BANQUE D'INVESTISSEMENT ET DE DEVELOPPEMENT DE LA CEDEAO
ECOWAS BANK FOR INVESTMENT AND DEVELOPMENT
BANCO DE INVESTIMENTO E DE DESENVOLVIMENTO DA CEDEAO

ECOWAS Bank for Investment and Development (EBID), based in Lomé, Togolese Republic, is seeking to recruit a qualified person, who is citizen of the Community, to fill the following vacancy in the Professional Staff category.

Position	Main duties and Responsibilities	Required Qualification, Experience and Skills
CHIEF INFORMATION SECURITY OFFICER (CISO) **(Grade P3-1)**	**Job summary** The successful candidate shall work under the supervision of the Head of the Risk Management Department of the Bank and shall be responsible for establishing and maintaining the enterprise vision, strategy, and programs to ensure information assets and technologies are adequately protected. As the Chief Information Security Officer (CISO), he/she will offer direction on compliance obligations, assist the bank in devising robust risk management approaches, and spearheading initiatives to protect the Bank's data, intellectual property, and technological framework from both internal and external risks. This position plays a pivotal role in ensuring adherence to regulatory standards and industry benchmarks, while also nurturing a security-conscious culture across the Bank. **Duties** **1. Strategic Planning and Vision :** • Develop and implement the Bank's information security strategy and roadmap by building security architecture	• A Master's Degree from a recognized university, in computer science, Information Technology, or a related field; • Proven experience (minimum of 7 years) in cybersecurity leadership roles, with a track record of successfully implementing and managing cybersecurity programs. • Strong understanding of cybersecurity principles, frameworks, and technologies, including but not limited to NIST, ISO, CIS Controls, SIEM, IDS/IPS, DLP, encryption, and cloud security. • Excellent leadership, communication, and interpersonal skills, with the ability to collaborate effectively across departments and influence stakeholders at all levels of the organization.

	and policies based on business needs, risk assessments, and regulatory requirements. • Define security policies, standards, and procedures aligned with business objectives and industry best practices. • Assess emerging threats and trends and adjust security strategies accordingly. **2. Risk Management :** • Identify, evaluate, and prioritize security risks across the organization. • Develop and maintain a risk management framework to mitigate risks effectively. • Manage the risk management programme through planning, developing, coordinating, and implementing information technology disaster recovery and business continuity planning. **3. Security Operations :** • Oversee the design, implementation, and maintenance of security controls, technologies, and processes. • Coordinate incident response activities and lead efforts to mitigate security incidents. • Conduct regular security assessments and audits to ensure compliance and effectiveness.	• Industry certifications such as CISSP, CISM, CISA, or equivalent are highly desirable. • Experience in regulated industries (e.g., healthcare, finance, government) and familiarity with applicable regulations (e.g., HIPAA, GDPR, SOX) is a plus. • Strong analytical and problem-solving skills, with the ability to make risk-based decisions in a fast-paced environment. • Proven ability to lead and develop a diverse team of cybersecurity professionals.

	4. Compliance and Gouvernance : • Ensure compliance with relevant laws, regulations, and industry standards (e.g., GDPR, HIPAA, ISO 27001). • Establish and maintain governance structures to support effective information security management. • Liaise with internal and external auditors and regulators in reviewing special investigations results, internal audits, research studies, forecasts, and modelling exercises to provide direction and guidance. **5. Security Awareness and Training :** • Develop and deliver security awareness programs to educate employees about their roles and responsibilities in maintaining security. • Provide training to IT staff and other relevant stakeholders on security best practices. • Execute all other tasks assigned by the Head of Department and Management.	

❖ **OTHER REQUIREMENTS**

- Be a national of one of the ECOWAS Member States;
- Must not be above 45 years at the time of recruitment;
- Have sound knowledge of computer tools (Word, Excel, Access and Power Point);

❖ **APPLICATION MUST INCLUDE THE FOLLOWING:**

- A detailed curriculum vitae;
- A cover letter;
- Copies of academic and professional certificates;
- A copy of national identity card or passport;
- A copy of birth certificate.

Interested candidates should submit by email, their applications to recrutbidc@bidc-ebid.org, no later than August 30, 2024, with the subject "2024 RECRUITMENT PROGRAMME".

N.B.: Only shortlisted candidates will be invited for interview. EBID reserves the right to withdraw the notified vacancy or offer position at a lower grade. Female applications are strongly encouraged.