



新世界發展有限公司

New World Development Company Limited

(Stock Code: 17.HK)

Risk Management Policy

New World Development Company Limited

Table of Content

	<i>Page</i>
1. Background	1
2. Scope	1
3. Enterprise Risk Management Framework	1
3.1 Risk Management Approach	3
3.2 Early Risk Flagging Mechanism	4
4. Risk Governance Structure	7
4.1 Risk Management and Reporting Structure	7
4.2 Risk Management Roles and Key Responsibilities	8
5. Risk Management Process	10
5.1 Risk Identification	10
5.2 Risk Analysis	10
5.3 Risk Evaluation	10
5.4 Risk Treatment	11
5.5 Risk Monitoring	12
5.6 Risk Reporting	12
6. Implementation and Review of the Policy	13
 Appendices	
Appendix I – Risk Identification Template	14
Appendix II – Suggested List of Major Risks	15
Appendix III – Risk Analysis and Evaluation Template	16
Appendix IV – Risk Treatment Worksheet	17
Appendix V – Risk Identification and Assessment Checklist	18
Appendix VI – Risk Management Committee - Terms of Reference	24

1. Background

Pursuant to the amended "Corporate Governance Code and Corporate Governance Report" under Appendix 14 of the Main Board Listing Rules issued by the Hong Kong Exchanges and Clearing Limited, a resolution was passed by the Board of Directors of New World Development Company Limited ("NWD" or the "Company") at a meeting held on 23rd February 2016 to approve the Risk Management Policy (the "Policy") which sets forth the Enterprise Risk Management ("ERM") Framework for the Company together with its subsidiaries (the "Group"). This structured framework is to assist the Group to comply with Appendix 14 of the Main Board Listing Rules in relation to risk management.

This ERM framework is implemented across the Group, where the responsibilities for identifying, assessing, and managing risks will be shared with Risk Owners of all NWD corporate departments (i.e. department heads) and business units of the Group (i.e. senior management of business units) on an ongoing basis. Application of this framework ranges from day-to-day activities to strategic processes at the Board of Directors (the "Board") level, which enables a consistent view of risks across the Group.

It also provides a governance structure where all key risks (including but not limited to business, operation as well as environmental, social and governance ("ESG") related risks) are identified, assessed, and accounted for, as well as ensuring that risks are managed to an acceptable level with reference to the Group's objectives. In addition, operational efficiency and effectiveness through continuous improvement of processes to address the identified risks and/or opportunities allows the management to more focus on addressing performance and profitability goals and safeguarding resources against loss.

