REQUEST FOR INFORMATION

Governance, Assurance, Risk & Compliance System

202408 - 01

CONTACT PERSON	Name: Merry Kache Email: Kachem@bankwindhoek.com.na Telephone: +264 61 299 1638
CLARIFICATION DUE DATE:	Date: 30th August 2024 Time: 16H00 (Central Africa Time (CAT) +0200 UTC)
RESPONSE DUE DATE:	Date: 6th September 2024 Time: 12H00pm (Central Africa Time (CAT) +0200 UTC)

TABLE OF CONTENTS

RESPONDENT'S INFORMATION

NAME OF RESPONDENT:	
REGISTRATION /IDENTITY NUMBER:	
CONTACT PERSON:	
POSTAL ADDRESS:	
PHYSICAL ADDRESS:	
TELEPHONE:	
EMAIL:	
WEBSITE:	

BACKGROUND

COMPANY OVERVIEW

Capricorn Group (the Group) is a Namibian-owned group listed on the Namibian stock exchange, comprising the following subsidiaries: Bank Windhoek including Capricorn Private Wealth, Bank Gaborone, Capricorn Asset Management, Entrepo and Namib Bou. The Group competes in the Personal, Wealth and SME/Commercial/Corporate banking segments within Namibia and Botswana. With a strong commitment to innovation and excellence, the Group strives to maintain its competitive edge and meet the evolving needs of its customers and stakeholders.

PURPOSE OF REQUEST FOR INFORMATION

The Group is seeking to understand the existing Governance Assurance Risk and Compliance System that are in the market today. The aim is to understand what are the different systems that exist today, what are their capabilities, how have such systems evolved in terms of modern-day technology and which systems could meet the Group's future needs.

SYSTEM SPECIFICATION AND CAPABILITIES

The system must have capabilities for risk management, assurance engagements / management, compliance management and governance.

1. RISK MANAGEMENT

a) GENERAL

a. Industry awareness

- Banking - or asset management - specific knowledge built into the system (e.g. pre-defined library objects and other types of data that cater for our industries, this adds to productivity without the need to reinvent the wheel).

b. Knowledge and document management

- Ability to capture and manage risk management knowledge on the system, e.g. through built-in wiki or similar (with change control).
- User friendly document management system.

c. Organisation and users

- Able to represent organigrams

- Able to represent multiple legal entities of different levels, e.g. group parent company and subsidiaries.
- Able to support multiple regions and countries
- User friendly set up for roles and user groups to support a role-based model.

d. Workflow

- User friendly workflow that can easily be configured.
- Ability to work in teams of people, while enabling specific users to "claim" workflow tasks if needed.
- Ability of main task owner to delegate tasks (or subtasks related to the main task) to other users (e.g. in cases where multiple users must work on different components of a task).
- Able to re-assign user tasks and ownership of tasks (i.e. currently active tasks or tasks to which the user is linked). Able to perform bulk-reassignment of tasks, i.e. in cases where a user has multiple tasks, the tasks can be viewed, filtered and re-assigned to someone else in a single action.
- Able to handle the tasks of users that are out of office for prolonged periods.
- Social features that enable easy sharing of information and tasks with others.

e. Integration Capabilities

- Should be able to integrate with other systems (e.g. for data collection, dashboards and reporting purposes).
- Ideally the platform should support good data exchange standards such as graphXML or similar.

f. Data collection

- Support for a variety of different data collection timetables, e.g. daily, weekly, etc. (should be configurable)
- Historical data: able to keep any period of historical data for data analysis purposes.

g. Bulk data capture and upload

- Capability for easy-to-use bulk data capture and bulk data upload and integration.
- Input validation of data captured on forms and in bulk data capture / upload.

h. Automated Notifications

- Capability for notifications to users on pending and overdue tasks.
- Ideally the system should have a solution to the "email spam" problem, i.e. too many emails.

i. Currencies

- Able to represent multiple configurable currencies that are in line with the ISO.
- Able to capture exchange rates frequently or infrequently.
- Able to represent the various reporting currencies of different group subsidiaries (e.g. loss events captured in a foreign currency can be viewed by each entity in its own reporting currency).

