KENINDIA

KENINDIA ASSURANCE COMPANY LIMITED

REQUEST FOR PROPOSALS

Provision of Co-Sourced Risk-Based Information Systems and Cybersecurity Internal Audit Services

RFP AT A GLANCE

RFP Number	KACL/RFP/CRISCIAS/001/11/2026
Issue Date	November 4, 2026
Proposal Due Date	November 13, 2026
Questions Deadline	November 9, 2026
Submission Method	Electronic (email) — administration@kenindia.com
Clarifications To	administration@kenindia.com. All material clarification responses shall be circulated to all participating bidders through an official addendum.
Proposal Validity	Minimum 180 days from submission date
Assignment Period	12 Months from the agreed commencement date

1. BACKGROUND AND CONTEXT

Kenindia Assurance Company Limited, a leading composite insurance company in Kenya, is seeking proposals from qualified firms to provide independent, co-sourced risk-based Information Technology (IT) and Cybersecurity Internal Audit Services.

The selected service provider will assess IT and cybersecurity risks, develop a proposed risk-based annual IT audit plan for approval, and execute specialist audit assignments during the contract period.

2. ASSIGNMENT OBJECTIVE

The primary objective of this engagement is to appoint a qualified firm to provide co-sourced, risk-based IT and cybersecurity internal audit services over a period of twelve (12) months by:

- **Assessing IT and cybersecurity risks:** Conducting a documented risk assessment of Kenindia's technology environment, including the ongoing core system implementation.
- **Developing a risk-based audit plan:** Preparing an indicative audit universe, a prioritized twelve-month audit plan and a quarterly audit assignment schedule for approval.
- **Executing specialist audit assignments:** Undertaking substantive IT and cybersecurity audit assignments each quarter and issuing reports on each.
- **Providing cybersecurity assurance:** Performing vulnerability assessments, security configuration reviews and penetration testing as part of relevant audit assignments.
- **Following up on audit recommendations:** Tracking, verifying and reporting the implementation of agreed management actions.
- **Supporting Internal Audit and the Board:** Supporting the Head of Internal Audit in reporting significant results to the Board Audit Committee (BAC).

3. ASSIGNMENT SCOPE

Kenindia operates an IT environment supporting its insurance operations across various locations in Kenya. The environment includes:

IT Environment Component	Description
Core Insurance Systems	Two core insurance systems supporting general insurance, life insurance and pensions, integrated with other business applications and external systems.
Applications and Databases	Web-based applications, business support systems and databases.
IT Infrastructure and Hosting	A combination of on-premises and cloud-based infrastructure, including Windows and Linux servers.
Network and Cybersecurity	Network infrastructure, firewalls, VPNs, identity and access management, and other information security controls.
Digital Portals and Integrations	Customer and intermediary portals, APIs and interfaces with third-party service providers.
Business Continuity and Disaster Recovery	Backup and disaster recovery arrangements supporting critical systems.
Ongoing System Implementation	Implementation of a new general insurance core system intended to replace the existing system.

The selected service provider shall obtain an understanding of the IT environment and ongoing system implementation during the initial risk assessment to identify significant technology risks and develop a risk-based IT audit plan. Additional technical information will be made available as necessary, subject to confidentiality and information security requirements.

The engagement spans seven (7) core service lines over a period of twelve (12) months:

3.1 IT and Cybersecurity Risk Assessment

i. Conduct an initial IT and cybersecurity risk assessment, considering the Company's technology environment, ongoing system implementations, emerging risks, relevant IT strategies, risk registers, policies, incidents, regulatory requirements, system criticality, previous audit findings and outstanding issues, in consultation with relevant stakeholders.

ii. Prepare a documented IT and cybersecurity risk assessment, indicative audit universe, prioritized twelve-month risk-based audit plan and quarterly audit assignment schedule.

3.2 Risk Domains for Consideration

The following constitute an indicative risk universe, not a requirement to audit every domain. Final coverage shall follow the documented risk assessment and approved audit plan.

