NATIONAL LIBRARY OF SOUTH AFRICA

228 Johannes Ramokhoase Street
Private Bag X397
Pretoria
0001

5 Queen Victoria Street
Cape Town
8001

APPOINTMENT OF A SERVICE PROVIDER FOR THE PROCUREMENT OF INTERNAL AUDIT AND RISK AND COMPLIANCE MANAGEMENT SOFTWARE TOOL INCLUDING SUPPORT.

Bid No: NLSA 09/2025-2026

Should you wish to deliver Bid documents, please note that the NLSA's working hours are from **08h00** to **17h00** on weekdays. Upon the submission of the Bid Documents Service Providers are requested to sign the register at reception.

COMPULSORY BRIEFING SESSION. **N/A**

CLOSING DATE: 29 January 2026 **TIME: 11H00**

BID DOCUMENTS ARE AVAILABLE ON

- NLSA website (www.nlsa.ac.za/tenders-and-procurement)

NB. Completed Bid Documents must be deposited at the following address.

ADDRESS	CLOSING DATE	TIME
NLSA **Pretoria Campus**, 228 Johannes Ramokhoase Street, Pretoria CBD.	**29 January 2026**	11H00

1. BACKGROUND

1.1. National Library of South Africa (NLSA), hereafter referred to as NLSA, is a world class African National Library and Information Hub. The NLSA is responsible for collecting, recording, preserving, and making available the national documentary heritage of South Africa. The NLSA promotes awareness, appreciation, and access to published documents, nationally and internationally and in doing so contributes to the development and prosperity of South Africa. The NLSA has Campuses in Pretoria and Cape Town.

1.2. Internal Audit, Risk and Compliance Management requires cloud-based Audit and Risk Management software tool that enables automation of audit and risk processes. This software will equip Internal Audit and Risk Management Unit to streamline processes and minimize manual intervention. This is critical as it will assists with increasing the efficiency and productivity of the entire process, including scheduling, planning, execution, review, report generation, trend analysis, automated tracking and follow-up of previously raised findings, audit committee reporting and storage. It also enables teams including management to work centrally on one output.

2. OBJECTIVES

The objectives are as follows:

- To automate the internal audit process and enable comprehensive audit planning, execution, and reporting.
- To automate the risk management and reporting process.
- To automate compliance management processes in line with regulatory and internal requirements
- To automate the process to follow up on corrective action agreed upon by management and enable management to provide status update using the software.
- To provide user-friendly dashboards for real-time reporting and stakeholder communication.
- To facilitate continuous auditing, risk monitoring and compliance oversight
- To incorporate built in functionality to run data analytics to provide deeper insights and anomaly detection.
- Utilize AI capabilities to streamline risk assessment and support predictive analytics.

3. SCOPE OF WORK

Scope of work entails the following:

- A cloud- based Audit and Risk Management software that will enable automation processes, centralizing documentation, facilitating third-party risk assessments, and improving efficiency and compliance.
- Disaster Recovery and Business Continuity capabilities

The bid should include the following:

- Software installation fee.
- Licences fees per annum (5 users).
- Introduction/ Foundation Training for 5 Users.

- Service provider must provide detailed implementation methodology

NB: Online support and maintenance should be provided by the successful bidder at no extra cost.

4. DELIVERABLES

4.1. INTERNAL AUDIT RISK AND COMPLIANCE MANAGEMENT

Internal Audit Features:

