ANNEXURE E:

BUSINESS REQUIREMENTS LIST

Table of Contents

1. MANAGEMENT SUMMARY 3
2. BUSINESS DRIVER 4
3. BUSINESS OBJECTIVES 4
4. ACCRONYMS AND GLOSSARY 5
5. SCOPE 5
5.1. BUSINESS AREA SCOPE 5
5.2. SOLUTION SCOPE 6
5.3. TERMS OF REFERENCE ..... ERROR! BOOKMARK NOT DEFINED.
5.4. ASSUMPTIONS 6
5.5. DEPENDENCIES 6
6. BUSINESS REQUIREMENTS 7
6.1. FUNCTIONAL REQUIREMENTS 7
6.2. INFORMATIONAL REQUIREMENTS ..... ERROR! BOOKMARK NOT DEFINED.
6.3. NON-FUNCTIONAL REQUIREMENTS ..... ERROR! BOOKMARK NOT DEFINED.

1. MANAGEMENT SUMMARY

Sasria SOC Limited is a financial institution and a state-owned company that offers special risk insurance. The organization is faced with a lot of risks externally such as public disorders and commotion, riots and strikes, etc. which could potentially impact the organization should Sasria get an influx in claims resulting from those actions. There are additional risks such as non-life underwriting risk, credit risk, market risk, operational risks, and strategic risks. Sasria is also required to comply with PFMA requirements as a state-owned company.

The risk management division is responsible for taking measures to identify, assess, monitor and report on the risks that affect the organization both externally and internally to minimize their likelihood by putting controls in place as efforts to mitigate those risks.

Currently, Risk management value chain is using the Isometrix system which was implemented 2014. The system has limited functionality and does not cater for all the required risk management functions as per the standards and requirements of Risk Management.
This creates inefficiencies as manual interventions must be used alongside the system which ultimately creates additional work instead of reducing it.
Furthermore, the system is on a broad perspective when coming to risk and largely caters for industries within the mining and manufacturing space and predominantly focuses on Health and Safety Risk.

There is a need for the Risk Management division to have an efficient tool that will cater for risk that is particular to our business in Sasria and the short-term insurance industry. Business also wants to partner with a service provider that has understanding of the risk management practice, its landscape, emerging trends, challenges, opportunities, and advise on new and innovative products, so that they can evolve and perform their duties better.

Looking at the identified inefficiencies stated above and the business need, it is imperative that the organization gets a new solution that will support the Risk Management value chain. This tool will increase efficiency in data capturing, reporting, workflow management, document management and improve processes.

2. BUSINESS DRIVER

The driver for the Risk Management project comes from Sasria's five-year strategy for the period beyond 2020 – a renewed focus on customer centricity, **efficiency**, sustainability, and social impact to provide superior service, relevant and appropriate products.

3. BUSINESS OBJECTIVES

The business objectives for the Risk Management tool are as follows:

Figure 2: Risk Management Tool Objectives

4. ACCRONYMS AND GLOSSARY

The table below shows the abbreviations and descriptions:

Term/Abbreviation	Definition
ERP	Enterprise Resource Planning
BCM	Business Continuity Management
IT	Information Technology
KRI	Key Risk Indicator
PFMA	Public Finance Management Act
RCSAs	Risk and Control Self-Assessments

