1.	DEPARTMENT	:	Risk & Compliance Management
2.	JOB REF	:	RCD2.02
3.	JOB TITLE	:	Head Information Security & Business Continuity Division
4.	RANK	:	Deputy Director
5.	REPORTS TO	:	Head Risk & Compliance Management Department
6.	SUPERVISES	:	Team Leader Business Continuity Management
			Team Leader Information Security Management

7. **PURPOSE:**

Providing strategic direction, leadership, and oversight of Information Security & Business Continuity Management to ensure the development, implementation, and maintenance of robust information security and business continuity programs.

Responsible for driving the bank's efforts to safeguard its assets, protect sensitive information, and ensure the continuity of critical operations.

8. **DUTIES AND RESPONSIBILITIES**

- Provide strategic direction and leadership of the Bank's Information Security & Business Continuity Management initiatives.

- Lead the development, review, and implementation of information security policies, procedures, and guidelines for Bank of Uganda, Supervised Financial Institutions (SFIs), and Payment Systems Operators (PSOs).

- Oversee the management of the Bank's Information Security Management System (ISMS), including tracking compliance with ISO 27000 controls and recommending remedial actions.

- Lead the ISO 27000 certification process of Bank of Uganda, establishing and maintaining an internationally recognized Information Security Management System (ISMS).

- Coordinate the development and implementation of ISMS policies, procedures, and controls to meet ISO27001 requirements.

- Collaborate with internal stakeholders and external auditors to prepare for and undergo ISO 27001 certification audits.

- Ensure ongoing compliance with ISO 27001 requirements and drive continuous improvement of the ISMS.

- Collaborate with internal stakeholders, senior management, and external partners to promote a culture of information security awareness, business continuity planning, and compliance.

- Provide guidance and support in conducting training and awareness programs on Information Security and Business Continuity management concepts, methodologies, and best practices.

- Engage with regulatory authorities, industry associations, and other relevant entities to stay abreast of emerging threats, regulatory developments, and industry trends.
- Conduct or commission independent assessments to provide assurance of satisfactory compliance with information security policies, procedures, and standards.
- Monitor the operating environment for information security vulnerabilities and proactively identify areas for improvement.
- Develop and implement comprehensive strategies and initiatives to enhance the bank's resilience to information security threats and business disruptions.
- Provide leadership and oversight for the development, implementation, and maintenance of business continuity plans to ensure the bank's resilience in the face of disruptions or disasters.
- Collaborate with internal stakeholders to conduct business impact analyses, identify critical processes, and prioritize recovery efforts.
- Coordinate business continuity exercises and drills to test the effectiveness of plans and enhance staff preparedness.

9. EXPECTED OUTPUTS

- Comprehensive Information Security Management System (ISMS) aligned to the ISO 27000 family of standards.
- Comprehensive Information Security Policies, Procedures, and Guidelines
- Information Security Baseline Standards
- Bank of Uganda ISO 27001 Certification
- Information Security Compliance Assessment Reports
- Information Security Risk Assessment Reports
- Information Security Incident Response Plans
- Information Security Incident Reports
- Business Continuity Plans
- Business Impact Analysis Reports
- Information Security, Business Continuity, and ISO 27001 certification Progress Reports
- Information Security & Business Continuity Awareness Campaigns

10. PERSON SPECIFICATIONS

A. QUALIFICATIONS
- First class / upper second Honours Bachelor's Degree from an accredited institution in the fields of Computer Science, Software Engineering, Information Technology,

Computer Engineering, Computer Network & Security, Cybersecurity, Information Security & Assurance, or any other related field.
- Master's degree in the fields listed ~ is an ~de~ added advantage (not Mandatory)
- Professional certifications such as CISSP, CEH, SSCP, CASP, CompTIA Security+, GSEC, CompTIA CySA+, CISM, CRISC, or CISA are an added advantage.
- Certification in any of the Risk frameworks like ISO 31000, ISO 22317, ISO 37301, ISO 27001, ISO 22301 is an added advantage.

B. EXPERIENCE

8 years working experience 2 of which at middle management level in Risk Management, Information Technology, Information Security Risk Management, IT Audit or related fields.
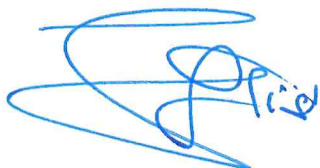
C. AGE

Applicants must have at least 1½ years left to retire.

D. COMPETENCIES

(i) Technical Competencies

- Understanding of information security principles, practices, and technologies.
- Knowledge of international information security standards such as ISO 27000 family of standards, ISO 22301, ISO 22317, PCI DSS, COBIT and NIST Cybersecurity Framework.
- Experience with information security management systems (ISMS) and governance frameworks.
- Familiarity with conducting Information Security risk assessments, vulnerability assessments, and penetration testing.
- Knowledge of security controls, cryptography, access control, and network security.
- Experience with incident response planning, detection, and mitigation techniques.
- Ability to evaluate and recommend security technologies and solutions.
- Familiarity with business continuity planning methodologies, frameworks, and tools.
- Familiarity with disaster recovery planning, data backup, and restoration procedures.
- Understanding of the Bank's operations, their interaction, processes, and systems.
- Analytical skills
- Report writing skills.

- Coordination and control
- Problem solving skills.
- Organizational skills

(ii) Behavioural Competencies
- Transparency and accountability
- Integrity
- Excellence
- Teamwork
- Analytical thinking and problem solving
- Interpersonal and stakeholder engagement
- Planning and organizing skills.
- Innovativeness
- Self-drive

11. PHYSICAL DEMANDS OF THE JOB:
N/A

12. WORKING CONDITIONS:
-

13. VERSION
1/2024

14. DATE LAST REVIEWED/ UPDATED
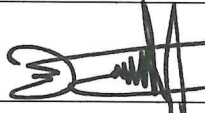August 2024

15. SIGNED OFF BY:

HEAD OF DEPARTMENT_____ DATE __17/9/2024__

HEAD OF DIRECTORATE_____ DATE __17/9/2024.__

16. APPROVING AUTHORITY: _____ DATE __20/9/24__