



37/45 KAMPALA ROAD, P.O. BOX 7120, KAMPALA; Telephone: 256-414-258441/6, 258061, 0312-392000, 0417-302000. Telex: 61069/61344; Fax: 256-414-233818 Web site: [www.bou.or.ug](http://www.bou.or.ug) E-mail address: [info@bou.or.ug](mailto:info@bou.or.ug)

## EMPLOYMENT OPPORTUNITIES

Applications are invited from suitably qualified Ugandans to fill the following positions in various Departments of Bank of Uganda;

**1. DEPARTMENT:** Commercial Bank Supervision Department  
**2. JOB REF:** CBS4.58

**3. JOB TITLE:** Examiner-IT and Cyber Security (CBs & NBFIs)

**4. RANK:** SBOII

**5. REPORTS TO:** Team Leader - Cyber Security Audits (CBs & NBFIs)

**6. SUPERVISES:** None

**7. JOB PURPOSE:**

To assess, monitor, and enforce compliance with IT governance, cybersecurity, and digital banking risk management standards in Commercial Banks and Non-Bank Financial Institutions. The role ensures that financial institutions maintain secure, resilient, and compliant technology environments to safeguard the stability of the financial system and protect customer data. This includes conducting regular inspections, identifying potential vulnerabilities, and recommending enhancements to mitigate IT and Cyber threats.

### 8. DUTIES AND RESPONSIBILITIES:

#### a) Examination and Assessment

- Conduct onsite and offsite IT and Cyber examinations of financial institutions.
- Evaluate IT governance structures, cybersecurity frameworks and resilience against operational disruptions.
- Review core banking systems, payment platforms and emerging digital banking channels.
- Assess the adequacy of IT General Controls (ITGCs), application controls, and disaster recovery/business continuity plans.

#### b) Risk & Compliance Review

- Evaluate banks' compliance with regulatory requirements, including BOU guidelines, Basel III operational risk standards and data protection regulations.
- Assess implementation of cybersecurity frameworks (ISO 27001, NIST CSF, CIS Controls).
- Identify and report deficiencies, systemic risks, and non-compliance issues.

#### c) Incident Response Oversight

- Regularly monitor banks' responses to major IT or cybersecurity incidents.
- Assess incident root cause analysis, remediation actions, and communication to stakeholders.
- Recommend improvements banks' incident detection and response capabilities.

#### d) Reporting & Enforcement

- Prepare clear and concise examination reports with findings, risks, and regulatory recommendations.
- Present examination outcomes at both EXCO and Board exit meetings.
- Recommend enforcement actions for non-compliance, including sanctions where necessary.

#### e) Policy Development & Advisory

- Contribute to the development and updating of IT and Cyber supervisory policies.
- Provide technical advisory to other examiners and bank supervision teams on IT risk trends.

#### f) Continuous Improvement & Training

- Stay updated on emerging threats, technologies and international best practices in banking cybersecurity.
- Carry out regular training of team members and participate/conduct annual training session to provide guidance to SFIs Board members and Executive management to improve their cybersecurity practices and compliance with regulations.
- Mentor other examiners and deliver training to enhance examination capabilities.

#### g) Stakeholder collaboration

- Work closely with SFIs, other regulatory bodies and cybersecurity experts to enhance the overall cybersecurity framework.

### 9. EXPECTED OUTPUTS/ DELIVERABLES

- IT and Cybersecurity institutional and sector wide risk profile
- IT and Cyber Security inspection Reports
- Proposed Cyber and Technology

guidelines.

- Incident reports and remediation actions.
- Draft collaboration reports, which document collaboration with other regulatory authorities, stakeholder feedback reports and cybersecurity experts.
- Quarterly and Annual sector wide IT and cybersecurity report.

### 10. PERSON SPECIFICATION

#### A. Minimum Qualifications

- First Class or Second Class Upper Bachelor's degree in Information Technology, Computer Science, Information Systems, Cybersecurity, Computer Engineering or a closely related field.

- Possession of at least one of the certifications as: a Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), Offensive Security Certified Professional (OSCP), Certified in Risk and Information Systems Control (CRISC) with ISO 27001 Lead Auditor or CompTIA Security+ is mandatory.
- A master's degree in any of the aforementioned fields is an added advantage.

#### B. Experience

- Minimum 5 years of relevant work experience in IT audit, cybersecurity, or risk management, preferably in a Financial Institution or Audit Firm.
- Familiarity with national and international cybersecurity standards such as NIST, ISO 27001 among others.

#### C. Age

- 30.0 to 37.0 Years

#### D. Competencies

- Technical skills**
  - Excellent Report writing skills
  - In-depth knowledge of cyber security principles, threat landscape and best practices.
  - Strong understanding of the SFIs systems and the regulatory environment.
  - Proficiency in cybersecurity risk assessment and management.