- The software should provide capabilities that allow Internal Audit to plan and allocate its projects and resources at the beginning of each financial year in line with the approved internal Audit plan.
- The software should have audit documentation templates/capabilities that allow for documentation of audit projects from planning, fieldwork through to reporting.
- The software should provide report generation capabilities that allow Internal Audit to generate an Audit report from the working papers completed on the tool during fieldwork.
- The software should have Audit finding tracking capabilities that allow both Internal Audit and the business process owners who own the findings visibility on such findings.
- The software should provide for adequate segregation of uses within the system, e.g., work paper preparers, reviewers at various levels (audit supervisor, audit manager etc.), administrators etc.
- The software should have backup and storage capabilities that allow it to consistently backup data to enable recovery in the event of a disruption.
- The software should have the capability of allowing more than one auditor to work on the same project at the same time.
- The software should include dashboards for real-time reporting and stakeholder communication.
- The software must be able to facilitate continuous monitoring and a data-driven approach to audit processes.
- The software should incorporate built-in functionality to run data analytics to provide deeper insights and anomaly detection.
- The software should include dashboards for real-time reporting and stakeholder communication.
- The software must be able to facilitate continuous monitoring and a data-driven approach to audit processes.
- Integration with compliance processes for Combined Assurance visibility

Risk Management Features

- Adequate risk analysis and dashboards (e.g., heatmaps, age analysis, escalation of overdue mitigations).
- Capability to map risks to the lines of defence in line with the Combined Assurance Model.
- Support for multiple levels of risk assessments: Strategic, Operational, and Project.

- Determination and monitoring of risk appetite and tolerance levels.
- Reminders and escalations to line management for due actions and mitigations.
- Integration of risk management with Internal Audit and Compliance Management for a combined assurance view.
- Automated risk scoring and prioritization based on likelihood, impact, and control effectiveness.
- Trend analysis and historical risk reporting to identify emerging risks over time.
- Real-time notifications and alerts for new, modified, or critical risks.
- Capability to link risks to organizational objectives, KPIs, and strategic initiatives for performance monitoring.

Compliance Management Features

- Import and maintenance of legislation from third-party compliance content providers.
- Capture and classification of internal policies, procedures, and provisions.
- Categorisation of acts and regulations as core, secondary, or topical.
- Risk-based prioritisation using probability and seriousness ratings.
- Real-time compliance tracking and continuous self-assessments by business owners.
- Issue and action-plan tracking with automated reminders.
- Registers for non-compliance incidents, losses, conflicts of interest, gifts, and complaints.
- Early-warning alerts for overdue or high-risk items.
- Compliance dashboards and reports by act, provision, or responsible unit.
- Capability to perform internal compliance audits and generate compliance ratings.
- Integration with risk and audit modules for combined assurance visibility.

5. REQUIREMENTS

5.1. Internal Audit Functionality

THE AUDIT AND RISK MANAGEMENT SOFTWARE/ TOOL MUST COMPLY AND HAVE THE FOLLOWING REQUIREMENTS:	Comply (Yes)	Not Comply (No)
The Software/ Tool must be cloud based or has capabilities to be hosted in the cloud.		
The Software/ Tool should enable Internal Audit to allocate or assign employees to a specific audit as well as the total hours allocated to the project.		
The Software/ Tool should have audit documentation templates/capabilities that allow for documentation of audit projects from planning, fieldwork through to reporting. At a minimum the tool should provide templates for the following: **Planning:** working paper templates that enable the auditor to document system description, audit risks, audit objectives, controls, audit procedures including resource planning (team allocation and project hours). **Fieldwork:** working paper templates that enable the auditor to document audit results as well as conclusion. **Exception/Finding** **Creation capability:** The tool should have capability to create audit exceptions/findings and hyperlink/reference them to the relevant working papers containing audit results and conclusion. The exception/finding should contain the criteria/ standard, finding, root cause, impact/risk, recommendation, management comments/Agreed action plans and actions dates.		
The Software/ Tool should have audit finding tracking capabilities that allow both Internal Audit and the business process owners who own the findings visibility on such findings. Moreover, business units should be able to update status update and attached evidence for resolved findings.		
The Software/ Tool should provide for adequate segregation of users within the system, e.g. work paper preparers, reviewers at various levels (Internal Audit specialist (supervisor), Head/ Senior Manager reviews, etc.).		
The Software/ Tool should have capabilities to allow more than one auditor to work on the same project at the same time.		

The Software/Tool must include Compliance Management capabilities, including: RCU management, legislation import, internal policy capture, compliance dashboards, automated CRMP generation, issue/action-plan tracking, and integration with audit and risk modules for combined assurance visibility.		