j. Management information tools

- Built in features such as exception reports and dashboards to assist with self-admin of the system, e.g. system performance, user logins, password reset, etc.
- Built in report writing feature able to generate standardized reports from a template or adjustable report generation extracting information from one of the modules.

k. Security

- Secure authentication (multi factor authentication must be supported, e.g. OTP, security questions, biometrics etc. – particularly for non-SSO users)
- Self-password reset by users
- Password reset by sys admins
- Secure web technology (HTML5, SSL capable)
- Single sign-on support (Active Directory integration, preferably via Azure).

l. Deployment model

- Support for cloud deployment (SaaS, PaaS) or local internal deployment

m. Extensibility

- Users should be able to develop data objects, forms, workflows, reports and dashboards internally (e.g. if there are new requirements to create a simple register to track and manage a specific type of risk).
- Able to put custom developments into packages or plugins that can be imported and exported (e.g. export from testing environment and import into production environment)

n. Mobility

- A mobile version of the platform would be ideal (e.g. to enable users to manage data while in transit)
- A 'off-line' version of the platform for user to access, create or update tasks whilst in traveling remote areas.

o. System documentation

- Clear system documentation that enables users to resolve system queries with minimal interaction with the vendor.
- Ideally, documentation should be electronically built into the platform.

b) RISK MANAGEMENT IN GENERAL

a. Risk appetite

- Should include capabilities for support for risk appetite management (RCAT).
- Setting of risk appetite (qualitative and quantitative).
- Change control on risk appetite changes.

- Data collection for risk appetite measurement.
- Approval of risk appetite.
- Escalation of risk appetite breaches.

b. Risk frameworks

- Construction of risk frameworks in electronic form, e.g. risk owners should have a consolidated view of how their risks are defined and link to data objects that will be used to measure and assess risks.
- Ability to manage emerging risks that may not yet be part of a risk framework (and possibly link it to a framework at a later stage).

c. Reporting and risk views

- Reports and dashboards that enable risk owners and managers to view aggregated risk data in the context of the business units and risks they are responsible for.
- Able to create reports and dashboards for specific risks, e.g. top-level risks that give a view on all data related to that risk.

d. Escalation triggers

- Configurable rules that enable escalation and reporting of information to higher levels, e.g. significant new risks or events, risk appetite breaches, specific key controls that breach, etc.

c) OPERATIONAL RISK MANAGEMENT CAPABILITIES:

a. Risk assessments

- System should have the capability to conduct risk assessment for different scopes and different entities.
- Single central repository for all risk assessment data, including outcomes and evidence.
- Able to aggregate low-level risk assessment information into aggregated risk profiles. The aggregation model should be adaptable to different needs.
- Able to assign risks to different risk owners for regular scheduled or once-off assessment and monitoring.
- Able to link risk data, such as controls, issues, incidents, loss events, metrics, etc. to risks.
- During risk assessment, able to make use of visual guides of risk data to help with the assessment of risks that the data is related to.
- Able to define multiple levels of risks, e.g. level 1 risk = credit, level 2 risk = credit collateral, level 3 risk = collateral documents not legally in order, etc.
- Able to represent risk assessment outcomes visually
- Able to assess risks using different types of variables and factors, such as likelihood and impact.

- Able to incorporate the results of control assessments into risk assessments.
- Adherence to ISO 31000 standard for risk identification, analysis, evaluation and treatment

b. Loss Events / Incident Management

The system should have capabilities for:

- Incident management capability in addition to capturing losses and near-misses, gains and provisions.
- Able to capture and monitor multiple loss events for multiple organisations and business units in a single central repository.
- Able to differentiate multiple statuses for each incident, e.g. an incident may have a potential loss portion, a provision portion, a portion already written off, a near-miss portion we managed to avoid, a gain portion where we might have recovered a sub-item more than it cost us, etc.
- Able to link multiple incidents to create aggregate views of their total loss and provision profile.
- Able for users to submit requests for provisions and write-offs, with provisions and write-offs being approved in terms of pre-approved rules.
- Able to set loss approval rules globally and per business unit for different categories of losses and provisions.
- Loss approval rules and workflow should be customizable and user friendly.
- Integration between loss events, provisions, legal case register, forensic case register, etc.
- First line capturing of incidents and loss events, i.e. a publicly accessible form that can be completed without needing a user account.
- Ideally, able to configure an operational loss budget or target per entity and business unit so that events can be measured against the budget/target.
- Able to capture and track external events (e.g. in the industry or with outside companies), including classification and measurement thereof.
- Able to track gross losses, net losses and recoveries. Ideally, able to provide recovery ratios for different loss types.
- Support for root cause analysis.
- Support for classification of operational loss events in terms of Basel operational loss categories.

