À propos de Nous

Banking Intelligence Consulting (BIC) est une société spécialisée dans les services Swift, la gouvernance IT, la cybersécurité et la formation.
BIC accompagne les banques dans la gestion, la sécurisation et l'évolution de leurs environnements Swift, notamment à travers le support opérationnel, les mises à jour annuelles et les évaluations de conformité au programme Swift CSP.
Grâce à ses propres solutions dédiées aux environnements bancaires, BIC aide les banques à renforcer la sécurité, la supervision, le reporting, la traçabilité et la performance de leurs opérations critiques.
BIC intervient également dans l'intégration de solutions technologiques et de cybersécurité adaptées aux exigences des banques, tout en proposant des formations spécialisées sur Swift, la cybersécurité et les normes internationales.

Certifiée ISO/IEC 27001 par TÜV Rheinland, BIC allie une connaissance approfondie du secteur bancaire à une expertise technique avancée afin d'aider les banques à bâtir des opérations sécurisées, conformes et prêtes pour l'avenir.

BANKING INTELLIGENCE CONSULTING
INTELLIGENT EXPERIENCE FOR A BETTER WORLD

Nous croyons fermement en l'importance d'offrir à nos clients un service d'excellence.

Contactez Nous

Tél:
+216 20 556 655
+216 20 554 555
+216 20 557 557

E-mail:
Sales@b-i-consulting.com

Addresse:
Résidence Opera Garden, Duplex C04, La Marsa, Tunis 2046, Tunisie.

Site Web:
www.b-i-consulting.com

Services de Banking Intelligence Consulting

INTELLIGENT Experience for a better world

TÜVRheinland CERTIFIED
ISO/IEC 27001:2022
Valid until: 2027-09-04
www.tuv.com ID 9000034376

SOC

- Conception, mise en place et optimisation de Security Operations Centers (SOC) internes ou mutualisés, adaptés aux standards internationaux.
- Intégration et configuration de solutions SIEM pour la collecte, la corrélation et l'analyse avancée des événements de sécurité.
- Surveillance en temps réel des menaces, détection proactive et gestion des incidents de cybersécurité.
- Mise en œuvre de services de Threat Intelligence et de Threat Hunting pour anticiper, détecter et neutraliser les menaces émergentes.
- Définition des processus de réponse aux incidents, de gestion de crise et de continuité d'activité en cas d'incident critique.
- Accompagnement à l'exploitation opérationnelle du SOC afin d'améliorer la visibilité, la réactivité et l'efficacité des équipes sécurité.

Sourcing premium

- Mise à disposition de consultants qualifiés pour des missions ponctuelles, courtes ou critiques, selon les besoins des projets.
- Mobilisation de profils spécialisés : administrateurs Swift, analystes SOC, experts cybersécurité, support applicatif et consultants IT.
- Intervention dans des environnements sensibles et réglementés, avec maîtrise des enjeux métier, sécurité et conformité.
- Consultants certifiés ISO/IEC 27001, ISO 22301, SOC 2 et/ou Swift CSP, selon leur expertise.
- Accompagnement opérationnel pour sécuriser les activités, accélérer les projets stratégiques et renforcer la conformité.

Services Swift

- **Évaluation Swift CSP**
- Évaluer le niveau de conformité de la banque aux exigences Swift CSP, identifier les écarts et proposer les actions correctives prioritaires.
- **Mise en œuvre du CSP**
- Accompagner la banque dans l'application des contrôles requis, la préparation des preuves et le suivi du plan de remédiation.
- **Gouvernance Swift**
- Structurer la gestion de l'environnement Swift à travers des rôles clairs, des responsabilités définies et un suivi régulier des risques.
- **Procédures et politiques**
- Élaborer et mettre à jour les procedures et politiues nécessaires pour assurer une gestion conforme, sécurisée et traçable des opérations Swift.
- **Support technique Swift**
- Assister les équipes dans l'exploitation quotidienne, la résolution des incidents, les mises à jour et l'amélioration continue de la plateforme Swift.

GRC

- Mise en place de systèmes de management de la sécurité de l'information SMSI / ISMS selon ISO/IEC 27001.
- Élaboration des plans de continuité d'activité PCA selon ISO 22301.
- Évaluation et traitement des risques informationnels et opérationnels selon ISO 31000.
- Définition des politiques, procédures et documents de gouvernance IT alignés avec les exigences réglementaires.
- Réalisation d'audits de conformité et d'analyses d'écarts selon les référentiels internationaux.
- Accompagnement à la certification ISO 27001, ISO 22301 et référentiels associés.

Cybersécurité

- Réalisation d'audits de sécurité avancés pour évaluer la robustesse des dispositifs de protection et de gouvernance IT.
- Définition des politiques et procédures de sécurité alignées avec les exigences réglementaires
- Réalisation de tests de pénétration internes et externes, incluant l'ethical hacking.
- Identification et priorisation des vulnérabilités selon leur criticité, leur impact métier et leur exposition.
- Élaboration de rapports techniques et stratégiques avec recommandations et plan d'action priorisé.
- Accompagnement à l'intégration de solutions de cybersécurité : EDR, XDR, NDR, PAM, MFA, DLP, SCCM, SIEM, VMS, WAF, etc.