South African Revenue Service

SARS REQUEST FOR INFORMATION

SARS RFI 04/2025

THE IMPLEMENTATION OF AN INTEGRATED GOVERNANCE, RISK AND COMPLIANCE (GRC) SOLUTION

BUSINESS REQUIREMENTS SPECIFICATION

TABLE OF CONTENTS

Implementation of Integrated Governance, Risk and Compliance (GRC) Solution

This RFI document sets out the business requirements that SARS has to gather information from interested industry players on market for Integrated Governance, Risk and Compliance (GRC) Solution.

1. USAGE OF TERMS IN THIS DOCUMENT

1.1References to Other Documents in the RFI pack

- *RFI Main Document*

1.2Glossary Table

The capitalised terms in this document appearing in the glossary table below will have their corresponding meanings. The Vendor/Supplier is referred to the *RFI Main Document* for the use and meaning of capitalised terms generally in the RFI pack.

Term	Meaning
SARS	South African Revenue Services
GRC	Governance, Risk and Compliance
BRS	Business Requirement Specification
LSP	License Software Supplier
LSM	License Software Management
SQL	Structured Query Language

2. INTRODUCTION

This Business Requirement Specification (BRS) sets out the requirements that SARS has identified for an integrated Governance, Risk and Compliance (GRC) Solution, which must be considered by the Bidder in compiling a proposal. The required solution should be aligned to the PFMA and other key South African legislation and best practices such as ISO 31000:2018, ISO 37000: 2021, ISO 37301:2021, King V and other leading practices such as the Generally Accepted Compliance Practice Framework in Southern Africa.

SARS has undertaken to simplify the GRC processes by adopting an integrated approach to managing risks, improving decision-making and monitoring compliance to relevant internal and external regulations. To support this approach, the GRC unit requires a comprehensive solution to integrate the GRC functions into a single platform, to improve efficiency to the management of risk exposures while ensuring adherence to laws and regulations and cultivating a proactive risk culture. The initiative is essential to enable the achievement of organisation key results (OKRs) and for maintaining the organization's reputation, safeguarding its assets, and ensuring sustainability.

3. BUSINESS REQUIREMENTS

3.1. GENERAL REQUIREMENTS FOR THE GRC TOOL

- Dashboard display and reports.
- Incident management
- Voting, survey, questionnaire and workshop functionality
- Data analytics - predictive analysis
- Risk reports
- Compliance Reports
- Library e.g. Risk library, control library
- Control effectiveness and adequacy reporting
- Allocation of ownership (Risk owner, Action Owner, Control Owner)
- Automated notifications and Escalation functionality
- Internal control repository

3.2. RISK MANAGEMENT REQUIREMENT

- Risk management process aligned to international standards (e.g. ISO31000: 2018).
  - ❖ Context/Objective setting
  - ❖ Risk identification
  - ❖ Risk analysis – quantitative and qualitative
  - ❖ Risk evaluation
  - ❖ Risk treatment
  - ❖ Risk monitoring
  - ❖ Risk prioritization
- Built-in or customised risk registers
- Risk Appetite and Risk Tolerance levels setting
- Key Performance Indicator (KPI) and Key Risk Indicator (KRI) functionalities
- Risk categorisation
- Objective prioritization

3.3. GOVERNANCE REQUIREMENTS

- Automated workflows – streamlining processes and reducing manual processes
- Reporting – generate customised reports and audit trails
- Collaborations – enabling collaboration and communications with stakeholders
- Integration – ability to integrate with other systems for sourcing information
- Real time monitoring and dashboards – ability to monitor in real time governance controls and failures
- Policy management – creating and managing policies.
- Enterprise Governance Guideline aligned with ISO 37000: 2021 and King V
- Information Technology Guideline aligned with COBIT:2019 and ISO 38500:2024
- Policy assessment functionality
- Control adequacy and efficiency assessment functionality
- Control monitoring and reporting

3.4. REGULATORY COMPLIANCE REQUIREMENTS

- Regulatory Compliance Guideline aligned with ISO 37301: 2021 and the Generally Accepted Compliance Practice Framework GACP
- Built-in or customised Compliance Risk Management Plans (CRMPs)
- Compatibility with Legal Software products. e.g. Lexis Nexus, Page Law, Juta
- Notifications for new legislations
- Monitoring of internal controls adequacy design and effective implementation. legislation, regulations, policies and procedures.
- Identification and maintenance of the compliance universe and risk profile as defined.
- Integrated methodology to risk assess applicable regulatory requirements
- Reporting on monitoring and all aspects of the compliance process.

3.5. USER/LICENCE REQUIREMENTS

- Provide licence structure information
  - ❖ Administration access rights
  - ❖ Access to full module (Capture, edit, Update all information, reporting)
  - ❖ Minimal access rights: View, update actions, re-rate risks