c. Issue / Assurance finding management

The system should have capability for:

- Capturing of issues (such as audit findings, regulatory findings, etc.) in a single central repository and in a configurable process (i.e. who approves) that enables them to the tracked, updated, closed and reported on from start to end.

- Issues captured in other modules (audit, compliance, risk) to auto transfer to the Issue Management module for management and administration
- Workflow should cater for specific approval types and levels, like MD/CEO approval on due date extensions, and the original due date and extended date(s) should be retained (for analysis).
- Able to link multiple actions (or child issues) to a single issue/finding and to view them on a consolidated basis
- Able to formulate remediation plans with action due dates for each issue.
- Able to link multiple issues to each other and view them on a consolidated basis, e.g. useful when several issues relate to the same project, or if there is an executive that needs a view of multiple issues.
- Ideally should support for final due dates (final) and milestone due dates (preliminary).
- Provide for the monitoring of "overdue" issues, including notification of upcoming and actual overdue items.
- Able to perform progress assessments on remediation plans attached to issues, i.e. to evaluate progress made to address the issue.
- Able to create issues that are linked or attached to other risk data (e.g. control weaknesses, metrics that breach, loss events that need specific actions), but also able to create ad-hoc issues.
- Support for a user-friendly issue closure process that is customizable and that can cater for different levels of approval. Should allow multiple owners for one issue (or child issues linked to a parent issue) and allow for each owner to "close" their responsibility pertaining to the parent issue (e.g. – an issue may need both the Compliance and IT teams to complete various actions in their domain to remediate one specific issue).
- Able to report on "issue closure failures", including reasons for failure (e.g. should be able to select reason for failing an issue closure request from a dropdown menu).

d. Fraud and forensic

- Built-in forensic case register (or option as an add-on)
- Integration of forensic register with litigation register and loss events.

e. Litigation

- Built-in legal case register (or as an add-on)
- Integration of the legal register with the forensic register and loss events.

f. Metrics

- Able to define, track, report on and capture data for different types of metrics, e.g. key risk indicators, key performance indicators, etc.

- Single central repository for all metric definitions and data.
- User-friendly interface for metric data capture, including bulk metric data capture or upload.
- Automated escalation/notification of metric breaches that is configurable.
- Change control over metric definitions and thresholds. i.e. should support different levels of approval.
- Visual analysis and reporting on metrics via dashboards.
- Automated metric trend analysis
- Calculated metrics, i.e. metrics whose value van be automatically be determined based on other metric values.
- Able to handle manual and automated metric data (i.e. integrate with other systems for automated data collection).
- Able to distinguish between different types of metrics, e.g. leading, lagging, regulatory, etc. (should be adaptable).
- Support for different types of measurements (i.e. number, text dropdown, date, amount, percent, etc.)
- Support for thresholds that can depict different metric states, e.g. not breaching, near breaches, breaches. Ideally this should be adaptable. Should support a wide range of values and value types.
- Ideally, should support normalization. For example, metric thresholds are compared to metric values and normalized into a standardized scale that is comparable between metrics. The goal is to enable comparability between metrics even though all of them have different thresholds.

g. Control assessment

- Able to maintain a central control register or library.
- Able to handle multiple control versions, e.g. slight differences between a control in one business unit/entity compared to how the same control is used in a different business unit/entity.
- Able to distinguish different types of controls, e.g. key, pro-active, re-active, corrective, etc. (should be adaptable).
- Able to set up control assessments for narrow or wide scopes.
- Able to assess control design and operating effectiveness.
- Ideally, automated analysis of common control gaps (e.g. where gaps may exist across multiple business units or entities).

h. Scenario analysis

- Ideally, able to create and monitor operational risk scenarios, assign them to specific owners, link them to operational risk data, define stress factors and variables, and monitor stress

outcomes. One of the purposes of this is to determine or assess the adequacy of operational risk capital requirements.