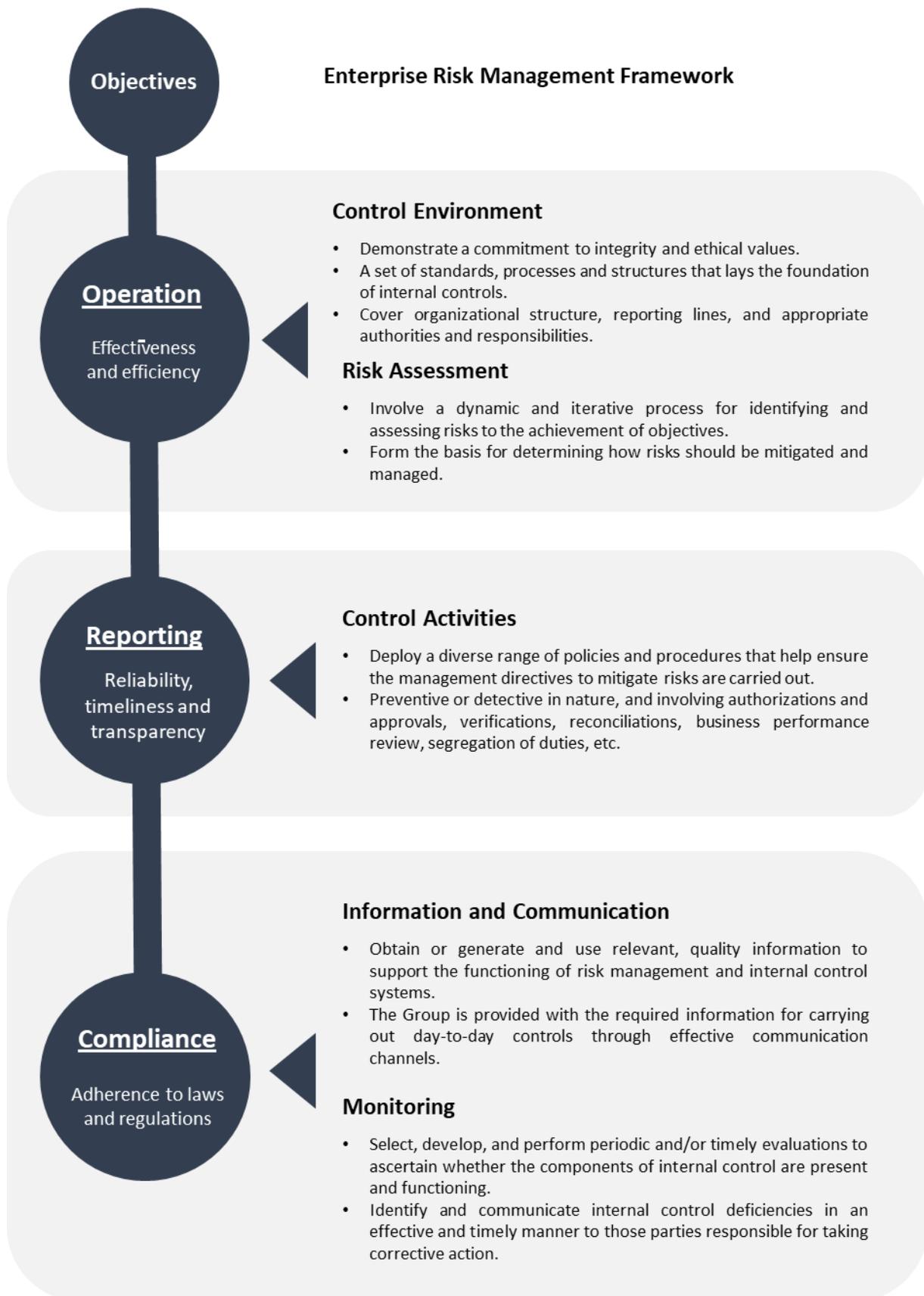
2. Scope

The key objective of this Policy is to establish a consistent basis for identifying, analyzing, evaluating, treating, monitoring and reporting risks across the Group at all levels to support the achievement of the organization's overall strategic objectives. The ERM framework described in this Policy applies to all business functions and operations of the Group in different geographical areas.

3. Enterprise Risk Management Framework

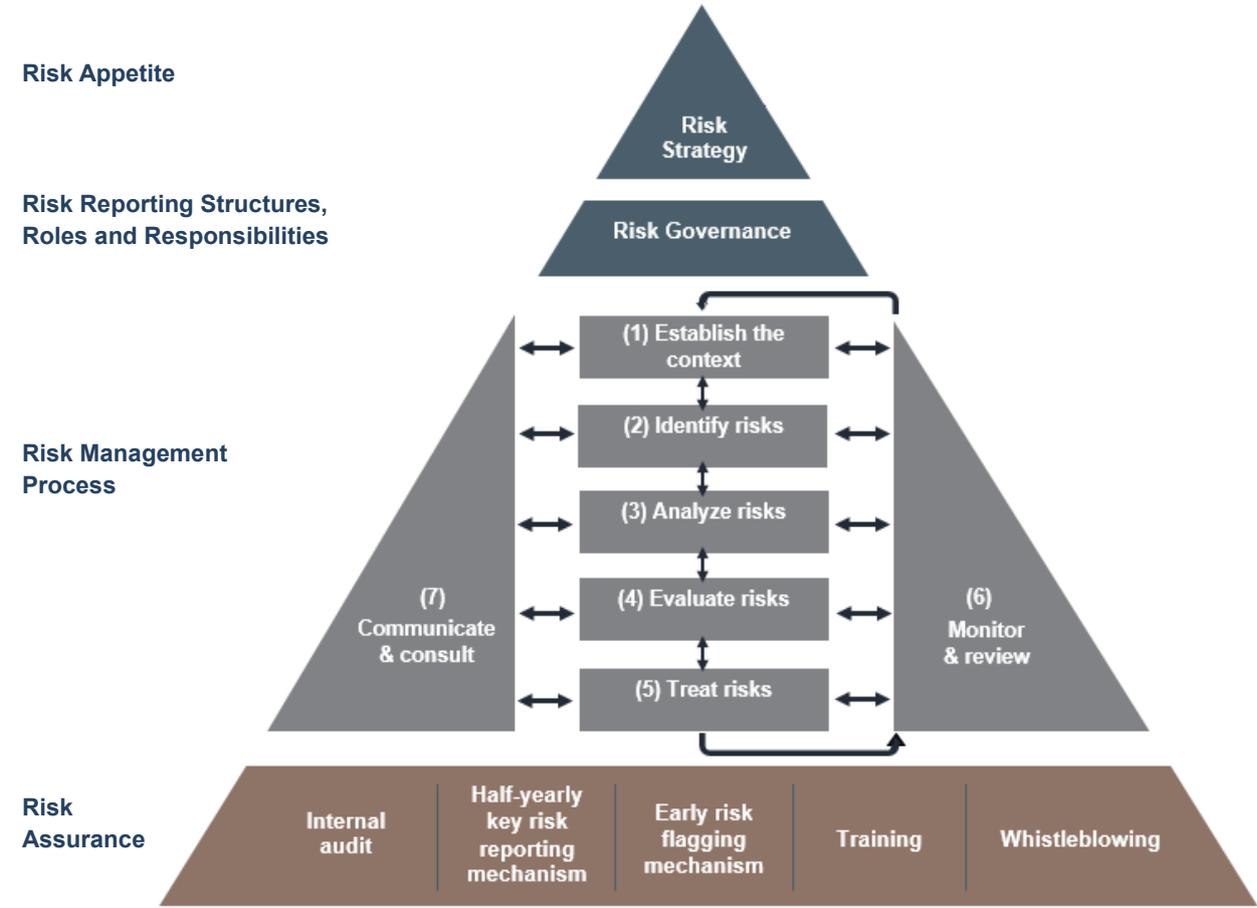
Robust and effective management of risks is an essential and integral part of corporate governance. It helps to ensure that the risks encountered in the course of achieving the Group's strategic objectives are managed within the Group's risk appetite. An ERM framework is established for identifying, assessing, responding to and reporting on risks that might affect the Group in pursuit of its objectives and goals. The main purpose of ERM implementation is to provide senior management and the Board with a holistic view of the Group's material risk exposures and steps taken to manage and monitor such exposures. With reference to the "Internal Control – Integrated Framework" issued by the Committee of Sponsoring Organizations of the Treadway Commission, the key features of the ERM system are illustrated below:

Enterprise Risk Management Framework



3.1 Risk Management Approach

NWD adopts both top-down and bottom-up approaches in relation to risk management. It involves collating and appraising bottom-up input from Risk Owners of all NWD corporate departments and business units of the Group, with refinements and adjustments through top-down input from the Board in an iterative manner.



