الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

CODE D'ETHIQUE PROFESSIONNEL POUR LES EXPERTS AUDITEURS CERTIFIES ANSI

Version du 4éme trimestre 2012

Document Public Document Interne Document Confidentiel Document Top-Secret

Préambule

L'expert auditeur certifié ANSI s'engage à respecter les principes et les règles définis dans le présent code d'éthique professionnel.
Le non-respect du présent code d'éthique professionnel peut entraîner à son encontre des mesures disciplinaires qui peuvent aller jusqu'au retrait définitif du certificat d'expert auditeur.

SECTION 1 : Déontologie générale

- Préserver et renforcer l'intégrité de l'infrastructure publique.
- Réaliser ses tâches avec objectivité, diligence raisonnable et professionnalisme, en conformité avec les normes et les meilleures pratiques professionnelles.
- S'acquitter avec probité de ses devoirs envers l'audité, l'ANSI, et ses confrères.
- Encourager à assimiler, accepter et améliorer les solutions et mesures de sécurité, et décourager les pratiques non sécurisées.
- Veiller à contribuer à l'application des normes, des procédures et des mesures de réglementation appropriées aux systèmes d'information et à encourager la conformité.

SECTION 2 : Conduite de l'auditeur

Article 1 : Confidentialité

- Préserver la confidentialité des informations obtenues dans le cadre de ses fonctions à moins de divulgation exigée par l'ANSI ou une autorité juridique. L'information ne doit pas être utilisée à des fins personnelles ni être divulguée à des parties non concernées.

Article 2 : Impartialité

- Veiller à ne pas se retrouver dans des situations qui risquent d'affecter son jugement objectif et de limiter son indépendance. Eviter de se laisser influencer ou mettre sous pression.

Article 3 : Professionnalisme

- Accepter d'entreprendre uniquement des missions d'audit dont on maîtrise l'environnement et les technologies associées, et qu'on juge pouvoir accomplir dans leur totalité de façon professionnelle et dans les délais.
- Veiller à présenter un CV dont le contenu est exact et mis à jour à chaque fois que l'occasion se présente.

Article 4 : Relation avec l'audité

- Faire preuve de respect personnel et professionnel à l'égard de l'audité et agir avec tact.
- Veiller à ne pas dépasser la limite de la confiance et des privilèges qui lui sont attribués dans le cadre de l'audit.

Article 5 : Relation avec l'ANSI

- Informer l'ANSI de toute mission d'audit conduite sous sa supervision directe ou à laquelle il a participé, de toute interruption d'une mission d'audit et de toute contestation ou conflit avec l'audité dans les meilleurs délais.
- Informer l'ANSI de toute entrave au bon déroulement d'une mission d'audit.
- Ne participer à une mission d'audit en tant que expert auditeur certifié ANSI que lorsque son certificat est en cours de validité.
- Informer l'ANSI, dans les meilleurs délais, des problèmes de sécurité qui peuvent avoir un impact grave non seulement sur le SI de l'audité mais également sur les SI auxquels il est interconnecté.
- Autoriser l'ANSI à publier les informations de contact (Tél., mail) de l'expert auditeur et veiller à les mettre à jour.

Article 6 : Relation avec les confrères

- Veiller au respect de ses confrères et éviter de toucher à leur réputation par malveillance ou indifférence.

Article 7 : Mise à niveau et amélioration des compétences

- Veiller constamment à la mise à niveau et à l'amélioration des compétences professionnelles d'ordre réglementaire, normative et technologique en relation avec son activité d'expert auditeur.

SECTION 3 : Conduite de la mission d'audit

Article 8 : Respect du règlement intérieur de l'audité

- Respecter les consignes applicables au règlement intérieur de l'audité et examiner tous les contrats et les accords, expresses ou implicites.

Article 9 : Ressources requises pour l'audit

- Demander toutes les ressources requises pour la mission (documents, habilitations, logistiques, etc), en particulier le rapport d'audit précédent.
- Mentionner, au niveau du rapport d'audit, toute ressource demandée de l'audité et non reçue, et dont l'absence a influé la qualité des résultats de l'audit.

Article 10 : Equipe intervenante

- Pour toute mission conduite sous sa supervision directe, veiller à présenter à l'audité, lors de la réunion d'ouverture, l'équipe intervenante et l'affectation de chacun. Toute modification de la composition de cette équipe doit être approuvée par l'audité.

