

Investigation Officer Job Description

Job Title:	Investigation Officer	Reports to:	Head of Security& Investigations, Kenya
Unit:	Security & Investigations	Department:	Technology & Operations
Grade:	Band 5	Date:	18 th February 2026
Job holder:	Vacant	Supervisor:	Head of Security and Investigations, Kenya
Signature:		Signature:	

Job Purpose Statement
<p>The incumbent is responsible for planning, organizing, coordinating, and managing investigations into cases of; alleged misconduct, fraud, cybercrime, and violations of the Bank's internal policies and ensuring adherence to best investigative practices and governance standards. The main tasks entail: -</p> <ul style="list-style-type: none"> a) Handling internal investigations of all reported or suspected fraud incidents, cybercrime, misconduct, and policy/procedure breaches and timely issuance of reports for management use either or internal or external actions to address root causes, enhance controls, and support potential litigation. b) Liaising and collaborating with law enforcement agencies, as well as professional and commercial organizations in this area of expertise. c) To collect, preserve, and analyze relevant financial and digital evidence for internal investigations and regulatory or legal reporting, and to support employee awareness of the Bank's anti-fraud, cybersecurity, and compliance policies d) Develop initiatives to prevent, detect, investigate and respond to fraud related incidences within the Bank.

Key Accountabilities (Duties and Responsibilities)		
Perspective	% Weighting	Output
Conducting Investigations	55%	<ul style="list-style-type: none"> a) Conduct end-to-end investigations, ensuring compliance with established investigative and operational protocols for all types of cases, with detailed planning for high-priority or complex investigations. b) Collect, preserve, and analyze all relevant financial, digital, and documentary evidence; derive meaningful insights and provide actionable recommendations based on investigative findings. c) Conduct interviews with witnesses, suspects, and victims, obtaining written statements where necessary to support the investigation. d) Prepare comprehensive investigation reports in line with prescribed methodologies, accurately documenting all findings and conclusions. e) Ensure that each investigation culminates in a precise, value-adding conclusion appropriate to the nature of the case. f) Recommend corrective actions to address system, process, or personnel vulnerabilities, as well as internal

		<p>and external threats, supporting risk mitigation and regulatory compliance.</p> <ul style="list-style-type: none"> g) Make meaningful recommendations to the mandated officials regarding the raising of loss provisions, refunds to clients, repudiations, recovery actions, and write-offs. h) Assist line management/HR with relevant findings/documentation for use in disciplinary processes. i) Ensure that each investigation is concluded within the prescribed and acceptable time limit for the particular type of investigation. j) Inform management of any suggestions or proposals to enhance investigative methodology/operating procedures. k) Represent the Bank in any criminal or civil court proceedings where the Bank is summoned to enter appearance. l) Collect timely intelligence to avert fraud and security incidents.
Case Management	15%	<ul style="list-style-type: none"> a) Maintain case files and the central investigations database (MIs) in accordance with operational standards. b) Attend progress meetings with investigation teams and management to provide updates and insights. c) Continuously develop professional skills through training programs and practical work experience. d) Contribute to the preparation of weekly, monthly, and ad hoc Management Information (MI) reports, as required. e) Ensure that all information in the SID MIs relating to forensic Investigations and Recoveries is accurate, reliable, and verifiable. f) Prepare and submit whistle-blowing reports to the Head of Security and Investigations in a timely manner. g) Collaborate with HR and Risk Management teams to support fraud awareness, training initiatives, and sensitization campaigns. h) Assist with the pre-employment screening process for new employees, ensuring compliance with internal policies.
Risk Identification and Awareness	15%	<ul style="list-style-type: none"> a) Ensure that all risks and/or emerging risks, which are identified during an investigation / interaction with stakeholders, are escalated to line management upon discovery. b) Identify high-risk business units and where requested to do so, participate in awareness initiatives.
Stakeholder Management	15%	<ul style="list-style-type: none"> a) Develop and maintain relationships with internal and external stakeholders to build synergies and teamwork. b) Actively interact with counterparts in the industry to gain understanding of threats and risks and to share important information on current frauds and fraudsters involved. c) Any other duty as may be assigned Head of security & Investigations.

Job Dimensions

Reporting Relationships: jobs that report to this position directly and indirectly	
Direct Reports	None
Indirect Reports	Business Units, Departments, Branches and Services Centres

Stakeholder Management: key stakeholders that the position holder will need to liaise/work with to be successful in this role.	
Internal; All departments, Branches and Services Centres.	External: Government Investigative arms, CBK and CMA inspectors and external Auditors

Ideal Job Specifications
<p>a) Academic Qualifications: Bachelor's degree in IT, Law, Business Administration, Finance, Economics, Criminology, or other related disciplines. Cybersecurity skills are an added advantage.</p> <p>b) Professional Qualifications: Possession of a recognized professional certification in a relevant field, such as CFE, ASIS (Certified Fraud Examiner).</p> <p>c) Work Experience: Minimum of 4 years of professional experience in investigative procedures and practices, particularly within DCI or banking environments as an Investigator.</p> <p>d) Desirable Experience: Experience as a Cybercrime Investigator or demonstrated expertise in cyber-related investigations is highly desirable.</p> <p>e) Technical Expertise: Strong knowledge of investigative techniques, especially in cases involving criminal conduct that may lead to prosecution in local courts.</p> <p>f) Computer proficiency; demonstrable proficiency in the use of computers and common business applications including word processing, spreadsheets, presentations, email, and internet-based systems and other Microsoft productivity tools.</p>

NCBA Bank Core Value Behaviours (Performance Drivers)
Driven Open Responsive Trusted

Ideal Job competencies

Technical Competencies	
Understanding of Criminal Law	Good understanding of Penal code and Criminal Procedure Code.
Report writing	Ability to reduce complex investigations into a clear and concise investigations report.
Interviewing Skills	Ability to interview witnesses and extract info valuable to the ongoing investigations.
Communication Skills	Should have good oratory and written skills