2. COMPLIANCE MANAGEMENT

The system should be able to support:

a. Compliance universe / Compliance Risk Management Plans (CRMPs)

1. Overall, the methodology in the system/module should support the GACP. The system parameters should be easily customisable and user friendly to accommodate the Group's compliance methodology.

- Able to define and maintain different compliance/legislative universes, e.g. per entity and to support special use cases.
- Able to automate creation (using information captured on the system – i.e. regulatory provisions, controls) and thereafter manually maintain compliance risk management plans (CRMPs) on the system and provide for a repository thereof per compliance universe. CRMPs form the foundational elements of each compliance universe. Ability to populate and link controls to the regulatory provisions. Users should have ability to rate each control as adequate/ inadequate/ partially adequate as well as effective/ ineffective/ needs improvement. Ability to categorise each control as directive, preventive, detective. Ability to download CRMP in spreadsheet format.
- Able to define the different components of the compliance universe, e.g. regulators, legal and regulatory documents (laws, regulations, standards, etc.) and link these to the compliance universe. The goal is, for example, to be able to conclude on the overall compliance status associated with a key regulator.
- Able to prioritise or risk rate the compliance universe based on adaptable factors, e.g. financial impact, reputational impact of non-compliance.
- The loading of legislative pieces (Acts) as well as the requirements under the respective legislative pieces. Ability to import acts (sections, sub sections, clauses) from MS Word as well as capability to populate the same manually. Include ability to amend existing provisions, if required.
- Being able to do a risk assessment regarding inherent risk only on the Legislative Universes considering multiple factors (e.g. financial and reputational risk).
- Being able to do a risk assessment regarding inherent and residual risk on the CRMPs. The residual risk should be calculated automatically using the metrics loaded by the user.
- The setup of risk assessments should be user-friendly and adaptable.

- Being able to download usable and adaptable reports for Legislative Universes and CRMPs.
- "Base" information, as loaded into the system at the beginning, should pull through to the end e.g. if a legislative piece was categorized in a specific way, the category should pull through into the risk assessment and well as the report to be downloaded. Alternatively, the system should have the option for the user to choose which information pulls through to the end and which information does not pull through to the end.

2. Ability to create and track compliance checklists and CSAs using content already loaded.
3. Ability to separately monitor and track non-compliance incidents and control weaknesses that are identified by the management of each subsidiary (outside of audits).

b. Penalties for non-compliance

- Able to track regulatory penalties (or uses the operational losses component of the system for this).
- Able to link penalties to the compliance universe.
- Able to track penalties against a financial compliance budget/target.

3. ASSURANCE ENGAGEMENTS / MANAGEMENT

a. Compliance Monitoring

- Visual views of aggregate compliance data and compliance universes, such as the state of non-compliance, with ability to drill down into specific areas.
- Able to create compliance assessment plans that are linked to the compliance universe.
- Able to assign portions of a CRMP to specific teams for monitoring and testing purposes.
- Compliance monitoring capabilities and automated workflows for assessments of CRMPs per section thereof, including workflows for information requests / notifications and escalations if not actioned within the certain period.
- Repository of compliance assessment working papers (including evidence) and assessments reports per subsidiary.
- Able to create issues for compliance controls that need to be rectified.
- Outcomes of compliance monitoring should flow into an electronic compliance register/log to track compliance breaches and near-breaches (and to support compliance reporting).

4. Ability to allow linking compliance audit findings to the relevant regulatory provisions loaded. Ability to allow the control assessment and residual risk to be impacted by the audit finding and finding rating.
5. System should have the ability to note exceptions individually as reportable or not reportable, not only on an issue basis.