Risk Domain	Illustrative Audit Coverage
IT governance and strategy	IT oversight, risk ownership, policies, technology investments and performance
Cybersecurity and information security	Security governance, threat detection and response, vulnerability management, security configurations and incident readiness
Identity and access management	User lifecycle, privileged access, authentication and segregation of duties
IT general controls	Change management, IT operations, patching, logging and configuration management
Business Applications, Data Protection and Privacy	Application controls, interfaces, data integrity, personal data protection, privacy, retention and compliance with applicable data protection requirements
Business Continuity and Disaster Recovery	Backups, disaster recovery, recovery testing and operational resilience
IT Projects and Core System Implementation	Project governance, system security controls, access management, data migration, integrations, security testing, user acceptance testing, go-live readiness and transition from the existing system

Risk Domain	Illustrative Audit Coverage
Third-party and cloud services	Outsourcing, vendor assurance, cloud controls and service continuity

3.3 Quarterly Audit Execution, Review and Reporting

The service provider shall:

i. Undertake substantive audit assignments in each quarter in accordance with the approved risk-based plan.
ii. Prepare engagement-level objectives and scope, and develop appropriate audit criteria and procedures.
iii. Perform testing, document sufficient and appropriate evidence, discuss findings with responsible management and issue an individual report for each completed assignment.
iv. Provide a consolidated quarterly IT and cybersecurity audit report for incorporation into Internal Audit's report to the Board Audit Committee (BAC), summarizing assignments completed, significant findings, risk ratings, management responses, overdue actions and emerging risks.
v. Review the status of agreed recommendations and report outstanding and high-risk actions.
vi. Support the Head of Internal Audit in presenting and discussing significant audit results with the BAC, as required, and deliver reports in time for committee-paper deadlines.

Note: Quarterly progress updates alone, without substantive audit execution, shall not constitute completion of the quarterly audit service.

3.4 Cybersecurity Assurance and Targeted Security Testing

Cybersecurity assurance shall form an integral part of the risk-based IT audit engagement.

The service provider shall undertake vulnerability assessments, security configuration reviews and penetration testing as part of relevant audit assignments, with the extent of testing determined by the assessed risks and approved audit plan.

The service provider shall ensure that testing is appropriately scoped, coordinated with relevant IT personnel and conducted with adequate safeguards to protect the Company's systems and operations.

All cybersecurity testing undertaken within the agreed audit assignments shall be included in the total annual contract price, with no additional charges.

3.5 Follow-Up of Audit Recommendations

The service provider shall:

i. Maintain an IT and cybersecurity audit issues tracker recording agreed management actions, responsible owners, target completion dates, implementation status and evidence supporting closure.
ii. Review the implementation status of agreed IT and cybersecurity audit recommendations, including outstanding findings from previous audits, and verify evidence of implementation.
iii. Incorporate the results of follow-up reviews, including overdue and high-risk actions, into the quarterly IT and cybersecurity audit reports.

3.6 Technical Supervision and Quality Assurance

The service provider shall:

i. Assign suitably qualified and experienced IT audit and cybersecurity specialists to undertake the audit assignments.
ii. Ensure that all technical audit work is appropriately supervised and quality-reviewed by qualified specialists.
iii. Be responsible for the technical adequacy of audit procedures, testing, supporting evidence, findings and conclusions.
iv. Conduct audit assignments in accordance with applicable professional internal auditing standards and recognized IT audit and cybersecurity frameworks.

3.7 Ad Hoc Technical Advisory Support

The service provider shall provide ad hoc IT and cybersecurity technical advisory support to the Head of Internal Audit, as reasonably required during the engagement, including advice on emerging technology risks, significant cybersecurity incidents, system implementation risks and proposed control improvements.

Such support shall be incidental to the engagement, included in the agreed contract price and shall not replace or reduce the required quarterly audit assignments. The service provider shall maintain independence and objectivity and shall not assume management responsibilities or undertake the design, implementation or operation of controls subject to audit.

4. KENINDIA'S RESPONSIBILITIES

Kenindia will support the service provider by:

- Providing functional direction through the Head of Internal Audit.
- Making additional technical information available as necessary, subject to confidentiality and information security requirements.
- Facilitating consultation with relevant stakeholders and coordination with relevant IT personnel for audit assignments and security testing.
- Considering the proposed risk-based audit plan for approval, and approving any adjustments to assignments and the quarterly schedule.
- Reviewing and accepting reports and deliverables, and making quarterly payments upon acceptance.