5.2. Risk & Compliance Management Functionality

THE AUDIT AND RISK MANAGEMENT SOFTWARE/ TOOL MUST COMPLY AND HAVE THE FOLLOWING REQUIREMENTS:	Comply (Yes)	Not Comply (No)
The Software/ Tool should provide for adequate risk analysis and dashboards (e.g. heatmaps and age analysis of and escalations of overdue mitigations		
The Software/ Tool should provide for adequate capability to map the risks to the lines of defence in line with Combined Assurance Mode.		
The Software/ Tool should provide for levels of risk assessments i.e. Strategic Risk Assessments, Operations Risk Assessments and Project Risk Assessments		
The Software/ Tool should provide for determination and monitoring of risks appetite and tolerance levels		
Integration with Internal Audit and Compliance Management for combined assurance visibility.		
Automated risk scoring and prioritization based on likelihood, impact, and control effectiveness.		
Trend analysis and historical risk reporting to identify emerging risks.		
Real-time notifications and alerts for new, modified, or critical risks.		
Capability to link risks to organizational objectives, KPIs, and strategic initiatives for performance monitoring.		

5.3. Internal Audit Security

THE AUDIT AND RISK MANAGEMENT SOFTWARE/ TOOL MUST COMPLY AND HAVE THE FOLLOWING REQUIREMENTS:		Comply (Yes)	Not Comply (No)
Access management	The Software/ Tool must have a capability to provide the following • Authentication of users through user name and password before a user is granted access to the system. • Enforce standard access control principles such as segregation of duties, role-based access control based on least privilege and need to know principle.		
Audit capabilities	The Software/ Tool must enable the logging of the following activities undertaken by users and systems at a minimum: • Working paper sign offs; • User last logins.		

Information security	The Software/ Tool must be a web-based tool • The bidder should provide confirmation in the form of a signed off letter that: ▪ The solution should be consistently upgraded to provide protection against the OWASP threats as new threats emerge (i.e. the latest upgrade of the solution should cover at least the top 10 Open Web Application Security Project (OWASP) 10 threats at any given time) • The Software/ Tool meets privacy requirements (e.g., the need to protect the confidentiality of customer records or personally identifiable information (PII) such as employee and customer details) as per the legal and regulatory requirements (e.g. POPIA, GDPR, ECT). • The bidder confirms that they will adhere to the NLSA's information security policies, standards and procedures.		
Encryption	The bidder should provide confirmation in the form of a signed off letter that the Software/ Tool has adequate protection for sensitive information in transit (e.g. between the web server and a user's web browser) and at rest; the information must be protected against unauthorised disclosure.		
Audit Tool Hosting	The Software/Tool should have the capability to be hosted on cloud platforms such as Microsoft Azure, Amazon Web Services (AWS) or similar. These cloud hosting environments provide secure, scalable, and highly reliable infrastructure for hosting applications and data. This is to ensure robust system performance, business continuity, and optimised operational efficiency for the NLSA. If the service provider prefers own hosting, the service provider must bear the cost of self-hosting.		
Integration	The Software/ Tool must provide standardised integration capabilities to facilitate integration into NLSA's internal systems.		
Customisation	The Software/ Tool must be easily modified/ customised to meet Internal Audit, Risk, and Compliance Management needs, preferences and/ or requirements.		

Bidders must indicate system capabilities as per the above.

6. NLSA'S RIGHTS

6.1. The NLSA is entitled to amend any tender conditions, tender validity period, tender terms of reference, or extend the tender's closing date, all before the tender closing date. All Bidders, to whom the Bid documents have been issued and where the NLSA have a record of such Bidders, may be advised in writing of such amendments in good time and any such changes will also be posted on the NLSA's website under the relevant Bid information. All prospective Bidders must, therefore, ensure that they visit the website regularly and before they submit their Bid response to ensure that they are kept updated on any amendments in this regard**.**

7. DURATION OF THE PROJECT

The contract will comprise a once-off installation, configuration, and deployment of the Internal Audit, Risk and Compliance Management Software Tool, followed by a 36-month support, maintenance, and licensing Service Level Agreement (SLA)

The appointed service provider shall commit to completing all installation, configuration, onboarding, user training, and system commissioning activities **within 120 days** from the date of receiving the official purchase order, unless otherwise agreed in writing and incorporated into the SLA.

