

Coast Investment and Development Co. (K.S.C.P.)  
Risk Management Unit  
Internal Audit Report - Final

December 2024

تحت المرافقة في اجتماع مجلس الإدارة  
الرجاء العلم مع بتاريخ ٢٠٢٠/٠٤/٠٤

## EXECUTIVE SUMMARY

### Background

As part of the internal audit services provided to Coast Investment and Development Co. (K.S.C.P.), hereinafter referred to as "Coast" or "the Company," RSM Albazie Consulting W.L.L. ("RSM Kuwait Consulting") performed an internal audit review during October 2024 over the Risk Management Unit (hereinafter referred to as "RMU" or the "Department") covering the scope period from 1 October 2023 to 30 September 2024.

This report was prepared for use by the Board of Directors, Audit Committee and senior management. Recommendations for improvement are presented for effective implementation of corrective action plans.

### Objective and Scope

The objective of this review was to obtain an understanding of and evaluating the Control Environment at Coast pertaining to Risk Management Unit processes, to ensure the adequacy and effectiveness of the key internal controls affecting Risk Management Unit processes and identify opportunities for control and process improvements.

- Enterprise Risk Management.
- Risk Policies and Procedures.
- Business Strategies and Risk Appetite Statement.
- Risk Incorporation into Strategic Planning Process and Strategy Documentation.
- Risk Management Organizational Model (Three Lines of Defense).
- Risk Reporting to Management and CMA.
- CMA Executive Bylaw.
- Risk Register and Risk Matrix.
- Risk Awareness and Culture.
- Risk and Control Self-Assessment (RCSA).
- Incident Reporting.
- Business Continuity Plan (BCP) and testing results.

- Value at Risk (VaR).

### Limitations of Our Work

The formation of our observations is achieved through a risk-based plan of work, agreed with senior management and approved by the Audit Committee. Our work is subject to inherent limitations, as detailed below:

- Internal audit has not reviewed all risks and assurances relating to the organization.
- The work is based on the findings and conclusions from the work undertaken, the scope of which has been agreed with management.
- Where strong levels of control have been identified, there are still instances where these may not always be effective. This may be due to human error, incorrect management judgement, management override, controls being by-passed or a reduction in compliance.

The factors considered which might influence our conclusions are:

- Inherent risk in the area being audited.
- Limitations in the individual audit assignments.
- The adequacy and effectiveness of the risk management and governance control framework.
- The impact of weakness identified.
- The level of risk exposure; and
- The response to management actions raised and timeliness of actions taken.

Overall Summary/Highlights

Testing resulted in the identification of 7 observations (6 rated as “Moderate” and 1 rated as “Low”). Based on this, an overall report rating of ‘Marginal’ was assigned to help management understand our assessment of the overall design and operating effectiveness of the company.

The observations, recommendations, and Coast’s management responses to address each are described in the Detailed Observation section of this report.

A summary of the Observations noted during the review is noted in the table below:

| Overall Rating (See Appendices A&B for definitions) |               |                                       |          |     |
|---|---------------|---------------------------------------|----------|-----|
|   | Report Rating | Number of Observations by Risk Rating |          |     |
|   |               | High                                  | Moderate | Low |
| Current Audit                                       | Marginal      | -                                     | 6        | 1   |
| Prior Audit   | Satisfactory  | -                                     | -        | 1   |





## EXECUTIVE SUMMARY

### Ratings and Conclusions

Following is a summary of observations noted in the areas reviewed. Definitions of the rating scales are included in the Appendices.