5. SCOPE

5.1. BUSINESS AREA SCOPE

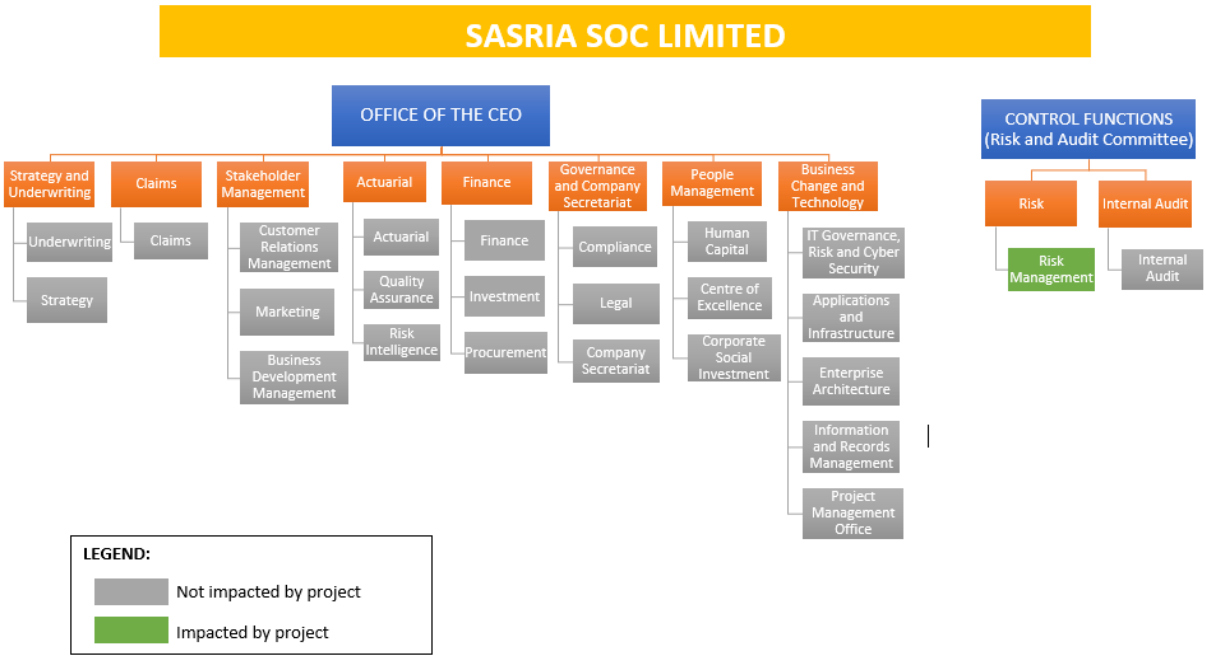

Figure 3: Business Area Scope

5.2. SOLUTION SCOPE

The scope of the solution is positioned as per the diagram below:

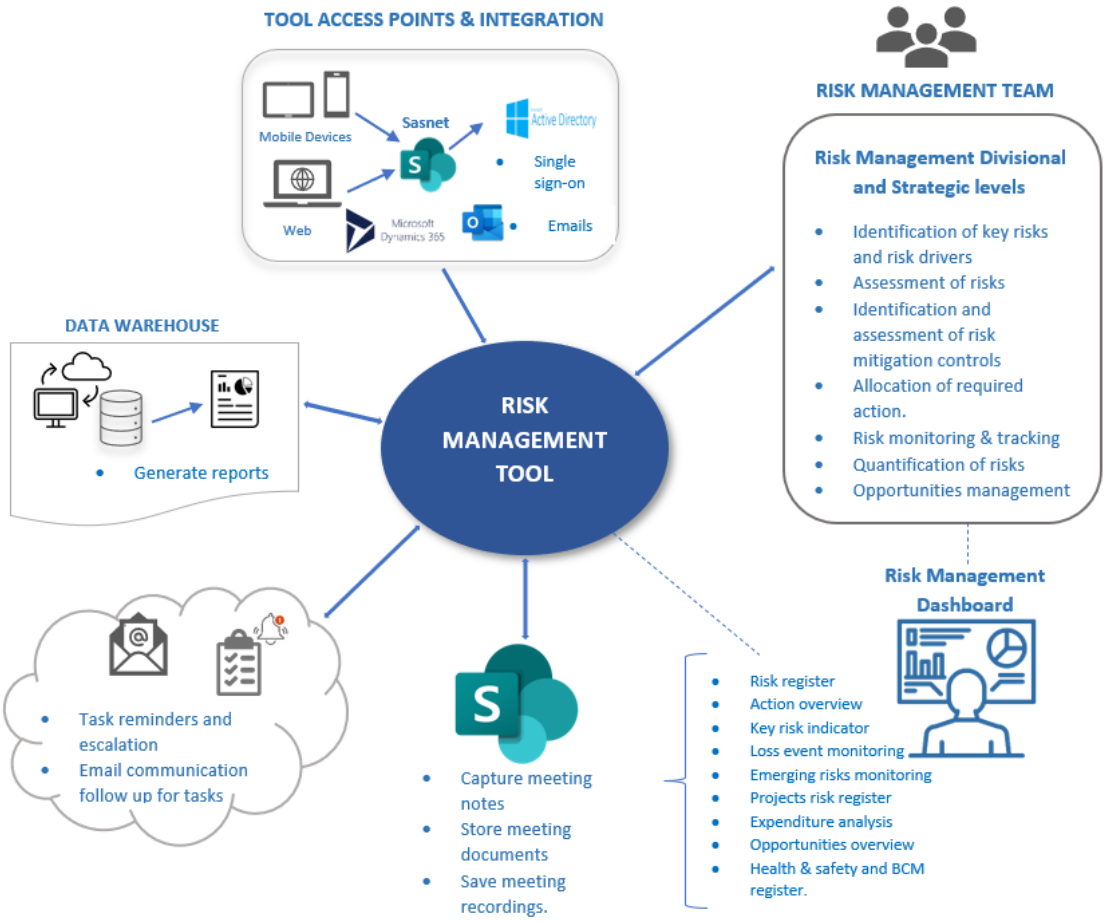

Figure 3: Risk Management Tool Solution Scope

5.3. ASSUMPTIONS

- The Risk Management tool will cater for the Risk Management requirements.
- All required resources for the project will be available.
- The Risk Management tool will be customizable to Sasria's requirements. Minimum customization preferred.

5.4. DEPENDENCIES

- The dependency is on the service provider that will be appointed to be able to deliver the project as per the business requirements

6. BUSINESS REQUIREMENTS

Use the response column to indicate whether the proposed solution has:

- **F =** If the solution already has this feature Out of the box
- **M =** If the solution requires minor customisation/configuration to cater for this requirement
- **D =** If the solution requires major development to cater for this requirement
- **TP =** If the solution requires integration with another tool to cater for this requirement
- **N/A =** If this requirement cannot be catered for.

Use the comment column to indicate how this requirement will be met by your proposed solution.

6.1. FUNCTIONAL REQUIREMENTS

REF	Requirement	Requirement Description	F/M/D/TP/NA	Comments
Risk Management Requirements				
FR1	**Risk management process**	The solution must enable risk management capabilities (stated below) at Divisional and Strategic Levels. At **Divisional** level, the solution must have the following capabilities (RCSA): • Identification of key risk events • Assessment of inherent risks • Identification of risk drivers		

		• Identification of mitigating controls • Assessment of mitigating controls • Assessment of residual risks • Allocation of required actions • Monitoring and reporting; and • Quantifications of risks at a divisional level. This should also include opportunities management as follows: • Identification of opportunities • Assessment of opportunities • Management of opportunities • Monitoring of opportunities and • Quantification of opportunities. At **Strategic** level, the solution must have the following capabilities: • Identification and assessment of strategic risks and opportunities. • Identification and assessment of mitigating controls • Measurement of strategic risks • Monitoring and management of strategic risks and opportunities • Reporting of strategic risks and opportunities; and • Quantification of risk and opportunities at a strategic risks level.		
FR2	**Key Risk Indicator**	The solution must have the key risk indicator capability that must include the following functions:		

		• Development and approval of Key Risk Indicators • Key Risk Indicator assessment and validation • Key Risk Indicator analysis and monitoring • Key Risk Indicator reporting		
FR3	**Loss event monitoring**	The solution must provide the capability for monitoring losses, performing root cause analysis, monitoring controls and improvements. The following functions must be executed on the tool: • Identification and recording of loss events • Investigation of the loss event/root cause analysis • Identification of additional controls/improved controls • Monitoring of control implementation • Loss analysis • Reporting of losses The solution must also have the capability to classify losses into categories i.e., actual loss, potential loss, near miss, irregular expenditure, fruitless and wasteful expenditure, theft, fraud, health, and safety.		

