BANQUE AFRICAINE DE DEVELOPPEMENT
AVIS DE VACANCE DE POSTE N° ADB/12/196

Titre du poste:		N° du poste:	Date de clôture:
Chief Information Security Officer (CISO)	Grade: **PL-3**	**SAP 50000592**	**20 AUGUST 2012**
Département/Division:	Nom et titre du supérieur hiérarchique:		
Security Unit (SECU)	**Mr. William GODBOUT, Head Of Unit, SECU**		

Objectives: The Chief Information Security Officer (CISO) will be responsible for protecting the Bank's IT resources and information assets by: (i) Ensuring strategic alignment of information security in support of business objectives; (ii) Ensuring availability, confidentiality, integrity, audit ability of the Bank's information systems; (iii) Ensuring continued availability of the Bank's information systems; (iv) Ensuring reduction of adverse impacts on the Bank's business operations to an acceptable level; (v) ensuring conformity of applicable laws, regulations and standards; (vi) preventing non repudiation at computer based activities.

Duties and Responsibilities: Under the supervision of the Director, the incumbent will carry out the following functions:

Information Security Governance: Establish and maintain a framework to provided assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations.

- Define and elaborate the information security strategy in support of the Bank's business strategy and direction.
- Liaise with CHRM to ensure that each jab description include information security governance activities.
- Identity current and potential legal and regulatory issues affecting information security and assess their impact on the Bank.
- Establish and maintain information security policies that support business goals and objectives.

Risk Management: Identify and manage information security risks to achieve business objectives:

- Develop systematic, analytical and continuous risk management process.
- Ensure that risk identification, analysis and mitigation activities are integrated in projects and processes life cycle.
- Identify and analyze risks through suitable and recommended methods.

Information Security Programme Management: Design, elaborate and manage information security programme to implement the information security governance framework.

- Establish and maintain plans to implement the information security governance framework.
- Define annual information security budget and obtain Information Security Steering Committee approval.
- Manage the information security budget in implementing the information security programme.

Information Security Management: Oversee and direct information security activities to execute the information security programme.

- Lead the Bank's IT security team: plan, organize, assign, supervise and monitor the work of team members
- Ensure that the rules of use for information systems and the administrative procedures for information systems comply with the Bank's information security policies.
- Ensure that services provided by other enterprises, including outsourced providers are consistent with established information security policies.

Response Management: Establish and manage capability to response to and recover from disruptive and destructive information systems events:

- Design, elaborate and implement processes for detecting, identifying and analyzing security related events.
- Develop response and recovery plans including organizing, training, and equipping teams.
- Ensure periodic testing of the response and recovery plans where appropriate.

Business Continuity and Disaster Recovery Plan Management: Design, elaborate, coordinate, maintain and supervise comprehensive Business Continuity and Disaster Recovery Programmes, strategies, plans and procedures in order to assist the Bank's survival from major interruptions of data processing services.

- Coordinate and manage activities related to the Business Continuity Plan (BCP) including the Disaster Recovery Plan (DRP).
- Coordinate the maintenance of the BCP/DRP documentation.
- Liaise with all resources that intervene in the Bank's BCP: Senior Management, Directors and Managers, Staff, Consultants, vendors and auditors.
- Any other duties reasonably requested by management.

Selection Criteria: (including desirable skills, knowledge and experience)

- Minimum of a Master's Degree in Information Security, Computer Science, Information Technology or related field.
- Preferably seven (7) years of relevant post qualification experience, with at least three (3) years of demonstrated IT infrastructure implementation and management.
- Mixed managerial, analytical and technical skills and knowledge in all aspects of computer security in multi IT areas: database, development, network, operating systems, IT security, specific applications security, etc.
- Good understanding and writing skills of computer systems security strategies, policies, principles, procedures, and standards.
- Good technical knowledge and experience across multiple platforms and technologies: Windows, Unix, Linux, networking, applications concepts, databases; wide area networks; computer operations, Intranet/Internet, LAN/WAN Connectivity with good knowledge of firewalls, switches and routers (especially Cisco products).
- Good technical knowledge and experience in defining access and authorization controls within the Bank's critical applications: SAP. SWIFT, SUMMIT, etc.
- Good technical knowledge and experience in Business Continuity Planning areas.
- Good knowledge of structured systems analysis techniques and practices as well as strong analytical and problem solving

skills

- Good Knowledge of risk assessment processes
- Good understanding of 1SO17799, and current legal and regulatory requirements relating to information security and privacy
- Up to date knowledge at information security; industry certifications covering information security are added advantages.
- Demonstrable experience with networks and systems involved in keeping an organization secure.
- Strong management and leaderships skills and the ability to influence senior management are essential.
- Competence in the use of standard Microsoft office applications (Word, Excel, Access, and PowerPoint).
- Excellent written and verbal communications in English or French with a working knowledge of the other language.

Soumis par: Harold AKINGBADE-TAYLOR, Officer-In-charge, CHRM.1	**Date** :
Approuvé par: Gemina ARCHER-DAVIES, Director, CHRM	**Date** :

Only applicants who fully meet the Bank's requirements and are being considered for interview will be contacted. Applicants will only be considered if they submit an online application, and attach a comprehensive Curriculum Vitae (CV). The President, AfDB, reserves the right to appoint a candidate at a lower level. **The African Development Bank is an equal opportunity employer and female candidates are strongly encouraged to apply:** www.afdb.org/jobs