



Wakulima House,
KPCU Building 2nd Floor
Along Haile Selassie Ave
P. O. Box 36886 – 00200,
Nairobi, Kenya
Tel: 0733-222 223

Email: nce@nairobicoffeexchange.co.ke

REQUEST FOR PROPOSAL

Provision of Independent Vulnerability Assessment and Penetration Testing Services for a Digital Platform

Procurement Item	Details
RFP Reference	NCE/CEO/RFP/2026-2027/001
Issue Date	12TH OCTOBER 2026
Clarification Deadline	21ST OCTOBER 2026, 5:00PM EAT
Proposal Submission Deadline	29TH OCTOBER 2026, 05:00PM, EAT
Submission Method	Electronic submission to CEO@NCE.CO.KE
Procuring Entity	Nairobi Coffee Exchange

Bidder Notice

Nairobi Coffee Exchange (NCE) invites qualified and independent cybersecurity firms to submit technical and financial proposals for an authorized Vulnerability Assessment and Penetration Testing (VAPT) engagement covering its digital platform and approved supporting components.

**KENYAN
CONTEXT**

The assignment will support secure digital service delivery within Kenya's coffee market ecosystem. Testing must be lawful, expressly authorized, non-disruptive, evidence-based, and respectful of personal, commercial, settlement, and market-sensitive information.

Procurement Data Sheet

Item	Requirement
Procuring entity	Nairobi Coffee Exchange
Assignment	Independent Vulnerability Assessment and Penetration Testing Services
Contract type	Professional services, fixed-price or deliverable-based contract
Language	English
Currency	Kenya Shillings (KES), inclusive of all applicable taxes
Proposal validity	Ninety (90) calendar days from the submission deadline
Bid security	Not required, unless introduced through an addendum
Clarifications	Clarification requests shall be submitted only to ceo@nce.co.ke by 21st October 2026 at 5:00 p.m. EAT.
Submission	Separate technical and financial proposals, clearly labelled
Expected commencement	2nd November 2026
Primary contact	Chief Executive Officer, Nairobi Coffee Exchange

Table of Contents

1. Background and Context
2. Purpose and Objectives
3. Scope of Work
4. Testing Standards and Rules of Engagement
5. Deliverables and Acceptance Criteria
6. Assignment Management and Indicative Schedule
7. Bidder Eligibility and Qualification
8. Proposal Preparation and Submission
9. Evaluation, Scoring and Award Methodology
10. Contractual, Confidentiality and Data Protection Requirements
11. General Conditions
12. Forms and Schedules
- Appendix A: Indicative Asset and Test-Scope Register
- Appendix B: Bidder Response Checklist

1. Background and Context

NCE is advancing a connected digital ecosystem that supports stakeholder onboarding, role-based access, coffee traceability, operational workflows, auction-related information exchange, integrations, and settlement-related processes. The environment includes stakeholder-facing applications, APIs, cloud infrastructure, identity and access controls, audit trails, and interfaces with authorised third parties.

The engagement is intended to provide independent assurance before production use and enhancement. It also responds to NCE's governance requirement for an external ethical-hacking assessment ahead of broader regulatory and information-security reviews.

1.1 Legal and Governance Framework

The successful bidder shall perform the assignment in compliance with the contract, written authorisation, approved rules of engagement, and all applicable Kenyan laws and regulatory requirements. Relevant considerations include:

- The Data Protection Act, 2019 and applicable regulations, including privacy, security safeguards, breach handling, and lawful processing obligations.
- The Computer Misuse and Cybercrimes Act, Cap. 79C, with testing undertaken only under express written authority and within the approved scope.
- The Capital Markets Act and applicable Capital Markets (Coffee Exchange) Regulations and directives.
- The Crops (Coffee) (General) Regulations, 2019 and applicable coffee-sector requirements.
- NCE policies, trading rules, information security procedures, access control requirements, and contractual obligations.
- Any regulator, cloud-provider, banking, integration-partner, or third-party conditions that NCE identifies before testing.