CONDITIONS OF THE BID

7.1. The NLSA reserves the right not to accept the lowest proposal.

7.2. The NLSA reserves the right to appoint one or more Bidders.

7.3. The NLSA reserves the right not to award the contract.

7.4. The NLSA reserves the right to have any documentation, submitted by the successful Bidder checked or inspected by any other person or organisation.

7.5. The General Conditions of Contract will be applicable to this Bid.

7.6. The NLSA will not be held responsible for any costs incurred by the Bidder in the preparation and submission of the Bid.

7.7. The Bidder may be required to prepare for a possible presentation should the NLSA require such and the Bidder shall be notified thereof in good time before the actual presentation date. Such presentation may include a practical demonstration of products or services as called for in this Bid.

7.8. No upfront Payment will be done by NLSA.

7.9. The bid is valid for a period of 90 days and may be extended at the discretion of the NLSA.

8. EVALUATION CRITERIA

8.1 Pre evaluation (standard bid documents)

8.1.1 Fully Completed SBD 1, SBD 3.1, SBD 4, SBD 6.1, SBD 7.2 forms.

8.1.2 The bidder must be registered on the Central Supplier Database (CSD).

NB: If there are any materials omission on the stated SBDs, bidders will be afforded a maximum of 2 working days to respond to the omission.

8.2 SUBMISSION FORMAT

Bid proposals should be submitted in the format as indicated below:

NB! One (1) signed original Bid document and One (1) signed electronic copy on a USB or CD (PDF protected with a code).

Bidders will be evaluated in three stages. First stage will be the technical evaluation and the second stage will be the presentation and third stage will be the price evaluation.

8.3 EVALUATIONS

8.3.1 First Stage: Technical Evaluation

Bidders are expected to obtain a minimum of seventy (70) points out of one hundred (100) points available to proceed to the next evaluation stage. Failure to obtain the prescribed points will automatically disqualify the bidder from proceeding to the next evaluation stage.

Evaluation Criteria		Weight	Point	Score
1	**INTERNAL AUDIT**	**30**		
	Bidders must provide a minimum of five (5) contactable reference letters of the service provided within the past five (5) years. The name of the organisation at which the Internal Audit tool was provided. ▪ The component that was used from the tool, e.g. Internal Audit, Risk management, etc. ▪ The letter must be on the company/ organisation letterhead, ▪ Contact Person, ▪ Address, ▪ Date and period of the contracted project, ▪ A brief description of the service(s) provided ▪ Level of satisfaction from the client ▪ Contact Numbers. Points allocation:			

	• 5 and more reference letters with all the required elements listed = 5 points • 4 reference letters with all the required elements listed = 4 points • 3 reference letters with all the required elements listed = 3 points • 2 reference letters with all the required elements listed = 2 points • 1 reference letter with all the required elements listed = 1 points • 0 reference letters = 0 points **The NLSA reserves the right to validate all reference letters submitted. The reference letter(s) must be in the form of individual letter(s) from the respective clients.** **If the reference letter does not comply with the requirements, it will not be considered. No appointment letters from prospective clients will be accepted as reference letters.**			
2	**RISK AND COMPLIANCE MANAGEMENT**	30		
	Bidders must provide a minimum of five (5) contactable reference letters of the service provided within the past five (5) years. The name of the organisation at which the Risk and Compliance Management tool was provided: ▪ The component that was used from the tool, e.g. Internal Audit, Risk management, etc. ▪ The letter must be on the company/ organisation letterhead, ▪ Contact Person, ▪ Address, ▪ Date and period of the contracted project, ▪ A brief description of the service(s) provided ▪ Level of satisfaction from the client ▪ Contact Numbers. Points allocation: • 5 and more reference letters with all the required elements listed = 5 points • 4 reference letters with all the required elements listed = 4 points • 3 reference letters with all the required elements listed = 3 points • 2 reference letters with all the required elements listed = 2 points • 1 reference letter with all the required elements listed = 1 points • 0 reference letters = 0 points **The NLSA reserves the right to validate all reference letters submitted. The reference letter(s) must be in the form of individual letter(s) from the respective clients.** **If the reference letter does not comply with the requirements, it will not be considered. No appointment letters from prospective clients will be accepted as reference letters.**			

