HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique
Spécialisé sur Unix, Windows, TCP/IP et Internet

Qualification des prestataires en sécurité

Centre de Conférence Arpèges Paris Trocadéro
17 & 18 septembre

Conférence RGS, Paris
17 septembre 2013

Hervé Schauer
<Herve.Schauer@hsc.fr>

Sommaire

- Qualification et Certification
- Qualifications professionnelles
- Qualification des prestataires en sécurité dans le cadre du RGS
- Qualification des prestataires d'audit de sécurité dans le cadre du RGS (PASSI)
- Utilité de la qualification des prestataires d'audit de sécurité
- Autres pays, autres cas
- Conclusion

Les transparents seront disponibles sur `www.hsc.fr`

Qualification et Certification

- Mécanisme d'**apport de confiance**
- Sous le contrôle des États
- Apporte une **plus-value**
  - À l'organisme, à ses clients, aux parties intéressées
- Créé de la valeur

- Qualification : règlementaire
- Certification : pas nécessairement règlementaire

Qualification et Certification

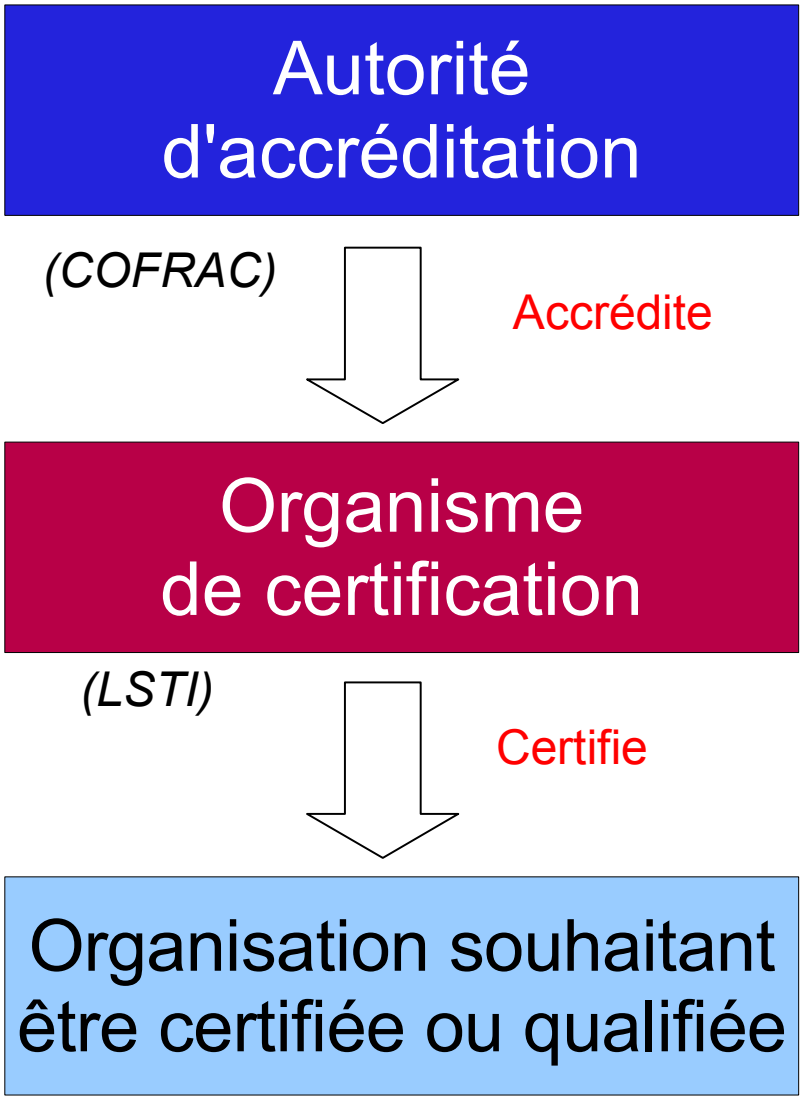
- ① Certification des **produits**
  - **Guide ISO 65 / EN 45011**
- Certification des **organisations**
  - ② Certification des **services**
    - **NF X 50-091**
  - ③ Certification des **systèmes de management**
    - **ISO 17021**
- ④ Certification de **personnels**
  - **ISO 17024**

