OUTSTANDING CAREER OPPORTUNITIES

(OPEN TO BOTH INTERNAL AND EXTERNAL CANDIDATES)

Pride Microfinance Limited (MDI) is a Microfinance Deposit- taking Institution regulated and supervised by Bank of Uganda (BoU) under the MDI Act, 2003 and MDI Regulations, 2004. Pride's purpose is to transform lives responsibly. Pride offers innovative financial solutions to largely people at the base of the economic pyramid and serves its customers through 42 networked branches and 5 contact offices. Pride is an equal opportunity employer looking for competent and experienced individuals to fill the following vacancies.

1. AUDITOR MANAGER - FINANCE

The **Auditor Manager – Finance** will report to the Head of Internal Audit and will be based at Head Office. He/ she will be responsible for planning, reviewing and co-ordinating Audit assignments, reviewing and certification of BOU periodic returns (weekly and monthly returns), scrutinising and evaluating financial data to authenticate and validate accuracy and ensure generally accepted Accounting and Auditing Standards are followed, prepare audit reports, identify emerging risks and develop a professional and competent audit team in line with Audit manual, international audit standards, regulatory requirements, Pride policies and Business Plan.

Specific responsibilities include: -

1. Plan and implement audit resource allocation in line with the annual internal audit work plan
2. Review audit plans and field work to guarantee they are risk based and comply with Pride's internal audit manual and policies.
3. Continuously improve and update the audit manual and audit methodologies to enhance efficiency of audit operations.
4. Actively participate in the formulation of Pride's annual internal audit work plan and preparation of the departmental budget.
5. Manage or perform financial analysis and identify emerging risks in line with Pride's policies and regulatory requirements.
6. Supervise the review of weekly, monthly and quarterly returns to Bank of Uganda as per the regulatory requirement and Pride policies and procedures.
7. Prepare audit engagement plans, supervise, and monitor progress of audit assignments for all Pride departments and branches in line with set standards.
8. Ensure all audit projects and populated in teammate and followed up for timely closure.
9. Supervise audit staff and review draft reports from supervisees in charge of assignments.
10. Organizing and distributing resources and manpower in harmony with abilities and schedules. .
11. Draft audit methodology improvement papers to train staff and confirm compliance with IIA standards & BOU regulations/Acts
12. Prepare Board reports for review by head of Department before submission to the Board in line with set standard.
13. Ascertain financial and other business process threats
14. Developing Professional development procedures for the low-ranking staff within the department.
15. Confirm that all assignments are done in compliance to global international auditing standards.
16. Manage staff performance, discipline, mentoring and development in line with the policy and audit training needs

Minimum academic qualifications, Experience & competences

- A Bachelor's degree in accounting / finance/ Statistics/ Economics
- Professional qualification in ACCA / CPA/CIA
- Membership to ICPAU is a MUST
- The desired candidate should have atleast 6 years audit experience of which 3 years should be at supervisory level in a regulated financial institution or recognized Auditing firm.
- **He/she should not be more than 40 years of age**.

2. SENIOR INTERNAL AUDITOR - IT

The Senior Internal Auditor – IT report to the Audit Manager – IT and will be based at Head Office. He/ she will be responsible for conducting IT risk-based internal audits to provide assurance on the governance, risk management, and control of the Pride's Information Systems and Infrastructure to ensure the confidentiality, integrity, and availability of information systems, safeguarding the Pride's critical assets and operations in compliance with the regulatory frameworks and Internal policies and procedures.

Specific responsibilities include: -

1. Identify business objectives, assess the inherent risks in activities to be audited and develop comprehensive audit plans for assigned audit engagements.
2. Review IT controls within technical environments, evaluating risk-based controls across key IT functions such as networks, firewalls, vulnerability management, systems development, information security, database management, and project management to identify and evaluate fraud and emerging risks in the IT control environment.
3. Lead in analysis of IT control environment and identify any IT deficiencies and come up with actionable/corrective recommendations for securing or enhancing Pride's IT business environment.
4. Review of various IT special projects and corporate IT initiatives and advise on any areas of improvement noted.
5. Complete all IT or any other audit assignments within the agreed timeframe and budget.
6. Build and maintain relationships and effectively communicate, as key audit partner, with all levels of management, other members of the Internal Audit Team and external reviewers.
7. Perform field work and prepare quality working papers in compliance with audit standards and policy.
8. Provide input in developing appropriate audit tests aimed at addressing identified IT risks and achieving the desired audit objectives to provide assurance that IT risks are effectively managed or mitigated.
9. Conduct all assigned IT audits end-to-end; including planning, evaluating and documenting the results, reporting and following up in accordance with the annual audit plan and Audit Standards.
10. Prepare clear and concise IT audit reports on audit findings, detected non-compliance with Pride policies, guidelines, statutory requirements and procedures for discussion with the line manager, before final reports are issued to Management for corrective action.
11. Providing input to the annual IT audit plan/strategy to be included in the overall departmental Risk Based Annual Audit Plan.
12. Provide first level assurance services on all key levels of system development life cycle and acquisition process on all Information Technology System and modules being integrated into Pride's IT environment.
13. Conduct data extraction and analysis using software tools on the Pride's system databases.

Minimum academic qualifications, Experience & competences

- Bachelor's degree in information system/accounting/ finance/ Statistics/ Economics or related subjects.
- Professional qualification in CISA/CISM/CRISC/CIA will be an added advantage.
- The desired candidate should have at least 3 years of working knowledge of technology (Infrastructure, networks, databases, internal/external IT threats, application controls etc) or related experience in performing general IT operations for a reputable institution
- **He/she should not be more than 35 years of age**.