5. SERVICE PROVIDER DELIVERABLES

The service provider shall deliver the following over the twelve-month engagement period:

#	Deliverable	Timing
1	**Documented IT and cybersecurity risk assessment, indicative audit universe, risk-based audit plan and quarterly audit activity schedule**	During the initial phase of the engagement
2	**Execution of approved IT and cybersecurity audit assignments**	Each quarter, in accordance with the approved audit plan
3	**Individual audit reports, including findings, recommendations and management responses**	Upon completion of each audit assignment
4	**Consolidated IT and cybersecurity audit report for incorporation into Internal Audit's BAC report**	Quarterly, in advance of BAC reporting deadlines
5	**Updated IT and cybersecurity audit issues tracker, including follow-up on agreed recommendations**	Quarterly
6	**Technical reports on vulnerability assessments, security configuration reviews and penetration testing**	Upon completion of relevant testing

The service provider shall agree a detailed delivery schedule with the Head of Internal Audit at the commencement of the engagement, considering the Company's quarterly BAC reporting calendar.

6. SERVICE PROVIDER RESPONSIBILITIES

The selected service provider will be required to fulfil the following cross-cutting responsibilities:

- **Reporting and accountability:** Work under the functional direction of the Head of Internal Audit while retaining responsibility for the technical execution, supervision and quality of its audit work.
- **Independence and objectivity:** Disclose any actual or potential conflicts of interest, including previous involvement in the design, implementation or operation of systems or controls subject to audit, and describe the safeguards proposed to preserve independence and objectivity.
- **Protection of Kenindia's systems:** Ensure that security testing is appropriately scoped, coordinated with relevant IT personnel and conducted with adequate safeguards.
- **Technical quality:** Ensure all technical audit work is supervised and quality-reviewed by qualified specialists in line with professional standards and recognized frameworks.
- **Handover:** On completion or termination, hand over completed and ongoing audit reports, relevant working papers, supporting evidence, issue-tracking records and the status of outstanding assignments.

7. MANDATORY SUBMISSION REQUIREMENTS

All proposals must include the following documents:

#	Mandatory Document
1	Evidence that the bidder is a duly registered professional firm e.g. Certificate of Incorporation or business registration.
2	KRA PIN and Valid Tax Compliance Certificate
3	Profiles of the proposed engagement team, indicating professional certifications, relevant experience and assigned roles
4	Valid Certified Information Systems Auditor (CISA) certification for the proposed IT audit engagement lead and the relevant IT qualification for the proposed IT auditors.
5	Relevant professional certifications (e.g. CISM, CISSP, CEH or equivalent) for the proposed cybersecurity specialists
6	Details of comparable engagements and client references (including insurance or financial services sector experience)
7	At least three (3) reference or recommendation letters from past clients for similar consultancies completed in the past three years.
8	Disclosure of any actual or potential conflicts of interest, and the safeguards proposed to preserve independence and objectivity

8. TECHNICAL PROPOSAL REQUIREMENTS

Bidders shall submit a Technical Proposal that addresses the following elements:

Section	Required Content
Understanding of the assignment	The bidder's understanding of the engagement objectives, scope and expected deliverables, including familiarity with Kenindia's insurance operations and technology environment.
Proposed methodology	Proposed IT and cybersecurity internal audit methodology, including the approach to initial risk assessment, audit universe prioritization, execution of quarterly assignments, reporting, and follow-up of audit recommendations.
Cybersecurity assurance and technical testing	Approach to cybersecurity audit coverage, integration of vulnerability assessments, penetration testing, and security configuration reviews.
Work plan and execution capacity	Proposed work plan, resource capacity, and arrangements for delivering quarterly audit assignments and reports aligned with Board Audit Committee (BAC) reporting deadlines.
Key personnel and team composition	Profiles of the proposed engagement team, including valid professional certifications (CISA for IT auditors; CISM, CISSP, CEH for cybersecurity specialists), roles, and allocation of responsibilities.
Independence, objectivity and safeguards	Disclosure of actual or potential conflicts of interest (specifically regarding prior system implementations), proposed independence safeguards, and technical supervision/quality assurance arrangements.
Value addition proposition	Proactive strategic insights on emerging technology risks, knowledge transfer and capacity-building plans for internal teams, and innovative value-added tools, benchmarks, or frameworks or any other relevant value add proposition to be provided at no extra cost.

