REQUEST FOR INFORMATION

RFI NO: RFI/COP/2025/3
RFI Title: Request for Information for Integrated System of Internal Audit and Governance, Risk and Compliance (GRC)

RFI Objective: The objective of this RFI is to obtain information, functionality and cost of an annually maintained, single integrated system of Internal Audit, Governance, Risk and Compliance to be used for a period of five years.

RFI documents are obtainable from **26 May 2025** from the following websites:

- **Government E-Portal http://www.etenders.gov.za**
- **SABC Website http://www.sabc.co.za/sabc/tenders**

Closing Date: 13 June 2025 at 12H00

For enquiries: E-mail: tenderqueries@sabc.co.za

SOUTH AFRICAN BROADCASTING SABC SOC LIMITED
("The SABC")
REQUEST FOR INFORMATION (RFI)

RFI NUMBER	**: RFI/COP/2025/3**
RFI TITLE	**: Request for Information for Integrated System of Internal Audit and Governance, Risk and Compliance (GRC)**

EXPECTED TIME FRAME

RFI PROCESS	EXPECTED DATES
RFI Advertisement Date	**26 May 2025**
RFI Available from	**Government E-Portal** **http://www.etenders.gov.za SABC Website** **http://www.sabc.co.za/sabc/tenders**
Compulsory Briefing Session	**05 June 2025 at 10h00 – On Teams** **Join the meeting now** **Meeting ID: 382 120 040 323 4** **Passcode: iD9Bp6FP**
RFI Closing Date and Time	**13 June 2025 at 12H00**
Contact details for questions/ queries	RFPSubmissions@sabc.co.za and tenderqueries@sabc.co.za

The SABC retains the right to change the timeframe whenever necessary and for whatever reason it deems fit.

Respondents interested in participating must register their interest by providing company name, contact person, telephone, cell number and email address to RFPSubmissions@sabc.co.za, please indicate RFI number on the subject line. This will ensure that any addenda and clarification to this RFI are communicated to all participants.

Submissions are to be made electronically to the above-mentioned address (RFPSubmissions@sabc.co.za.

PDF Documents will be available on the SABC Website.

Please note that this is a Request For Information and not a Request For Proposal. No award will be made from this request.

REQUEST FOR INFORMATION:

1. DEFINITIONS

1.1 "**RFI**" - a request for information, which is a written official enquiry document encompassing all the terms and conditions of the information in a prescribed or stipulated form.

1.2 "**RFI response**" - a written response in a prescribed form in response to an RFI.

1.3 "**Hosting Partners**" - companies who entered into an agreement with SABC LOC in the areas of application management; application hosting, application service provision, and marketplace hosting are incorporated in this category.

1.4 "**Respondent**" – any person (natural or juristic) who forwards an acceptable RFI in response to this RFI with the intention of being the main contractor should the RFI be awarded to him.

2. CONFIDENTIALITY

All information related to this request for information both during and after completion is to be treated with strict confidence. Should the need however arise to divulge any information gleaned from the service which is either directly or indirectly related to the SABC, written approval to divulge such information will have to be obtained from SABC.

The Respondents must ensure that confidential information is: maintained confidential; not disclosed to or used by any unauthorised person; so as to prevent any disclosure or unauthorised use with at least the standard of care that Respondents maintain to protect their own confidential information; only used for the purpose of considering and responding to this RFI; and not reproduced in any form except as required for the purpose of considering and responding to this RFI. Respondents must ensure that: access to confidential information is only given to those of its partners, officers, employees and advisers who require access for the purpose of considering and responding to this RFI; and those partners, officers, employee and advisers are informed of the confidential information section and keep that information confidential. This RFI remains at all times the property of the SABC. No rights other than as provided in this RFI and in respect of the confidential information are granted or conveyed to bidder/s

NAME OF Respondent:

_____

PHYSICAL ADDRESS: _____

_____

Respondent's contact person: Name : _____

Telephone : _____

Mobile : _____

Fax.: _____

E-mail address: _____

The manner of submission of the RFI

3.1 Respondent shall submit RFI response in accordance with the prescribed manner of submissions as specified below.

3.2 Respondent shall submit one (1) electronic copy. Electronic copies may be e-mailed to: RFPSubmissions@sabc.co.za and tenderqueries@sabc.co.za

3.3 All additions to the information documents i.e. appendices, supporting documentation, photographs, technical specifications and other support documentation covering suggested solutions etc. shall be neatly bound as part of the schedule concerned.