LEGAL REVIEW

This RFP is a procurement and technical document. NCE should subject the final publication copy and resulting contract to internal procurement, legal, compliance, finance, and management approval.

2. Purpose and Objectives

The purpose is to appoint an independent provider to identify, verify, rate, and clearly communicate security weaknesses, while enabling NCE to remediate verified risks without unnecessary service disruption.

- Establish a defensible view of the platform's current external and internal attack surface.
- Assess whether authentication, authorization, tenant or organization isolation, maker-checker controls, role-based permissions, and session controls operate as intended.
- Test web applications, APIs, integrations, cloud configurations, and approved infrastructure components.
- Identify exploitable vulnerabilities, insecure configurations, business-logic weaknesses, and control gaps.
- Provide prioritized remediation actions that are practical for NCE's technical team and service providers.
- Validate closure of critical and high-risk findings through an independent retest.
- Produce executive and technical evidence suitable for governance, audit, regulatory engagement, and secure production-readiness decisions.

3. Scope of Work

3.1 In-Scope Security Assessment Domains

Domain	Minimum Coverage
Web applications	Authentication, session management, input handling, file upload or download, access control, error handling, security headers, sensitive data exposure, and OWASP-aligned testing.
APIs and integrations	Authentication and authorisation, object-level access, rate limiting, replay, injection, mass assignment, schema validation, logging, secrets, transport security, and business-flow abuse.
Identity and access	Password and MFA controls where enabled, account lifecycle, privilege escalation, role segregation, maker-checker approval, inactive accounts, and administrative access.
Business logic	Workflow bypass, prerequisite enforcement, record ownership, organization-level data isolation, duplicate or altered transactions, approval circumvention, and unauthorised state changes.
Cloud and hosting	Approved configuration review of internet-facing services, network exposure, storage permissions, encryption, secrets, monitoring, logging, backup access, and platform configuration.

Domain	Minimum Coverage
Mobile or responsive services	API and session controls used by mobile clients, storage of sensitive information, transport security, deep links, and application package review where expressly included.
Third-party interfaces	Only interfaces and endpoints for which NCE has authority and written permission. No testing of a third party's systems without its prior written approval.
Social engineering / physical testing	Excluded unless separately approved in writing through an addendum and supported by a specific scenario, target group, safeguards, and reporting protocol.

3.2 Minimum Technical Activities

- Kick-off, document review, threat modelling, attack-surface mapping, and confirmation of the authorised target register.
- Automated scanning supported by manual verification. Tool output alone will not be accepted as a completed penetration test.
- Authenticated and unauthenticated testing using approved test accounts and roles.
- Manual exploitation sufficient to validate impact, without unnecessary persistence, destructive actions, or data extraction.
- Business-logic and cross-role testing across representative stakeholder workflows.
- Configuration and exposure review for approved cloud, DNS, TLS, network, storage, and application components.
- Validation of logging, monitoring, alerting, lockout, rate-limiting, and incident-escalation controls where testable.
- Daily or immediate communication of critical findings, followed by formal evidence and remediation guidance.
- Retest of agreed critical and high-risk findings after NCE confirms remediation readiness.

3.3 Exclusions Unless Specifically Authorised

- Denial-of-service, distributed denial-of-service, stress testing, or uncontrolled high-volume traffic.
- Destructive deletion, corruption, encryption, alteration, or exfiltration of production data.
- Installation of persistent agents, backdoors, malware, ransomware simulators, or command-and-control infrastructure.
- Testing against systems, IP addresses, tenants, cloud subscriptions, banks, regulators, vendors, or partners not listed in the signed scope.
- Unannounced social engineering, phishing, physical intrusion, wireless testing, or employee surveillance.
- Access to live personal or commercially sensitive records beyond the minimum evidence needed to verify a finding.

4. Testing Standards and Rules of Engagement

4.1 Recognized Practices

The bidder shall propose a risk-based methodology aligned to recognized practices such as the OWASP Web Security Testing Guide, OWASP Application Security Verification Standard, OWASP API Security Top 10, NIST guidance, PTES, CVSS, and relevant cloud security benchmarks. Equivalent or improved approaches may be proposed and must be clearly explained.