The overall risk management process is summarized as follows:

- 1) **Establish the context** - Define the criteria by which it is decided whether a risk is acceptable or not, and form the basis of options for managing risks.
- 2) **Identify risks** - Identify what, why and how risks can arise as the basis for further analysis.
- 3) **Analyze risks** - Consider the range of potential consequences and how likely those consequences are to occur, both of which can be combined to produce an estimated level of risk.
- 4) **Evaluate risks** - Compare estimated levels of risk against the pre-established criteria so that risks can be ranked so as to identify management priorities.
- 5) **Treat risks** - Develop and implement specific management actions for those risks of higher priority while accept and monitor low-priority risks.
- 6) **Monitor & review** - Monitor and review the performance of the risk management process and changes which might affect it.

7) **Communicate & consult** - Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process.

The risk management process is integrated into our daily operations and is an ongoing process involving all parts of the Group from the Board down to each individual staff. The Risk Owners and Risk Oversight Parties are clearly defined across the Group. They are required to identify, analyze and evaluate the risks (including but not limited to business, operation as well as ESG risks) facing their businesses with proper management execution to avoid, reduce or transfer those risks accordingly.

3.2 Early Risk Flagging Mechanism

Ongoing risk monitoring can help to identify and assess broad areas of change, emanating from both internal and external factors that might generate new risks. Establishing an early risk flagging mechanism supports the Group to proactively identify emerging risks and act on them in a timely manner. To ensure risk management practices are effective, a list of potential risk adverse events (which are not exhaustive) is set forth by the NWD Risk Management Committee. Giving the changing business environment, such list of potential risk adverse events will be reviewed and updated regularly by the NWD Risk Management Committee. Risk Owners of all NWD corporate departments and business units of the Group have to flag and report immediately when and where a potential risk is perceived in any business areas that constitute such adverse events:

List of Potential Risk Adverse Events (examples only, non-exhaustive)	Responsible Parties
<p>Any risk adverse events which may have material impacts on the achievement of organizational objectives and goals or any other material risks which have to be flagged and escalated as deemed necessary by Risk Owners. Examples of potential risks are as follow:</p> <p><u>Political, economic, social and legal related issues:</u></p> <ul style="list-style-type: none"> • Outbreaks of civil unrest, changes in political direction, market conditions, economic downturns, and decline in business and consumer sentiment; • Adverse change in laws, constitutional change, government policies and regulations; <p><u>Market condition and business environment related issues:</u></p> <ul style="list-style-type: none"> • Keen competition in the market, and change of customer needs and behavior; • Significant fluctuation in the exchange rate or interest rate; • Fluctuation in labour costs, and prices of materials and equipment; <p><u>Environmental related issues:</u></p> <ul style="list-style-type: none"> • Environmental and waste management issues, pollution, climate change impacts and disruptions to company assets and operations; 	<p>Risk Owners¹ of both NWD corporate departments and business units of the Group (where appropriate)</p>

¹ Risk Owners should be defined in accordance with organizational structure and management system of each corporate department or business unit.

List of Potential Risk Adverse Events (examples only, non-exhaustive)	Responsible Parties
<ul style="list-style-type: none"> • Natural catastrophes and adverse weather conditions; <p><u>Operation related issues:</u></p> <ul style="list-style-type: none"> • Significant cost overruns and delay of major construction projects; • Quality issues in products and services, business and financial failure of key suppliers, contractors and customers; • Liquidity problems and failure to obtain adequate financing; • Loss of key personnel and labor dispute; • Health and safety (e.g. contagious diseases, increasing incidents for both corporate employees and supply chain partners); • Cyber risks and disruption in information systems; • Reputational risks (e.g. serious impact on its brand value, negative media reports in headlines of national newspapers, etc.); <p><u>Fraud, mal-practices and non-compliance related issues:</u></p> <ul style="list-style-type: none"> • Bribery, corruption, fraud, extortion money laundering, and terrorist financing; • Significant leakage of sensitive and confidential information; • Non-compliance resulting in fines (say, HK\$100,000 or above) and/or temporary disruptions to operations; <p><u>Financial and business performance disclosure related issues:</u></p> <ul style="list-style-type: none"> • New accounting pronouncements (e.g. new or revised HKFRS) which may have adverse effects on financial statements; • Decrease in financial performance (say, 5% decrease in sales, operating profit, capital expenditure, total assets, and/or net assets against budget of each Risk Owner (depending on the nature of the department/function)). 	

The following Risk Oversight Parties should be immediately alerted before a problem becomes catastrophic, and at a stage when action can be taken to mitigate or overcome the situation:

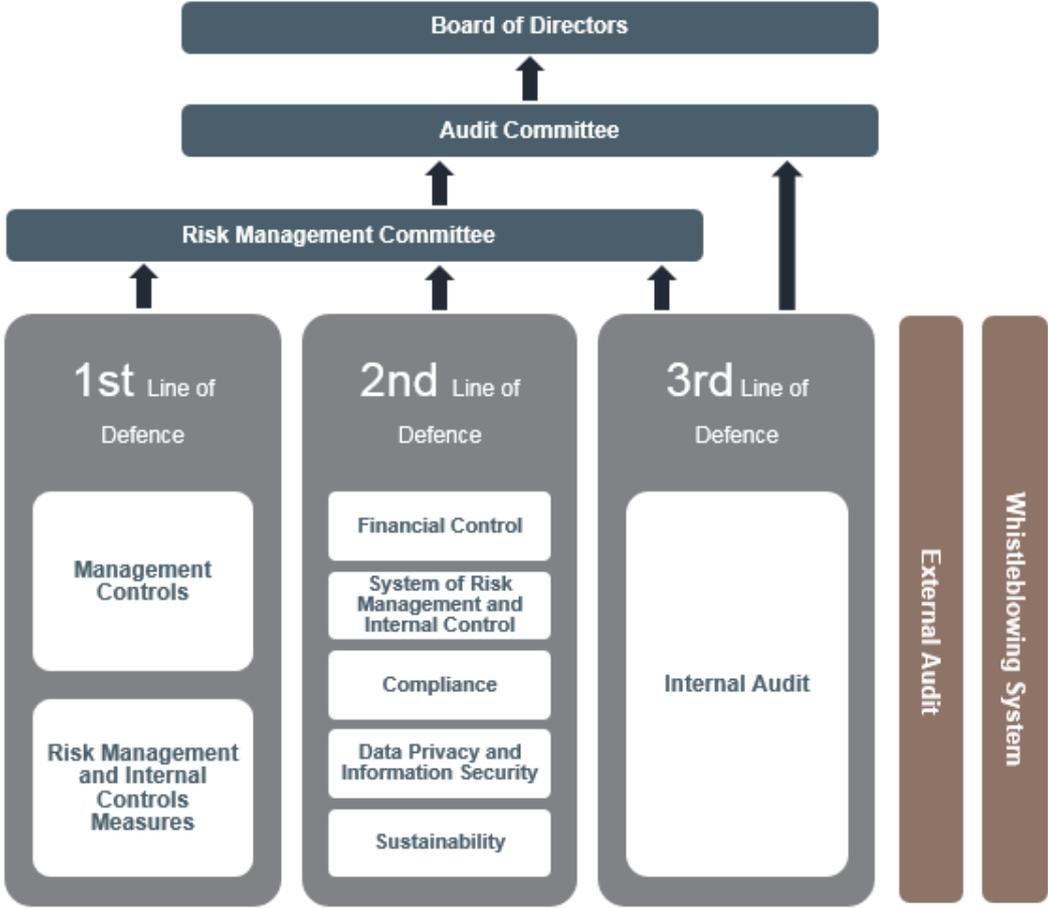
Risk Owners	Risk Oversight Parties
NWD corporate departments	<p>NWD Executive Vice-chairman and Chief Executive Officer and Risk Management Committee</p> <p><i>(NWD Corporate Communication, Human Resources, Investor Relations, and other relevant departments should also be involved, where appropriate, depending on the nature of the risk adverse event)</i></p>
Business units of the Group	<p>First Level: Executive Directors, Executive Committee, Risk Management Committee and/or designated department/function (subject to the risk governance structure of respective business units)</p> <p>Second Level: NWD Executive Vice-chairman and Chief Executive Officer and Risk Management Committee</p> <p><i>(NWD Corporate Communication, Human Resources Investor Relations, and other relevant departments should also be involved, where appropriate, depending on the nature of the risk adverse event)</i></p> <p>Both first and second level Risk Oversight Parties should be notified at the same time.</p>

In order to efficiently pool information and track any impending crises or issues within the Group as and when they arise, every corporate department and business unit will use the **Issue Alert System** in which they will enter all relevant details related to the issue and follow up on the impending crises or issues in a timely manner.

4. Risk Governance Structure

4.1 Risk Management and Reporting Structure

NWD’s risk management governance and reporting structure is depicted as follows:



The Group’s risk governance structure is guided by the “Three Lines of Defence” model. This is manifested by the oversight and directions from the Board, the Audit Committee and the Risk Management Committee of the Group. The Board has the overall responsibility for evaluating and determining the nature and extent of the risks it is willing to take in achieving the Group’s strategic objectives, and ensuring that the Group establishes and maintains appropriate and effective risk management and internal control systems.

As the first line of defence, risk owners of all corporate departments and business units of the Group identify and evaluate the risks which may potentially impact the achievement of their business objectives, mitigate and monitor the risks (including but not limited to business, operation as well as environmental, social and governance (“ESG”) risks) by designing and executing control procedures in their day-to-day operations. They conduct risk assessment and control self-assessment on a regular basis to evaluate the adequacy and effectiveness of controls that are in place to mitigate the identified risks.

As the second line of defence, the Group establishes specific functions to effectuate risk management and ensure the first line of defence is properly in place and operating as intended. The responsibilities of these functions include but not limited to financial control, risk management and internal control, compliance, data protection and information security, sustainability, and so forth. The Risk Management Committee also oversees and monitors the overall operation of the risk management and internal control systems.

As the third line of defence, the Group Audit and Management Services (“GAMS”) Department acts as an independent assessor. It is responsible for reviewing the major operational, financial, compliance and risk management controls of the Group on a continuous basis. It schedules its work in an annual audit plan which is reviewed by the Audit Committee every year. The audit plan is derived from annual risk assessment covering all businesses of the Group and is aimed at covering each significant corporate department and business unit in which the Group involves in day-to-day management within a reasonable period. The GAMS Department also carries out independent and timely review or investigation works, where and when necessary, on risks and control related incidents identified from time to time.

On top of the “Three Lines of Defence”, through independent audit and review, the external auditor provides reasonable assurance on the effectiveness of the risk management and internal control systems. Whistleblowing System is established for staff and other relevant parties to report misconduct cases. Every reported case will be handled in confidentiality and followed through in accordance with the Whistleblowing Policy and its related procedures.

4.2 Risk Management Roles and Key Responsibilities

There are principally five levels of accountability and responsibility for managing risks that are set out in descending order below:

Risk Management Role	Responsible Party	Key Responsibilities
1. Risk Oversight	Board of Directors	<ul style="list-style-type: none"> • Set forth proper risk management culture and risk appetite for the Group. • Evaluate and determine the level of risk that the Group should take and monitor regularly. • Set the strategic direction by putting forward strategies that are focusing on all key business, operation, as well as ESG-related risks, and such strategies should reflect and align with the Group’s values and core business. • Ensure that annual disclosure (including but not limited to ESG-related risks) is compliant with relevant regulations. • Demonstrate openness, integrity and accountability to stakeholders in the decision-making process.

