Audits de sécurité qualifiés PASSI

Mettez à l'épreuve la cyber résilience de vos systèmes et de vos processus métier

Les audits de sécurité qualifiés PASSI : une garantie de qualité dans la stratégie de Cybersécurité

Des règlementations renforcées

Le Règlement Général sur la Protection des Données (GDPR) et la directive sur la Sécurité des Réseaux et Systèmes d'Information (NIS) exigent ou suggèrent fortement aux organisations de réaliser régulièrement des audits de sécurité des SI.

Des menaces cyber de plus en plus significatives

WannaCry, NotPetya et d'autres incidents de sécurité récents ont montré l'impact dévastateur que l'existence de failles de sécurité dans les systèmes pouvait entraîner. La détection de ces failles et leur correction rapide devient un enjeu fort pour les organisations.

Les régulateurs, les consommateurs, les clients B2B, les investisseurs, les citoyens : tous exigent maintenant un niveau de confiance accrue dans les capacité des organisations à protéger les données, notamment personnelles, les infrastructures et les processus critiques.

Les défis sont nombreux pour les responsables en charge des audits de sécurité des SI :

Un périmètre conséquent et hétérogène
Les briques fonctionnelles et techniques sont nombreuses et variées au sein de votre organisation et sur Internet. Elles sont toutes des cibles potentielles pour les menaces cyber.

Des contraintes budgétaires
Un grand volume des systèmes et processus doivent être couverts, avec des budgets forcément limités.

Une maîtrise indispensable des risques liés aux tests
La disponibilité des systèmes de production, ainsi que l'intégrité et la confidentialité des données ne doivent pas être mises en danger par la réalisation des audits de sécurité.

Des interlocuteurs variés
De multiples interlocuteurs (IT, métier, management, fonction de contrôle) doivent s'approprier les travaux réalisés et les résultats obtenus, afin de prendre les bonnes décisions.

Des contraintes de planification
La réalisation d'audits de sécurité ne doit pas entraîner des contraintes supplémentaires de planning pour les systèmes en développement ou en production.

Nos prestations qualifiées PASSI

Attestation de qualification N° : 20118
Date de prise : lundi 25 septembre 2017
Fin de validité : jeudi 24 septembre 2020
Version : 1

KPMG est qualifié **Prestataire d'Audit de la Sécurité des Systèmes d'Information** par l'ANSSI, pour 5 activités d'audit de sécurité :

Activités d'audit qualifiées PASSI

- Audit organisationnel et physique
- Audit de code source
- Audit de configuration
- Audit d'architecture
- Tests d'intrusion

La qualification PASSI par l'ANSSI atteste :

- Des compétences des auditeurs en charge des audits de sécurité SI,
- De la déontologie des auditeurs,
- De la protection et la confidentialité des données, rapports et documents échangés,
- D'une méthodologie d'audit de sécurité appropriée.

Les prestations d'audit de sécurité des SI de KPMG sont qualifiées PASSI RGS par l'ANSSI.

Toutes nos activités d'audit de sécurité des SI ne sont pas qualifiées PASSI.

Nos atouts

La capacité de nos auditeurs à **dialoguer avec le top management** sur des problématiques stratégiques, ainsi qu'avec les **équipes métiers** ou **techniques**.

Une démarche de **mise en perspective** systématique des failles identifiées avec les **risques métier** propres à vos processus et votre secteur.

Un véritable **accompagnement** dans l'organisation et la réalisation des audits de sécurité ainsi qu'un support proactif dans la **remédiation** de failles.

Un **laboratoire** dédié à la Cybersécurité et **conforme aux exigences de la qualification PASSI**, situé dans nos locaux à Paris.

Notre laboratoire possède tous les équipements et technologies nécessaires :

- à la réalisation des tests de sécurité,
- au développement de nouvelles attaques et outils,
- à la formation continue des consultants à travers la simulation d'environnements vulnérables.

Contacts

Vincent Maret
Associé, responsable de l'offre Cybersécurité et Protection des données personnelles
Tel : +33 1 55 68 26 64
Mob : +33 6 17 12 22 13
Email : vmaret@kpmg.fr

Guillaume Rablat
Directeur, responsable de l'offre CyberDefense
Tel : +33 1 55 68 39 88
Mob : +33 6 61 57 21 43
Email : grablat@kpmg.fr

L'étendue et la nature des services détaillés dans ce document sont soumis aux règles déontologiques de la profession, selon que nous sommes commissaires aux comptes ou non de votre entité ou de votre groupe. Les informations contenues dans ce document sont d'ordre général et ne sont pas destinées à traiter les particularités d'une personne ou d'une entité. Bien que nous fassions tout notre possible pour fournir des informations exactes et appropriées, nous ne pouvons garantir que ces informations seront toujours exactes à une date ultérieure. Elles ne peuvent ni ne doivent servir de support à des décisions sans validation par les professionnels ad hoc. KPMG S.A. est le membre français du réseau KPMG International constitué de cabinets indépendants adhérents de KPMG International Cooperative, une entité de droit suisse (« KPMG International »). KPMG International ne propose pas de services aux clients. Aucun cabinet membre n'a le droit d'engager KPMG International ou les autres cabinets membres vis-à-vis des tiers. KPMG International n'a le droit d'engager aucun cabinet membre.

© 2020 KPMG S.A., société anonyme d'expertise comptable et de commissariat aux comptes, membre français du réseau KPMG constitué de cabinets indépendants adhérents de KPMG International Cooperative, une entité de droit suisse. Tous droits réservés. Le nom KPMG et le logo sont des marques déposées ou des marques de KPMG International