NESTCON GROUP

BUILDING INTEGRITY . CONNECTING COMMUNITIES

RISK MANAGEMENT POLICY

TABLE OF CONTENTS

1.0 RISK MANAGEMENT FRAMEWORK

1.1 GENERAL

Nestcon Group is committed to an effective risks management as it is central to our continued growth and success.

A risk is an effect of uncertainty that may bring either a positive or a negative impact to our business objective. It is often described by an event, a change in circumstances, a consequence, or a combination of these and how they may affect the achievement of objectives. Risk management shall support Nestcon Group's business objectives by managing risks they entail.

1.2 RISK MANAGEMENT OBJECTIVE

Risk management shall be implemented and maintained by the Group and all Subsidiaries within the Group (the "Group") to achieve below objectives:

(a) To encourage proactive rather than reactive management of risks;
(b) To improve identification of opportunities and threats, and to minimize loss;
(c) To improve financial reporting and corporate governance;
(d) To comply with relevant legal and regulatory requirements and international norms;
(e) To improve stakeholders' confidence and trust;
(f) To establish a reliable basis for decision making and planning;
(g) To improve controls and minimize loss;
(h) To effectively allocate and use resources in risk mitigation;
(i) To improve operational effectiveness and efficiency;
(j) To improve incident management and prevention; and
(k) To improve organizational learning and resilience.

1.3 RISK MANAGEMENT PRINCIPLES

The Group shall adhere to the following principles in managing risks:

(a) It should create value and contribute to the achievement of business objectives;
(b) It should be an integral part of organisational processes;
(c) It should be part of a decision making;
(d) It should explicitly address uncertainty;
(e) It should be systematic, structured and timely;
(f) It should be based on best available information;
(g) It should be tailored to align with the external and internal context and risk profile of the Group;
(h) It should take human and cultural factors into account;
(i) It should be transparent and inclusive, and involving all level of stakeholders;
(j) It should be dynamic, iterative and responsive to change; and
(k) It should facilitate continual improvement and enhancement of the organisation.

1.4 RISK MANAGEMENT FRAMEWORK

Risk management shall function within the Enterprise Risk Management framework, depicted below, which provides a holistic and systematic approach to enable the Board of Directors ("the "Board") and the management to understand the risks faced by the Group from the holding company level down to the Subsidiaries and the individual entity levels (e.g. profit centre and/or department and/or division), and embeds the way that the business operations are managed, from the risks perspective.

2.0 RISK MANAGEMENT STRATEGY AND POLICY

2.1 ADOPTION OF GROUP'S UMBRELLA RISK MANAGEMENT POLICY

The below umbrella policy statement sets the Board's expectations on the Group's management of risks:

(a) Risk management is an integral part of overall governance, management, reporting processes, policies, philosophy and culture of the Group;
(b) Risk management should create value and contribute to the achievement of business objectives;
(c) Risk management is applicable to the Group;
(d) Management shall articulate and endorse the risk management policy, allocate adequate resources and apply the framework to the extent that is reasonably practicable;
(e) Business units shall ensure alignment of their risk management objectives with those of the Group;
(f) Management shall ensue legal and regulatory compliance at all times;
(g) Management shall assign management accountabilities and responsibilities at appropriate levels within the Group;
(h) Management shall determine risk management performance indicators that align with organizational performance indicators;
(i) Management shall communicate risks and risk management, formally and informally, to all stakeholders; and
(j) Management shall ensure that the framework for managing risk continues to remain appropriate.

2.2 ARTICULATION AND RISK APPETITE

Risk appetite is an expression of the willingness to accept a particular risk type and level of risk and the resultant volatility of earnings in order to achieve strategic objectives. It is expressed in terms of maximum likelihood and impact acceptable to the Group as a whole and for each Subsidiary. Risk appetite can be described both in quantitative and qualitative terms, depending on the type of risks and on the culture of the organization.

Risk capacity is the maximum amount of risk an organization could assume. Risk capacity is a function of various constrains examples of which include financial impact, investment return, business objective, project objective, schedule deadline, customers and suppliers, legal and compliance, reputation, health and safety, and environment and community.

The Group's risk appetite shall be set by the Board and the management as part of an interactive strategic process. The subsidiary level boards and management teams shall fulfill a similar role for each of the key Subsidiaries. The respective appetites and tolerances should be checked to see that they are aligned with the Board's. The actual level of risks carried shall be monitored against the tolerance set beforehand.