Risk Management Role	Responsible Party	Key Responsibilities
2. Risk Oversight	Audit Committee	<ul style="list-style-type: none"> • Review the effectiveness of the Group’s risk management system which identifies, assesses, monitors and reports risks (including but not limited to business, operation and ESG-related risks). • Evaluate and ensure that appropriate and effective business, operation and risk management and internal control systems are in place. • Provide market insights and advices on enhancing the Group’s business performance and risk management. • Assess strategic risks and related reporting from respective Risk Owners.
3. Risk Governance	Risk Management Committee (“RMC”)	<ul style="list-style-type: none"> • Facilitate the risk assessment process and timely communication to Audit Committee, at least twice a year as required under the RMC’s Terms of Reference and to the Board of Directors where appropriate. • Ensure that all key risks (including but not limited to business, operation and ESG-related risks) are properly identified, managed and monitored.
4. Risk Owners	Heads of NWD corporate departments, and senior management of business units of the Group	<ul style="list-style-type: none"> • Identify, assess, monitor and report risks (including but not limited to business, operation and ESG-related risks) to the respective Risk Oversight Parties as stipulated in section 3.2 and section 5.6. • Ensure the effectiveness of risk management system and mitigation strategies • Execute all proper risk management and mitigation measures and actions as required to protect the Group’s interest and efficacy of business performance.
5. Risk Managers	Group Financial Controllers, Key Operation Heads, or Designated Responsible Officers	<ul style="list-style-type: none"> • Support the Risk Owners in setting proper risk culture, implementation of risk management framework, and oversight of risk information management. • Ascertain that risk management processes are properly in place and functioning as intended. • Make sure that operations are conducted effectively and efficiently with proper risk consideration, assessment and management (including but not limited to business, operation and ESG-related risks).

5. Risk Management Process

While all major risks constituting the risk adverse events as illustrated in section 3.2 above must be reported to responsible Risk Oversight Parties immediately, a regular risk review and assessment process to ensure that all major risks (including but not limited to business, operation and ESG-related risks) are properly identified, evaluated and monitored is important to the sound and effective risk management system.

On a half yearly basis, Risk Owners of all NWD corporate departments and business units of the Group are required to perform proper risk review and assessment by making use of either the **Risk Identification and Assessment Checklist** or any risk evaluation form specific to respective Risk Owners' division or business unit to perform such risk review and assessment.

5.1 Risk Identification

Risk identification is critical because a potential risk not identified at this stage is excluded from further analysis. Identification should include all risks whether or not they are under the control of the organization. Risk Owners also needs to consider carefully the factors that contribute to or increase risk, including issues such as past experience of failure to meet objectives; quality of personnel; significant changes, such as increased competition; legislative, regulatory and personnel changes; market developments, and the significance of particular activities to the entity and their complexity. For illustration purpose, **Appendix I** can be used to facilitate the risk identification process, and **Appendix II** provides a suggested list of major risks (which is not exhaustive) for reference.

5.2 Risk Analysis

Major risks that are identified by using Appendix I can be quantified as the likelihood (the probability that a risk event will occur) multiplied by its impact or consequence. Such a calculation yields an estimate of risk level. The purpose of the risk analysis phase is to gain an understanding of the level of risks to determine priorities according to their impact and likelihood and support decision-making about future actions. Please refer to **Appendix III** for the Risk Analysis and Evaluation Template which is used to facilitate the risk analysis and evaluation step.

5.3 Risk Evaluation

Having identified and then prioritized the significant risks in gross terms, risk evaluation is to make decisions about future risk actions which may include but not limited to:

- Whether a risk strategy should be undertaken
- Whether a risk needs mitigation
- Priorities for risk management

Risk evaluation involves comparing the levels of risk found during the risk analysis process with risk criteria established when the context is considered. It indicates predefined qualitative measures that identify the criteria for each level of risk (e.g. Catastrophic, High, Medium, Low and Negligible) on the **Risk Matrix**. Low and accepted risks should be monitored and periodically reviewed to ensure they remain acceptable. If

risks do not fall into the low or acceptable risk category, appropriate risk strategy and control measures should be in place and ready per **Risk Management Action Table**. The output of a risk evaluation is a prioritized list of risks for further action.

Risk Matrix (Risk Level = Probability x Impact):

Catastrophic	5	M(5)	H(10)	H(15)	VH(20)	VH (25)
High	4	L(4)	M(8)	H(12)	H(16)	VH(20)
Medium	3	L(3)	M(6)	M(9)	H(12)	H(15)
Low	2	VL(2)	L(4)	M(6)	M(8)	H(10)
Negligible	1	VL(1)	VL(2)	L(3)	L(4)	M(5)
Impact / Probability		1	2	3	4	5
		Remote	Unlikely	Possible	Likely	Almost certain

Proper delineation of risk level will help Risk Owners to facilitate better communication and consistent execution of risk actions in managing risks concerned.

Risk Management Action Table:

Risk Level	Risk Management Actions
Very Low (1-2)	Put into watch list
Low (3-4)	Keep higher awareness, on-going monitor, start a risk control strategy
Medium (5-9)	Risk strategy in place and control measures ready
High (10-16)	Risk strategy in place, control measures in action and communication with relevant risk oversight parties
Very High (20-25)	Risk strategy in place, control measures in action, as well as extensive communication with and involvement by the relevant risk oversight parties

5.4 Risk Treatment

Arising from risk evaluation, there will be a prioritized list of risks requiring treatment. Possible risk treatment options include:

- avoiding the risk entirely
- transferring or sharing the risk
- reducing the probability and/or the consequences of the risk
- accepting or retaining the risk

Selection of the most appropriate option involves balancing the cost of implementing each option against the benefits derived from it. In general, the cost of managing risks needs to be commensurate with the benefits obtained. Please refer to **Appendix IV** for the Risk Treatment Worksheet for identifying a range of options for treating these risks, assessing the likely effectiveness of those options, preparing treatment plans and implementing them.