FR4	**Emerging risks monitoring**	The solution must provide the capability for monitoring emerging risks and enable Risk Management to capture the following:
		• Identification and assessment of emerging risks
		• Emerging risk assessment
		  ○ Emerging risk rating
		  ○ Expected period when the risk will occur.
		• Monitoring, mitigation, and reporting		

FR5	**Risk dashboards**	The solution must include the following risk management dashboards: • Action overview • Inherent and residual risks overview (Heat maps) • Risk register (both inherent and residual risks and linked to controls) • KRI overview (including KRI analysis) • Loss event overview (including loss event analysis) • Irregular and fruitless and wasteful expenditure overview (Including analysis of expenditure) • Project risks and opportunities register/overview • Opportunities overview; and • Emerging risks register • Baseline Health and Safety Risk Register • BCM Risk Assessment Register The dashboard must be configurable for updates when business needs to change them.		
FR6	**Apply risk taxonomy model**	The solution must allow Risk Management to use the risk taxonomy model that breaks down a risk as per the set categories and levels. The 3 risk taxonomy levels and categories must be as follows: **Level 1:** Risk Areas i.e., Strategic, Underwriting, Market (including Liquidity), Operational (Including regulatory), Credit & Counterparty risks. **Level 2:** Sub-category of what is selected in level 1. E.g., Expenses, Premium, Process failure, etc.		

		Level 3: A further sub-category of what is selected on level 2. Level 3 will only be available if the Operational risk category is selected in level 1, if any other category is selected then the categorization will end at level 2.		
FR7	**Project risk management**	The solution must provide the capability to manage the project risk management module and do the following functions: • Identification of key risk events • Assessment of inherent risks • Identification of risk drivers • Identification of mitigating controls • Assessment of mitigating controls • Assessment of residual risks • Allocation of required actions; and • Monitoring and reporting. The solution should also include opportunities management as follows: • Identification of opportunities • Assessment of opportunities • Management of opportunities; and • Monitoring of opportunities.		
FR8	**Insurance management**	The solution must allow Risk Management to manage the insurance management risk module as follows: • Annual renewal of insurance policies • Renewal forms • Asset replacement values and insurance cover limits		

		• Receipt and comparison of insurance quotes • Sign-off of recommendation of final quote • Endorsement of new asset cover • Monthly Fixed Asset Register Review; and Claims process.		
FR9	**Health and Safety**	The solution must enable Risk Management to manage health and safety results and reports for the following functions: • Fire alarm/gas system testing and servicing • Evacuation • Shelter-in place • Health and Safety incident management • Health and Safety Inspections • Annual staff Health and Safety Training • Health and Safety trainings for H&S Reps • Baseline Health and Safety Risk Assessment		
FR10	**Business Continuity Management (BCM)**	The solution must enable Risk Management to handle BCM module risks by performing the following tasks: Business Impact Analysis (BIA) and Risk Assessment (RA): • Identification of time critical processes and functions • Establishment of Maximum Tolerable Periods of Disruption (MTPD) • Setting of Recovery Time Objectives (RTO); and • Setting of Recovery Point Objectives (RPO). Design • Verification of requirements of the BIA		

		• Approval of the BIA by Executives/Line Management Implementation • Emergency Response Plan • Business Continuity Plan • IT Disaster Recovery Plan; and • Crisis Management Plan Validation • Exercising and testing of BCM plans • Post exercise reports • Actions to address gaps. Maintenance Departmental BCM documents		
FR11	**Risk Meetings**	The solution must allow Risk Management to capture Annual Workshops and Monthly Risk Champion meetings notes and store meeting recordings and documents at a central place on the tool. The solution must also allow Risk Management to send email communication with the stored information and documents. The uploaded documents must be downloadable as well. The meeting notes and documentation may include the following: • Matters arising • New developments and projects • Emerging Risks		

		• New contracts and contract management risks • Update on KRI monitoring • Changes to divisional risk register • Open and overdue actions • Losses, near misses and potential losses • Strategic risks and objectives • Changes to BCM documentation		
FR12	**Combined Assurance**	The solution must allow Risk Management to capture quarterly combined assurance monitoring information. The information must include: • Combined assurance plan • Combined assurance level.		
FR13	**Bow-tie analysis**	The solution must enable Risk Management to use the bow-tie analysis method to manage risks and controls. The analysis must include the following activities: • Identify a material risk event • Identify root causes of the risk event • Identify preventative measures to mitigate against the root causes • Identify additional measures that should be implemented • Identify potential impacts and consequences • Identify mitigations to address the negative risk impacts • Identify additional measures that should be implemented.		