In practice, the Board and senior management should:

(a) consider their appetite for a limited number of key risk categories at the Group Level (i.e. all "**Level 1**" Risk);

(b) identify specific limits and minimum operating standards (or policies) that should be adhered to for individual risk types (i.e. determine risk tolerances at a more granular level of risk, "**Level 2**" Risk);

(c) ensure that the Group strategy is in line with these risk appetite and tolerance statements; and

(d) Repeat the above steps at Subsidiary level.

Risk appetite shall provide guideposts for formulating strategies and plans at both the Group and Subsidiary levels, and help to achieve alignment of objectives and plans across the Group.

2.3 DETERMINATION OF RISK CATEGORY AND RISK TYPE

The Group's key risk category, which provides the basis for grouping similar risks together, is defined below:

(a) Business and Strategic Risks – Risks related to business factors such as customer demand, revenue growth, macro-economic conditions, competition and regulatory environment that are faced by each business lines and their ability to meet earnings target.

(b) Financial Risks – Risks resulting from volatility in the underlying financial market factors such as interest rates, foreign exchange and equity prices.

(c) Operational Risks – Risks of direct or indirect loss resulting from inadequate or failed internal processes, people or systems.

2.4 INTERNAL COMMUNICATION AND REPORTING MECHANISM

Internal communication and reporting mechanism shall be established at both the Group and Subsidiary levels, so as to ensure that:

(a) key components of the risk management framework and any subsequent amendments are communicated properly;
(b) there is adequate internal reporting on the effectiveness of the framework;
(c) relevant information derived from the application of risk management is available at appropriate levels and times; and
(d) there are processes for consultation with internal stakeholders.

The mechanism should include processes to consolidate risk information where appropriate from a variety of sources within the Group taking into account its sensitivity.

2.5 EXTERNAL COMMUNICATION AND REPORTING MECHANISM

External communication and reporting mechanism shall be established only at the Group level to communicate with external stakeholders. Below are examples of communication and reporting mechanism include, but not limited to:

(a) engaging appropriate external stakeholders and ensuring an effective exchange of information;
(b) external reporting or disclosure to comply with legal, regulatory, and corporate governance requirements;
(c) using communication to build confidence in the organization; and
(d) communicating with stakeholders in the event of a crisis or contingency.

3.0 RISK MANAGEMENT PROCESS

3.1 RISK MANAGEMENT PROCESS

Risk management shall take place systematically and as a continuous part of day-to-day business operations at both the Group and Subsidiary levels for all key decision-making processes and core business activities. This includes but not limited to strategic initiatives, annual planning and budgeting process, individual investment decisions, project management, designing new services or processes, choice of partners, customers, suppliers and so on.

3.2 KEY ACTIVITIES OF RISK MANAGEMENT PROCESS

Risk management process is a continual process that involves five key activities: communication and consultation, establishing the context, risk assessment, risk treatment, monitoring and review.

(a) Communication and Consultation

Appropriate involvement of internal and external stakeholders should occur at each stage of the risk management process as well as on the process of a whole. Stakeholders shall contribute to the interfacing of the risk assessment process with other management disciplines, including but not limited to, change management, project and program management, and financial management.

(b) Establishing the Context

Internal and external parameters shall be taken into account when managing risk and setting the scope and criteria for the remaining process being applied. The context shall be relevant for the organization. The management of risk should be undertaken with full consideration of the need to justify the resources used in carrying out risk management.

Risk appetite against which risks are evaluated shall be established and the structure of the analysis be defined.

(c) Risk Assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

Risk Identification Process

Risk identification shall identify source of risk, areas of impacts, events and their causes, and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might enhance, prevent, degrade, or delay the achievement of the objectives. It is also important to identify the risks associated with not pursuing an opportunity.

For each risk identified, the risk identification process shall include:

(i) Event: the event or circumstances which may have a material impact on the business objectives (e.g. high staff turnover).
(ii) Causes: the cause or source of the risk (e.g. staff job dissatisfaction).
(iii) Impacts: the nature of that impact (i.e. inability to achieve strategic objectives).

A systematic 3-step, bottom-up approaches shall be adopted to identify, recognize and record risks against each key risk categories.