3	**PROPOSAL SUBMISSION**	40		
	Implementation Methodology The Service provider must provide a detailed implementation methodology that demonstrates a clear, structured, and practical approach to deploying the Internal Audit, Risk, and Compliance Management Software Tool. The methodology should include, at a minimum: 1. **Project Governance** ▪ Detailed project plan, including milestones, deliverables, and timelines. ▪ Roles and responsibilities of the implementation team. ▪ Reporting and communication mechanisms with NLSA project stakeholders. **2. Installation and Configuration** ▪ Step-by-step process for installation of the software. ▪ Configuration plan to align the tool with NLSA's audit, risk, and compliance workflows. ▪ Data migration strategy, if applicable, including validation and reconciliation steps. **3. User Onboarding and Training** ▪ Approach for onboarding NLSA users, including administrators and key stakeholders. ▪ Training plan and materials for five (5) users, covering all modules: Internal Audit, Risk Management, and Compliance. ▪ Support for training evaluation and feedback. **4. System Testing and Commissioning** ▪ Plan for functional testing, integration testing, and user acceptance testing (UAT). ▪ Issue resolution and mitigation approach. ▪ System go-live checklist and commissioning activities. **5. Post-Implementation Support** ▪ Ongoing maintenance and support model, including online support. ▪ Service Level Agreement (SLA) commitments. ▪ Process for software upgrades, security patches, and continuous improvement.			
	TOTAL POINTS		**100**	
	Minimum points to pass this evaluation stage		**70**	

8.3.2 Second Stage: Demonstration

Demonstration of the Software or Tool

Bidders that meet the minimum threshold as per stage 1 evaluation will be invited to conduct a demonstration of the proposed Software/Tool. The demonstration must clearly show how the solution meets the functional and technical requirements outlined in this Terms of Reference, including but not limited to the user requirements listed in the table below.

The demonstration should refer directly to these requirements and illustrate the Software/Tool's capabilities, features, workflows, configuration options, and relevant integrations.

The bidder may refer to the method of demonstration outlined below, which may be conducted physically or via Microsoft Teams, as determined by the Bid Evaluation Committee (BEC).

INTERNAL AUDIT DEMONSTRATION FEATURES		Yes	No
1	The Software/ Tool must be cloud based or has capabilities to be hosted in the cloud.		
2	The Software/ Tool should enable Internal Audit to allocate or assign employees to a specific audit as well as the total hours allocated to the project.		
3	The Software/ Tool should have audit documentation templates/capabilities that allow for documentation of audit projects from planning, fieldwork through to reporting. At a minimum the tool should provide templates for the following: • Planning: working paper templates that enable the auditor to document system description, audit risks, audit objectives, controls, audit procedures including resource planning (team allocation and project hours). • Fieldwork: working paper templates that enable the auditor to document audit results as well as conclusion. Exception/Finding creation capability: The tool should have capability to create audit exceptions/findings and hyperlink/reference them to the relevant working papers containing audit results and conclusion. The exception/finding should contain the criteria/ standard, finding, root cause, impact/risk, recommendation, management comments/Agreed action plans and actions dates		
4	The Software/ Tool should have audit finding tracking capabilities that allow both Internal Audit and the business process owners who own the findings visibility on such findings. Moreover, business units should be able to update status update and attached evidence for resolved findings.		
5	The Software/ Tool should provide for adequate segregation of users within the system, e.g. work paper preparers, reviewers at various levels (Internal Audit specialist (supervisor), Head/ Senior Manager reviews, etc.).		
6	Compliance Management module: dashboards, CRMP, issue tracking, legislation and policy management integrated with audit and risk.		
RISK AND COMPLIANCE MANAGEMENT DEMONSTRATION FEATURES		Yes	No
7	The Software/ Tool should provide for adequate risk analysis and dashboards (e.g. heatmaps and age analysis of overdue findings)		
8	The Software/ Tool should provide for adequate capability to map the risks to the lines of defence in line with Combined Assurance Model		