#### Ratings by Observation

| Observations  | Rating   | Effort   |
|---|----------|----------|
| <b>1. Department Policies and Procedures Manual</b><br><b>a) Incomplete Documentation of Key Processes:</b><br>Our review identified the following gaps in the documentation of key processes: <ul style="list-style-type: none"><li>- While the Risk Management Committee reports and the risk register categorize risks under "Financial Risks," the company's policies and procedures do not include any references to these financial risks.</li><li>- There is no documented guidance on the required frequency for reviewing the Risk Appetite Statement, leaving it open to inconsistency.</li><li>- Timelines for submission of risk committee reports, and CMA risk reports not clearly defined.</li></ul> <b>b) Absence of Risk Management Strategy:</b><br>No Risk Management Strategy has been developed. |          |          |
| <b>c) Absence of Detailed Process Maps for Business Functions</b><br>The Risk Management Unit does not prepare detailed process maps for each business function.  | Moderate | Moderate |
| <b>d) Absence of Review of Insurance Policies</b><br>The Risk Management Unit does not review any of the company's insurance policies to assess the adequacy of risk coverage and insured amounts.  |          |          |
| <b>e) Lack of Risk Management Review for Information System Access Requests</b><br>The Risk Management Function has not reviewed the access requests for a sample of employees.   |          |          |
| <b>f) Periodic Review of System Access Rights</b><br>Periodic review of IT access rights is conducted by the IT Department. However, this review is not subject to oversight by the Risk Management Unit.   |          |          |
| <b>2. Target Dates for Risk Mitigation Action Plans</b><br>The Q1 and Q2 2024 Risk Management Committee reports include a "Controls & Mitigation Action Plans" section for each key risk; however, target dates are not specified for any of the actions. Additionally, the "Action   | Moderate | Low      |



## Ratings by Observation

| Observations   | Rating   | Effort   |
|--|----------|----------|
| Deadline" column in the Risk Register lists "N/A" for all risks, indicating completion. However, some of these risks are ongoing and continuous in nature, making it unclear how they are being monitored over time.   |          |          |
| <b>3. Lack of Risk Review for New Activities, Processes or Systems</b><br>The Asset Management Group is currently in the trial phase of a software update. However, this activity is not subject to a risk review by the Risk Management Unit.   | Moderate | Low      |
| <b>4. Inconsistencies in Risk Reporting</b><br>The risk reports, including the Risk Management Committee (RMC) Reports and the CMA Reports, do not consistently adhere to the prescribed risk matrix template. Instead, these reports utilize differing configurations without documented justification.   | Moderate | Low      |
| <b>5. Limited Involvement in Disaster Recovery Testing and Inadequate BCP Testing</b><br>The disaster recovery tests related to backups and servers are conducted by an external IT consultant and verified by the IT Department, with no involvement from the Risk Management Unit. Additionally, other aspects of the BCP, such as mock drills or power failure simulations, are not tested.   | Moderate | Moderate |
| <b>6. Lack of Defined Risk Awareness Program</b><br>We noted the following:<br><ul style="list-style-type: none"> <li>The current policies and procedures do not specify the frequency and topics for risk awareness sessions.</li> <li>A risk awareness presentation is shared with all employees, but there is no comprehensive tracking to confirm that employees have read and acknowledged the material. The Risk Management unit currently relies on email-read receipts to track employee engagement, but there is no formal acknowledgment system in place to ensure complete confirmation.</li> </ul> | Moderate | Moderate |
| <b>7. Outdated Job Description</b><br>The Supervisor is currently operating under an outdated job description that lists their title as "Risk Management Officer" which was signed in 2021 and has not been updated or signed to reflect the employee's current title and responsibilities.  | Low      | Low      |



## EXECUTIVE SUMMARY (CONTINUED)

### Status of Prior Audit Observations

The following is a status report on observations noted in our previous internal audit report(s). The reported status notes the progress made toward the plan completion and as reported to the internal audit. Through interviews with management and staff, internal control testing and our current observations, the accuracy of the reported progress was verified and is reported as "Complete," "In-Process" or "Open." Any in-process or open items from the prior review are cross-referenced below to the audit observations noted during this review.