(i) Step 1 – Entity Risks

Each entity (e.g. profit centre and/or department and/or division) shall identify and indicate the relative significance of each risk category faced by its operations, and report in entity-level risk register.

(ii) Step 2 – Subsidiary Risks

The entity-level risk register will then be reviewed by the respective Subsidiary's Head and management. After discussing the results of the review and the relative risk impact on the Subsidiary's business objectives, a similar Subsidiary-level risk register will then be developed for each Subsidiary.

(iii) Step 3 – Group Risks

On the same basis, the Subsidiary risk register will then be reviewed at the corporate level by the Group Managing Director ("GMD") and Chief Financial Officer ("CFO"), and the risks are assessed on their relative impacts from the Group's perspectives. A group-level risk register will then be developed.

Risk Analysis Process

Risk analysis involves assessment of their positive and negative consequences and the likelihood that those consequences can occur after taking into account the causes and sources of risk and the presence (or absence) and effectiveness of existing controls. The likelihood and consequences are then combined to determine the level of risk.

For each risk identified, the risk analysis process shall include the following:

(i) Existing Control: the adequacy of existing risk controls.

(ii) Likelihood: the likelihood of occurrence of each consequence associated with the risk. Such likelihood estimation is based on the realistic, worst case of a potential exposure over a 24-month-period.

(iii) Consequence: the potential impact or consequence if risk does occur. Such consequence analysis is based on a realistic but worst case of a potential exposure over a 24-month-period.

(iv) Level of risk: the ranking of risk after considering the effect of controls/counter measures that are currently in place in order to reduce the possible impact of risk (i.e. the net impact).

Risks shall be ranked by assigning scores (i.e. an alphabet ranging from A to E for likelihood and a number ranging from 1 to 5 for consequence) to the two dimensions of each risk category based on the judgmental view of Risk Owners.

Level of risks shall subsequently be assessed in the most suitable terms for that type of risk and in the form that aids risk evaluation. In some instance, a risk can be expressed as a likelihood distribution over a range of consequences. It shall then be mapped against the risk criteria to determine the significance of the level and type of risk.

Risk Evaluation Process

Risk evaluation shall involve comparing estimated levels of risk with the established risk criteria when the context was established to determine the significance of the level and type of risk.

Factors affecting decision may include but not limited to, whether a risk needs treatment, priority for treatment, whether an activity should be undertaken and which of a number of paths should be followed. If the level of the risk established is low, then risk may fall into an acceptable category and treatment may not be required.

Risk Assessment Documentation

The risk assessment process shall be documented together with the results of the assessment. Risk should be expressed in understandable terms, and the units in which the level of risk is expressed should be clear. The documentation shall include, but not limited to the following:

(i) Objective and scope;
(ii) External and internal context and how it is related to the risks being assessed;
(iii) Risk criteria and their justification;
(iv) Limitations, assumptions, and justification of hypotheses; and
(v) Description of relevant parts of the system.

Risk Assessment Methodologies

Risk assessment may be undertaken in varying degrees of depth and details and using one or a number of methods ranging from simple to complex. Various factors influence the selection of methodologies and approach to risk assessment: the available resources; the nature and degree of uncertainty; and the potential consequences of risks.

Risk identification methods may include but not limited to evidence-based methods (examples of which are checklists, and review of historical data), inductive reasoning techniques (event trees, logic diagrams) and brainstorming techniques, where appropriate.

Risk analysis methods may be qualitative, semi-quantitative or quantitative depending on the different risks that are required to assess, the availability of reliable data, the decision-making needs or as prescribed by legislation.

Risk evaluation may then use the understanding of risk obtained during risk analysis to make decisions about future actions. Ethical, legal, financial and other considerations including perceptions of risk shall be also inputs to the decision.

(d) Risk Treatment

Risk treatment involves selecting and agreeing one or more relevant options for changing the occurrence of, or mitigating the effect of risks, and implementing these options.

Once risks have been assessed and discussed, risk treatments shall be recommended to address the risks to ensure that the Group's risks are identified and addressed in line with the entities' business objectives. The risk treatment options generally include but not limited to the following:

(i) Risk Transfer – This involves another party bearing or sharing all or part of the risk by the use of contracts, insurance, outsourcing, joint ventures, and partnership, etc.