3.4 A compulsory briefing session will be held on Teams, from 10h00.

Join the meeting now
Meeting ID: 382 120 040 323 4
Passcode: iD9Bp6FP

3. BACKGROUND

Section 51 (1)(a)(i) of the Public Finance Management Act No. 1 of 1999 (as amended), prescribes an effective and efficient system of risk management, amongst others, which the Accounting Authority must implement. This would also imply the electronic system that enables the recording of data, processing, storage and the reporting of information to be used for decision making.

Procurement of an electronic system will assist the SABC not to use manual and error-prone avenues through Microsoft applications like MS Word and MS Excel. High-level features:

Governance, Risk and Compliance (GRC) comprises of these departments:

a) Enterprise Risk Management (ERM),
b) Compliance Management,
c) Internal Control and
d) Business Continuity Management (BCM).

These GRC departments are currently using separate and distinct electronic application systems of input, processing, output and reporting. Internal Audit has separate system from GRC.

Internal Audit's Audit Plan is risk based and the non-integration of its system together with that of the GRC function, may have caused extra effort of sourcing and providing information between these two related divisions when there are systems in the market which may enable seamless processes and procedures for the same purpose with less effort, cost and time saving.

4. Scope

The scope of this RFI should comprise of these areas:

a) Internal Audit Management,
b) Enterprise Risk Management (ERM),
c) Compliance Management,
d) Internal Control Management and
e) Business Continuity Management (BCM).

5. BUSINESS REQUIREMENTS

5.1 Mandatory System Requirements

The following mandatory requirements must be embedded in the system:

a) Integration of internal audit management and GRC functions.
b) Ability to capture, edit, store, display, process, retrieve and report information anytime, anywhere based on the Active Directory (AD) access granted to the user per segregated duties assigned per division or department.
c) Ability to provide audit trails on log-ons, edit and display access/activities and these audit trails should be able to be exported to a report.
d) Provide archiving functionality for the duration of the contract and enable migration of archived information to another platform.
e) Data insights and dashboards.

f) Reports must be able to be generated into Adobe Reader documents and be exportable to MS Outlook, MS Word, MS Excel and MS PowerPoint.
g) System upgrade should be done by the service provider as and when needed at no extra cost, remotely or by personal consultation.
h) Enable remote support by the service provider in the system's SABC server.
i) The performance and response time for the system must be excellent when connected to a network cable and good when working remotely though data lines/VPN.
j) Capacity to handle unusual and peak loads.
k) Manage more than 100 logged in users simultaneously.
l) Must be able to generate graphical reports consistent with data processed and information stored in the system and with information from previous periods (data snapshots).
m) Ability to generate customized reports, dashboards, technical and analytical standard reports.
n) Must be able to perform automatic precise calculations e.g. inherent risk and residual risk and overall control effectiveness. And any other data aggregation calculation.
o) Compulsory import of data take-on.
p) Uploading of evidence in any electronic and/or Microsoft application system.

The following are the requirements which the system should meet:

5.2 INTERNAL AUDIT

The ideal audit management technology solution should include but not limited to the following features:

a) Comprehensive Audit Lifecycle Management: Manage the entire audit process from planning to reporting and follow-up including data analytics.
b) Risk Assessment Tools: Dynamic capabilities to identify and prioritize risks associated with audits.
c) User-Friendly Interface: An intuitive design that simplifies navigation and reduces the learning curve.
d) Collaboration Features: Tools for teamwork, including shared workspaces and real-time updates.
e) Automated Workflows: Automation of repetitive tasks like scheduling and report generation.
f) Reporting and Analytics: Advanced reporting capabilities with customizable dashboards for clear insights.
g) Document Management: A centralized repository for storing and managing audit-related documents and the ability to manage document version at a past date and time.
h) Integration Capabilities: Seamless integration with other systems (e.g., ERP, compliance tools) to streamline workflows.
i) Mobile Access: Support for mobile devices, allowing auditors to work on the go. (View and approvals)

j) Compliance Tracking: Tools to ensure adherence to regulatory requirements and internal policies.
k) Customizable Templates: Pre-built templates for audit plans, checklists, and reports that can be tailored.
l) Audit Trail and Security: Robust security features to protect sensitive data, along with an audit trail for tracking changes.
m) Feedback and Improvement Mechanisms: Features to capture feedback post-audit for continuous improvement.