4.2 Mandatory Rules of Engagement

Control	Requirement
Written authorisation	No testing may begin before the contract, NDA, target register, testing window, emergency contacts, and Rules of Engagement are signed.
Testing window	Testing shall occur only within approved dates and time windows in East Africa Time (EAT), unless NCE provides written approval.
Safety	Use non-destructive techniques and the least intrusive proof necessary. Stop immediately where availability, integrity, confidentiality, or stakeholder operations may be affected.
Critical finding escalation	Notify NCE's authorised contacts immediately through the agreed secure channel. Do not wait for the draft report.
Evidence handling	Minimise evidence, mask personal and confidential data, encrypt all working files, maintain chain of custody, and restrict access to named personnel.
Communications	Maintain a test log and regular status updates. Any scope change requires written approval.
Clean-up	Remove test accounts, tokens, files, payloads, scripts, and other artefacts at the end of testing, then certify clean-up.
Responsible disclosure	Findings are confidential to NCE. No public disclosure, conference presentation, portfolio use, or client naming without written approval.

4.3 Severity Rating

Findings shall be rated using CVSS or an equivalent recognized method, then adjusted through clear professional judgement for NCE's business context, exploitability, data sensitivity, market impact, settlement exposure, service availability, regulatory impact, and control dependencies.

Rating	Expected Treatment
Critical	Immediate secure notification and urgent remediation planning. Evidence must be concise and access strictly limited.
High	Prompt notification and prioritized remediation before production approval or within the agreed risk-treatment period.
Medium	Planned remediation with ownership and due date, supported by compensating controls where appropriate.
Low / Informational	Tracked improvement, hardening, or hygiene action with documented rationale.

5. Deliverables and Acceptance Criteria

Deliverable	Minimum Content	Acceptance Basis
1. Inception report	Confirmed scope, assumptions, methodology, team, schedule, dependencies, communication plan, and draft Rules of Engagement.	Approved in writing before active testing.
2. Test plan and target register	Domains, URLs, APIs, IPs, environments, roles, accounts, exclusions, test windows, and emergency contacts.	Signed by NCE and provider.
3. Critical finding notices	Finding, affected asset, verified impact, concise evidence, immediate containment, and recommended action.	Securely communicated within the agreed escalation window.
4. Draft VAPT report	Executive summary, scope, method, limitations, findings, evidence, risk rating, impact, root cause, and remediation.	Complete, reproducible, quality-reviewed, and discussed with NCE.

Deliverable	Minimum Content	Acceptance Basis
5. Vulnerability register	Unique ID, asset, category, severity, CVSS, status, owner, recommendation, target date, and retest result.	Editable format suitable for tracking.
6. Management briefing	Key exposures, business implications, remediation priorities, residual risks, and production-readiness considerations.	Presented to authorised NCE representatives.
7. Retest report	Original finding, remediation evidence, retest method, status: closed, partially closed, open, or risk accepted.	Covers agreed on critical and high-risk items.
8. Final report and clean-up certificate	Resolved clarifications, final findings, residual risk, retest outcome, limitations, and confirmation of evidence retention or deletion.	Formally accepted by NCE.

5.1 Report Quality Requirements

- Executive content must be clear to management and governance committees without overstating risk.
- Technical findings must be reproducible, include affected components and evidence, and avoid exposing unnecessary secrets or personal data.
- Each finding must state the condition, risk, impact, evidence, recommendation, and validation status.
- Duplicate scanner findings must be consolidated. False positives must be removed before submission.
- Reports shall be delivered in searchable PDF and editable formats, with the register in Excel-compatible format.
- All reports and evidence must be securely transmitted and remain NCE confidential information.

6. Assignment Management and Indicative Schedule

Phase	Activity	Indicative Timing
1	Contracting, NDA, kick-off, document request	Day 1
2	Scope validation, threat model, target register, Rules of Engagement	Days 1-2
3	Active vulnerability assessment and penetration testing	Days 3-8
4	Analysis, quality review, draft reporting	Days 9-11
5	Technical validation workshop and management briefing	Day 12
6	Final report	Within 2 working days after consolidated comments
7	Retest	Within the agreed window after NCE confirms remediation readiness

Bidders may propose a different schedule where justified by scope and safety. The final timetable will be agreed during contracting and must account for NCE operating windows, stakeholder activity, change controls, and third-party permissions.