Qualification et Certification

- **Assurance** par une démonstration indépendante que le produit, le service ou le système de management est :
  - Conforme au référentiel ou aux exigences spécifiées
  - Capable de réaliser de manière fiable ce qu'il déclare
  - Mis en oeuvre de manière efficace

- Attesté par un organisme indépendant et contrôlé : organisme de certification

Qualification et Certification



- Schéma universel à toutes les qualifications et certifications
- Autorité d'accréditation
  - Une seule par pays
  - Organisme d'état
- Organisme de certification
  - Plusieurs (*normalement*)
  - Généralement des sociétés privées
  - Peut être un organisme gouvernemental

Qualification ou Certification

- Article L115-28 du Code de la consommation

*Peuvent seuls **procéder à la certification de produits ou de services** les organismes qui bénéficient d'une **accréditation délivrée par l'instance nationale d'accréditation**, ou l'instance nationale d'accréditation d'un autre Etat membre de l'Union européenne, membre de la coopération européenne pour l'accréditation (...).*

*Un organisme non encore accrédité pour la certification considérée peut, dans des conditions définies par décret, effectuer des certifications, **sous réserve d'avoir déposé une demande d'accréditation**.*

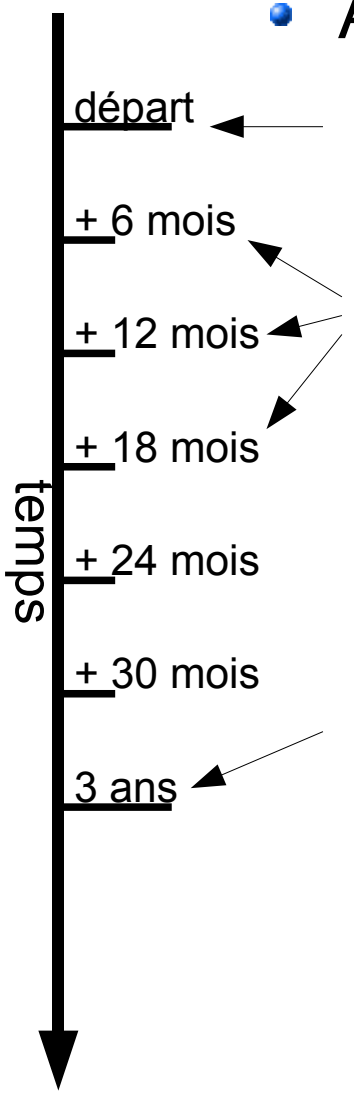
Toute référence à la certification dans la publicité, l'étiquetage ou la présentation de tout produit ou service, ainsi que sur les documents commerciaux qui s'y rapportent doit être accompagnée d'informations claires permettant au consommateur ou à l'utilisateur d'avoir facilement accès aux caractéristiques certifiées. (...)

*Le signe distinctif qui, le cas échéant, accompagne ou matérialise la certification est déposé comme **marque collective de certification**, conformément à la législation sur les marques de fabrique, de commerce et de service.*

- Accréditation par instance reconnue en France : **COFRAC**

Qualification ou certification

- Audit de certification ➔ processus sur trois ans
  - Audit initial
  - Audits de surveillance
    - Généralement tous les 6 mois
    - Durée fonction du schéma d'accréditation
  - Audit de renouvellement de la certification
    - Tous les 3 ans
    - Permet de remettre en concurrence les organismes de certification



Qualifications professionnelles

- Certificats de qualification professionnelle de prestataires
- Qualipropre (`www.qualipropre.org`)
  - Organisme de certification de la qualification des entreprises dans le domaine de la **propreté** et des services associés
- OPQCM
  - Office professionnel de Qualification des **Conseils en Management** (`www.opqcm.com`)
- OPQF
  - Office Professionnel de Qualification des **organismes de Formation** (`www.opqf.com`)
- OPQUIBI (Services d'ingéniérie), Qualibat, Qualifelec, Qualisport
- Qualification des prestataires en sécurité du **même principe**

