous ne vous imaginez pas ce que certains peuvent raconter aux stagiaires...

Pour conclure, il faut faire la part des choses : une formation avec ou sans certification peut répondre aux attentes. Mais il faut vérifier l'expérience des formateurs, s'assurer qu'ils vont réellement partager avec les stagiaires une expérience sur le terrain et qu'ils ne sont pas des formateurs à la chaîne. Ensuite, il faut bien comprendre le système de certification : s'il y en a un, son modèle économique et comment il est contrôlé. L'accréditation est incontestablement le système minimum indispensable, même s'il n'est pas suffisant.

Il leur faut de véritables garanties de compétences. ■



Emmanuel Gazay  
directeur sécurité  
France,  
Accenture



Frédéric Peters,  
directeur sécurité  
France,  
Accenture

## > ACCENTURE ET ISO 27001 : LA QUÊTE DU GRAAL ?

**Pour savoir comment un grand cabinet de conseil et d'audit reconnu considère la norme 27001, nous avons interrogé deux personnes d'Accenture. Emmanuel Gazay et Frédéric Peters ont accepté de répondre à nos questions.**

**Mag Securs : Comment se présente l'application de la norme 27001 pour Accenture ?**

**Emmanuel Gazay et Frédéric Peters :** Chez Accenture, la sécurité est une source d'économies pour l'entreprise. On améliore les systèmes d'information, qui coûtent du coup moins cher à opérer. La norme 27001 apporte le gage d'une amélioration continue de la sécurité des systèmes d'information. Les investissements sont ainsi en parfaite adéquation avec les besoins métiers. La sécurité est alors enfin vécue par les directions fonctionnelles et les directions générales comme un atout majeur pour leurs lignes métiers.

**MS. : Comment positionnez-vous votre offre sécurité sur le marché ?**

**Emmanuel Gazay et Frédéric Peters :** Nous constatons que l'approche métier et l'approche sécurité sont aujourd'hui complémentaires. Notre présence historique au côté des entreprises nous aide à apporter cette vision métier de la sécurité. Cela permet ainsi de donner un sens nouveau à la sécurité et de créer de réelles opportunités de retour sur investissement. Par exemple, la gestion des identités a pour conséquence de réduire le nombre d'appels au help-desk, limite les erreurs humaines et réduit ainsi les coûts d'exploitation du SI. L'ISO 27001 peut aider à structurer un certain nombre de ces processus.

L'information est devenue critique et sensible au sein des entreprises – c'est tout simplement elle qui, aujourd'hui, porte la valeur des entreprises. La protéger, et du même coup être capable de la valoriser représente l'un des axes essentiels de notre approche de la sécurité. Encore une fois, ISO 27001 est un excellent outil permettant d'accélérer la définition du périmètre à protéger et d'assurer ensuite son évolution en fonction des besoins métiers.

**MS. : Quels sont les points positifs et les points négatifs de ISO 27001 ?**

**Emmanuel Gazay et Frédéric Peters :** Le point positif le plus important, c'est qu'on peut démarrer sur

un petit périmètre, si on le désire. Adopter une démarche ISO 27001 sur un projet de sécurité ne coûte pas plus cher qu'une démarche sécurité dite classique. ISO 27001 est une norme internationale, publiée au Journal officiel, qui peut être étendue à d'autres thèmes de sécurité du client. Enfin, l'ISO 27002, qui est un catalogue de bonnes pratiques à mettre en place, est l'un des piliers essentiels à la réalisation d'une démarche ISO 27001.

En revanche, le point négatif réside dans le fait que les clients peuvent avoir la perception qu'ISO 27001 est « trop lourde » à mettre en place. C'est notre rôle, souvent en début de mission, de changer cette perception en apportant aux clients les éléments présentant les bénéfices et l'efficacité d'ISO 27001.

**MS. : Le marché a-t-il reconnu toute la valeur du processus normatif ?**

**Emmanuel Gazay et Frédéric Peters :** Aujourd'hui, il y a une reconnaissance du marché sur les compétences à mettre en œuvre pour que l'entreprise soit certifiée ISO 27001. La qualité du processus normatif 27001 doit aussi beaucoup aux compétences et à la légitimité des gens qui s'occupent de la sécurité dans leur entreprise. Il faut qu'ils aient une expérience pratique de la gestion de la sécurité et qu'ils soient, par exemple, certifiés Lead Auditor. L'examen de Lead Auditor de LSTI est très sélectif, n'y seront reçus que des gens qui ont une légitimité de plusieurs années dans la sécurité des systèmes d'information. Le dossier de chaque candidat est étudié, et celui-ci se retrouve en situation avec un véritable examen de 3 heures 30.