7. Bidder Eligibility and Qualification

7.1 Mandatory Requirements

Requirement	Evidence
Legal registration	Certificate of incorporation or business registration and current company profile.
Tax compliance	Valid Kenya Revenue Authority Tax Compliance Certificate or applicable equivalent.
Authority to operate	Relevant permits, registrations, or professional authorisations required for the services.
Lead tester qualification	Valid CEH, OSCP, CREST, GPEN, or equivalent hands-on offensive-security credential. CEH alone should be supported by demonstrable practical experience.
Relevant experience	At least three comparable assignments within the most recent five years, with references or acceptable completion evidence.
Team competence	CVs, roles, certifications, and availability of proposed personnel.
Independence	Signed conflict-of-interest and independence declaration.
Confidentiality and privacy	Signed commitment to NDA, data minimization, secure evidence handling, and deletion or return

Requirement	Evidence
	of information.
Professional standing	Disclosure of material litigation, sanctions, debarment, or professional disciplinary matters.
Insurance	Evidence of professional indemnity and cyber liability cover, or a commitment to obtain the required cover before contract signature.

7.2 Desirable Qualifications

- Recognized application, cloud, infrastructure, audit, or information security certifications such as OSWE, OSEP, CISSP, CISM, CCSP, ISO/IEC 27001 Lead Auditor, or comparable credentials.
- Experience in regulated, financial, commodity market, payment, settlement, exchange, or critical digital-service environments.
- Experience testing multi-tenant platforms, complex role matrices, APIs, cloud environments, and integrations.
- Capacity to explain technical risks to management and collaborate with developers on remediation.

8. Proposal Preparation and Submission

8.1 Technical Proposal

1. Signed proposal submission letter using Form 1.
2. Bidder profile, legal status, ownership, office location, and primary contact.
3. Understanding of the assignment and key security risks.
4. Detailed methodology, coverage, proposed tools, manual-testing approach, and quality assurance.
5. Draft work plan, team mobilisation, dependencies, and timing.
6. Team structure, named personnel, CVs, certifications, responsibilities, and availability.
7. Relevant assignments and client references using Form 2.
8. Draft Rules of Engagement, escalation procedure, evidence-handling approach, and clean-up process.
9. Sample redacted executive and technical report, where legally permissible.
10. Signed declarations covering confidentiality, data protection, independence, conflict of interest, anti-bribery, and accuracy of information.

8.2 Financial Proposal

The financial proposal shall be submitted separately and state all prices in Kenya Shillings (KES). It must show professional fees, taxes, expenses, retest costs, optional services, assumptions, and the total evaluated price. Unstated costs may be treated as included in the total.

Cost Item	Amount (KES)	Taxes (KES)	Total (KES)
Inception and scope validation			
Vulnerability assessment and penetration testing			
Reporting and presentations			
Retest of agreed findings			
Other approved costs (specify)			
Grand Total			

8.3 Required Proposal Documents

Bidders shall submit a signed proposal submission letter together with the following documents:

- Company profile or consultant profile.
- Certificate of incorporation, business registration, or equivalent registration document.
- Valid tax compliance certificate or equivalent tax status confirmation.
- Evidence of Certified Ethical Hacker certification for the proposed lead tester or key personnel.
- Copies of additional relevant cybersecurity certifications, where available.
- Summary of similar assignments completed, including scope, period, client sector, and references where permissible.
- Proposed methodology, work plan, timelines, and rules of engagement.
- Team composition and brief profiles of key personnel.
- Confidentiality, data protection, conflict of interest, and anti-corruption declarations.
- Detailed financial proposal clearly showing professional fees, applicable taxes, reimbursables if any, assumptions, payment milestones, and deliverables covered.