Qualifications professionnelles

- A titre d'exemple : **OPQF**
  - Organisme de certification accrédité par le COFRAC
  - Reconnu par l'Etat
  - Représentation tripartite
    - Prestataires de formation
    - Clients : entreprises et OPCA
      - Organismes Paritaires Collecteurs Agréés = organismes de financement des formations continues professionnelles
        `www.emploi.gouv.fr/boite_outils/_pdf/OPCA.pdf`
    - Représentant de l'Etat (Ministère du travail et de l'emploi, DGEFP (Délégation générale à l'emploi et à la formation professionnelle)
      `www.emploi.gouv.fr/presentation/presentation_generale.php`
  - Audit
    - Respect de la réglementation
    - Adéquation des compétences et des moyens techniques et humains mis en oeuvre aux actions de formation
    - Satisfaction des clients
    - Pérennité financière

Qualifications professionnelles

- Article 45-II du Code des marchés publics

Le pouvoir adjudicateur peut demander aux opérateurs économiques qu'ils produisent des certificats de qualité. Ces certificats, délivrés par des organismes indépendants, sont fondés sur les normes européennes.

Pour les marchés qui le justifient, le pouvoir adjudicateur peut exiger la production de certificats, établis par des organismes indépendants, et attestant leur capacité à exécuter le marché.

Pour les marchés de travaux et de services dont l'exécution implique la mise en oeuvre de mesures de gestion environnementale, ces certificats sont fondés sur le système communautaire de management environnemental et d'audit (EMAS) ou sur les normes européennes ou internationales de gestion environnementale.

Dans les cas prévus aux trois alinéas précédents, le pouvoir adjudicateur accepte tout moyen de preuve équivalent ainsi que les certificats équivalents d'organismes établis dans d'autres Etats membres.