| #  | Prior Audit Observation   | Rating | Status   | Previous Management Response   | Follow up results   | Current Management Response  |
|----|---|--------|----------|--|---|--|
|    | <b>Business Continuity Plan</b><br><br>Business Continuity Planning (BCP) is a comprehensive management process that identifies potential threats that are building resilience and the capability to address any types of events that may disrupt the continuity of the people, processes, systems, or services. As per better practices, the responsibility for BCP is a collaborative effort involving multiple departments and stakeholders with risk department playing a significant role. | Low    | Complete | We will incorporate the recommended risk points into Business Continuity Planning (BCP) shortly and ensure risk management unit to have a shared role in oversight and support of BCP. | We reviewed the updated BCP policies and procedures and ensured that there is a section (1.6.3) which specifies the role of Risk Management Unit in BCP. Also, section 2.3.9 states the actions to be taken in case of wars and political violence. | We have updated the Business Continuity Plan (BCP) regarding events such as wars and political violence, which have been successfully completed. |
| 1. | We noted that: <ul style="list-style-type: none"> <li>The business continuity plan lacks specific actions or measures to be taken in the event of wars or political violence, which raises concerns about the organization's preparedness for such scenarios.</li> <li>The responsibility for the development and maintenance of the business continuity plan is not with the Risk Department.</li> </ul>   |        |          | <b>Target Date:</b><br>Q1 2024   |   | Furthermore, the Risk Management Unit has formally assumed responsibility for the supervision and oversight of the BCP.                          |



DETAILED OBSERVATIONS

1. Department Policies and Procedures Manual

Risk Rating: Moderate

Effort Rating: Moderate

COSO Framework Components: Control Activities, Control Environment, and Risk Assessment

a. Incomplete Documentation of Key Processes

Effective risk management requires that organizational policies and procedures comprehensively document all relevant risk dimensions and define regular assessment protocols to ensure consistent oversight and compliance.

Our review identified the following gaps in the documentation of key processes:

- While the Risk Management Committee reports and the risk register categorize risks under "Financial Risks," the company's policies and procedures do not include any references to these financial risks.
- There is no documented guidance on the required frequency for reviewing the Risk Appetite Statement, leaving it open to inconsistency.
- Timelines for submission of risk committee reports, and CMA risk reports not clearly defined.

**b. Absence of Risk Management Strategy**  
Sections 2.3.1 and 2.3.2 of the CRM-1 policy states that, "The Risk Management Strategy shall be developed describing the objectives of Risk Management, the company's risk appetite and tolerance limit and the strategy for managing the risk. The Risk Management strategy shall be approved by the BOD and shall drive the Risk Management function of the company".

No Risk Management Strategy has been developed.

**c. Absence of Detailed Process Maps for Business Functions**

Section 2.3.4 of the CRM-1 policy states that "Detailed process maps shall be prepared for each business function, detailing the sub-processes within each business function to identify the risks associated with each function and sub-process."

The Risk Management Unit does not prepare detailed process maps for each business function.

**d. Absence of Review of Insurance Policies**

Section 5.5.16 of the CRM-1 policy states that, "The Risk Management Function shall review the company's insurance policies to ensure adequacy of risk covered and the sum insured".

The Risk Management Unit does not review any of the company's insurance policies to assess the adequacy of risk coverage and insured amounts as outlined in the table below:

| Insurance Policy | Policy Term           |
|------------------|-----------------------|
| Building         | July 2023 - July 2026 |
| Medical          | July 2024 - June 2025 |
| Life             | July 2024 - June 2025 |

**e. Lack of Risk Management Review for Information System Access Requests**



Section 5.7.3 of the CRM-1 policy states that, "Request for access to all information system resources are to be routed through a formal access request to the IT Department. All requests for access shall be reviewed by the Risk Management Function."

