Internal Control Policy Framework

- Treet Corporation Limited
- Treet Battery Limited
- First Treet Manufacturing Modaraba
- Renacon Pharma Limited

Contents

Internal Control Policy

Purpose

This policy establishes a robust internal control framework for **Treet Corporation Limited**, **Treet Battery Limited**, **First Treet Manufacturing Modaraba**, and **Renacon Pharma Limited**. The objective is to ensure that all assets are safeguarded, financial reporting is accurate, risk management is effective, and compliance with laws, regulations, and internal policies is maintained.

Scope

This policy applies across all divisions and departments, covering financial, operational, and compliance controls. It outlines the roles and responsibilities of employees, management, and the board of directors in maintaining a strong internal control system.

1. Introduction

Effective internal controls are crucial to the successful operation of any business. They:

- Ensure the organization achieves its objectives.
- Protect assets from loss or theft.
- Prevent and detect fraud.
- Ensure the accuracy and reliability of financial reporting.
- Ensure compliance with laws and regulations.

2. Key Internal Control Components

2.1 Control Environment

The control environment forms the foundation of the entire internal control system. It reflects the organization's culture, governance structure, and commitment to integrity and ethical behavior.

Key Elements:

A. Ethical Values:

○ Promote a culture of honesty, transparency, and accountability across the organization.	○ *Example:* Implementing a comprehensive **Code of Ethics** that all employees must read and sign. This code should outline expected behaviors, provide guidelines for ethical decision-making, and include procedures for reporting unethical conduct. Regular training sessions on ethical behavior and compliance can reinforce these values.
○ Encourage ethical behavior at all levels.	

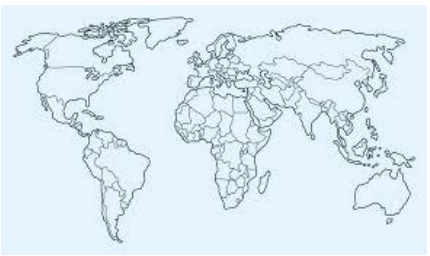
B. Tone at the Top:

○ Senior management and the board of directors must demonstrate strong commitment to ethical behavior and internal controls.	○ *Example:* Senior management and the board of directors consistently demonstrate ethical behavior and integrity. For instance, the CEO and other senior executives regularly communicate the importance of ethics and compliance through meetings, newsletters, and personal interactions. They also adhere to the same standards and policies, setting a strong example for all employees.
○ Lead by example to foster a culture of integrity.	

C. Board Oversight:

○ The board is responsible for overseeing the control environment.	○ *Example:* The board of directors actively oversees the internal control system by establishing an **Audit Committee**. This committee is responsible for reviewing financial reports, monitoring compliance with internal controls, and ensuring that management addresses any identified deficiencies. Regular meetings and detailed reports from internal auditors assist the board in maintaining effective oversight.
○ Ensure that internal controls are implemented effectively.	

D. Organizational Structure:



○ Clearly define roles, responsibilities, and reporting lines.	○ *Example:* Promoting a culture of **transparency and accountability** where employees feel comfortable reporting issues without fear of retaliation. This can be achieved through open-door policies, regular feedback sessions, and anonymous reporting mechanisms like a whistleblower hotline. Encouraging teamwork and collaboration also strengthens the organizational culture.
○ Ensure that the structure supports effective internal controls.	

E. Human Resources Policies:

○ Establish policies that emphasize employee competence, training, and accountability.	○ *Example:* Developing and enforcing HR policies that support internal controls, such as: • **Recruitment and Selection**: Implementing thorough background checks and reference verifications to ensure the hiring of competent and trustworthy employees. • **Training and Development**: Providing ongoing training programs on internal controls, compliance, and ethical behavior. • **Performance Evaluations**: Including adherence to internal controls and ethical standards as part of employee performance reviews. • **Disciplinary Procedures**: Establishing clear consequences for violations of internal controls or ethical standards, ensuring consistent enforcement.
○ Ensure employees understand their roles in maintaining controls and are trained accordingly.	

2.2 Risk Assessment

Risk assessment is the process of identifying and analyzing risks that could prevent the organization from achieving its objectives. A dynamic risk management process ensures the internal control system is responsive to emerging risks.

Key Steps in Risk Assessment:

A. Risk Identification:

○ Identify risks associated with business operations, regulatory changes, financial transactions, and external factors.	○ *Example:* Conducting a **brainstorming session** with key stakeholders to identify potential risks. This could include risks related to supply chain disruptions, regulatory changes, or technological failures. For instance, identifying the risk of a critical supplier going out of business and the impact it could have on production schedules.
○ Consider both internal and external risks.	