9	The Software/ Tool should integrate and generate a report on risks, strategic objective, Organizational Performance (KPI)		
10	The Software/ Tool should provide for reminders and escalation to line management when the actions items and mitigations become due		
11	The Software/ Tool should provide for levels of risk assessments i.e. Strategic Risk Assessments, Operations Risk Assessments and Project Risk Assessments		
12	The Software/ Tool should provide for determination and monitoring of risks appetite and tolerance levels		
13	Risk Module integration with audit and compliance for combined assurance		
14	Automated risk scoring and prioritization		
15	Trend analysis and historical reporting		
16	Real-time alerts for new/critical risks		
17	Linking risks to objectives and KPIs		
SECURITY REQUIREMENTS DEMONSTRATION FEATURES		Yes	No
Access management	The Software/ Tool must have a capability to provide the following • Authentication of users through user name and password before a user is granted access to the system. • Enforce standard access control principles such as segregation of duties, role-based access control based on least privilege and need to know principle.		
Audit capabilities	The Software/ Tool must enable the logging of the following activities undertaken by users and systems at a minimum: • Working paper sign offs; • User last logins.		
Audit Tool Hosting	The Software/ Tool should have a capability of being hosted on cloud on either of the following platforms: - Microsoft Azure If the service provider prefers own hosting, the service provider must bear the cost of self-hosting.		
Session Management	It is important to have a stringent mechanism that accurately identifies each user. This ensures that every action they undertake is directly linked to their profile/user. This is to safeguard both user integrity and system security.		

8.3.3 Stage 3: Price Evaluation

Preference Point System

In terms of Regulation 5 of the Preferential Procurement Regulations of 2022/23, Gazette Number 47452 dated 4 November 2022 pertaining to the Preferential Procurement Policy Framework Act, 2000 (Act 5 of

2000), responsive bids will be adjudicated by the State on the 80/20-preference point in terms of which points are awarded to bidders based on: -

- The bid price (maximum 80 points)
- Specific Goals (maximum of 20 points):

The following formula will be used to calculate the points out of 80 for price in respect of an invitation for a tender, inclusive of all applicable taxes.

$$Ps = 80\left(1 - \frac{Pt - P\min}{P\min}\right)$$

Where-

Ps = Points scored for price of tender under consideration;

Pt = Price of tender under consideration; and

Pmin = Price of lowest acceptable tender.

- **Specific Goals (maximum of 20 points): -**

<u>Company Ownership</u>:

- Companies with 100% black ownership will receive 20 points.
- Companies with less than 100% black ownership will receive 10 points.

NB . Submit certified sworn affidavit or BEE certificate as evidence.

Item No.	Pricing Component	Description / Notes	Year 1 (Price Unit)	Year 2 (Price Unit)	Year 3 (Price Unit)
1	Software Licensing Costs	Covers Internal Audit, Risk, and Compliance modules.			
2	Implementation and Configuration Costs	Includes all work related to installing and configuring the software for NLSA.			
3	User Training Costs	Training for a minimum of 5 users across all relevant modules.			
4.	Support and Maintenance Costs	Annual support fees, SLA commitments, and ongoing maintenance.			
5.	Hosting Costs	Costs if bidder proposes self-hosting instead of Microsoft Azure.			
8	**TOTAL (VAT Inclusive)**				

9. ENQUIRIES

All enquiries regarding this tender must be directed to the SCM Office:

For any Bid related enquiries please sent to the following email address quoting the Bid Number. Description as a Reference; kenny.netshiongolwe@nlsa.ac.za OR (012) 401 3017/9700/81