The Risk Management Function has not reviewed the access requests for the below sample of employees:

| Designation                            | Date of Access Granted or Disabled |
|--|------------------------------------|
| Supervisor – Client Portfolios         | 09/04/2023                         |
| Consultant – Asset Management Group    | 30/06/2023                         |
| Vice President – Client Portfolios     | 30/09/2023                         |
| Vice President – Business Development  | 21/04/2023                         |
| Senior Settlement Officer - Operations | 07/08/2023                         |

#### f. Periodic Review of System Access Rights

Section 5.8.7 of the CRM-1 policy states that, "Periodic review of access rights granted to the employees for various IT systems shall be conducted by the Risk Management Function".

Periodic review of IT access rights is conducted by the IT Department. However, this review is not subject to oversight by the Risk Management Unit.

#### Implication

- Without complete and clear documentation of key processes, there is a risk of inconsistent risk management practices, non-compliance with regulatory requirements, and delays in critical decision-making processes.
- The absence of a Risk Management Strategy undermines the alignment of risk management activities with the organization's objectives, weakens oversight by the Board of Directors, and increases exposure to unmanaged and unmitigated risks.
- Absence of detailed process maps hinders the organization's ability to systematically identify risks associated with each function and sub-process, potentially leading to unaddressed risks and gaps in risk management practices.
- Absence of a review process for insurance policies exposes the organization to insufficient coverage of critical risks, which could result in significant financial losses or disruptions in the event of adverse incidents.
- Failure to review information system access requests increases the risk of unauthorized access, and data breaches undermining the organization's information security framework.
- Without Risk Management oversight of periodic IT access rights reviews, there is a heightened risk of unauthorized or outdated access privileges, which can compromise information security and lead to potential breaches.

#### Recommendation

- Develop and update the risk management policies to include financial risks, define timelines for report submissions, and specify the frequency for reviewing the Risk Appetite Statement.
- Develop and implement a Risk Management Strategy in accordance with the policy.



- c. Develop and maintain detailed process maps for each business function as outlined in the policy.
- d. Establish a formal mechanism to periodically review all insurance policies, ensuring they adequately cover relevant risks and the insured amounts.
- e. Implement a robust review process where all information system access requests are routed through and formally assessed by the Risk Management Function.
- f. Establish a formal process where the Risk Management Unit periodically reviews the IT Department's access rights assessments to provide an additional layer of oversight.

Management's Action Plan

|   | Responsible Party: Risk Management Unit | Target Date:   |
|---|---|--|
| a. Financial risks encompass market risk, credit risk, liquidity risk, and operational risk. Therefore, a separate section specifically for "financial risks" is unnecessary. We will update the wording to align with the risk register and reports.<br>Risk Committee reports will be submitted after the finalization of CIDCO's financial statements and review by both the Risk Management Unit and the external outsourcing firm. Setting a fixed timeline for this process is not practical.<br>The Risk Appetite Statement is reviewed annually, as outlined in the Risk Management Plan, and was approved by the Board of Directors. Any additional reviews, if required, will be conducted by the Risk Management Unit in the forthcoming period. |   | a. Q1 2025<br>b. Implemented<br>c. Q1 2025<br>d. Q1 2025<br>e. Q1 2025<br>f. Q1 2025 |
| b. CIDCO has a consolidated strategy which was approved by the BOD. We will amend this point in policies and procedures as risk is already identified for each department as per the overall process map/review of CIDCO.   |   |  |
| c. We will amend the Policies and procedures manual.  |   |  |
| d. We will amend the Policies and procedures manual.  |   |  |
| e. We will amend the Policies and procedures manual.  |   |  |
| f. We will amend the Policies and procedures manual.  |   |  |

