HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Qualification des prestataires en sécurité

OSSIR Afterworks, Paris
23 octobre 2012

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
- Utilité de la qualification des prestataires d'audit de sécurité
- Autres cas
- Conclusion

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

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

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

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

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**

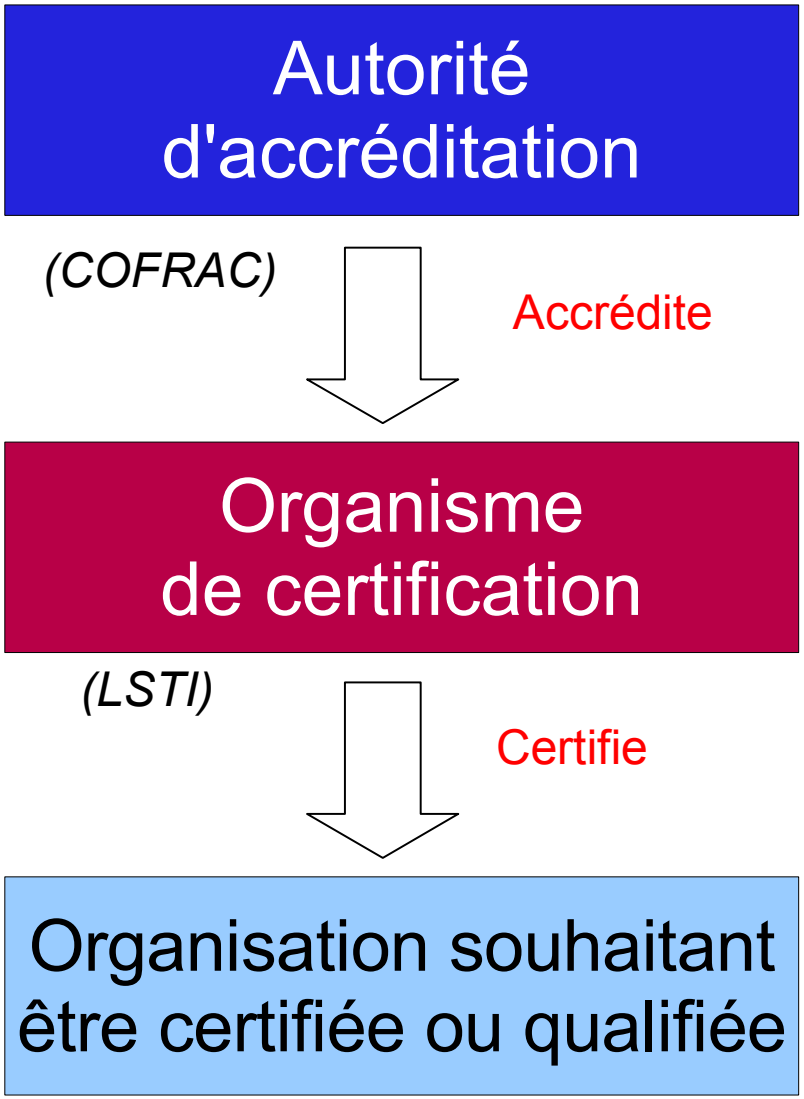
Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

Qualification et Certification

- **Assurance** par une démonstration indépendante que 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