9. COST PROPOSAL REQUIREMENTS

Bidders shall submit a separate Financial Proposal in accordance with the requirements of this RFP. The Financial Proposal shall be presented in Kenya Shillings (KES) and shall be valid for a period of not less than one hundred and eighty (180) days from the proposal submission deadline.

The Financial Proposal shall be submitted separately from the Technical Proposal and shall contain sufficient detail to enable the evaluation of the proposed costs.

The quoted fees shall be deemed to include all expenses necessary for the successful execution of the assignment and no additional costs shall be payable unless expressly approved in writing by the Client.

#	Cost Element	Description	Pricing Basis
1	**Total professional fees**	Total fixed professional fees for the twelve-month IT and cybersecurity internal audit engagement. This should be broken down into proposed roles (e.g Engagement partner, cybersecurity specialist, IT auditor etc.), estimated level of effort (LOE) in days for each engagement role, daily rate and total consultancy fees.	By resource category showing LOE, daily rates and total fees
2	**Cybersecurity Assessment Costs**	Breakdown of proposed fees per year covering Vulnerability Assessments, Penetration Testing, Security Configuration Reviews and any Other Technical Assessments as required in the RFP.	Detailed breakdown by testing activity
3	**Reimbursable and Administrative costs**	Breakdown of the proposed administrative costs required for implementation of this assignment e.g. travel, printing, internet etc.	Breakdown included in total fixed price
4	**Applicable Taxes**	Any applicable taxes clearly identified.	All applicable taxes as shown separately
5	**Grand Total Contract Price**	A consolidated Grand Total Fixed Annual Contract Price comprising all professional fees, cybersecurity assessment costs, reimbursable costs, administrative costs, taxes and any other applicable charges. This amount shall constitute the bidder's evaluated financial proposal price.	Total evaluated bid price

Note: The proposed price shall cover all personnel, technical resources, supervision, quality assurance and reporting necessary to deliver the services specified in this RFP. The Client's preference is for a fixed annual contract price covering all services described in this RFP.

- The staffing profile, level of effort, proposed roles and deployment assumptions reflected in the Financial Proposal shall be consistent with those presented in the Technical Proposal.
- All reimbursable and administrative costs shall be included within the total proposed contract price and shall not be separately claimable during contract execution unless expressly approved in writing by the Client.
- All taxes shall be clearly shown separately. Bidders shall indicate:
    - Total price exclusive of taxes;
    - Applicable taxes;
    - Total price inclusive of taxes.
- The bidder shall separately indicate the pricing allocation for:
    - Vulnerability Assessments;
    - Penetration Testing;
    - Security Configuration Reviews; and
    - Any additional cybersecurity testing activities proposed.
- Bidders shall clearly indicate: Any assumptions used in arriving at the proposed price and any exclusions from the proposed price.
- Failure to disclose exclusions at the proposal stage shall be deemed to mean that the bidder's price includes all costs necessary to deliver the assignment.
- No separate pricing for mandatory cybersecurity testing activities shall be permitted after contract award.

- Financial proposal completeness: The bidder shall be deemed to have examined and understood all requirements contained in the RFP. The proposed price shall cover all personnel, travel, cybersecurity testing tools, reporting, presentations to Management and the Board Audit Committee, quality assurance reviews, project management, and any other resources required to fully perform the services described in the Terms of Reference.
- The Client reserves the right to seek clarification on any aspect of the Financial Proposal, including unusually low prices, pricing assumptions, exclusions, or arithmetic inconsistencies.

9.1 Evaluation of Financial Proposals

Financial Proposals shall only be opened and evaluated for bidders who attain the minimum technical score of seventy-five (75) points and satisfy all mandatory technical requirements.

The lowest evaluated financial proposal shall receive the maximum financial score of 100 points. Financial scores for other bidders shall be calculated using the formula:

Financial Score (FS) = (Lowest Evaluated Price ÷ Bidder's Evaluated Price) × 100

10. EVALUATION CRITERIA

The technical proposals shall be evaluated out of a maximum score of one hundred (100) points using the criteria set out below:

10.1 Technical & Capacity Evaluation

No.	Technical Evaluation Criteria	Description/core focus	Score
1	**Firm's experience and profile**	Demonstrated experience in IT and cybersecurity internal audits within the insurance, financial services, or comparable regulated sectors, supported by verifiable references and evidence of successful engagements.	15
2	**Key Personnel Qualifications and Team Composition**	Professional certifications (CISA, CISM, CISSP, CEH or equivalent) and relevant domain expertise.	15
3	**Proposed Methodology and Approach**	Quality of risk assessment, risk-based audit planning, audit execution, and follow-up mechanism	25
4	**Cybersecurity Assurance and Technical Testing Approach**	Integration of vulnerability assessments, penetration testing, and security configuration reviews.	15
5	**Proposed Project Plan and Execution Capacity**	Work plan alignment with quarterly Board Audit Committee (BAC) reporting deadlines and delivery capacity.	15
6	**Independence, Objectivity and Conflict Disclosure**	Quality of conflict disclosures, safeguards, and technical supervision/quality assurance framework	10
7	**Proposed value addition**	Strategic insights, technology trend advisory, knowledge transfer, and ancillary value-add tools/frameworks at no additional cost.	5
	TOTAL		**100**

10.2 Minimum Technical Qualification Threshold

Only bidders attaining a minimum technical score of seventy-five (75) points out of one hundred (100) shall be considered technically responsive and qualify for the financial evaluation stage. Proposals scoring less than seventy-five (75) points shall be eliminated from further evaluation and their financial proposals shall not be considered.

10.3 Minimum Scores for Critical Technical Areas

To ensure that bidders demonstrate adequate competence in the key aspects of the assignment, bidders shall additionally be required to attain the following minimum scores in the specified criteria:

- Proposed Methodology and Approach (Criterion 3): Minimum score of twelve (12) out of twenty (25) points.
- Cybersecurity Assurance and Technical Testing Approach (Criterion 4): Minimum score of nine (9) out of fifteen (15) points.

- Key Personnel Qualifications and Team Composition (Criterion 2): The proposed Engagement Lead must hold a valid CISA certification or equivalent, and the proposed cybersecurity specialist(s) must possess recognized cybersecurity certifications such as CISM, CISSP, CEH, or equivalent credentials.

Failure to attain the above minimum scores or meet the mandatory qualification requirements shall render the bidder technically non-responsive irrespective of the overall technical score achieved.

10.4 Combined Technical and Financial Evaluation

The final ranking of bidders shall be based on a combined quality and cost evaluation using the following weighting:

Component	Weight
Technical Proposal	80%
Financial Proposal	20%
Total	**100%**

The bidder achieving the highest combined score shall be ranked first and may be invited for contract negotiations and award, subject to satisfactory due diligence and approval by the Client.

11. MINIMUM QUALIFICATIONS

Qualification Area	Requirement
Firm Registration and Experience	Duly registered professional firm with proven experience in providing IT and cybersecurity internal audit services.
Sector Experience	Relevant experience in the insurance or financial services sector, including audits of core business applications, IT infrastructure and cybersecurity controls.
Engagement Lead	IT audit engagement lead holding a valid Certified Information Systems Auditor (CISA) certification, with demonstrated experience in managing IT internal audit engagements.
IT Auditors	Suitably qualified and experienced IT auditors, holding CISA certification, assigned to IT internal audit assignments.
Cybersecurity Specialists	Specialists with relevant professional certifications, such as CISM, CISSP, CEH or equivalent, with demonstrated expertise in vulnerability assessments, penetration testing, security configuration reviews and cybersecurity assurance.
Technical Expertise	Relevant expertise in IT governance, application controls, data protection, cloud security and system implementation audits.
Capacity and Quality Assurance	Capacity to execute quarterly audit assignments, provide appropriate technical supervision and quality assurance, and deliver reports within agreed timelines.
Team Profiles and References	Profiles of the proposed engagement team, indicating professional certifications, relevant experience and assigned roles, together with details of comparable engagements and client references.

12. CONTRACT PERIOD AND SCOPE CONTROL

- **Contract period:** The engagement period shall be twelve (12) months from the agreed commencement date.
- **Scope control:** Approved audit assignments and the quarterly schedule may be adjusted to reflect emerging risks, subject to documented approval, agreed fee limits and applicable procurement and contractual requirements. Any extension or renewal shall follow the Company's approval and procurement requirements.

> **Confidentiality:** Additional technical information will be made available as necessary, subject to confidentiality and information security requirements, which the service provider must observe throughout the engagement.