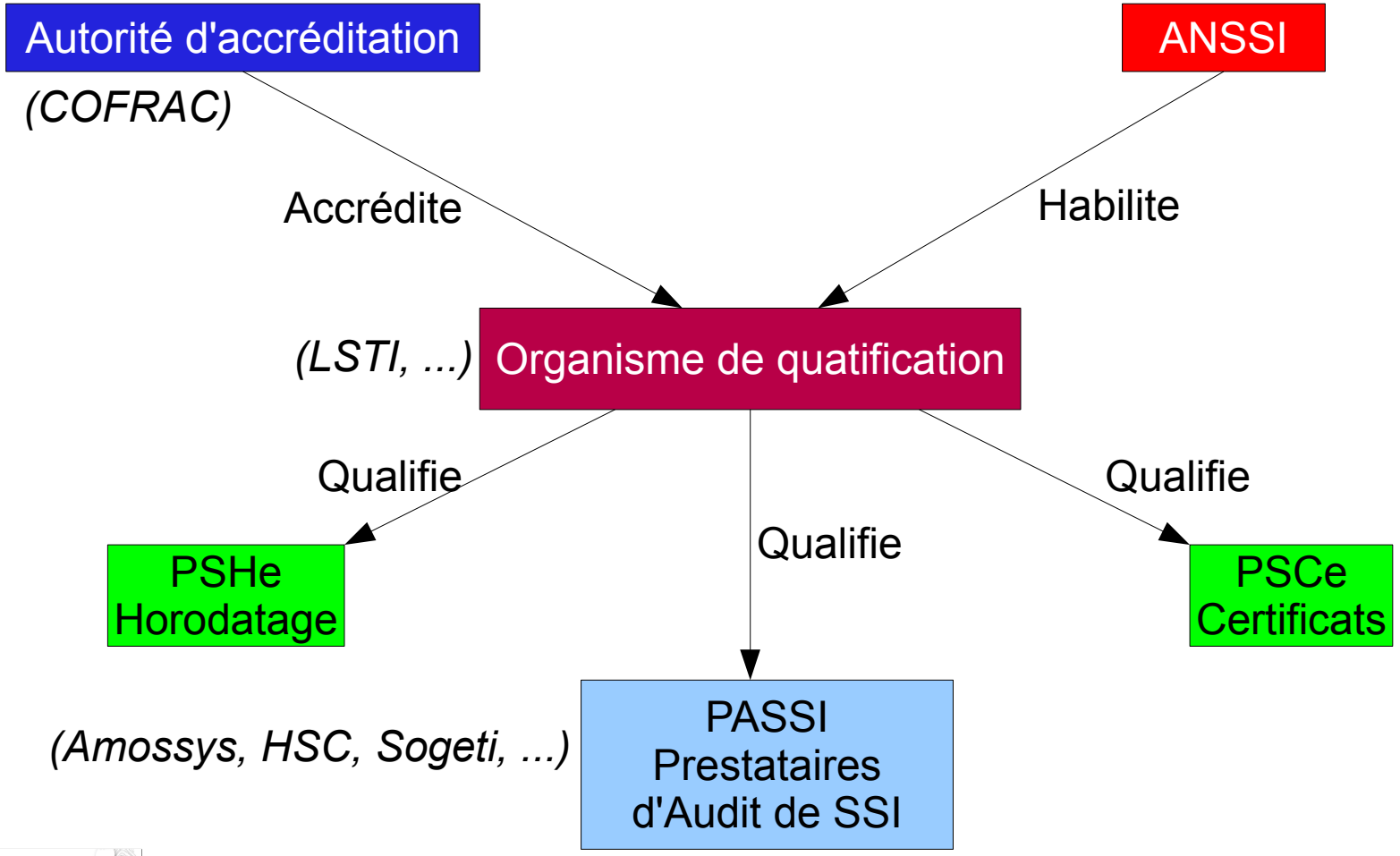
Qualifications professionnelles

- Article 45-II du Code des marchés publics
- Permet au pouvoir adjudicateur d'exiger un certificat de qualification professionnelle
  - Même si un seul prestataire qualifié répond, il est sélectionné

Qualifications professionnelles existent dans tous les métiers
→ normal qu'elles arrivent dans les métiers de la sécurité

Qualification des prestataires en SSI

- Dans le cadre du **RGS** (Référentiel Général de Sécurité)
  - Même principe que pour tous les prestataires de confiance



Qualification des prestataires en SSI

- PASSI : Prestataires d'Audit de Sécurité des Systèmes d'Information
  - Référentiel v1 publié en décembre 2011 après 6 mois de relectures publiques
  - Expérimentation réalisée de janvier 2012 à juin 2013
- Prestataires de détection d'incidents de sécurité
  - Référentiel en cours d'élaboration
- Prestataires d'investigation numérique
  - Référentiel en cours d'élaboration
- Prestataires de recouvrement
- Prestataires d'informatique en nuage (*Cloud Computing*)
  - Référentiel en cours d'élaboration

Qualification des prestataires en SSI

- Ordonnance n°2005-1516 portant création du RGS

Article 9

I. - Un référentiel général de sécurité fixe les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique telles que les fonctions d'identification, de signature électronique, de confidentialité et d'horodatage.

II. - Lorsqu'une autorité administrative met en place un système d'information, elle détermine les fonctions de sécurité nécessaires pour protéger ce système. Pour les fonctions de sécurité traitées par le référentiel général de sécurité, elle fixe le niveau de sécurité requis parmi les niveaux prévus et respecte les règles correspondantes.

*III. - Les produits de sécurité et les **prestataires de services de confiance** peuvent obtenir une **qualification** qui atteste de leur conformité à un niveau de sécurité du référentiel général de sécurité.*

Cette délivrance peut, s'agissant des prestataires de services de confiance, être confiée à un organisme privé habilité à cet effet.