B. Risk Evaluation:

○ Assess the likelihood of each risk occurring.	○ *Example:* Using a **risk matrix** to evaluate and prioritize identified risks. This involves assessing the likelihood of each risk occurring and the potential impact on the organization. For example, evaluating the risk of a cyber-attack as high likelihood and high impact, leading to prioritizing investments in cybersecurity measures.
○ Evaluate the potential impact on the organization's objectives.	

C. Fraud Risk:

○ Consider the potential for fraud in all risk assessments.	○ *Example:* Implementing a **fraud detection system** that monitors for unusual transaction patterns. This could include setting up automated alerts for transactions that exceed a certain threshold or for multiple transactions just below the approval limit. Regularly reviewing these alerts helps in identifying and preventing fraudulent activities. For instance, detecting a pattern of small, frequent payments to a new vendor that could indicate a fictitious vendor scheme.
○ Establish controls to detect and prevent fraudulent activities.	

D. Change Management:

○ Periodically assess risks arising from changes in business strategies, regulatory environments, or operational structures.	○ *Example:* Establishing a **change management process** to handle changes in business strategies, regulatory environments, or operational structures. This could involve creating a change request form that must be approved by senior management before any significant changes are implemented. For example, when introducing a new IT system, the change management process would include steps for testing, training, and phased implementation to minimize disruption.
○ Adapt controls to address new risks.	

2.3 Control Activities

Control activities are the policies, procedures, and mechanisms established to mitigate risks and ensure that management's directives are effectively carried out.

Key Control Activities:

A. Segregation of Duties:

○ Divide key responsibilities to prevent fraud or errors.	○ *Example*: Separate the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets.
○ Ensure no single person has control over all aspects of any significant transaction.	

B. Authorization & Approval:

○ Ensure that all transactions are authorized by individuals with the appropriate level of authority.	○ *Example*: Approval from the appropriate authority is required for all expenditures exceeding a specified threshold.
○ Document approval processes.	

C. Reconciliation:

○ Regularly reconcile financial records, including cash accounts, inventory, and other key assets.	○ *Example*: Monthly reconciliation of bank statements with the general ledger.
○ Ensure accuracy and identify discrepancies.	

D. Physical Security:

○ Safeguard assets with physical controls such as restricted access, locked facilities, and inventory management systems.	○ *Example*: Use access control systems to restrict entry to sensitive areas.
○ Protect against theft and unauthorized access.	

E. Information Systems:

○ Implement robust IT controls to protect data integrity.	○ *Example*: Use encryption and multi-factor authentication for sensitive data.
○ Prevent unauthorized access to systems.	

2.4 Information and Communication

A well-functioning information and communication system ensures that relevant, accurate, and timely information flows through the organization, enabling effective decision-making and monitoring.

Key Focus Areas:

A. Internal Communication:

○ Management must ensure that employees at all levels have access to the information they need to carry out their responsibilities.	○ *Example*: Regular team meetings to discuss updates and address concerns.
○ Facilitate open and transparent communication.	

B. External Communication:

○ The organization must communicate clearly with external stakeholders, including auditors, regulators, and shareholders.	○ *Example*: Annual reports detailing internal control measures and compliance status.
○ Provide updates on the internal control framework and any issues that arise.	

C. Transparency:

○ Encourage open communication within the organization about control deficiencies or issues.	○ *Example*: Implement a whistleblower hotline for anonymous reporting of concerns.
○ Ensure employees can report concerns without fear of retaliation.	

2.5 Monitoring

Monitoring ensures that internal controls are functioning effectively and continuously. This is achieved through ongoing assessments, periodic audits, and management reviews.

Monitoring Activities:

A. Internal Audits:

○ Conduct regular audits to evaluate the effectiveness of internal controls.	○ *Example*: Quarterly internal audits to review transactions and compliance with control procedures.
○ Identify deficiencies and ensure compliance with policies and procedures.	

B. Management Reviews:

○ Senior management conducts periodic reviews to assess the effectiveness of controls in achieving business objectives.	○ *Example*: Periodical management meetings are held to review key performance indicators and assesses the effectiveness of internal controls.
○ Adjustments are made as needed based on the findings of these reviews.	

C. Self-Assessments:

○ Employees are encouraged to identify and report control issues to management proactively.	○ *Example*: Self-assessment questionnaires for employees to evaluate their understanding and adherence to internal controls.
○ Foster a culture of continuous improvement.	

D. Corrective Actions:

○ When deficiencies are identified, corrective actions should be promptly implemented.	○ *Example*: Implementing additional training sessions following the identification of control weaknesses.
○ Monitor the effectiveness of these actions.	

3. Compliance and Fraud Prevention

A key component of internal control is to ensure that the organization is fully compliant with all relevant laws, regulations, and internal policies.