8.4 Submission Instructions

- Requests for clarification may be submitted in writing to ceo@nce.co.ke no later than 21st October 2026 at 5:00 p.m. Responses to material clarifications may be issued through the official communication channel to ensure fairness, transparency, and equal access to information by all prospective bidders.
- Completed proposals shall be submitted on or before 29th October 2026 via email to ceo@nce.co.ke. The email subject should clearly indicate: RFP NCE/CEO/RFP/2026-2027/001 – Request for Proposal – Vulnerability Assessment & Penetration Testing Services for a Digital Platform.
- Bidders should clearly label all attachments and ensure that submissions are complete, signed where applicable, and received before the deadline.

- Late, incomplete, unsigned, incorrectly referenced, corrupted, incorrectly addressed, or materially non-responsive proposals may not be considered.
- NCE may issue written clarifications, addenda, or amendments before the submission deadline. Only written information issued through the authorised channel shall form part of this RFP.

8.5 Official Contact and Submission Details

Unless otherwise amended before publication, the official contact and submission details shall be:

Issued				by:
Nairobi		Coffee		Exchange
Wakulima	House,	1st	and	2nd
Haile		Selassie		Floor
P.O.		Box		Avenue
Nairobi,				36886-00200
Email:				Kenya
Website: www.nairobicoffeexchange.co.ke				ceo@nce.co.ke

All final dates, named contacts, telephone numbers, email addresses, and publication approvals shall be confirmed before issue.

9. Evaluation, Scoring and Award Methodology

9.1 Stage 1: Preliminary and Mandatory Review

Only proposals that are complete, properly submitted, signed where required, and accompanied by all mandatory administrative and eligibility documents shall proceed to technical evaluation. Nairobi Coffee Exchange may verify registration status, tax compliance, professional certifications, references, personnel credentials, independence declarations, insurance evidence, and any other information submitted by bidders. A proposal may be rejected where it is materially incomplete, inaccurate, misleading, unsigned where required, submitted late, or non-compliant with the published RFP requirements.

Mandatory review shall be assessed on a pass/fail basis and shall include, at minimum, certificate of incorporation or business registration, valid KRA Tax Compliance Certificate or applicable equivalent, company or consultant profile, signed proposal submission letter, confidentiality and conflict-of-interest declarations, evidence of relevant cybersecurity certification for proposed key personnel, and duly completed submission forms.

9.2 Stage 2: Technical Evaluation (80 Points)

Criterion	Points
Understanding of the assignment and NCE risk context	10
Methodology, coverage, manual testing, safety, and Rules of Engagement	25
Relevant organisational experience and comparable assignments	15
Qualifications and practical experience of proposed team	15
Work plan, mobilisation, reporting, quality assurance, and retest approach	10
Knowledge transfer and value-added recommendations	5
Total Technical Score	80

Minimum technical qualifying score: 56 out of 80 points (70% of the technical score), subject to approval in the final procurement plan and evaluation guide.

9.2.1 Technical Scoring Guide

The evaluation committee shall apply the following scoring guide to ensure consistency, transparency, and fairness in the assessment of all technically responsive proposals.

- **Understanding of the assignment and NCE risk context – 10 points:** Award higher marks where the bidder demonstrates a clear understanding of NCE's digital platform, stakeholder-facing workflows, access-control requirements, data sensitivity, regulatory context, business continuity needs, settlement-related exposure, and cyber-risk implications.
- **Methodology, coverage, manual testing, safety, and Rules of Engagement – 25 points:** Award higher marks where the bidder proposes a practical, risk-based, non-disruptive methodology covering web applications, APIs, access controls,

role-based permissions, business logic, configurations, cloud or hosting exposure, evidence handling, escalation, clean-up, and authorised testing controls.