Qualification des prestataires en SSI

- Décret d'application n° 2010-112

Article 3

Dans les conditions fixées par le référentiel général de sécurité mentionné à l'article 2 du présent décret, l'autorité administrative doit, afin de protéger un système d'information :
*1° Identifier l'ensemble des **risques** pesant sur la sécurité du système et des informations qu'il traite, eu égard notamment aux conditions d'emploi du système ;*
2° Fixer les objectifs de sécurité, notamment en matière de disponibilité et d'intégrité du système, de confidentialité et d'intégrité des informations ainsi que d'identification des utilisateurs du système, pour répondre de manière proportionnée au besoin de protection du système et des informations face aux risques identifiés ;
*3° En déduire les **fonctions de sécurité** et leur niveau qui permettent d'atteindre ces objectifs et respecter les règles correspondantes du référentiel général de sécurité.*

Article 4

*Pour mettre en oeuvre dans un système d'information les fonctions de sécurité ainsi déterminées, l'autorité administrative recourt à des produits de sécurité et à des **prestataires** de services de confiance ayant fait l'objet d'une **qualification** dans les conditions prévues au présent décret ou à tout autre produit ou prestataire pour lesquels elle s'est assurée de la conformité de leurs fonctions de sécurité au référentiel général de sécurité.*

- Utiliser des prestataires qualifiés permet d'être conforme au RGS

Qualification des prestataires d'audit

- Qualification des prestataires d'**audit** en **sécurité des systèmes d'information**
- Référentiel : **Annexe C** du RGSv2
  - Version 2.0 du 14/02/2013 entrée en production le 21/06/2013
  - `http://www.ssi.gouv.fr/IMG/pdf/RGS_PASSI_v2-0.fr`
- Impose de nombreuses règles
- Reprend les bonnes pratiques et les normes en vigueur
  - Beaucoup, beaucoup d'évidences
    - Ou qui devraient en être...
  - Référence à l'ISO 19011

Qualification des prestataires d'audit

- Qualification des prestataires d'**audit** en **sécurité des systèmes d'information**
- Qualification de l'entreprise d'audit
- Qualification des auditeurs un par un
- Départ de dernier auditeur remet en cause la qualification de l'entreprise
  - 6 mois pour retrouver un auditeur qualifié PASSI
- Pour conserver sa qualification, l'organisme doit assurer qu'il possède toujours les compétences adéquates
  - Au moins un auditeur qualifié dans la catégorie où l'entreprise est qualifiée
  - Au moins un responsable d'équipe d'audit qualifié

Qualification des prestataires d'audit

- Qualification des prestataires d'**audit** en **sécurité des systèmes d'information**
- Définit différents types de prestation d'audit (appelées activités) : (2)
  - Audit d'architecture
  - Audit de configuration
    - Réseaux, équipements de sécurité, OS, SGBD, serveurs, services, PC, téléphonie, virtualisation, ...
  - Audit de code source
    - Injection, XSS, … sans forcément avoir l'application qui tourne
  - Tests d'intrusion
    - Boite noire, grise, blanche (6.4.4.a)
  - Audit organisationnel et physique

Qualification des prestataires d'audit

- Qualification des prestataires d'**audit** en **sécurité des systèmes d'information**
- Impose des documents parfois lourds
  - Contrat (appellé convention d'audit [6]) **doit** contenir 14 items **imposés** dont :
  - Stipuler que le prestataire d'audit ne fait pas travailler d'auditeur sans relation contractuelle avec lui, ou condamné pour intrusion, etc
  - Règles de titularité des éléments protégés par la propriété intellectuelle
    - Comme le rapport d'audit
    - Comme les outils développés par l'audité pendant l'audit
  - Décrire les publics destinataires des recommandations
  - Droit applicable français