Article 11 : Périmètre de l'audit

- Veiller à définir exactement la portée de l'audit, tout changement au niveau du périmètre de l'audit doit être approuvé par l'audité.
- Veiller à examiner tout composant du périmètre de l'audit suivant la méthodologie d'audit approuvée par l'audité.
- Ne procéder à l'échantillonnage que suite à l'approbation par l'audité de la méthode d'échantillonnage.

Article 12 : Plan d'audit

- Préparer un plan d'audit détaillant la nature, les objectifs, le calendrier, l'étendue et les ressources nécessaires pour l'audit, en particulier les tests intrusifs, conformément à ce qui a été convenu à la réunion d'ouverture.
- Veiller à respecter ce plan, en particulier les interventions sur terrain.
- Veiller à appuyer chaque intervention sur terrain par un PV signé par les personnes impliquées.

Article 13 : Normes, méthodologies et outils d'audit utilisés

- Adopter une méthodologie d'audit (organisationnel, physique, technique, analyse de risque) adaptée à l'audité et veiller à la mentionner au niveau du rapport et à la respecter.
- Veiller à utiliser les outils de test les plus adaptés pour chaque système cible et utiliser des copies mises à jour.

Article 14 : Constats de l'audit

- Présenter des constats fiables et pertinents, formulés clairement, de manière synthétique et sans équivoque et qui doivent être perçus comme tels par toute tierce personne bien informée.
- Eviter de limiter ses constats uniquement aux résultats de la revue documentaire ou aux résultats bruts des rapports générés par les outils de test automatisé de vulnérabilités. En l'absence de l'interviewé ou de réponse claire, éviter de répondre par soi-même au questionnaire et veiller, tout au long de l'audit, à conserver une attitude impartiale caractérisée par l'absence de tout préjugé.

- Veiller à examiner minutieusement les configurations des différents composants, en plus des tests automatisés, et les confronter avec la politique de sécurité de chacun même si cette dernière est informelle.
- Eviter de se baser uniquement sur les résultats des tests intrusifs pour accomplir l'audit technique.
- Eviter de donner des constats sans présenter les éléments probants suffisants, fiables, pertinents et utiles.
- Eviter de généraliser ses constats suite à des vérifications sur un échantillon non significatif.
- Ne pas se limiter à mentionner l'existence d'une procédure mais étudier son efficacité.

Article 15 : Plan d'action

- Proposer un plan d'action personnalisé, réaliste et optimisé, qui s'adapte avec la réalité humaine, financière et culturelle de l'audité et qui supporte les projets futurs, à court et à moyen terme, de l'audité.
- Proposer des estimations en ressources humaines et financières étudiées.
- Veiller à étudier les solutions proposées avec l'audité en termes de faisabilité et efficacité.
- Eviter de proposer des solutions orientées vers des produits commerciaux.
- Eviter le conflit d'intérêt entre le rôle d'auditeur et le rôle de maître d'œuvre.
- Eviter de proposer toujours les mêmes solutions pour différents audités sans prendre en compte les besoins spécifiques de chacun.

Article 16 : Livrables de l'audit

- Etre responsable du contenu des rapports d'audit délivrés à l'audité, et montrer son engagement par la signature du rapport.
- En cas de présence de plusieurs auditeurs certifiés ANSI, ne signer que les parties du rapport auxquelles il a participé effectivement.
- Ne pas distribuer, ni diffuser, ni communiquer les livrables, quelque soit leur forme (papier, magnétique, électronique ou autre), sans le consentement écrit de l'audité. Tous les livrables sont la propriété exclusive de l'audité.

Article 17 : Transparence avec l'audité

- Agir en toute transparence avec l'audité et l'informer de toute action sur son SI à temps, en particulier de toute brèche de sécurité observée même si le système cible n'est pas couvert par le périmètre de l'audit.
- Informer l'audité de toute manipulation qui agit sur son système d'information même de manière passive ou indirecte.

Article 18 : Avis de l'ANSI sur le rapport d'audit

- Assurer par soi-même le traitement des remarques soulevées par l'ANSI suite à l'étude du rapport d'audit relatif à une mission conduite sous sa supervision directe.
- En cas de présence de plus d'un auditeur certifié dans la même mission, chaque auditeur doit assurer le traitement des remarques qui concernent la partie à laquelle il a participé effectivement.
- Entreprendre les actions nécessaires pour combler les manquements soulevés dans l'avis de l'ANSI.