(ii) Risk Avoidance – removing the source of the risk or deciding not to start or continue with the activity that gives rise to the risk if practicable.

(iii) Risk Reduction – reducing the likelihood of the risk occurring and the consequences of the risk if it does occur:

- ❖ Possible actions to reduce the likelihood include: preventative maintenance, audit and compliance programs, supervision, contract conditions, policies and procedures, testing, investment and portfolio management, training of staff, technical controls and quality assurance program etc.

- ❖ Possible actions to reduce the consequences include: contingency or crisis management planning, contract conditions, disaster recovery and business continuity plans, off-site back-up, public relations, emergency procedures, staff training and fraud control planning, etc.

(iv) Risk Acceptance/Retention – retaining the risk by choice. If, after controls are put in place, the remaining risk is deemed acceptable to The Group, the risk can be retained. However, plans should be put in place to manage/fund the consequences of the risk, should it occur.

Risk treatment shall be recorded in the Risk Template and Risk Register accordingly and shall be maintained by Risk Owner and reviewed by Risk Coordinator.

(e) Monitoring and Review

Risk Monitoring Process

Risks and controls shall be monitored and reviewed on a regular basis to verify that:

(i) Assumptions about risks remain valid;
(ii) Assumptions on which risk the assessment is based, in particular, the external and internal context, remain valid;
(iii) Expected results are being achieved;
(iv) Results of risk assessment are in line with actual experience;
(v) Risk assessment techniques are being properly applied; and
(vi) Risk treatments are effective.

Accountability for monitoring and performing reviews shall be established by both the Group and Subsidiaries levels.

Risk Reporting Process

(i) Annual Risk Management Reporting Scheme

There shall be annual, bottom-up risk assessments by Subsidiary and the corporate functions. The annual risk management report shall be submitted by all Subsidiaries concomitantly with the submission of the Business Plan and Budget for the ensuing years. The presentation if an updated key risk profile shall be formally included into the Annual Business Plan Presentation by all Subsidiaries.

The completed Risks Register and the accompanying Risk Reports are then consolidated at the Group level to develop a Group Risk Profile so as to provide an overview and an ongoing monitoring tool to assist the Board in forming an opinion as to whether there is a systematic process for identifying and addressing the Group's key risks.

The Group Risk Report shall be reviewed by the GMD and CFO, and subsequently submitted to the Audit Committee ("AC") for review. The Chairman of the AC reports to the Board.

The table below sets out the indicative timeline of a yearly cycle and its deliverables. Detailed timetable and instruction in any particular year will be provided in the Annual Business Plan and Budget memo.

Time	Level	Responsibility	Deliverables
January to October	Subsidiary	- Review and update of risks on a regular basis	
October	Subsidiary	- Final review of risks as part of the annual budget exercise - Identification and treatment of risks - Completion of Subsidiary Risks Report - Submission to The Group Head Office	- Subsidiary Risk Register - Subsidiary Risk Report
Mid December	Group	- Review of risks from the Group's perspective - Identification and treatment of risks at the Group level - Aggregating Subsidiary risks profile to develop a Corporate Risks Profile - Completion of Group Risks Report - Submission to the AC	- Group Risk Register - Group Risk Report
December	Group	- Discussion with the AC on the Group Risks Report	

(ii) Ad Hoc Risk Management Reporting

Ad Hoc risk reporting may be required at the request of the Board and the AC or the Group management which may include but not limited to Special Risk Report, more frequent refresh and submission of Risk Register, etc.

(iii) Risk Management Reporting Responsibilities

The below table defines risk management reporting responsibilities at both the Group and Subsidiaries levels.

Party	Responsibilities
The Board	- Review Group report - Communicate Group risks issues back to the Management - Identify new and emerging risks affecting the Group
AC	- Review Group report - Identify new and emerging risks affecting the Group - Advise the Board on Group risk issues
GMD/CFO	- Review risks report - Closely monitor extreme risks - Identify new and emerging risks
Risk Owners	- Monitor and review the risks which they own - Prepare reports for the risks which they own - Provide the Risk Coordinator with information on the risks which they own - Identify new and emerging risks at the Subsidiary level
Risk Coordinators	- Prepare reports - Gather risk information from the relevant Subsidiary people, for example, Risk Owners - Identify new and emerging risks
Management and Staff	- Provide risk information to those that request it - Monitor and review risks within their areas - Identify new and emerging risks

Other roles and responsibilities of the respective parties involving in the risk management are detailed in “Risk Management Structure” below.