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

Qualification et Certification



- Schéma commun 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

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

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**.*

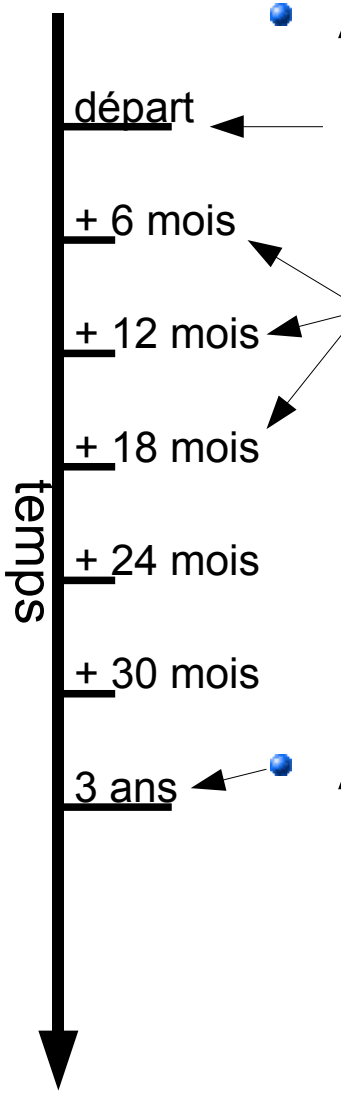
Toute référence à la certification dans la publicité, l'étiquetage ou la présentation de tout produit ou service, ainsi que sur les documents commerciaux qui s'y rapportent doit être accompagnée d'informations claires permettant au consommateur ou à l'utilisateur d'avoir facilement accès aux caractéristiques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

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

Qualification ou certification



- Audit de certification ➔ processus sur trois ans
  - Audit initial
  - Audits de surveillance (ou de contrôle)
    - Généralement tous les 6 mois
    - Si plus de 12 mois entre deux audits la certification est perdue
  - Audit de renouvellement de la certification
    - Tous les 3 ans
    - Permet de remettre en concurrence les organismes de certification
      - Quand il y en a plusieurs...

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

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**

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

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

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

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.

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

Qualifications professionnelles

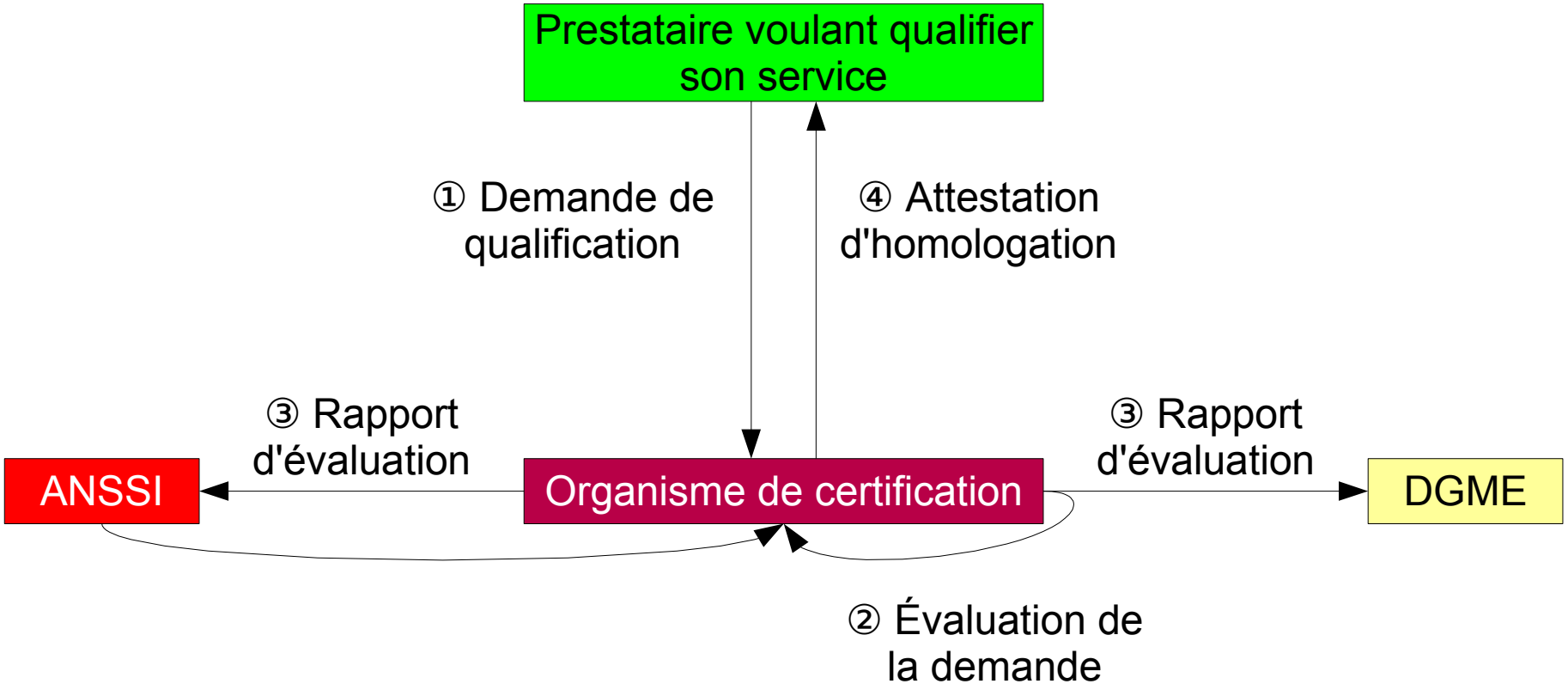
- Article 45-II du Code des marchés publics
- Permet au pouvoir adjudicateur d'exiger un certificat de qualification professionnelle
  - Même si un seul prestataire qualifié répond, il est sélectionné