| 2. Target Dates for Risk Mitigation Action Plans  |  | Risk Rating: Moderate                   | Effort Rating: Low   |
|---|--|---|----------------------|
| COSO Framework Components: Monitoring Activities  |  |   |                      |
| As per better practices, each risk mitigation action plan should include a clearly defined target date to ensure timely implementation and enable effective monitoring of progress.   |  |   |                      |
| The Q1 and Q2 2024 Risk Management Committee reports include a "Controls & Mitigation Action Plans" section for each key risk; however, target dates are not specified for any of the actions. Additionally, the "Action Deadline" column in the Risk Register lists "N/A" for all risks, indicating completion. However, some of these risks are ongoing and continuous in nature, making it unclear how they are being monitored over time. |  |   |                      |
| Implication   |  |   |                      |
| Absence of clearly defined target dates for mitigation action plans hinders the organization's ability to track progress effectively and ensure timely implementation. This can result in delays, inadequate risk response, and insufficient accountability for managing ongoing risks.   |  |   |                      |
| Recommendation  |  |   |                      |
| Establish and enforce the inclusion of specific, realistic target dates for each risk mitigation action plan in the Risk Register and Risk Management Committee reports.  |  |   |                      |
| Management's Action Plan  |  |   |                      |
| We will update the risk register and reports accordingly and update the action deadline as ongoing (wherever required)  |  | Responsible Party: Risk Management Unit | Target Date: Q4 2024 |



| 3. Lack of Risk Review for New Activities, Processes, or Systems  |  | Risk Rating: Moderate                   | Effort Rating: Low   |
|---|--|---|----------------------|
| COSO Framework Components: Control Environment  |  |   |                      |
| Section 5.5.9 of the CRM-1 policy states that "All new activities, processes, and systems shall be subject to risk review by the Risk Management function to assess the operational risk inherent in them as part of assessment procedures before they are introduced or undertaken." No new activities, processes, or systems were implemented during the scope period. The Asset Management Group is currently in the trial phase of a software update. However, this activity is not subject to a risk review by the Risk Management Unit. |  |   |                      |
| Implication   |  |   |                      |
| Failure to conduct risk reviews for new activities, processes, or systems may lead to unassessed operational risks being introduced into the organization. This oversight increases the likelihood of operational disruptions, compliance breaches, or financial losses.  |  |   |                      |
| Recommendation  |  |   |                      |
| Ensure that all new activities, processes, or systems, including software updates, are subjected to risk review by the Risk Management Unit as part of the assessment procedures before implementation.   |  |   |                      |
| Management's Action Plan  |  |   |                      |
| We will amend the Policies and Procedures.  |  |   |                      |
| Auditors' Response  |  | Responsible Party: Risk Management Unit | Target Date: Q2 2025 |
| The management response is noted. However, we emphasize that implementing this practice is critical to aligning with industry standards in the investment sector. Subjecting all new activities, processes, and systems, including software updates, to a structured risk review by the Risk Management Unit before implementation is essential to ensure operational and strategic resilience. We recommend prioritizing this practice to mitigate potential risks and enhance governance within the organization.                           |  |   |                      |



4. Inconsistencies in Risk Reporting

COSO Framework Components: Risk Assessment

Risk Rating: Moderate

Effort Rating: Low

Section 2.4 of the CRM-2 policy specifies that a standardized risk matrix template (3x3 matrix with a risk scale of 0 to 10) should be used and updated consistently in line with the risk register. Deviations from this template may lead to inconsistencies in the risk assessment process. The risk reports, including the Risk Management Committee (RMC) Reports and the CMA Reports, do not consistently adhere to the prescribed risk matrix template. Instead, these reports utilize differing configurations without documented justification. Refer below table:

| Document           | Risk Scale        | Terms Used for Impact                      | Terms Used for Likelihood   |
|--------------------|-------------------|--|---|
| RMC Reports        | 1 to 4 and 1 to 5 | Critical, High, Moderate, Low, Minor       | Active, Likely, Not Likely, Rare and; Expected, High Likely, Likely, Not Likely, Slight |
| CMA Report H1 2024 | 1 to 4            | Critical, High, Moderate, Low              | Expected, Likely, Not Likely, Rare  |
| CMA Report H2 2023 | 1 to 5            | Incidental, Minor, Moderate, Major, Severe | Rare, Unlikely, Possible, Likely, Frequent  |

Implication

Deviations from the standardized risk matrix template can result in inconsistencies in risk assessments, leading to inaccurate evaluations of risk levels and potentially flawed decision-making. This could undermine the effectiveness of the risk management process, creating gaps in identifying, prioritizing, and mitigating risks.