3.1 Legal and Regulatory Compliance	
○ The organization must adhere to all applicable laws, industry regulations, and internal policies.	○ *Example*: Regularly update compliance checklists to reflect changes in regulations.
○ Compliance with local and international financial reporting standards, tax regulations, and environmental laws is mandatory.	

3.2 Fraud Prevention		
Fraud Detection	○ Implement early detection mechanisms to identify potential fraudulent activities. ○ Include whistleblower policies and anonymous reporting systems.	○ *Example*: Use data analysis to detect unusual transaction patterns.
Fraud Mitigation	○ Ensure proper segregation of duties and review processes. ○ Prevent any single individual from committing fraud without detection.	○ *Example*: Require dual authorization for high-value transactions.
Employee Training	○ Train all employees on fraud risks and prevention techniques. ○ Emphasize the role of internal controls in mitigating fraud.	○ *Example*: Fraud awareness training sessions for all staff.

4. Best Practices for Internal Controls

4.1 Recommended Practices:

Document Procedures	○ Ensure that all policies, procedures, and internal controls are clearly documented. ○ Make them accessible to employees.	○ *Example*: Develop an internal control manual that is regularly updated.
Enforce Accountability	○ Assign clear responsibilities for maintaining and monitoring controls at every level. ○ Hold individuals accountable for their roles.	○ *Example*: Use performance reviews to assess adherence to control responsibilities.
Regularly Review Controls	○ Perform periodic reviews of the internal control system. ○ Ensure it remains effective and relevant.	○ *Example*: Conduct annual reviews of control procedures and update them as necessary.
Promote Ethical Conduct	○ Encourage an ethical work culture where integrity and honesty are prioritized. ○ Lead by example.	○ *Example*: Implement a code of conduct that all employees must adhere to.
Provide Training	○ Continuously train employees on their roles and responsibilities in maintaining the internal control framework. ○ Update training regularly.	○ *Example*: Training on internal controls and compliance.
Leverage Technology	○ Use technology to automate and monitor control activities where feasible. ○ Enhance efficiency and accuracy.	○ *Example*: Enterprise resource planning (ERP) systems to streamline control processes.
Escalate Issues Promptly	○ Report any control deficiencies or irregularities to management immediately. ○ Address issues promptly.	○ *Example*: Establish a clear escalation process for reporting control issues.
Monitor Key Performance Indicators	○ Use KPIs to track and monitor the effectiveness of internal controls across departments.	○ *Example*: Financial accuracy, compliance, Operational efficiency.

4.2 Practices to Avoid

Bypassing Controls	○ Never bypass established authorization or approval processes. ○ Even under pressure to meet deadlines.	○ *Example*: Always follow the approval process for expenditures, regardless of urgency.
Conflicts of Interest	○ Ensure that no employee is in a position where their decisions could benefit themselves or related parties. ○ Maintain objectivity.	○ *Example*: Implement policies to disclose and manage potential conflicts of interest.
Ignoring Red Flags	○ Any unusual activity, discrepancies, or irregularities must be addressed immediately. ○ Investigate thoroughly.	○ *Example*: Follow up on any discrepancies found during reconciliations promptly. For instance, if a reconciliation reveals an unexplained difference between the bank statement and the general ledger, initiate an investigation to determine the cause and resolve the discrepancy. This might involve reviewing transaction records, contacting the bank for clarification, or checking for any unauthorized transactions.

Practices to Avoid (continued)

Relying Solely on One Control	○ Internal control must involve multiple layers of preventive and detective controls. ○ Diversify control measures.	○ *Example*: Utilize both automated and manual controls to ensure accuracy. For instance, implement automated systems to flag unusual transactions, along with manual reviews to verify these flagged transactions. This dual approach helps identify errors or fraud that might be overlooked if relying solely on a single control method.
Delaying Reconciliations	○ Timely reconciliations are critical for identifying discrepancies before they escalate. ○ Perform reconciliations regularly.	○ *Example*: Reconcile bank statements regularly to identify and correct errors promptly.

5. Review of Policy

The Internal Control Policy will be reviewed annually to ensure its continued relevance.

6. Enforcement Date

This policy shall take effect upon receiving all necessary approvals.

7. Approvals

Prepared by	Muhammad Ali	Group CAO		
Reviewed by	Mansoor Murad	Group CFO		
Reviewed by	Zunaira Dar	Group CLO & CS		
Reviewed by	Tariq Hussain Khan	Group CHRO		
Approved by	Syed Sheharyar Ali	Group CEO		

8. Version Control

Version Number	Date of Revision	Description of Changes	Approved By	Effective Date
TCICSA. 141024.V003MA				15.10.2024