- **Relevant organisational experience and comparable assignments – 15 points:** Award higher marks where the bidder provides evidence of at least three comparable cybersecurity assessment, vulnerability assessment, penetration testing, ICT audit, application security, API testing, cloud security, regulated-sector, financial, exchange, settlement, or critical digital-service assignments within the last five years.
- **Qualifications and practical experience of proposed team – 15 points:** Award higher marks where proposed personnel hold relevant hands-on cybersecurity credentials and demonstrate practical experience in application, API, infrastructure, cloud, identity and access, business-logic, and reporting assignments. CEH, OSCP, CREST, GPEN, CISSP, CISM, ISO/IEC 27001, cloud security, or equivalent recognised certifications may be considered.
- **Work plan, mobilisation, reporting, quality assurance, and retest approach – 10 points:** Award higher marks where the bidder provides a realistic schedule, named team availability, quality-review process, clear reporting structure, vulnerability register approach, management briefing plan, remediation support, and retesting process for agreed critical and high-risk findings.
- **Knowledge transfer and value-added recommendations – 5 points:** Award higher marks where the bidder proposes practical knowledge transfer, actionable remediation guidance, secure-development recommendations, control-improvement advice, and clear communication suitable for management and technical teams.

A bidder must achieve the minimum technical qualifying score of 56 out of 80 points, equivalent to 70% of the technical score, unless revised and approved before evaluation through the final evaluation plan or formal addendum.

9.3 Stage 3: Financial Evaluation (20 Points)

Only financial proposals from technically qualified bidders will be evaluated. Unless otherwise stated in an addendum, the lowest evaluated responsive price will receive 20 points. Other qualified proposals will be scored using: $\text{Financial Score} = (\text{Lowest Evaluated Price} / \text{Bidder's Evaluated Price}) \times 20$.

Financial proposals shall be reviewed for completeness, arithmetic accuracy, tax treatment, reimbursable costs, payment milestones, assumptions, exclusions, and value for money. The lowest price shall not automatically determine award where the proposal is materially non-responsive, unrealistic, incomplete, or insufficient to deliver the required scope safely and professionally. NCE may seek clarification on financial assumptions, provided such clarification does not alter the substance of the proposal or cure material non-responsiveness.

9.4 Combined Score, Due Diligence and Award Recommendation

$\text{Combined Score} = \text{Technical Score} + \text{Financial Score}$. The final ranking shall be based on technical merit, financial score, responsiveness, value for money, due diligence outcome, and NCE's operational requirements.

Before award, NCE may conduct reference checks, certification validation, personnel verification, methodology clarification, interviews, capability presentations, or other due diligence considered necessary. NCE may adjust evaluation conclusions or decline award where submitted references, certifications, past assignments, personnel claims, insurance evidence, or other material information cannot be verified.

Award shall be subject to internal approvals, agreement on final scope, price, deliverables, timelines, confidentiality obligations, data protection requirements, Rules of Engagement, and execution of a formal contract by authorised representatives. Submission of a proposal does not guarantee award.

9.5 Evaluation Governance

Evaluation shall be documented, consistent, objective, conflict-free, and based only on the published criteria and formally issued addenda. Evaluators shall disclose any actual, potential, or perceived conflict of interest before participating in the evaluation. Clarifications may be requested from bidders where necessary, but clarifications shall not be used to introduce missing mandatory documents after the deadline or cure material non-responsiveness. Financial proposals shall only be opened or evaluated for bidders who meet the approved technical qualification threshold, unless NCE's approved procurement procedure provides otherwise.

FAIRNESS

Evaluation shall be documented, consistent, conflict-free, and based only on the published criteria and formally issued addenda.

10. Contractual, Confidentiality and Data Protection Requirements

- The provider shall act only on documented instructions and within the signed authorisation and Rules of Engagement.

- All NCE data, credentials, reports, screenshots, logs, findings, working papers, and evidence are confidential and remain NCE property or under NCE control as defined in the contract.
- The provider shall use least privilege, encryption in transit and at rest, MFA where available, restricted named access, secure storage, and auditable transfer mechanisms.
- Personal and sensitive information shall be minimized and masked. Production data shall not be copied unless strictly necessary and expressly approved.
- Any suspected breach, unauthorized access, loss of evidence, or material service impact shall be reported immediately through NCE's agreed incident channel.
- Subcontracting, offshore processing, or use of third-party AI or public cloud services for NCE data or findings requires prior written approval.
- The provider shall return or securely delete NCE information at contract close, subject to agreed legal retention requirements, and provide written confirmation.
- Intellectual property in pre-existing tools remains with the provider. Assignment-specific reports, registers, evidence, and deliverables shall vest as agreed in the contract.
- The provider shall maintain independence, disclose conflicts promptly, and not test controls that it designed or implemented where that would impair objectivity.
- No use of NCE's name, logo, systems, findings, or engagement in advertising, case studies, tenders, or public statements without prior written approval.

