JOB DESCRIPTION

JOB TITLE:	Information Technology Risk Officer	**JOB GRADE:**	ABO		
DIVISION/ DEPARTMENT:	Risk Department	**BUS. SEGMENT:**	Non Sales	**VER. NO:**	0.1

JOB OBJECTIVE(S)

TO identify, assesses, and mitigate risks related to information technology systems and processes, ensuring compliance with regulatory requirements and organizational policies. Safeguarding IT infrastructure and data while supporting business operations

REPORTING RELATIONSHIPS

Functionally reports to: Head of Risk

Administratively reports to: Head of Risk

JOB DESCRIPTION

1. Risk Identification and Assessment:

- Conducting Risk Assessments: Identifying potential risks to IT systems and data, including threats like cyberattacks, system failures, and data breaches.
- Analyzing Existing Risks: Evaluating the likelihood and impact of identified risks.
- Identifying Vulnerabilities: Pinpointing weaknesses in systems and processes that could be exploited by attackers or lead to failures.

2. Risk Mitigation and Management:

- Developing Mitigation Strategies:
- Designing and implementing plans to reduce or eliminate identified risks.
- Implementing Controls:
- Establishing technical, physical, and administrative safeguards to protect IT systems and data.
- Monitoring and Improving Controls:
- Continuously reviewing and enhancing existing controls to ensure their effectiveness.
- Managing Risk Registers:
- Maintaining comprehensive documentation of identified risks, their assessments, and mitigation actions.

3. Compliance and Regulatory Oversight:

- Ensuring Compliance: Verifying that IT systems and processes comply with relevant regulations, industry standards, and internal policies.

- Staying Updated: Keeping abreast of changes in regulations and industry best practices.
- Supporting Compliance Programs: Contributing to the development and implementation of compliance programs.

4. Communication and Collaboration:

- Providing Guidance and Training:
- Training other employees and other stakeholders on IT risk management practices.
- Collaborating with Stakeholders:
- Working with IT teams, audit departments, and other relevant groups to address IT risk concerns.
- Reporting and Communication:
- Preparing and presenting regular reports on IT risk status and progress to management and other stakeholders.

5. Other Responsibilities:

- Business Continuity Planning: Developing and maintaining business continuity plans to ensure operational stability during disruptions.
- Outsourcing Oversight: Managing IT risks associated with outsourcing activities.
- Developing and Maintaining IT Risk Policies and Procedures: Ensuring a comprehensive framework for managing IT risks within the organization.

JOB REQUIREMENTS

Academic: • Minimum of a bachelor's degree in cybersecurity, computer science, information systems, information security or similar technology-related field - Minimum Upper 2nd Class honors or 3.0 GPA. Professional: • Relevant certifications in information security and risk management knowledge areas, such as Information Systems Audit, Information Security Management and Ethical Hacking. Desired work experience: • 3 years of experience working in a highly computerized and regulated environment	**EXPERIENCE** • Minimum of 2 years banking experience in a similar capacity

• At least 2 years of experience within technology security, risk or assurance functions. • Practical knowledge of risk and control frameworks and application in financial services industry	
COMPETENCIES	
Technical Competencies: Ability to undertake threat and vulnerability assessments so as to identify, quantify, and prioritize the vulnerabilities and threats to information systems. Ability to undertake security assessment and testing to reveal flaws in the security mechanisms of information systems including specific elements of confidentiality, integrity, authentication, availability, authorization and non-repudiation. Knowledge and good understanding of Information Security and Control Objectives Fair understanding of information systems architecture and operational practices	**Behavioral Competencies**: Interpersonal skills to effectively communicate with and manage expectations of all team members and other stakeholders who impact performance. Knowledge and effective application of all relevant banking policies, processes, procedures and guidelines to consistently achieve required compliance standards or benchmarks Self-empowerment to enable development of open communication, teamwork and trust that are needed to support true performance and customer-service oriented culture Must possess a high level of integrity

WHAT WE EXPECT FROM YOU: • High degree of professional ethics, integrity and responsibility. • Highly organized, proactive, ability to work independently and take ownership of tasks assigned. • Team player with the ability to work under pressure and ability to work with a wide variety of people and maintain an excellent business relationship. •	• High sense of confidentiality and discreteness.

JOB HOLDER:		**SIGN:**		**DATE:**	

DISCLAIMER

The above statements are intended to describe the general nature and level of work to be performed by people assigned to this job. They are not to be construed as an exhaustive list of all responsibilities, duties and skills required of personnel so classified. All personnel may be required to perform other responsibilities in addition to those specified from time to time, as needed. UBA reserves the right to modify job duties or descriptions at any time.