5.5 Risk Monitoring

Daily risk monitoring is done by respective Risk Owners (who are supported by Risk Managers if available). On a half yearly basis, they should perform proper risk assessment on major risks identified, and submit to the responsible Risk Oversight Parties (to be further elaborated in section 5.6 below) a properly completed **Risk Management and Internal Control Assessment Checklist** (RM & ICA Checklist). Detailed risk assessment by respective Risk Owners can be conducted by either using:

- (i) **Risk Identification and Assessment Checklist** (RIA Checklist) per **Appendix V**; or
- (ii) Any risk evaluation form specific to respective Risk Owners’ division or business unit. Each Risk Owner is required to identify and delineate the top ten risks (together with necessary risk mitigation actions thereto) in the RM & ICA Checklist based on the risk assessment results.

NWD Risk Management Committee, assisted by GAMS Department, shall review all the submitted RM & ICA Checklists submitted by each Risk Owner, register all major risks and evaluate the risk management processes being undertaken by the respective Risk Owners concerned, and report the consolidated results to the Audit Committee where appropriate.

5.6 Risk Reporting

5.6.1 Reporting to NWD Risk Management Committee and GAMS Department

Risk Owners	Submission Document(s)	Collected and consolidated by	Reviewer(s)
NWD Corporate Departments	Mandatory: RM & ICA Checklist	GAMS Department	<ul style="list-style-type: none"> ▪ NWD Risk Management Committee ▪ GAMS Department
Business Units of the Group	Voluntary: RIA Checklist or any risk evaluation form		

Through the use of RM & ICA Checklist, Risk Owners systemically review and assess the effectiveness of all the internal controls over their business operations that are in place to mitigate the risks, identify potential new risks affecting their businesses and operations, design and execute control enhancement plans to address such new risks. On a half-yearly basis, Risk Owners of NWD corporate departments and business units are required to submit the completed RM & ICA Checklist to GAMS Department for consolidation. Both NWD Risk Management Committee and GAMS Department will review and report to the Audit Committee any key findings of RM & ICA Checklists.

5.6.2 Reporting to the Board of Directors on Risk Management

The Audit Committee, assisted by the Risk Management Committee, shall report to the Board of Directors on the following:

- (i) consider what are the significant risks and assess how they have been identified, evaluated and managed;
- (ii) assess the effectiveness of the Group's risk governance structure in managing the major risks;
- (iii) consider whether necessary actions are being taken promptly to remedy any significant failings or weaknesses; and
- (iv) consider whether the findings indicate a need for more extensive monitoring of the risk management system.

Communication to the Board of Directors will be done at least twice a year as required under the Risk Management Committee's Terms of Reference as contained herein in **Appendix VI**.

6. Implementation and Review of the Policy

While the Audit Committee has overall responsibility for implementation, monitoring and periodic review of this Policy, it has delegated the day-to-day administration of this Policy to the Risk Management Committee in which Head of GAMS Department is one of the committee members.

If there are any questions about the contents or application of this Policy, please contact Head of GAMS Department by email to groupinternalaudit@nwd.com.hk.

Appendix I – Risk Identification Template

Risk identification is the process of determining the individual risks that are present and relevant to the Group (please refer to Appendix II – Key Risk Checklist for reference)

Risk Category		Specific Risks
External Factors	Political	
	Environmental	
	Social	
	Technological	
	Economic	
	Legal	
Internal Factors	Financial	
	Operational	
	People	
	Strategic	
Others		

Appendix II - Suggested List of Major Risks (Not Exhaustive)

The following Key Risk Checklist illustrates some of the major risks (including but not limited to business, operation as well as environmental, social and governance related risks) that may need to be considered, but this list is not exhaustive. Actual risks faced by a corporate department or business unit may include more industry-specific types of risks and relate to their particular circumstances.

External Factors

Political	Economic
Global political forces Central government interference Political/social instability/civil unrest (local) Political party/pressure group changes Political direction changes Government policy/constitutional changes Social group pressure Licensing requirements	Economic climate (local/global) GDP/GNP/CPI Oil/material prices Land/property/stock prices Interest rates/Forex/taxation Foreign investments Trade/market/economic cycles Unemployment rates
Environmental	Technological
Climate change impacts on business Environmental laws/regulations changes Pollution/contamination Hygiene/public health/contagious diseases Environmental group pressure Natural disasters	Technology change/breakthrough Cyber risk / hacking System/product life cycle/obsolescence Technology obsolescence Intellectual property rights Competing technologies
Social	Legal
Customer needs/tastes changes Ethical/religion issues Health and safety Demographic changes Culture/education	Changes in laws and regulations Contractual breaches Product liability/warranty Litigation Compliance

Internal Factors

People	Financial
Trade/labor union Key-man/leadership issue (succession) Money laundering/terrorist financing Compensation/reward/appraisal system Integrity, loyalty, commitment, morale Disputes/strike/claims Qualification/experience/caliber Business/social connections Bribery/corruption/fraud Workplace harassment/discrimination	Financial resources & gearing structure Cashflow/liquidity problems New accounting pronouncements Capex (investment) requirement Costing (fixed vs variable) Credit (accounts receivables/payables) Yield/return requirement Currency/interest rates Breach of financial undertakings/covenants Settlement
Operational	Strategic
Time/logistics/process of projects Quality/health/safety/environmental issues Stocks/overheads Supply chain partnership management Business impact Data security/knowledge management Material insurance coverage/legal claims	Competitive edge Merger & acquisition Market niche/segmentation Branding/reputation/accreditations Business model Strategic partnering/alliance Corporate governance/organization structure

Appendix III – Risk Analysis and Evaluation Template

Out of the major risks identified in Appendix I, please calculate and rank their risk levels (i.e. probability x severity)

Identified Key Risks		Probability	Severity (Impact)	Risk Level	Ranking
		<i>Unlikely 1 2 3 4 5 Very likely</i>	<i>Very low 1 2 3 4 5 Very high</i>	<i>Prob. x Impact</i>	
<i>Example</i>	<i>Terrorist attack</i>	<i>1 (Very unlikely)</i>	<i>5 (Very severe)</i>	<i>5</i>	
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Appendix IV – Risk Treatment Worksheet

Using the prioritized risks from the Risk Assessment, please identify a range of options for treating these risks, assessing the likely effectiveness of those options, preparing treatment plans and implementing them.