**MS. : En fin de compte, quel bilan faites-vous de l'application de la norme 27001 en France ?**

**Emmanuel Gazay et Frédéric Peters :** Globalement, un bilan positif peut-être fait. Les normes définissent des règles pertinentes, et nos clients se lancent dans la norme ISO 27001 pour asseoir un label de qualité qui sécurise leurs propres clients en montrant que leur SI est structuré et pérenne. ■

## > ALTRAN CIS : 30 CONSULTANTS SPECIALISES DONT 7 CERTIFIES ISO 27001 LEAD AUDITOR

De plus en plus d'entreprises clientes demandent des certifications ISO 27001 ou souhaitent aller vers ces certifications. Les consultants doivent donc posséder eux-mêmes les certifications appropriées. Le point avec Dan Nizard.

**Mag Securs :** *Y a-t-il une demande pour implémenter les normes ISO 27001 dans les entreprises ?*

**Dan Nizard :** Nos clients, de grandes entreprises, s'y intéressent en premier lieu. Ils font souvent référence à cette norme pour structurer leur activité sécurité. La norme ISO 27001 amène l'entreprise à mettre en place un processus vertueux d'implémentation des bonnes pratiques. De ce fait, de plus en plus d'entreprises s'y réfèrent sans toutefois rechercher systématiquement la certification.

**MS :** *Pour mener un audit de sécurité, une certification est-elle nécessaire ?*

**Dan Nizard :** C'est toujours mieux quand on l'a et elle est indispensable pour mener un audit de certification ISO 27001. Mener un audit de sécurité n'est pas une tâche aisée. Il faut de la réflexion, de la méthode et beaucoup de rigueur. L'équipe Sécurité d'Altran CIS Paris est composée de 30 consultants spécialisés, dont 7 sont certifiés ISO 27001 Lead Auditor. La formation se déroule sur cinq jours dans une ambiance agréable favorisant les échanges entre participants et avec les formateurs.

**MS :** *Quelle est la valeur sur le marché d'une certification Lead Auditor ?*

**Dan Nizard :** La réussite à l'examen Lead Auditor ISO 27001 certifie que le consultant est à même de mener l'audit qui conduit à la certification ISO 27001. Bien évidemment, cette certification accroît la valeur ajoutée des prestations de nos consultants. Nous avons beaucoup de demandes, même si toutes les entreprises ne veulent pas forcément aller tout de suite jusqu'à la certification ISO 27001.

**MS :** *Quels sont les points positifs et négatifs d'une certification ?*

**Dan Nizard :** Beaucoup de sociétés apprécient de se référer à une norme internationale et sont en quête d'une certification. L'aspect négatif réside principalement dans la nécessité d'adaptation liée au processus normatif. C'est très exigeant et demande un réel investissement. Il est donc préférable de faire appel à des consultants certifiés, véritable garantie pour l'entreprise cliente que la personne a suivi un parcours qui l'amène à être légitime en vu d'une certification. ■



Dan Nizard,  
directeur de l'offre  
des SI,  
Altran CIS

### > LISTE DES FORMATIONS CERTIFIANTES

Société de formation	ISO 27001 Lead Auditor	ISO 27001 Lead Implementer	ISO 27005 Risk Manager	ISO 20000-1 Lead Auditor	Organisme de certification	Autorité d'accréditation
Afnor Compétences	X			X	aucun	non-accréditable
Afnor Certification				X	ICA (AFNOR certification)	COFRAC
Ageris training	X		X		LSTI	COFRAC
Auditware	X				aucun	non-accréditable
BSI	X				IRCA	non-accrédité
Byward	X	X	X		LSTI	COFRAC
Cap Gemini	X	X		X	ICA (AFNOR certification)	COFRAC
Digicom	X				IRCA	non-accrédité
Fidens	X				LSTI	COFRAC
HSC	X	X	X	X	LSTI	COFRAC
Natheos	X	X			RABQSA	non-accréditable
Orsyp	X			X	ICA (AFNOR certification)	COFRAC
Orsys	X				LSTI	non-accrédité
Sekoia	X	X			RABQSA	COFRAC
Telindus	X	X			LSTI	COFRAC
Veridion	X	X			RABQSA	non-accrédité