FR14	**Provide system templates**	The solution should provide standardized templates for different functions/areas. The templates must be accessible to all authorized system users. These templates include reporting templates.		
FR15	**Admin function**	The solution must have an administrative function where the selected business stakeholders will have access to it and be able to make updates to the content of the tool that is configurable for change.		

6.2. INFORMATION REQUIREMENTS

REF	Requirement	Requirement Description	F/M/D/TP/NA	Comments
IR1	**Tasks, notifications, and escalations**	The solution must have a task and scheduling function which must alert users when Risk Management tasks need to be performed and include automated escalations as per the set SLA controls. Users must be notified on the tool if there's updates on the tasks and any tasks due.		
IR2	**Send automated emails for task reminders and feedback.**	The solution must be able to send reminders and feedback on tasks to all relevant stakeholders via email. The email must include task details and due dates.		
IR3	**Send manual emails**	The solution must include functionality for Risk Management to be able to send manual emails of the risk information, results, and reports as they proceed with the risk management work.		
IR4	**Reporting**	The solution must have a reporting function which Risk Management can use to generate Monthly, quarterly, and ad-hoc reports. The report must include the following: • Summary of risk events and top risks • Required actions against key risk exposures • Summary of project risks and mitigations • Update on open and overdue actions • Material emerging risks • Emerging risk watchlist • Strategic risks monitoring • Strategic opportunities and monitoring		

		• Risk appetite and profile monitoring • Underwriting, market and credit risk reporting • Losses, near misses and potential losses • Key risk indicator monitoring • Internal insurance • Business continuity management activities • Health and Safety Activities		

6.3. NON-FUNCTIONAL REQUIREMENTS

6.3.1. MINIMUM SERVER AND APPLICATIONS REQUIREMENTS

- **SERVER REQUIREMENTS**

Requirement	Requirement Description	F/M/D/TP/NA	Comments
Operating System	Windows Server 2018 R2		
.NET Framework	Latest .NET Framework		

- **DATABASE SERVER REQUIREMENTS**

Requirement	Requirement Description	F/M/D/TP/NA	Comments
Operating System	Windows Server 2016 R2		
Database	Microsoft SQL Server 2019 standard edition		
Hosting	Cloud-based / SaaS		

- **REQUIREMENTS FOR THE APPLICATION WORKSTATION**

Requirement	Requirement Description	F/M/D/TP/NA	Comments
Operating System	Windows 10		
.NET Framework	Latest .NET Framework		
Brower	Latest browsers….IE, Chrome, Safari & Edge		

6.3.2 OPERATIONAL REQUIREMENTS

Ref	Item	Description	F/M/D/TP/NA	Comments
NFR1	Accessibility	System should be accessible using Desktop and both Android and iOS mobile devices (Cell phones/Tablets) either by using network cable, WIFI and/or from 3G to 5G.		
NFR2	Response time	Front-end / host / back end: max 3 seconds.		
NFR3	Cater for large volumes of files	Solution to cater for large volumes of files of any format as attachments.		
NFR4	Cater for different data types	The solution should be able to read the documents uploaded on the system and allow different file formats for documents, emails, files and images such as but not limited to the following: doc, docx, xls, xlsx, pdf, png, jpg, jpeg, ppt, pptx, etc.		

6.3.3. SECURITY AND PRIVACY

Ref	Item	Description	F/M/D/TP/NA	Comments
NFR5	User Group Definitions	The system should be able to distinguish between authorized and non-authorized users. Only users with access to the Risk Management System should be allowed to access, view, and edit information according to their access levels. The access permissions for system data may only be changed by the system's data administrator. There will be a pre-defined set of groups that users can be assigned to. At any one time, there will be at least one user that belongs to the Administrator group. The user assigned to be the Administrator will then create and assign users to the defined groups.		
NFR6	Role-based Access control	Windows Client An active directory user object is associated with the Risk Management System user allowing for a Single Sign-On yet still providing granular permission-based access control to functionality in the application. Web/ Mobile Client The system must implement access control through access control dialogs with external users. Users must supply credentials in the form of a username and password.		
NFR7	Authentication	Windows Client		

