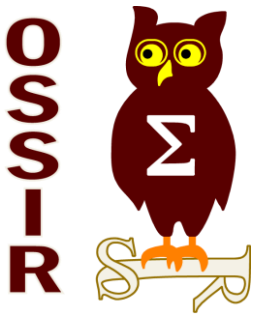

LA QUALIFICATION D'AUDIT PASSI

7 décembre 2015

Synthèse

Afin de renforcer la **qualité des audits** et la **confiance** vis à vis des intervenants en sécurité pour les acteurs importants de la nation, le gouvernement a mis en place une nouvelle qualification : celle de **Prestataire d'Audit de la Sécurité des Systèmes d'Information** (PASSI).

Ce label est délivré par un organisme indépendant, sous contrôle de l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI).

Elle vise à garantir :

- **la qualité des prestations** : compétences, méthodologie et processus ;
- **la protection des données manipulées** : stockage, localisation, échanges, rapport et données d'audit ;
- **la déontologie** : morale, probité et éthique.

1. Pourquoi un nouveau label ?

Les audits de sécurité font partie des prestations les plus sensibles, **identifier un acteur de confiance** présentant les **qualités déontologiques**, les garanties de **protection de l'information** et de **qualité de prestations** est un enjeu primordial et complexe.

Pour apporter de la confiance dans le choix d'un prestataire d'audit de sécurité, le gouvernement propose avec ce label, une liste d'auditeurs qualifiés.

Les entreprises qualifiées PASSI interviennent sur les **domaines** suivants :

- audit de code source ;
- audit d'architecture ;
- audit de configuration ;
- audit organisationnel et physique ;
- les tests d'intrusions.

2. Quelles sont les garanties apportées par la labélisation PASSI ?

La labélisation PASSI impose les critères suivants :

2.1. Qualité des prestations

Les auditeurs doivent avoir un niveau minimal d'expérience et de compétences, sanctionné par un examen.

L'application d'une **méthodologie stricte** est assurée par :

- des **processus** : plan d'audit, réunion de lancement, points réguliers, remontée des alertes, restitution ;
- une **traçabilité** des actions de l'auditeur (journal d'audit détaillé) ;
- l'utilisation de **référentiels** de mise en œuvre de la sécurité reconnus (notablement les guides et notes de l'ANSSI).

2.2. La protection des données manipulées

Les données d'audit sont protégées à minima au niveau **DIFFUSION RESTREINTE** impliquant un nombre de mesures de sécurité telles que décrites dans l'**instruction Interministérielle 901** :

- **chiffrement** des communications, stockage et échanges ;
- sécurisation du système d'information du prestataire d'audit. Le niveau de sécurité est **contre-évalué par l'ANSSI et la LSTI** ;
- données conservées sur le **territoire national**.

Attention, le traitement d'information au niveau DIFFUSION RESTREINTE, entraîne également des obligations fortes pour le client : chiffrement des données stockées et échangées, utilisation d'un SI qualifié, mesures techniques et organisationnelles, etc.

2.3. La déontologie

Les recours à un audit PASSI permet de disposer de **garanties sur la confiance accordée au prestataire**, notamment en matière de confidentialité et de déontologie.

2.4. Liste des prestataires qualifiés

La **liste des prestataires** est disponible sur les sites de l'ANSSI et de LSTI (un délai de synchronisation entre les deux sites peut exister) :

- http://**www.ssi.gouv.fr**/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-daudit-de-la-securite-des-systemes-dinformation-passi-qualifies/
- http://**www.lsti-certification.fr**/index.php/qualification-rgs/les-passi.html

Contexte légal et réglementaire

La qualification PASSI s'effectue dans un cadre normé qui s'appuie sur les textes législatifs et réglementaires (Décret N°2002-535 du 18 Avril 2002, ordonnance N°2005-1516 du 8 Décembre 2005, décret n°2010-112 du 2 Février 2010, le Référentiel Général de Sécurité, l'instruction N°1001/ANSSI.SR du 8 Avril 2011).

La qualification PASSI atteste que le prestataire fournit des audits conformes aux exigences décrites dans le Référentiel Général de Sécurité (RGS) et de l'ordonnance n°2005-1516 du 8 Décembre 2005 articles 9, 10 et 12.

La procédure de qualification PASSI est effectuée par l'organisme LSTI accrédité par le COFRAC et habilité par le premier ministre.

Remerciements

L'OSSIR tient à remercier l'ensemble des acteurs qui ont participé à ce groupe de travail PASSI ainsi qu'à la société LSTI pour la fourniture des documents permettant de comprendre l'exhaustivité de cette qualification.

Groupe de travail composé de : Marc Frédéric Gomez (Crédit Agricole), Christophe Labourdette (ENS-CACHAN/CNRS), Jean-Luc Lotti (ENSAM), Hervé Schauer (HSC by Deloitte), Vladimir Kolla (NetXP), Jérémy Lebourdais (ON-X), Gilles Brusson (Renault), Ary Kokos (Solucom), Guillaume Lopes (Technicolor)

Observatoire de la Sécurité des Systèmes d'Information et Réseaux

L'OSSIR est une association à but non lucratif (1901) visant à promouvoir
la sécurité des systèmes d'information et le partage des connaissances.

45, rue d'Ulm - 75230 Paris cedex 05

www.ossir.org