These features should collectively enhance the efficiency and effectiveness of the audit process, ensuring GIA can maximize the value of their audits.

Other desirable traits should be incorporation of the latest technologies such as Artificial Intelligence and cloud, data analytics etc.

5.3 GOVERNANCE, RISK AND COMPLIANCE

Over and above the standard functionality on input, processing, output and reporting of the system, it must be able to have the following:

GOVERNANCE

5.3.1 GOVERNANCE: BUSINESS CONTINUITY MANAGEMENT

Business Continuity Threat Risk Assessment

a) Ability to capture the identified business continuity threats in the process of developing a threat business continuity risk assessment.
b) Ability to assess the likelihood and the impact on a scale of 5 x 5 of such threats should they take place.
c) Automatic likelihood and impact analysis heat map and risks prioritised in the same order.
d) Ability to draw a business continuity threat risk register at a current or past date.
e) Ability to capture, review and update the captured mitigation strategies.

Business Impact Analysis (BIA)

a) Ability to capture business impact analysis items in a template format, e.g. business functions, business processes, operational impact ratings, period of disruption, etc.
b) Ability to capture the business impact analysis strategies.

Development of a Business Continuity Plan (BCP)

a) Ability to capture the outlined procedures for maintaining business operations during disruptions.

b) Ability to assign roles and responsibilities to Business Continuity Management team members during disruptions so that they can resume operations.
c) Ability to capture the business continuity plan per division or province from the BIA.
d) Ability to capture the BCP.

BCP Testing and Exercising

a) Ability to schedule and capture executed testing exercises performed.
b) Ability to send reminders through email, the deadline for BCM testing and exercising.
c) Ability to escalate non-attended emails by BCM process owners.

Communication and Reporting

a) Ability to produce a business continuity threat risk register.
b) Produce the BIA report.
c) Produce a BCP report.
d) Produce a BCP testing and exercising report.
e) Ability to use multi-purpose criteria for drawing reports.
f) Ability to draw reports for a present and a past date.
g) Produce reports through dynamic dashboards, graphical presentations and statistical comparative tables.
h) Ability to send messages through emails to critical stakeholders.
i) Standard reports within the system.
j) Ability to provide customisable reports and communication tools where possible.

5.3.2 GOVERNANCE: INTERNAL CONTROL MANAGEMENT

Gap Report Analysis

5.3.2.1 Ability to develop and generate a process flow.
5.3.2.2 Develop the risk and control matrix (RACM).
5.3.2.3 Capture the gap analysis.
5.3.2.4 Capture the gap analysis recommendations.
5.3.2.5 Extract the gap report which includes the gap analysis recommendations.

Control Self-Assessment

a) Input internal controls as identified in the gap report into the system per business processes.
b) Assign internal controls recommendations to internal control owners.
c) Link internal controls recommendations identified in the gap report to business activities within the business process.
d) Internal controls owners must be able to indicate their status of implementation of recommendations made as per the gap report.

e) System must be able to process the input captured by the internal control owners to the recommendations of the gap report.
f) Internal control user must be able to indicate if actioning of the recommendations made is not started or completed.
g) The control owner must be able to assess the control and indicate if the control is adequate and effective.
h) The system must be able to indicate if the recommendation is in progress.
i) System must be able to send an email notification of the existing gap report recommendations to the internal control owner regarding the deadline at which the task must be completed.

Monitoring and Reporting

a) Extract a performance report listing the business process, gap report recommendations, input from internal control owner against the gap report recommendations and indicate status if not started, in progress or completed.
b) The report must be able to indicate if the recommendation assignment is in progress, completed or overdue.
c) Display recommendation statistical report in a graphical and/or dashboard format.
d) Provide a control repository displaying statistics on effectiveness, lagging, weak, etc. at high level.