4.0 RISK MANAGEMENT STRUCTURE

4.1 RISK MANAGEMENT STRUCTURE AND RESPONSIBILITIES

Managing risk is a group effort beginning with the individual profit centre and/or department and/or division, followed by the operating Subsidiary and ultimately company's GMD, the Board, all working together to ensure an effective risk management system across the Group.

(a) Board of Directors ("Board")

Company's Board shall approve the Group's risk management framework which defines the objectives, principles, activities, and areas of responsibility of risk management.

The Board shall oversee the effectiveness of the framework and delegate the responsibility for implementing the related policies and procedures to management.

(b) Audit Committee ("AC")

Company's AC is accountable to the Board, and shall inter alia meet and report to the Board of its findings and recommendation on any matters regarding risks management.

(c) Group GMD and CFO and/or Corporate Level

The GMD and CFO shall be responsible for the method, implementation, and supervision of risk management across the Group and report on these to the Board and AC.

The Corporate risk management function shall be responsible for the development of group-wide risk management principles, practices and risk report, the development of tools and the application and adoption of these tools.

(d) Subsidiary Level

Risk management shall spread across all profit centres and/or departments and/or divisions. Each Subsidiary shall be responsible for assigning responsibilities for risk management and identifying, managing and reporting risks. All Subsidiaries shall develop their risk management procedures in line with this Policy and train their personnel in accordance with development plans that have been drawn up. All Subsidiaries shall devote sufficient resources to managing risks.

(e) All Employees of the Group

Every employee shall be familiar with the Group's risk management principles and practices and take a risk management approach in the discharge of their work; All employees shall highlight to management any risks arising and contribute to the control process so as to mitigate risks to an acceptable level.

4.2 PERIODIC REVIEW OF STRUCTURE AND RESPONSIBILITIES

The GMD and CFO shall periodically review and consider whether the current roles and resources for risk management across the Group remain appropriate and sufficient to sustain and continually improve the Group risk management framework. Such consideration shall form part of the planning involved in developing an annual risk management strategy.

4.3 ESTABLISHMENT OF RISK OWNERS AND RISK COORDINATORS

Risk Owners and Risk Coordinators shall be formally identified at both the Group and Subsidiaries levels. Once identified, these roles shall be formally acknowledged and these positions shall be formally established to reinforce the importance and accountability for the risk management framework.

(a) Risk Owner

Risk Owners are individuals with key roles in ensuring the effective management of specific risks for which they are responsible.

(b) Risk Coordinator

Risk Coordinator is an executive who is nominated to facilitate the implementation of the risk's management framework within a specific corporate function, department, process or activity. He / She is responsible for understanding the risks affecting his/her area of responsibility and the possible impact of these risks on other parts of the organisation.

5.0 RISK MANAGEMENT CULTURE

5.1 BUILDING RISK MANAGEMENT CULTURE

Risks management culture shall be developed so as to sustain and promote an integrated risk management system across the Group.

The Group believes that the cornerstone of a successful risk management program is promoting a risk conscious or aware culture and recognizes risk management as a collective effort beginning with individual profit centre and/or department and/or division, followed by the Subsidiary and ultimately the Board, working as a team. Risk management culture shall be aligned with both near and long-term corporate goals.

The Group advocates achieving an optimal balance between risk and return through taking calculated risks and embracing risk ownership. Concerted risk management efforts throughout the organization shall enable the Group to better manage risks and capitalise on opportunities.

5.2 DESIGNATED RISK MANAGEMENT CHAMPION

The GMD and the relevant Heads at the Subsidiary level shall spearhead the risk management effort and shall be the designated risk management champions at their respective levels so as to have sufficient authority to effect changes in business practice.

5.3 WHISTLE BLOWING PROGRAM

The whistle-blowing policy has been adopted by the Group as an official channel in place for staff to raise or report concerns. Please refer to “Anti-Fraud and Whistle-Blowing Policy” for details.