Recommendation

Ensure that all risk reports, including RMC and CMA reports, strictly adhere to the prescribed risk matrix template.

Management's Action Plan

We will amend the risk matrix and reports accordingly.

Responsible Party: Risk Management Unit  
Target Date: Q1 2025



|   |  |                             |
|---|--|-----------------------------|
| 5. Limited Involvement in Disaster Recovery Testing and Inadequate BCP Testing  | Risk Rating: Moderate                          | Effort Rating: Moderate     |
| <b>COSO Framework Components: Monitoring Activities</b><br><br>Effective business continuity management requires that disaster recovery tests and other aspects of the Business Continuity Plan (BCP) are periodically conducted and reviewed to ensure operational resilience in case of disruptions.<br>The disaster recovery tests related to backups and servers are conducted by an external IT consultant and verified by the IT Department, with no involvement from the Risk Management Unit. Additionally, other aspects of the BCP, such as mock drills or power failure simulations, are not tested. |  |                             |
| <b>Implication</b><br><br>Lack of involvement from the Risk Management Unit in disaster recovery testing and other critical aspects of the Business Continuity Plan (BCP) leaves gaps in monitoring and ensuring that operational resilience is tested and maintained. Without thorough review and oversight, the organization may not be fully prepared for unforeseen disruptions, increasing the risk of business interruptions that could have been mitigated.  |  |                             |
| <b>Recommendation</b><br><br>Risk Management Unit should take a more proactive role in overseeing disaster recovery tests and other aspects of the BCP. Regular mock drills, power failure simulations, and reviews of recovery procedures should be conducted and assessed.  |  |                             |
| <b>Management's Action Plan</b><br><br>Risk Unit will actively review the disaster recovery tests.<br>Mock drills and power failure simulations will be tested as and when required.  | <b>Responsible Party:</b> Risk Management Unit | <b>Target Date:</b> Q3 2025 |



| 6. Lack of Defined Risk Awareness Program   |  | Risk Rating: Moderate                          | Effort Rating: Moderate     |
|---|--|--|-----------------------------|
| <b>COSO Framework Components: Risk Assessment</b>   |  |  |                             |
| <p>As per better practices such as the COSO ERM framework, a structured risk awareness program with defined frequency and content is required to ensure all employees acknowledge and understand key risk information. Principle 4 of the COSO ERM framework emphasizes the importance of management communicating that managing risk is part of daily responsibilities and critical to the entity's success and survival.</p> <p>We noted the following:</p> <ul style="list-style-type: none"> <li>The current policies and procedures do not specify the frequency and topics for risk awareness sessions.</li> <li>A risk awareness presentation is shared with all employees, but there is no comprehensive tracking to confirm that employees have read and acknowledged the material. The Risk Management unit currently relies on email-read receipts to track employee engagement, but there is no formal acknowledgment system in place to ensure complete confirmation.</li> </ul> |  |  |                             |
| <b>Implication</b>  |  |  |                             |
| Absence of a structured risk awareness program with clear frequency, content, and formal acknowledgment mechanisms can lead to inadequate employee understanding of key risks.  |  |  |                             |
| <b>Recommendation</b>   |  |  |                             |
| Implement a formal risk awareness program with defined frequency and clear content topics. A more comprehensive tracking system should be introduced to monitor employee engagement and confirmation of understanding.  |  |  |                             |
| <b>Management's Action Plan</b>   |  |  |                             |
| We will amend the P&P with risk awareness program. Also, we will implement an acknowledgment form to confirm that employees have reviewed and understood the risk awareness material. This will ensure more reliable tracking and reinforce accountability across the organization.   |  | <b>Responsible Party:</b> Risk Management Unit | <b>Target Date:</b> Q2 2025 |