11. General Conditions

- This RFP is an invitation to submit proposals and does not constitute a contract or commitment to award.
- NCE may amend, suspend, cancel, or reissue the RFP, reject any proposal, or decline to award, subject to applicable approvals and fair process.
- Bidders bear all costs of preparing and submitting proposals and participating in clarification or due diligence.
- Canvassing, collusion, bribery, inducement, misrepresentation, or attempts to improperly influence the process may result in disqualification.
- NCE may seek clarification but is not obliged to permit correction of material non-responsiveness after the deadline.
- Proposal validity shall be ninety days unless extended by written agreement.
- The successful bidder shall agree to service levels, deliverable acceptance criteria, payment milestones, liability, indemnity, dispute resolution, termination, and audit rights in the final contract.
- Kenyan law shall govern the procurement and resulting contract, with the dispute-resolution mechanism specified in the final agreement.

12. Forms and Schedules

Form 1: Proposal Submission Letter

To:	Chief Executive Officer, Nairobi Coffee Exchange
RFP Reference:	NCE/CEO/RFP/2026-2027/001

We, the undersigned, offer to provide Independent Vulnerability Assessment and Penetration Testing Services in accordance with this RFP and our proposal. We confirm that the information submitted is accurate, that we have disclosed actual or potential conflicts of interest, and that our proposal will remain valid for ninety (90) calendar days from the submission deadline.

Field	Bidder Response
Legal name	
Registration number	
KRA PIN	
Physical and postal address	
Authorised representative	
Email and telephone	
Total proposal price in KES	
Signature and company stamp	

Field	Bidder Response
Date	

Form 2: Relevant Assignment Record

Client / Sector	Assignment and Scope	Period	Contract Value*	Reference Contact

* Contract value may be omitted where disclosure is contractually restricted; provide alternative completion evidence.

Form 3: Key Personnel Schedule

Name	Proposed Role	Qualifications / Certifications	Relevant Years	Availability

Form 4: Declaration of Independence, Confidentiality and Conflict of Interest

The bidder declares that it will perform the assignment independently; protect NCE information; disclose any actual, potential, or perceived conflict; avoid unauthorized disclosure or use; and ensure that all personnel and approved subcontractors are bound by equivalent obligations.

Declaration	Bidder Confirmation
No undisclosed conflict of interest exists	Yes / No
No proposed tester designed or implemented the controls under review, unless disclosed	Yes / No
All personnel will sign confidentiality undertakings	Yes / No
NCE information will not be used in AI tools or external services without approval	Yes / No
Any subcontractor has been fully disclosed	Yes / No
Authorised signatory, signature, stamp and date	

Appendix A: Indicative Asset and Test-Scope Register

The final register will be completed during mobilization and signed as part of the Rules of Engagement. The RFP does not itself authorize active testing.

ID	Asset / Environment	Owner	Test Type	Window	Status / Notes
A-01					
A-02					
A-03					
A-04					

Appendix B: Bidder Response Checklist

No.	Document / Evidence	Included (Y/N)	Reference / Page
1	Signed proposal submission letter		
2	Certificate of incorporation / registration		
3	Valid KRA Tax Compliance Certificate		
4	Company profile and ownership details		
5	Technical methodology and draft Rules of Engagement		
6	Work plan and schedule		
7	Team CVs and valid certifications		
8	Three comparable assignments and references		
9	Independence, confidentiality, conflict and anti-bribery declarations		
10	Insurance evidence or commitment		
11	Separate financial proposal in KES		
12	Redacted sample report, where permissible		