5.4 STAFF TRAINING AND EDUCATION

Topics on risk and risk management shall be embedded into the training sessions to introduce new initiatives and reinforce key principles to staff. Such training may comprise standalone modules on enterprise risk management or technical risk topics, or can be embedded into other induction or management training presentations that the staff and management attend.

6.0 RISK MANAGEMENT TOOL

6.1 RISK MANAGEMENT TOOL

Risk management tools shall be used to facilitate risk management process.

The internet system of the Group shall be the repository and medium for communicating policies, corporate governance practices, and training materials within the Group.

To ensure that all users have a clear understanding on the Group's internal control and risk management system, latest version of risk management framework and other Group policies and procedures are made available in the internet.

7.0 FRAUD RISK MANAGEMENT

7.1 FRAUD RISK MANAGEMENT

The Group is committed to having a high standard of ethical conduct and adopts a zero-tolerance approach to fraud.

Fraud risks are events or conditions that provide an opportunity, a motive or a means to commit fraud. All fraud risk shall be assessed and reported at both the Group and Subsidiaries levels, by considering potentially fraudulent activities, including but not limited to, the following:

(a) Fraudulent financial reporting arising from improper revenue recognition, improper capitalization of expenses, improper asset valuation, improper related-party transactions, improper management override of financial transactions;

(b) Misappropriation of assets;

(c) Improper or unauthorized expenditures;

(d) Self-dealings including kickbacks; and

(e) Violations of laws, rules and regulations.

Specific examples of fraudulent financial reporting risks and misappropriation of assets risks are set out in **Appendix A** of this Policy.

The Group's fraud risk management includes a whistle-blowing policy for the employees so as to prevent, deter and detect fraudulent financial activity.

7.2 WHISTLE-BLOWING AS PART OF FRAUD RISK MANAGEMENT

The whistle-blowing guidelines, as contained in the "Anti-Fraud and Whistle-Blowing Policy", has been adopted to encourage proper work ethics and stamp out any internal improprieties, unethical acts, malpractices, fraudulent act, corruptions and/or criminal activities in our organization. The aim is to provide official avenues or channels for staff to raise or report any concerns/issues that they may have on the aforementioned matters.

APPENDIX A – FRAUD RISK FACTORS

Examples of fraudulent financial reporting risk factors, misappropriation of assets risk factors are set out below.

(1) Risk Factors Relating to Misstatements Arising from Fraudulent Financial Reporting

Incentives/ Pressures

(a) Financial stability or profitability is threatened by economic, industry, or entity operating conditions such as:

(i) High degree of competition or market saturation, accompanied by declining margins.
(ii) High vulnerability to rapid changes, such as changes in technology or an increase in interest rates.
(iii) Significant decline in customers demand and increasing business failures in either the industry or overall economy.
(iv) Operating losses that may lead to a threat of bankruptcy or foreclosure, or when a hostile takeover is imminent.
(v) Recurring negative cash flows from operations or an inability to generate cash flows from operations while reporting earnings and earnings growth.
(vi) Rapid growth or unusual profitability especially compared to those of other companies in the same industry.
(vii) New accounting, statutory or regulatory requirements.

(b) Excessive pressure exists for management to meet the requirements or expectations of third parties such as:

(i) Profitability or trend level expectations of significant creditors/bankers, or other external parties (particularly expectations that are unduly aggressive or unrealistic), including expectations created by management in, for example, overly optimistic press releases or annual report messages.
(ii) Need to obtain additional debt or equity financing to stay competitive including financing of capital expenditures.
(iii) Marginal ability to meet exchange listing requirements or debt repayment or other debt covenant requirements.
(iv) Perceived or real adverse effects of reporting poor financial results on significant pending transactions, such as business combinations or contract awards.

(c) Information available indicates that the personal financial situation of management or those charged with governance could be threatened by the entity's financial performance arising from the following:

(i) Significant financial interests in the entity.
(ii) Significant portions of their compensation, such as bonuses, being contingent upon achieving aggressive targets for stock price, operating results, financial position or cash flow.
(iii) Personal guarantees of debts of the entity.

(d) Excessive pressure on management or operating personnel to meet financial targets set by those charged with governance, including sales or profitability incentive goals.