6. Ability to allow online review of working papers and audit trail thereof - workflow
7. Allow for testing controls loaded in the CRMP including documenting testing procedures and results thereof directly on the system. Ability to link controls to the relevant risks/regulatory provisions, link test procedures to the controls, link testing outcome/conclusion to the test procedure.
8. Sample selection, documentation and testing
9. Auditee response management (e.g. responding to audit queries and draft audit findings)
10. Ability to generate audit reports or list of audit findings.
11. Overall audit engagement management

- Able to assess compliance by testing controls or using self-assessments.

12. Ability to generate compliance reports/ dashboards (user friendly and adaptable) of the compliance universe.

b. Internal Audit

- Define Audit universe and audit planning linked to organizational structures and data of risk matrix and compliance universes.
- Able to define multiple-year audit plans based on audit universe (for different entities and risk frameworks)
- Reporting and tracking of audit planning for multiple-year audit plans or single year planning and for different entities.
- Audit engagement planning and management from each entity annual audit plan.
- Reporting and tracking of audit execution for each plan (single and combined for all entities)
- Audit engagement planning and management in terms of start date, fieldwork date, draft report date, final report date, assignment wrap-up date.
- Reporting and tracking of audit execution for each assignment and in total.
- Audit engagement planning and management in terms of resources assigned and management _ including creating auditor profiles with education and experience; assignment to specific audits; resource budgeting and time sheet management.
- Engagement notification and scope letters to be created from the engagement background information captured.
- Engagement notification and scope letters to be sent via the system/email as well as the acceptance and sign-off of the letter to be done via the system to keep correspondence in one place.
- Audit engagement structure linked to the Institute of Internal Auditors standards.
- Customizable audit process workflows that can be assigned to audit engagements

- Process workflows that dictate the workpaper management (e.g. templates, creation, change control, review & approval).
- Sample selection facilitate in the workpapers based on set criteria
- Evidence management (e.g. attachments) directly part of the workpaper management process (workpapers created and reviewed as part of the system and not "outside the system and uploaded")
- Audit working paper review process workflows that facilitate the submission, review, feedback and correction of workpapers with a robust review comment assignment and clearing process
- Audit finding management (integrated with issue management under the operational risk component above)
- Auditee response management (e.g. responding to audit queries and draft audit findings) via email/system
- Audit engagement report generation based on templates and linked to audit finding management system
- Customer Survey letters to be created from the engagement background information captured.
- Customer Survey letters to be sent via the system/email as well as the acceptance and sign-off of the letter to be done via the system
- Functional reporting by audit function to oversight committees on status and progress of audit plans overall; individual engagements; view per organisation/quarter; view of findings raised per quarter / year / r risk type.

c. Management Assurance Services

Audit engagement management

d. Notification letter

- Engagement letter to be created from the engagement background information captured.
- Engagement letter to be sent via the system/email as well as the acceptance of the letter to be done via the system to keep correspondence in one place.

e. Stakeholder Engagement letter

- Standardised template for stakeholder engagement letter to request areas of focus; created from the engagement background information captured.

A. *Audit process workflows*

Fieldwork- Auditee engagement

- Controls, procedures/tests, risks and impact levels to be prepopulated from the system – standardized working papers template for each control framework.
- Configurable impact levels should have the function to be amended.
- After fieldwork all identified exceptions should be grouped in designated groups (control framework) in the exception list - to make it more usable for daily and final discussions of results.
- The system should allow the outcome of the daily and final discussions results to populate to the final exception list (based on the selection of reportable and non-reportable items) then populate to the draft report.
- System should have the ability to note exceptions individually as reportable or not reportable, not only on an issue basis.

B. Audit finding management

Fieldwork – Identification and Reporting of exceptions

- The process of noting, raising and addressing exceptions during fieldwork should be streamlined through the support of the controls that have been populated in the system. (issues linked to controls) Additionally, more options should be built into system to define accumulative area of discrepancies and build up a database of findings – report of previously per area/risk/process.
- *Workpaper & Evidence management (standardized workpaper templates, creation, change control, approval, finalization)*

Evidence Management and Linkage

- The system should provide functionality for uploading and securely storing evidence gathered during control testing, such as screenshots, documents, and audit trails.
- It should enable users to link uploaded evidence directly to the corresponding risks and control tests within the system, establishing clear audit trails and supporting findings with concrete evidence. Additionally, the system should facilitate easy retrieval and review of linked evidence during audits, examinations, and regulatory inquiries, streamlining validation processes and enhancing transparency and accountability.