Identified Risk			
Managing Tactics			
Action Plan 1		Action Plan 2	
<input type="checkbox"/> Avoid <input type="checkbox"/> Transfer <input type="checkbox"/> Reduce <input type="checkbox"/> Accept	(state actions)	<input type="checkbox"/> Avoid <input type="checkbox"/> Transfer <input type="checkbox"/> Reduce <input type="checkbox"/> Accept	(state actions)
Consideration (Resources, time, manpower, etc.)			
Pros and Cons	Pros: Cons:	Pros: Cons:	
Decision			
Contingency Plan			

Appendix V – Risk Identification and Assessment Checklist

The Risk Identification and Assessment Checklist is a simple self-evaluation tool to facilitate your risk assessment by identifying the major risks (including but not limited to business, operation as well as environmental, social and governance (“ESG”) related risks) facing your Division/Business Units. A likelihood and impact decision-making table is included to generate an estimate of risk level (i.e. a combination of probability and impact) for each risk so that the major risks identified can be prioritized and appropriate risk management measures/strategies can be determined accordingly.

		Probability <i>(P) (1-5)</i> <i>(Note 1)</i>	Impact <i>(I) (1-5)</i> <i>(Note 2)</i>	Risk Level <i>(R= P x I)</i> <i>(Note 3)</i>	Risk Mgmt Actions, if any <i>(Note 4)</i>	Remarks
External Factors						
	Political					
1.	Change of political direction					
2.	Political / social instability / civil unrest					
3.	Government interference					
4.	Government policy / legislation / constitutional changes					
5.	Social group pressure					
6.	Licensing requirements					
7.	Others (pls specify)					
	Economic					
8.	Economic climate (local / global)					
9.	Oil / material prices					
10.	Land / property / stock prices					
11.	Interest rates / Forex / taxation					
12.	Trade / market / economic cycles					
13.	Unemployment rates					
14.	Others (pls specify)					
	Social					
15.	Change of customer demands					
16.	Ethical / religion issues					
17.	Health and safety					
18.	Demographic changes					
19.	Culture /education					
20.	Reputational risks (pls specify)					
21.	Others (pls specify)					
	Technological					

		Probability <i>(P) (1-5)</i> <i>(Note 1)</i>	Impact <i>(I) (1-5)</i> <i>(Note 2)</i>	Risk Level <i>(R= P x I)</i> <i>(Note 3)</i>	Risk Mgmt Actions, if any <i>(Note 4)</i>	Remarks
22.	Technology change / breakthrough					
23.	New products / services					
24.	Technology obsolescence					
25.	Intellectual property rights (both protection and infringement)					
26.	Competing technologies					
27.	Others (pls specify)					
	Environmental					
28.	Climate change impacts and disruptions to company assets and operations (e.g. extreme weather events, severe pollution, natural disasters, sea level rise, etc.)					
29.	Change of environmental law and regulation					
30.	Waste management / pollution / contamination					
31.	Hygiene / public health / contagious diseases					
32.	Public pressure (pls specify groups, e.g. NGOs, academia, key opinion leaders)					
33.	Others (pls specify)					
	Legal					
34.	Changes in laws and regulations					
35.	Contractual breaches					
36.	Product liability / warranty					
37.	Litigation					
38.	Compliance					
39.	Others (pls specify)					

		Probability <i>(P) (1-5)</i> <i>(Note 1)</i>	Impact <i>(I) (1-5)</i> <i>(Note 2)</i>	Risk Level <i>(R= P x I)</i> <i>(Note 3)</i>	Risk Mgmt Actions, if any <i>(Note 4)</i>	Remarks
Internal Factors						
	Financial					
40.	Financial resources & gearing structure					
41.	Cashflow / liquidity problems					
42.	Capex (investment) requirement					
43.	Costing (fixed vs variable)					
44.	Credit (accounts receivables / payables)					
45.	Yield / return requirement					
46.	Currency / interest rates					
47.	Breach of financial undertakings / covenants					
48.	Settlement					
49.	Litigation costs					
50.	Compliance costs					
51.	Losses resulted from bribery / corruption / fraud / extortion / money laundering					
52.	New accounting pronouncements					
53.	Others (pls specify)					
	Operational					
54.	Time / logistics / process of projects					
55.	Quality issues in products / projects / services					
56.	Safety issues in products / projects / services					
57.	Stocks / inventory management					
58.	Procurement / purchasing					
59.	Supply chain management (e.g. relationship with and training / support provided to partners, suppliers, subcontractors, etc.)					
60.	Overheads					
61.	Privacy and data security / knowledge management					