| 7. Outdated Job Description   |  | Risk Rating: Low                        | Effort Rating: Low       |
|---|--|---|--------------------------|
| <b>COSO Framework Components: Control Activities</b>  |  |   |                          |
| Job descriptions should be updated and signed when an employee's role changes to ensure that their responsibilities and title are clearly defined and aligned with current expectations. Failure to update and formally acknowledge changes in job descriptions can lead to lack of accountability and confusion about role responsibilities. |  |   |                          |
| The Supervisor is currently operating under an outdated job description that lists their title as "Risk Management Officer" which was signed in 2021 and has not been updated or signed to reflect the employee's current title and responsibilities.   |  |   |                          |
| <b>Implication</b>  |  |   |                          |
| Failure to update and formally acknowledge changes in job descriptions can create ambiguity around role responsibilities.   |  |   |                          |
| <b>Recommendation</b>   |  |   |                          |
| A formal process for regularly reviewing and revising job descriptions should be implemented to avoid similar issues in the future.   |  |   |                          |
| <b>Management's Action Plan</b>   |  |   |                          |
| Already signed the updated job description.   |  | Responsible Party: Risk Management Unit | Target Date: Implemented |

## APPENDIX A – RATING DEFINITIONS

| Observation Risk Rating Definitions |  | Effort Rating Definitions |  |   |
|-------------------------------------|--|---------------------------|--|---|
| Rating                              | Definition   | Rating                    | Impact   | Effort  |
| Low                                 | Process improvements exist but are not an immediate priority for the Company. Taking advantage of these opportunities would be considered best practice for the Company.   | Low                       | The recommended change, if implemented, would: <ul style="list-style-type: none"> <li>• Impact only one location</li> <li>• Improve efficiency</li> </ul>  | Level of effort to address improvement opportunity meets the following criteria: <ul style="list-style-type: none"> <li>• Completion in &lt; 3 months</li> <li>• Requires change to no more than two manual processes</li> <li>• Only local/department resources needed</li> </ul>                      |
| Moderate                            | Process improvement opportunities exist to help the Company meet or improve its goals, meet or improve its internal control structure and further protect its brand or public perception. This opportunity should be considered in the near term.                | Moderate                  | Opportunity meets the criteria for "Low" impact, and additionally meets one or more of the following criteria: <ul style="list-style-type: none"> <li>• Change affects a business segment</li> <li>• Generates cost reduction</li> <li>• Enhances availability of data used to make business decisions</li> </ul>  | Level of effort to address improvement opportunity meets the below criteria: <ul style="list-style-type: none"> <li>• Completion in 3 to 12 months</li> <li>• Requires modification to current system application set up</li> <li>• Cross-functional resources</li> </ul>                               |
| High                                | Significant process improvement opportunities exist to help the Company meet or improve its goals, meet or improve its internal control structure and further protect its brand or public perception presents. This opportunity should be addressed immediately. | High                      | Improvement opportunity meets the criteria for "Low" and "Moderate" impact, and additionally meets one or more of the following criteria: <ul style="list-style-type: none"> <li>• Change affects the entire organization</li> <li>• Cost reduction and improved efficiency</li> <li>• Improves operating effectiveness of upstream/downstream processes, including those involving third parties</li> </ul> | Level of effort to address improvement opportunity meets the below criteria: <ul style="list-style-type: none"> <li>• Completion requires more than 12 months</li> <li>• Requires new system or module or significant programming change to existing system</li> <li>• Entity-wide resources</li> </ul> |