Qualification des prestataires d'audit

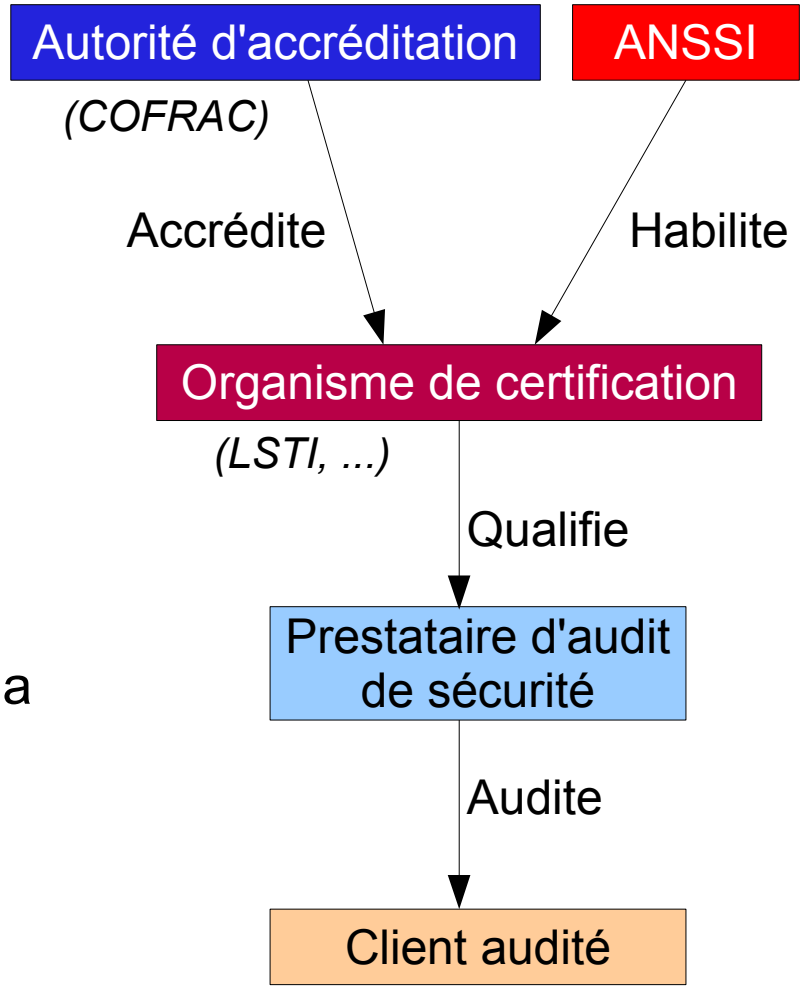
- Qualification des prestataires d'**audit** en **sécurité des systèmes d'information**
- Audit du prestataire sur site :
  - Locaux, sécurité physique
  - Documents utilisés dans le cadre des activités d'audit : politiques, procédures, etc
  - Diffution restreinte interprété comme du CD interconnecté
  - Organisation, formations du personnel, etc
  - Echantillonage pour les contrôles techniques
- Suivi d'audits témoins réels

Qualification des prestataires d'audit

- Qualification des prestataires d'**audit** en **sécurité des systèmes d'information**
- Qualification des auditeurs
  - CV, etc
  - Examens écrits
    - Examen commun, sur le RGS, l'ISO19001 ou les principes de l'audit
    - Examen par activité d'audit souhaitée
      - Aucune préparation nécessaire
        - Soit expérience donc le niveau
        - Si échec, nouvelle tentative possible tous les 6 mois
  - Examen oral si réussite à l'écrit
    - Avec les résultats des écrits sous les yeux
    - Examen de la capacité à être responsable d'équipe d'audit

Utilité d'une qualification des auditeurs

- Qualification par un organisme de certification indépendant **indispensable**
  - Commanditaires/clients des audits de sécurité ne savent pas toujours et ne peuvent pas toujours sélectionner leur prestataire
    - Qualification OPQF (prestataire de formation) → Auditeur interview un échantillonage de clients ayant suivis différentes formations
    - Qualification PASSI → Client de l'audit pas toujours en mesure de juger de la qualité, la complétude et la transparence de l'audit
  - Indépendamment du secteur d'activité du commanditaire/client



