BANKING INTELLIGENCE CONSULTING
INTELLIGENT EXPERIENCE FOR A BETTER WORLD

About Company

Banking Intelligence Consulting (BIC) is a company specialized in Swift services, IT governance, cybersecurity, and training.
BIC supports banks in managing, securing, and evolving their Swift environments, particularly through operational support, annual updates, and compliance assessments under the Swift CSP program.
Through its own solutions dedicated to banking environments, BIC helps banks strengthen the security, supervision, reporting, traceability, and performance of their critical operations.
BIC also supports the integration of technology and cybersecurity solutions tailored to banks' requirements, while providing specialized training on Swift, cybersecurity, and international standards.
Certified ISO/IEC 27001 by TÜV Rheinland, BIC combines in-depth knowledge of the banking sector with advanced technical expertise to help banks build secure, compliant, and future-ready operations.

We strongly believe in providing perfect service to our customers.

Contact Us

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

Email:
Sales@b-i-consulting.com

Address:
Opera Garden Residence, Duplex C04, La Marsa, Tunis 2046, Tunisia

Website:
b-i-consulting.com

Banking Intelligence Consulting Services

INTELLIGENT Experience for a better world

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

SOC

- Design, implementation and optimization of internal or shared Security Operations Centers (SOC), aligned with international standards.
- Integration and configuration of SIEM solutions for the collection, correlation and advanced analysis of security events.
- Real-time threat monitoring, proactive detection and cybersecurity incident management.
- Implementation of Threat Intelligence and Threat Hunting services to anticipate, detect and neutralize emerging threats.
- Definition of incident response, crisis management and business continuity processes in the event of a critical incident.
- Support for the operational running of the SOC to improve visibility, responsiveness and the effectiveness of security teams.

Premium Sourcing

- Provision of qualified consultants for one-off, short-term or critical assignments, according to project needs.
- Mobilization of specialized profiles: Swift administrators, SOC analysts, cybersecurity experts, application support specialists and IT consultants.
- Intervention in sensitive and regulated environments, with strong command of business, security and compliance requirements.
- Consultants certified in ISO/IEC 27001, ISO 22301, SOC 2 and/or Swift CSP, depending on their area of expertise.
- Operational support to secure business activities, accelerate strategic projects and strengthen compliance.

Swift Services

- Swift CSP Assessment
- Assess the bank's level of compliance with Swift CSP requirements, identify gaps, and propose priority corrective actions.
- CSP Implementation
- Support the bank in implementing the required controls, preparing evidence, and monitoring the remediation plan.
- Swift Governance
- Structure the management of the Swift environment through clear roles, defined responsibilities, and regular risk monitoring.
- Procedures and Policies
- Develop and update the necessary procedures and policies to ensure compliant, secure, and traceable management of Swift operations.
- Swift Technical Support
- Assist teams with daily operations, incident resolution, updates, and continuous improvement of the Swift platform.

GRC

- Implementation of Information Security Management Systems (ISMS) in accordance with ISO/IEC 27001.
- Development of Business Continuity Plans (BCP) in accordance with ISO 22301.
- Assessment and treatment of information and operational risks according to ISO 31000.
- Definition of IT governance policies, procedures and documentation aligned with regulatory requirements.
- Conducting compliance audits and gap analyses based on international standards.
- Support for certification against ISO/IEC 27001, ISO 22301 and related frameworks.

Cybersecurity

- Advanced security audits to assess the robustness of protection mechanisms and IT governance.
- Definition of security policies and procedures aligned with regulatory requirements.
- Internal and external penetration testing, including ethical hacking
- Identification and prioritization of vulnerabilities based on criticality, business impact and exposure level.
- Preparation of technical and strategic reports including recommendations and a prioritized action plan.
- Support for the integration of cybersecurity solutions: EDR, XDR, NDR, PAM, MFA, DLP, SCCM, SIEM, VMS, WAF, etc.