		The Risk Management System must make full use of Windows Authentication and Active Directory Services to control user access to the database and the application.		
NFR8	Database Security	Windows Client The database must be secured by allowing only authenticated Windows users access to the data. SQL authentication must be disabled to provide extra security. No access to any native data is possible unless it is done through the application. Web/Mobile Client The database is secured by only allowing the Web application to access data through a service account which forms part of Windows authentication.		
NFR9	Confidentiality	All data should be treated properly so that only authenticated users can access or modify the data. Passwords shall never be viewable at the point of entry or at any other time.		
NFR10	Data Loss (Disclosure of information about individuals or entities)	Security policies must be enabled to prevent leakage/disclosure of sensitive information to unauthorized users. Users must be trained on the functionality of the system to understand their responsibilities to safeguard sensitive information.		
NFR11	Data encryption	All data flows to and from external entities should be encrypted.		

NFR12	Data Integrity (Data Corruption)	All the information flowing within and across the Risk Management System modules should be the same and not be altered throughout its lifecycle. The information must not be compromised during changes and must still be intact after the changes or updates to the Risk Management System. Only authorized users must be able to edit or make changes to data.		
NFR13	Implementation and development lifecycle	The application should be accustomed and have been tested for input sanitisation and other flaws listed on the Open Web Application Security Project (OWASP) Top 10 i.e. Proof of a favourable application security testing report to be provided. All dependencies of the application must be enlisted in a software bill of material (SBOM).		
NFR14	Access Reports	Reports on user access and activities must be available to monitor policy violations.		

6.3.4. AUDIT TRAIL

Ref	Item	Description	F/M/D/TP/NA	Comments
NFR15	Audit trail	Enable transparent audit trail in the system, audit trails must be created for all user actions performed. The following information will be recorded in the audit log: • Username • Date and time of action • Field name • Before value • After value • Effective date • Source (Direct/Web/Mobile App) The audit logs are stored in a separate database.		
NFR16	File versions	The solution must store all the file versions (including previous versions) for stored documents.		

6.3.5. RELIABILTY

Ref	Item	Description	F/M/D/TP/NA	Comments
NFR17	Availability (Percentage of time available)	97 to 98 % Considering the updates/upgrades done on the system.		
NFR18	Hours of Use	• Monday to Friday: 00h00 – 23h59 • Saturday: 00h00 – 23h59 • Sunday and public holiday: 00h00 – 23h59		
NFR19	Maintenance Hours	• Sunday: 10h00 –23h59		

NFR20	Mean Time to Repair (MTTR)	• Critical: 1 hour • High: 2 hours • Medium: 3 hours • Low: 4 hours		

6.3.6. RECOVERABILITY

Ref	Item	Description	F/M/D/TP/NA	Comments
NFR21	Audit Trail Failure	If the audit trail function fails before the user saves updates to the transaction, the system shall be able to store and recover all changes made in up to one minute prior to the failure.		
NFR22	Update failure	When an update failure is detected, all updates performed during the failed session shall be rolled back to restore the data to pre-session condition.		
NFR23	Roll-back	All data recovered in a roll-back condition shall be recorded for use in forward recovery under user control.		
NFR24	Safe mode	When operating after a failure the user shall be informed that the application is operating in a “safe mode” and all data is available for review without update.		
NFR25	Module/Function Failure	The system shall prevent access to failed module/s while providing access to all currently operational modules.		
NFR26	Hardware failure	All hardware components of the assembly operation shall be replicated, such that failure of any one hardware component shall not render the assembly operation unavailable to end-users. It is acceptable for system performance to be poorer than normal for up to 3		

		business days following the failure and replacement of a piece of hardware.		

6.3.7. ARCHITECTURAL QUALITIES

Ref	Item	Description	F/M/D/TP/NA	Comments
NFR27	Information retention requirements	All stored data should be backed up and archived to be available immediately using live sync.		
NFR28	Capacity/Scalability	Solution should cater for future enhancements and increase in volume (users/data) without affecting the system performance.		
NFR29	Integration	The tool must integrate with the following systems: • Microsoft Active Directory for single sign on • Microsoft SharePoint for capturing and storing meeting information and documents • Microsoft Outlook for emails and follow ups		