3. SENIOR ICT RISK ANALYST

The Senior Risk Analyst will report to the Head of Risk and will be based at Head Office. He/ she will be responsible for the evaluation of complex risks to Pride's information systems, define appropriate security behaviors and practices and monitor adherences to the set standards to meet Management expectations and to adhere to regulatory, legal and partner requirements.

Specific responsibilities include: -

1. Create and manage an Institution wide map (cartography) of the storage areas and flows of sensitive data in view of appropriately securing them in line with relevant policies.
2. Create the appropriate security framework around every business project to ensure the appropriate and successful implementation of business initiatives and to reduce risk exposure based on risk appetite.
3. Identify and evaluate threats to the Institution's information assets and their mitigating controls while considering the current risk appetites to reduce the impact and probability of occurrences of threats applicable to the organization at an acceptable level.
4. Implement and execute an awareness program that considers all requirements, expectations and prevailing threats to ensure that all system users are aware of appropriate security behaviors.
5. Manage, test, improve and maintain an incident response plan for each relevant security event and coordinate the appropriate response in the event of an incident to enhance the Institution's ability to recover from these events, should they occur.
6. Perform the analysis of all security issues, reported, discovered or otherwise to define and incorporate lessons learnt to enhance the Business Units capabilities to proactively protect the information assets of the organization.
7. Perform the analysis of all security issues, reported, discovered or otherwise to define and incorporate lessons learnt to enhance the Business Units capabilities to proactively protect the information assets of the organization.
8. Propose mitigating solutions, follow-up on remediation plans and regularly report on the Institution's risk stance and progress made to reduce the risks levels to an acceptable threshold.
9. Provide advices and follow up on the implementation of associated security control through participating in the implementation of business projects and initiatives to reduce risk exposure of customers' information based on the risk appetite.
10. Support the institution in identifying security flaws by conducting authorized, controlled "attacks" on the IT environment in addition to coming up with recommendations for fixing these vulnerabilities before malicious actors can exploit them.
11. Assist in conducting effective risk assessments to assess all new IT systems or Processes, clearly identifying the risks and issues and the controls and measures required to mitigate those risks / issues
12. Conduct IT Security Controls Snap checks (CSA) and monitor IT Security activities e.g. application & system controls, physical and logical access security controls, review of disaster recovery and back-up procedures, media storage.
13. Follow-up on any IT Security gaps identified and put in place effective measures to safeguard the Institution's IT resources, information and reputation.
14. Monitor, update and maintain all the systems and related initiatives/activities which include the Enterprise Risk Management MIS, performing User Administration for key information security tools/ systems within the department and implementing system changes in the department where applicable as may be authorized by Business Technology

Minimum academic qualifications, Experience & competences

- A bachelor's degree in information technology/ computer science/ computer engineering or related field.
- The desired candidate should have atleast 4 years' experience in IT with at least 2 years in ICT Security Risk Management.
- Professional Qualification in Enterprise Risk Management, ISO Standards, CISA will be an added advantage.
- He/she should not be more than 35 years of age.

4. OPERATIONAL RISK ANALYST.

The Operational Risk Analyst will report to the Operational Risk Manager and will be based at Head Office. He/she will be responsible for supporting, designing, implementing and managing the Operational Risk Framework within the different units in Pride to support a common set of control standards and reporting structures, build accountability and responsibility in line with the Operational Risk Policy and regulatory requirements.

Specific responsibilities include: -

1. Support in the development and implementation of the operational risk management and incident reporting frameworks within Pride, as per approved Policy and regulatory requirement, and contribute to the identification, assessment, monitoring and controlling of operational risk.
2. Build Operational Risk Cartographies and ensure that the same are owned by the 1st line of defense to promote a risk culture within Pride.
3. Facilitate risk workshops for the 1st line of defense to draw and maintain the operational risk cartographies.
4. Gather, Identify and review relevant operational risk data to be shared with other functions to facilitate the monitoring of operational risk within Pride.
5. Oversee and coordinate the activities of risk champions across the Pride network.
6. Support in the implementation of Business continuity plans and ensure that the same are owned by the business and coordinate Business Continuity Management awareness training.
7. Coordination of the Risk control self-assessment (RCSA), related key risk indicators (KRI) and monitoring plans for operational risk management.
8. Attend to incidents timely as per approved Policy, and in adherence to regulatory requirements to contribute to the identification, assessment, monitoring and controlling of operational risk.

Minimum academic qualifications, Experience & competences

- A bachelor's degree in commerce, Business Administration, Statistics, Economics, Computer Science, IT or any related field.
- The candidate should possess at least 4 years' experience in either Banking Operations, Risk Management, Audit, internal controls or in a similar environment
- She / he must not be more than 35 years.

To Apply:

If you believe you have the necessary skills and experience and desire to make a difference, apply immediately and send a detailed CV to HEAD PEOPLE & CULTURE, using either the address below; emailing to: recruitment@pridemicrofinance.co.ug or using the link, https://www.pridemicrofinance.co.ug/career.html not later than Friday November 1st , 2024.

ONLY SHORTLISTED CANDIDATES WILL BE CONTACTED

PRIDE MICROFINANCE LIMITED (MDI),
Victoria Office Park, Block B, Bukoto,
Plot 6-9, Ben Kiwanuka Okot Close,
P. O. Box 7566, Kampala. Tel. No. 0312-262366;
Web. www.pridemicrofinance.co.ug.