Utilité d'une qualification des auditeurs

- Ce que devrait permettre d'**éviter** la qualification des prestataires d'audit de sécurité pour le client **commanditaire**
  - Sociétés d'audit liées à des groupes mafieux ou terroristes
  - Réalisation de l'audit par d'autres consultants que ceux présentés ou que ceux signant le rapport d'audit
    - Compétence moindre
    - Nationalités différentes
  - Absence de formation des auditeurs
  - Utilisation de sous-traitance non-déclarée
  - Sous-traitant ne déclarant pas une sous-sous-traitance
  - Prestations de test d'intrusion en marque blanche
  - Prestations sans assurance en responsabilité civile, sans responsable

Utilité d'une qualification des auditeurs

- Ce que devrait permettre d'**éviter** la qualification des prestataires d'audit de sécurité pour le client **commanditaire**
  - Audit applicatifs avec accès au code source, vendus comme réalisés par des consultants, réalisés par un logiciel automatique d'analyse
  - Tests d'intrusion, vendus comme artisanaux, réalisés par un logiciel de test de vulnérabilités
  - Auditeurs pas en mesure de prendre du recul, de replacer les résultats dans le contexte et les enjeux, et de produire un résumé managérial
  - Réalisation de l'audit ou du tests d'intrusion dans une durée significativement moindre que celle achetée
  - Sociétés d'audit dont la qualité habituelle des prestations s'effondre sans prévenir
  - Sociétés ne respectant pas les accords de confidentialités signés
    - CV détaillés avec le contenu des prestations d'audit réalisées fourni à quiconque fait croire qu'il veut acheter un audit...

Utilité d'une qualification des auditeurs

- Ce que devrait permettre d'**apporter** la qualification des prestataires d'audit de sécurité pour le client **commanditaire**

  - Mettre sur un pied d'égalité tous les établissements quelle que soit leur taille
  - Remédier au manque de moyens ou de connaissance du marché pour analyser les réponses
  - Proposer un contrepoids au choix du moins-disant
  - Permettre une qualité de la prestation rendue correspondant pleinement à l'objectif poursuivi

Autres pays

- Exemple : Grande-bretagne
  - Label étatique pour les tests d'intrusion depuis 2006 : CHECK
    - `http://www.cesg.gov.uk/servicecatalogue/CHECK/Pages/WhatisCHECK.aspx`
  - Prestataires labellisés :
    - `http://www.cesg.gov.uk/Finda/Pages/CHECKResults.aspx?post=1&sort=name`
  - Pour être un prestataire labellisé il faut
    - Fournir une équipe d'audit avec un responsable et un consultant, qui doivent chacun avoir certaines qualifications
      - Suivant TI infrastructure ou applicatif
    - Délivrées par des organismes privés qui font passer des examens
      - `http://www.tigerscheme.org` ou `http://www.crest-approved.org/`
  - *The Senior level qualification (CHECK Team Leader) is based on a written paper, a multiple choice paper, a six hour 'assault course' practical assessment, and an interview during which the candidate is asked to explain their findings from the practical assessment. The multiple choice paper is used by the assessor not only to examine the knowledge possessed by the candidate, but also to direct attention to areas of potential weakness to be examined in the practical and the viva. This is a rigorous examination, and should be attempted only by individuals with a significant degree of practical experience.*

Autres cas

- Professions règlementées
  - Avocats, médecins, expert-comptables, huissiers, notaires, …
- H3C (Haut Conseil du Commissariat aux Comptes)
  - Commissaires aux comptes
    - Vivendi, MCI-Worldcom (Verizon), Enron, etc
- ARJEL (Autorité de Régulation des Jeux en Ligne)
  - Processus simple dans un objectif plus limité
  - Problématique de la sortie d'un auditeur de certification une fois qualifié
- CNIL
  - Labellisation
- Autres pays
  - Reconnaissances internationales mutuelles de qualifications de prestataires d'audit ?

Conclusion

- Qualification des prestataires en sécurité utile à tous, au delà du RGS
- Pré-sélection des prestataires compétents
- Etat joue le rôle régalien qui lui incombe

Questions ?

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