Opportunities

(a) The nature of the industry or the entity's operations may provide opportunities to engage in fraudulent financial reporting from the following:

(i) Significant related-party transactions not in the ordinary course of business or with related entities not audited by the same audit firm.
(ii) Assets, liabilities, revenue, or expenses based on significant estimates that involve unusually subjective judgements or uncertainties that are difficult to corroborate.
(iii) Significant, unusual, or highly complex transactions, especially those close to year end, that pose difficult "substance over form" questions.

(b) Ineffective monitoring of management as a result of the following:

(i) Domination of management by a single person or small group without compensating controls such as effective oversight by a board of directors or audit committee.
(ii) Ineffective oversight by those charged with governance over the financial reporting process and internal control.

(c) Complex or unstable organizational structure as evidenced by high turnover of senior management, or those charged with governance.

(d) Inadequate or deficient control components as a result of the following:

(i) Inadequate monitoring of controls, including controls over interim financial reporting (where external reporting is required).
(ii) High turnover rates in or employment of ineffective accounting, internal audit, or information technology staff.
(iii) Ineffective accounting and information systems, including situations involving material weaknesses in internal control.

Attitudes/ Rationalizations

(a) Ineffective communication, implementation, support, or enforcement of the entity's values or ethical standards by management or the communication of inappropriate values or ethical standards.

(b) Non-financial management's excessive participation in or preoccupation with the selection of accounting principles or the determination of significant estimates.

(c) Known history of violations of securities laws or other laws and regulations, or claims against the entity, its senior management, or those charged with governance alleging fraud or violations of laws and regulations.

(d) Excessive interest by management in maintaining or increasing the entity's stock price or earnings trend.

(e) A practice by management to commit to analysts, creditors, and other third parties to achieve aggressive or unrealistic forecasts.

(f) Management's failing to correct known material weaknesses in internal control on a timely basis.

(g) The relationship between management and the current or predecessor auditor is strained, as indicated by the following:

(i) Frequent disputes with the current or predecessor auditor on accounting, auditing, or reporting matters.
(ii) Unreasonable demands on the auditor including unreasonable time constraints regarding the completion of the audit or the issuance of the auditor's report.
(iii) Formal or informal restrictions on the auditor that inappropriately limit the auditor's access to people or information or the auditor's ability to communicate effectively with those charged with governance.
(iv) Domineering management behaviour in dealing with the auditor, especially involving attempts to influence the scope of the auditor's work or the selection or continuance of personnel assigned to or consulted on the audit engagement.

(2) Risk Factors Relating to Misstatements Arising from Misappropriation of Assets

Incentives/ Pressures

(a) Personal financial obligations may create pressure on management or employees with access to cash or other assets susceptible to theft to misappropriate those assets.

(b) Adverse relationships between the entity and employees with access to cash or other assets susceptible to theft may motivate those employees to misappropriate those assets. For example, adverse relationships may be created by the following:

(i) Known or anticipated employee layoffs.
(ii) Recent or anticipated changes to employee benefits or compensation plans.
(iii) Promotions, compensation or other rewards inconsistent with expectations.

Opportunities

(a) Opportunities to misappropriate assets increase where there are the following:

(i) Large amounts of cash on hand or processed.
(ii) Easily convertible assets.
(iii) Fixed assets which are small in size, marketable, or lacking observable identification of ownership.

(b) Inadequate internal control over assets may increase the susceptibility of assets to be misappropriated. For example, misappropriation of assets may occur because of the following:

(i) Inadequate segregation of duties or independent checks.
(ii) Inadequate oversight of senior management expenditures, such as travel or other reimbursements.
(iii) Inadequate management oversight of employees responsible for assets, for example inadequate supervision or monitoring of remote locations.
(iv) Inadequate job applicant screening on employees with access to assets.
(v) Inadequate record keeping with respect to assets.
(vi) Inadequate system of authorization and approval of transactions, for example, in purchasing.
(vii) Inadequate physical safeguards over cash, investments or fixed assets.
(viii) Lack of complete and timely reconciliations of assets.
(ix) Lack of timely and appropriate documentation for transactions, for example, fixed assets return.

Attitudes/ Rationalizations

(a) Disregard for the need for monitoring or reducing risks related to misappropriation of assets.

(b) Disregard for internal controls over misappropriation of assets by overriding existing controls or by failing to correct known internal control deficiencies.

(c) Changes in behavior or lifestyle of employees that may indicate assets have been misappropriated.

(d) Tolerance of petty theft.