#### Behavioural skills

- Integrity
- Transparency and accountability
- Excellence
- Teamwork
- Analytical thinking and problem solving
- Interpersonal and stakeholder engagement
- Planning and organizing skills
- Innovativeness

### 11. PHYSICAL DEMANDS OF THE JOB:

- The job requires long hours of various system performance reviews and assessment to determine vulnerabilities.
- The job requires assessment of both CBs and NBFIs which is physically exhausting.

**1. DEPARTMENT:** Internal Audit

**2. JOB REF:** IA4.02

**3. JOB TITLE:** Officer, Operations Audit - Team 2 (2 positions)

**4. RANK:** SBOII

**5. REPORTS TO:** Team Leader, Operations Audit - Team 2

**6. SUPERVISES:** None

### 7. PURPOSE

To conduct audit and investigation assignments across Bank operations by assessing governance, risk management, and internal control systems to ensure compliance, operational efficiency, and value-for-money in accordance with the Internal Audit Charter.

### 8. DUTIES AND RESPONSIBILITIES

- Identify, assess and document risks and controls in the Auditable areas assigned
- Perform and document process walkthroughs and draft audit procedures in assigned auditable areas.
- Develop draft audit work programs in the assigned areas.
- Perform and document audit tests of the assigned auditable areas in line with the Bank's Internal Audit methodology.
- Review the economy, efficiency, and effectiveness to ascertain value for money in the deployment of Bank resources and provide advisory on assigned areas.
- Obtain sufficient and appropriate audit evidence addressing the

relevant audit objectives

- Document the results of the audit work in line with internal audit methodology.
- Prepare draft audit reports for the assigned audits.
- Conduct the follow-up of previous audit recommendations to ascertain the extent of implementation.
- Take part in Audit spot checks for cash holding areas.
  - Perform any other duties as may be assigned by audit management.

### 9. EXPECTED OUTPUTS

- Audit programs /Investigation plans.
- Process documentation.
- Tested systems and controls.
- Audit work papers.
- Draft audit reports.

### 10. PERSON SPECIFICATIONS

#### A. Qualifications

- A First Class or Second-Class Upper Bachelor's degree in Accounting, Finance, Commerce, Business Administration, Economics, Statistics, Financial Management.
- Full Professional qualification in any of the following: CPA, ACCA, CIA, CISA, CFE, and FCPA.
- A master's degree in the related fields is an added advantage.

- Membership of the Institute of Internal Auditors (IIA) is an added advantage.

#### B. Experience

- A minimum of at least five (5) years of relevant post qualification working experience in accounting / auditing with a reputable organization.

#### C. Age

- 30.0 to 37.0 years.

#### D. Competencies

- Technical Competencies**
  - Working knowledge of audit standards and frameworks, regulations and best practice in auditing and accounting
  - Planning and organizational skills
  - Analytical and problem-solving skills
  - Strong report writing and presentation skills
- Behavioural Competencies**
  - Integrity
  - Independent and objective
  - Team player
  - Good communication and interpersonal skills.
  - Leadership skills
  - Emotional intelligence

**1. DEPARTMENT:** Internal Audit

**2. JOB REF:** IA4.05

**3. JOB TITLE:** Officer, Information Systems Audit (3 Positions)

**4. RANK:** SBOII

**5. REPORTS TO:** Team Leader, Information Systems Audit

**6. SUPERVISES:** None

### 7. PURPOSE

To conduct audits and investigations across the Bank's IT environment by evaluating the effectiveness of information systems, infrastructure, and related processes, with the aim of assessing internal controls, identifying vulnerabilities, and ensuring robust IT governance, security, and compliance with regulatory and Bank policies.

### 8. DUTIES AND RESPONSIBILITIES

- Identify, assess and document risks and controls in the I.T Auditable areas assigned.
- Perform and document process walkthroughs and draft audit procedures in assigned I.T auditable areas.
- Develop draft audit work programs in the assigned areas.
- Perform audit tests of the assigned auditable areas in line with the Bank's Internal Audit methodology.
- Review the economy, efficiency, and effectiveness to ascertain value for money in the deployment of Bank resources and provide advisory on assigned areas.
- Obtain sufficient and appropriate audit evidence addressing the relevant audit objectives.
- Document the results of the audit work in line with internal audit methodology.
- Prepare draft audit reports for the assigned audits.
- Conduct the follow-up of previous audit recommendations to ascertain the extent of implementation.
- Take part in Audit spot checks for cash holding areas.

- Conduct training, mentoring, monitoring, and evaluation of performance for BOU/IL.
- Maintain the IT Audit Lab equipment and the wireless network, Design tests for continuous control monitoring on ACL Robotics.
- Perform any other duties as may be assigned by audit management.

### 9. EXPECTED OUTPUTS

- Audit programs /Investigation plans.
- Process documentation
- Tested systems and controls.
- Audit work papers.
- Draft audit reports.
- Continuous monitoring reports from systems

### 10. PERSON SPECIFICATIONS

#### A. Qualifications

- A First Class or Second-Class Upper Bachelor's degree in Computer Science, Information Technology, Information Systems, or Cybersecurity from a recognized institution.