5.3.3 ENTEPRISE-WIDE RISK MANAGEMENT

5.3.3.1 Compliance with Risk Management ISO 31000 standard and the COSO risk methodology.
5.3.3.2 Adherence to the risk management process.
5.3.3.3 Risk Profile input (capturing).
5.3.3.4 Risk Profile assessment (inherent risk, control effectiveness and residual risk assessment).
5.3.3.5 Status update of risk mitigation.
5.3.3.6 Ability to draw multiple risk *registers* from one screen input criteria.
5.3.3.7 Ability to draw multiple risk *reports* from one screen input criteria.
5.3.3.8 Ability to conduct the risk maturity survey/assessment.
5.3.3.9 Adobe Reader criteria selective, exportable to MS Excel, Ms Word and MS PowerPoint risk *registers* at project, department, division, provincial, and at corporate level.
5.3.3.10 Adobe Reader criteria selective, exportable to MS Excel, Ms Word and MS PowerPoint risk *reports* at project, department, division, provincial and corporate level.
5.3.3.11 Internal staff contact database update.
5.3.3.12 Other critical risk reports.
i. Dynamic Risk Dashboard.
ii. Top 10 inherent risk report in tabular and graphical presentation.
iii. Top 20 inherent risk report in tabular and graphical presentation.

iv. Criteria selective risk mitigation/task report with status on progress to date
v. Risk mitigation statistics in the risk mitigation report.
vi. Risk per page report with statistical and graphical presentation.
vii. Criteria selective residual risk report.
viii. Criteria selective control effectiveness report.
ix. Ability to draw risk registers and reports as at specific past dates or periods.
x. Dynamic risk maturity report.
xi. Risk ranking setup, input and reporting capability.
xii. Risk appetite and tolerance input capability and reporting.
xiii. Risk indicator setup, input and reporting capability.

5.3.3.13 Ability for internal customisation of reports based on available criteria selection.

5.3.3.14 Access and edit audit trail reports.

5.3.3.15 System administrator, user and audit functions.

5.3.3.16 Ability to allocate access/authorisation through active directory process.

5.3.3.17 System support and enhancement capabilities.

5.3.3.18 User query handling, consultative development and implementation by service provider.

5.3.3.19 Standard customised risk registers, functionality and reports.

5.3.3.20 The user or report extractor must be able to select from criteria, a report for current and past dates or periods, multiple divisions and business units from one screen, amongst other report criteria.

5.3.4 COMPLIANCE

a) The system must have the ability for all Acts and regulations that are relevant to the SABC to be pre-loaded on the compliance system. These should be accessible directly from the system, without having to interface with other Act service providers.
b) It must provide built-in Compliance Risk Management Plans (CRMPs); these are pre-populated with the regulatory requirements in the format prescribed by the Compliance Institute of Southern Africa.
c) It must have extensive reporting capabilities with dashboards, including but not limited to percentages of compliance per Act, division, etc.; percentages of responses to monitoring of legislation requirements, etc.
d) It must provide the functionality for monitoring compliance with regulatory requirements.
e) It must have built-in workflow processes to allow the flow of Compliance Risk Management Plan between Compliance team and Compliance champions (Users) in various business units.
f) It must have a keyword search functionality that enables the user to search for keywords across all the Acts and Compliance Risk Management Plans.
g) It must provide functionality for the updating of Acts, automatically update the Acts as and when they are captured into the system, thereafter, indicate to all

users of the latest update after successfully uploading (Knowledge Base or Library).

h) The system must have archived functionality for the archiving of Acts, Compliance Risk Management Plans, compliance monitoring results, etc.
i) The solution must use inhouse (hybrid) cloud storage and services. It must cater for scalability and security features.

5.4 TECHNOLOGY REQUIREMENTS

The following are the technical requirements to host the server to support the system:

a) Must be certified to execute in a VMWare environment.
b) Minimum Disk capacity required must be specified.
c) Minimum RAM and processor capacity required must be specified.
d) Cloud-hosted solutions will be considered but must be costed as separate cost to application.
e) If cloud-based solution, then a point in time backup as a service with daily, monthly and yearly backup must be included in the proposal as a separate cost.

6. Bidders are requested to provide a quotation for the system they will be presenting.

7. GENERAL INFORMATION

Enquiries in respect of this RFI should be addressed to:

Tender office

E-mail: tenderqueries@sabc.co.za

All queries to be e-mailed.

8. RFI SUBMISSION INFORMATION

SUBMISSION DETAILS:

RFI responses should be submitted to the below address.

Electronic copies may be emailed to RFPSubmissions@sabc.co.za and tenderqueries@sabc.co.za

END OF THE REQUEST FOR INFORMATION DOCUMENT