Qualifications professionnelles existent dans tous les métiers
→ normal qu'elles arrivent dans le métier de l'audit de sécurité

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

Qualification prestataires en sécurité

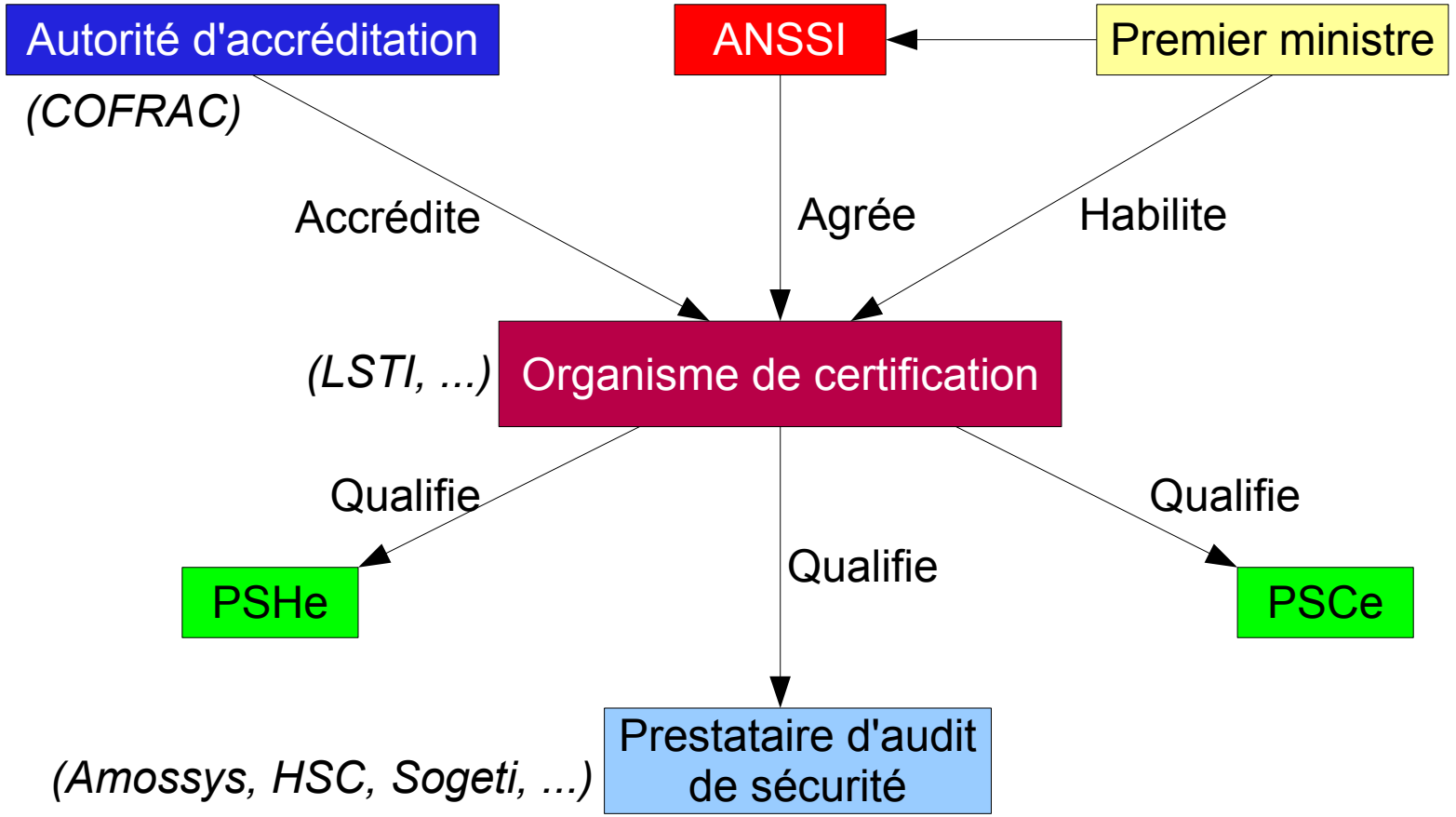
- Dans le cadre du **RGS** (Référentiel Général de Sécurité)



Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

Qualification prestataires en sécurité

- Dans le cadre du **RGS** (Référentiel Général de Sécurité)



- Préfiguration de la qualification des prestataires d'audit : ANSSI accompagne l'organisme de certification

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

Qualification des prestataires d'audit

- Qualification des prestataires d'**audit** en **sécurité des systèmes d'information**
- **Annexe C**, sera dans le RGSv2 à paraître en décembre 2012
- Appel à commentaires sur la v1.1 du 24 avril 2012 clôt le 31 juillet dernier :
  - `http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/appel-a-commentaires-rgs-2-0.html`
- Impose de nombreuses règles
- Reprend les bonne pratiques et les normes en vigueur
  - Beaucoup, beaucoup d'évidences
    - Ou qui devraient en être...
  - Référence à l'ISO 19011

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

Qualification des prestataires d'audit

- Qualification des prestataires d'**audit** en **sécurité des systèmes d'information**
- Qualification de l'entreprise d'audit avec ses auditeurs
- Qualification des auditeurs un par un
- Départ d'un auditeur remet en cause la qualification de l'entreprise
  - Principe de proportionalité : 1 intruseur expérimenté sur 5 ne remettra pas en cause la qualification, départ de 4 sur 5 la remettra en cause
- Pour conserver sa qualification, l'organisme doit assurer qu'il possède toujours les compétences adéquates :
  - Suffisamment d'auditeurs
  - Suffisamment formés

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

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

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

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

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

Qualification des prestataires d'audit

- Qualification des prestataires d'**audit** en **sécurité des systèmes d'information**
- Prestataires doivent :
  - Autoriser l'accès à leurs locaux
  - Donner l'accès à l'ensemble des documents utilisés dans le cadre des activités d'audit
  - Assurer l'accès à leur personnel et leurs auditeurs pour des entretiens individuels
  - Former ses auditeurs au RGS (il y a un examen)
  - Permettre l'observation complète d'un ou plusieurs audits auprès de leurs clients
  - Fournir toutes les vulnérabilités non-publiques découvertes au CERTA
    - CERT-FR : Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