## APPENDIX B – REPORT RATING DEFINITIONS

### Report Rating Definitions

| Rating         | Explanation  |
|----------------|--|
| Satisfactory   | Adequate internal controls are in place and operating effectively. Few, if any, improvements in the internal control structure are required. Observation should be limited to only low-risk observations identified or moderate observations that are not pervasive in nature.   |
| Marginal       | Certain internal controls are either: <ul style="list-style-type: none"> <li>• Not in place or are not operating effectively, which in the aggregate, represent a significant lack of control in one or more of the areas within the scope of the review.</li> <li>• Several moderate control weaknesses in one process, or a combination of high and moderate weaknesses that collectively are not pervasive.</li> </ul>  |
| Unsatisfactory | Fundamental internal controls are not in place or operating effectively for substantial areas within the scope of the review. Systemic business risks exist that have the potential to create situations that could significantly impact the control environment. <ul style="list-style-type: none"> <li>• Significant/several control weaknesses (breakdown) in the overall control environment in part of the business or the process being reviewed.</li> <li>• Significant non-compliance with laws and regulations.</li> <li>• High observations that are pervasive in nature.</li> </ul> |
| Not Rated      | Opportunity to improve efficiency or profitability of operations but does not indicate an internal control weakness or a material inefficiency.  |

## APPENDIX C – COSO PRINCIPLES

The COSO Framework sets out the following 17 principles (summarized):

|                             |  |
|-----------------------------|--|
| Control Environment         | <ul style="list-style-type: none"> <li>• Demonstrates commitment to integrity and ethical values</li> <li>• Exercises oversight responsibilities</li> <li>• Establishes structure, authority and responsibility</li> <li>• Demonstrates commitment to competence</li> <li>• Enforces accountability</li> </ul> |
| Risk Assessment             | <ul style="list-style-type: none"> <li>• Specifies suitable objectives</li> <li>• Identifies and analyzes risk</li> <li>• Assesses fraud risk</li> <li>• Identifies and analyzes significant change</li> </ul>   |
| Control Activities          | <ul style="list-style-type: none"> <li>• Selects and develops control activities</li> <li>• Selects and develops general controls over technology</li> <li>• Deploys through policies and procedures</li> </ul>  |
| Information & Communication | <ul style="list-style-type: none"> <li>• Uses relevant information</li> <li>• Communicates internally</li> <li>• Communicates externally</li> </ul>  |
| Monitoring                  | <ul style="list-style-type: none"> <li>• Conducts ongoing and/or separate evaluations</li> <li>• Evaluates and communicates deficiencies</li> </ul>  |




## APPENDIX D – FOLLOW UP

For each observation noted previously in this report, a responsible person and target date was identified as a means to assign responsibility for the agreed-upon resolution. It is the management's responsibility to verify that action plans are carried out and observations are adequately addressed.

### Report Distribution List

| Name                                   | Title                                    |
|--|--|
| Mr. Abdul Wahab Mohammad Ali Al Wazzan | Chairman - Audit Committee               |
| Mr. Ayad Al Sumait                     | Audit Committee Member                   |
| Mr. Osama Al Ayoub                     | Audit Committee Member                   |
| Mr. Asaad Ahmad A. Al-Barwan           | Chief Executive Officer                  |
| Mr. Fares Halal Madi                   | SVP – Compliance and Legal Affairs Group |
| Mr. Jithin Varughese                   | Supervisor – Risk Management Unit        |
| Ms. Geethu Jacob                       | Internal Audit Officer                   |

We appreciate the cooperation and assistance from all involved with this review.



This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM Albazie Consulting W.L.L. its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person.

RSM Albazie Consulting W.L.L. is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit [rsmus.com/about-us](http://rsmus.com/about-us) for more information regarding RSM Albazie Consulting W.L.L. and RSM International.

RSM® and the RSM logo are registered trademarks of RSM International Association. The power of being understood® is a registered trademark of RSM Albazie Consulting W.L.L.

© 2024 RSM Albazie Consulting W.L.L. All rights Reserved.