- Must possess any of the following professional qualifications: CISA, COBIT, CPDSE, CISM, CEH, CHFI, ISO27001.

- A master's degree in any of the aforementioned fields is an added advantage.

- Membership of the Information Systems Audit and Control Association (ISACA) and/or Institute of Internal Auditors (IIA) is an added advantage.

#### B. Experience

- A minimum of at least Five (5) years of relevant working experience in IT Audit and/or IT security related field.

#### C. Age

- 30.0 to 37.0 years.

#### D. Competencies

- Technical Competencies**
  - Working knowledge of I.T industry frameworks, regulations and best practice.
  - Ability to use Computer Aided Audit techniques (CAATs) e.g., ACL and Teammate.
  - Planning and organizational skills.
  - Analytical and problem-solving skills.
  - Strong report writing and presentation skills.
  - Proficiency in developing scripts using SQL.
  - Ability to supervise others.
- Behavioural Competencies**
  - Integrity.
  - Independent and objective.
  - Team player.
  - Good communication and interpersonal skills.
  - Leadership skills.
  - Emotional intelligence.

**1. DEPARTMENT:** Internal Audit

**2. JOB REF:** IA4.06

**3. JOB TITLE:** Officer, Information Systems Audit (1 Position)

**4. RANK:** BOII

**5. REPORTS TO:** Team Leader, Information Systems Audit

**6. SUPERVISES:** None

### 7. PURPOSE:

To support the execution of IT audit assignments by assisting in the review of systems, processes, and controls, gathering audit evidence, performing preliminary risk assessments, and documenting findings to help ensure the effectiveness, security, and compliance of the Bank's information systems and operations.

### 8. DUTIES AND RESPONSIBILITIES

- Assist in identifying and documenting IT-related risks and controls in assigned audit areas under the guidance of senior audit staff.
- Support the execution of process walkthroughs and contribute to the preparation of audit procedures.
- Provide input into the development of audit work programs and testing plans.
- Carry out assigned audit tests in accordance with internal audit methodology, focusing on the effectiveness and efficiency of IT systems and processes.
- Collect and compile relevant audit evidence to support findings and conclusions.
- Prepare and maintain well-organized audit working papers in line with audit standards.
- Contribute to the drafting of audit findings and reports for review by senior audit staff.

- Participate in follow-up activities to monitor the implementation status of prior audit recommendations.

- Take part in spot checks and verification exercises in cash-handling and other high-risk areas.
- Assist in maintaining IT Audit Lab equipment and support basic tasks related to the audit network and tools such as ACL Robotics.
- Perform any other duties as assigned by the Team Leader or senior audit staff.

### 9. EXPECTED OUTPUTS

- Audit programs /Investigation plans.
- Process documentation
- Tested systems and controls.
- Audit work papers.
- Draft audit reports.
- Continuous monitoring reports from systems

### 10. PERSON SPECIFICATIONS

#### A. Qualifications

- First Class or Second-Class Upper Bachelor's degree in Computer Science, Information Technology, Information Systems or Cybersecurity from a recognized institution.

- Membership of the Information Systems Audit and Control Association (ISACA) and/or Institute of Internal Auditors (IIA) is an added advantage.

#### B. Experience

No experience required

#### C. Age

- Applicants must not be above 26.0 years as at close of the advert.

#### D. Competencies

- Technical Competencies**
  - Working knowledge of I.T industry frameworks, regulations and best practice.
  - Planning and organizational skills.
  - Analytical and problem-solving skills.
  - Strong report writing and presentation skills.
- Behavioural Competencies**
  - Integrity.
  - Independent and objective.
  - Team player.
  - Good communication and interpersonal skills.
  - Leadership skills.
  - Emotional intelligence.

Salary and Benefits for the positions are generous and attractive.

- Applications should be submitted by filling out the online application link <https://forms.office.com/r/10yrMX8qKl>

- Please follow the stated instructions in the form as accurately as possible. Note that **inaccurate applications will be automatically disqualified.**

Applications should be accompanied by:

- 1) National ID (Front and Back) – Mandatory. Ensure both the front and back sides are scanned and visible.
- 2) Academic Qualification Documents – Mandatory. These should match all the required qualifications mentioned in the job descriptions.
- 3) Letter of Equivalence for the Class of Degree from the National Council of Higher Education for applicants whose first degree (Bachelor's) was obtained from a foreign University.
- 4) A duly registered Statutory Declaration for applicants with name and/or date of birth variations.

- Please ensure that all required documents are duly attached and **MUST be scanned as one single document.**

- Please note that **failure to attach the required documents** will lead to automatic disqualification.

Management reserves the right to terminate applicants found with concealed or falsified information and academic credentials. Only shortlisted candidates will be contacted.

Applications should reach NOT later than 5:00PM Wednesday 10 September 2025

MANAGEMENT  
27 AUGUST 2025