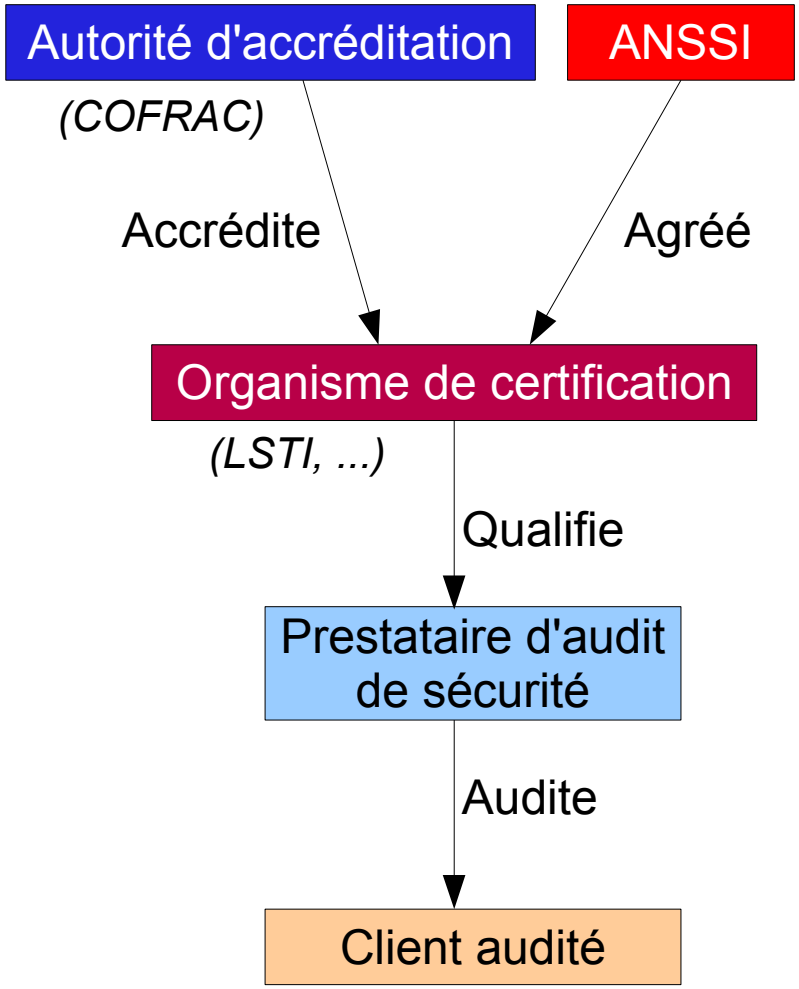
Qualification des prestataires d'audit

- Auditeur de qualification doit vérifier la compétence technique de chaque auditeur dans le domaine de la sécurité des systèmes d'information et leur savoir-faire en matière d'audit
  - ANSSI ? Organisme de certification

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

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 de prestataire d'audit de sécurité → 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



Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

Utilité d'une qualification des auditeurs

- Ce que devrait permettre d'**éviter** la qualification des prestataires d'audit de sécurité pour être **utile**
  - 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
  - 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

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

Utilité d'une qualification des auditeurs

- Ce que devrait permettre d'**éviter** la qualification des prestataires d'audit de sécurité pour être **utile**
  - Commanditaires imposant l'audit de tiers sans autorisation
  - Absence de formation des auditeurs
  - 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

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

Utilité d'une qualification des auditeurs

- Ce que devrait permettre d'**éviter** la qualification des prestataires d'audit de sécurité pour être **utile**
  - Audit applicatifs avec accès au code source, vendus comme réalisés avec une analyse 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
  - 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 achèter un audit...

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

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 ?

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite

Conclusion

- Qualification des prestataires en sécurité très compliquée mais utile et nécessaire
- Etat joue le rôle régalien qui lui incombe
- Pas encore au point, pas encore les bons objectifs atteints mais sur la bonne voie
- Tout acteur sérieux du marché ne peut qu'adhérer à un tel projet ☺

Questions ?

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

Copyright Hervé Schauer Consultants 2000-2012 – Reproduction interdite