C. *Audit finding management (integrated with issue management under the operational risk component above)*

Failing of action on issues reviewed

- Ability to fail issues, with a system process to raise/escalate these issues to the relevant stakeholder.

D. *Functional reporting by audit function to oversight committees*

Automated Data Collection and Analysis

- The system should feature automated data analysis functionalities to identify trends, anomalies, and potential areas of concern, enabling more efficient and effective risk assessment processes.

Combined assurance

Combined assurance reporting from various sources in terms of

- single view of the planning and progress of an assurance provider
- combined view of the planning and progress of all assurance providers
- single or combined view of findings for all assurance providers, categorized per risk / process / entity

4. GOVERNANCE

System must be capable of:

- managing the review and approval of governance documents (policies, frameworks, standards etc.) at a group level, i.e. holding company; as well as
- managing the cascading of governance documents (policies, frameworks, standards etc.) to each subsidiary for review and approval at a subsidiary level once approved at the group-level.
- Acting as a repository of all governance documents of the group entity and subsidiaries.
- The system must be able to be operated by multiple users.

RESPONSE REQUIREMENTS

1. Signed RFI Document
2. Responder's Company profile
3. System Capabilities, Demo, integration capabilities
4. Security features and compliance with relevant data protection regulations
5. Estimated costing of the system covering but not limited to;
    - ✓ Initial Costs -Software licenses once off cost, customization, and implementation costs.
    - ✓ Recurring Costs –Subscriptions, support and maintenance fees, and upgrades
    - ✓ Optional Costs - Additional services or features that are optional but may be considered valuable.

All submissions should be limited to electronic via email to the contact person. Email Address: Kachem@bankwindhoek.com.na

TERMS AND CONDITIONS

1. ACCEPTANCE OF CONDITIONS

By the act of submitting a response to this RFI, the service provider is deemed to have acknowledged and agreed to the conditions set forth in this RFI document.

2. RESPONSE SUBMISSION COSTS

There are no fees associated with the RFI submission. However, any costs incurred relating to the submission process are the sole responsibility of the party supplying the response. The Group will not be held liable for any cost incurred while preparing or responding to this RFI.

3. AWARD AND POSSIBLE REQUEST FOR PROPOSALS (RFP)

- There will be no appointment or award emanating from this RFI. This RFI is for information gathering only and should the Group decide to go out on a RFP at a later stage, it will use the gathered information accordingly.

- The Group has a prerogative to elect who it wishes to invite for a closed RFP should it decide to do so at a later stage.

4. CONFIDENTIALITY

- The Group and the Respondent will both take reasonable steps to protect the other party's Confidential Information.

- Neither party will disclose the other party's Confidential Information, including information that has not been expressly identified as being confidential, including but not limited to: information disclosed verbally, in writing or by any other means, exchanged as part of the RFI or any analysis, compilation, study, summary, extract or in a document of any description, developed by the Group relating to any of the information previously mentioned.

- Each party may disclose the other party's Confidential Information to anyone who is directly involved in the RFI process on that party's behalf, but only for the purpose of participating in the RFI. This could include (but is not limited to) officers, employees, consultants, contractors, professional advisors, evaluation panel members, partners, principals or directors. Where this occurs, the disclosing party must take reasonable steps to ensure the third party does not disclose the information to anyone else and does not use the information for any purpose other than participating in the RFI process.

- The Respondent may disclose the Group's Confidential Information to the extent strictly necessary to comply with the law or the rules of any stock exchange on which the securities of the Respondent or any related entity are currently listed. Unless prohibited by law, the Respondent must consult with the Group before making such a disclosure.

6. AGREEMENT

I/We hereby respond to this RFI subject to the conditions as indicated in this document with which I/we acknowledge myself/ourselves to be fully acquainted.

SIGNATURE OF TENDERER: …….

CAPACITY OF SIGNATORY: ……..

NAME OF SIGNATORY: ……..……

DATE: ……..