		Probability (P) (1-5) <i>(Note 1)</i>	Impact (I) (1-5) <i>(Note 2)</i>	Risk Level (R= P x I) <i>(Note 3)</i>	Risk Mgmt Actions, if any <i>(Note 4)</i>	Remarks
62.	Insurance coverage / legal claims					
63.	New accounting pronouncements					
64.	New business models, products or activities					
65.	Expanded foreign operations					
66.	Change in corporate structure					
67.	Environmental issues (e.g. toxic emissions, waste management, water stress, etc.)					
68.	Health and safety (e.g. increasing incidents for both corporate employees and supply chain partners; lack of measures and performance targets to reduce the chance of incidents)					
69.	Anti-competitive practices					
70.	Impacts of business activities on the community					
71.	Others (pls specify)					
	People					
72.	Disputes / strikes / claims / labour management					
73.	Succession (e.g. key-man / leadership issue)					
74.	Compensation / reward / appraisal system					
75.	Integrity, loyalty, commitment, morale					
76.	Qualification / experience / calibre					
77.	Bribery / corruption / fraud / extortion / money laundering / terrorist financing					
78.	Workplace harassment / discrimination					

		Probability <i>(P) (1-5)</i> <i>(Note 1)</i>	Impact <i>(I) (1-5)</i> <i>(Note 2)</i>	Risk Level <i>(R= P x I)</i> <i>(Note 3)</i>	Risk Mgmt Actions, if any <i>(Note 4)</i>	Remarks
79.	Illegal labour (hiring of illegal immigrants, child labour, forced labour, unlicensed workers as employees or supply chain partners)					
80.	Capacity for regulatory compliance (pls specify if any training or seminar is provided on health and safety, industry codes, and new policies and performance targets set for capacity building)					
81.	Others (pls specify)					
	Strategic					
82.	Competitive edge					
83.	Merger & acquisition					
84.	Branding / reputation / accreditations					
85.	Business model					
86.	Strategic partnering/alliance					
87.	Corporate governance / organization structure					
88.	Others (pls specify)					
	Others					
89.	(pls specify)					
90.	(pls specify)					
91.	(pls specify)					

Note 1:

Probability (P)	Description	Probability of Occurrence
1	Remote	<1%
2	Unlikely	1 - 10%
3	Possible	10 - 40%
4	Likely	40 - 75%
5	Almost certain	>= 75%

Note 2:

Impact (I)	Description	Impact on Operating Profit (example only)
1	Negligible	<1%
2	Low	1 - 3%
3	Medium	3 - 5 %
4	High	5 - 10%
5	Catastrophic	>= 10%

Note 3:

Risk Level (R) = Probability (P) x Impact (I)

Catastrophic	5	M(5)	H(10)	H(15)	VH(20)	VH (25)
High	4	L(4)	M(8)	H(12)	H(16)	VH(20)
Medium	3	L(3)	M(6)	M(9)	H(12)	H(15)
Low	2	VL(2)	L(4)	M(6)	M(8)	H(10)
Negligible	1	VL(1)	VL(2)	L(3)	L(4)	M(5)
Impact / Probability	1	2	3	4	5	
	Remote	Unlikely	Possible	Likely	Almost certain	

Note 4:

Risk Level	Risk Management Actions
Very Low (1-2)	Put into watch list
Low (3-4)	Keep higher awareness, on-going monitor, start a risk control strategy
Medium (5-9)	Risk strategy in place and control measures ready
High (10-16)	Risk strategy in place, control measures in action and communication with relevant Risk Oversight Parties
Very High (20-25)	Risk strategy in place, control measures in action, as well as extensive communication with and involvement by the relevant Risk Oversight Parties (e.g. senior management of business units)

Appendix VI – Risk Management Committee - Terms of Reference

1. Establishment:

The Risk Management Committee (the “Committee”) is established pursuant to a resolution passed by the Audit Committee of New World Development Company Limited (the “Company”) at a meeting held on 18th February 2016. The Committee is under the oversight and supervision of the Audit Committee of the Company.

2. Membership:

- (a) Members of the Committee shall consist of not less than four members (including the Head of Group Audit and Management Services Department).
- (b) The Chairman of the Committee shall be elected by its members, and shall ensure that the Committee operates and discharges its duties efficiently.
- (c) The company secretary of the Company or any person appointed by the Committee shall be the secretary of the Committee. In the absence of the secretary of the Committee, the members present shall elect one of themselves or appoint another person as the secretary for that meeting.
- (d) The appointment of the members or secretary of the Committee can be revoked, or addition of new members can be appointed by the Committee. If a member resigns, or for any other reason ceases to be a member of the Committee resulting in the number of members to fall below the minimum, Chairman of the Committee shall, within three months of that event, appoint such number of new members as may be required to make up the minimum.
- (e) Only members of the Committee or their delegates have the right to attend Committee meetings. Other persons including but not limited to any directors, management, external advisors or consultants may be invited by the Committee to attend for all or part of any meeting as and when appropriate.

3. Meeting:

(a) Notice

- (i) A meeting of the Committee may be convened by any of its members through the secretary of the Committee.
- (ii) Unless otherwise agreed by all the members of the Committee, either orally or in writing, notice of each meeting stating the purpose, time, date and place of the meeting shall be given to each member of the Committee and any other person invited to attend the meeting at least three days prior to the date of the meeting.
- (iii) Agenda and any supporting documents and papers shall be forwarded to each member of the Committee and any other person invited to attend the meeting at least three days prior to the date of the meeting or such other period as the members may agree.

(b) Quorum

- (i) The quorum of the Committee meeting shall be at least two. Each member shall be entitled the right of one vote. Any resolution of the Committee shall require a majority of vote.
- (ii) In the case of any equality of votes, the chairman of the meeting shall have an additional or casting vote.
- (iii) Members must abstain from voting in respect of any resolution in which he is an interested party.

(c) Participation

- (i) Members may participate in any meeting of the Committee by means of a conference telephone or other communication equipment through which all persons participating in the meeting can communicate with each other simultaneously and instantaneously and, for the purpose of counting a quorum, such participation shall constitute presence at a meeting as if those participating were present in person.
- (ii) A resolution in writing signed by all members of the Committee shall be as valid and effectual as if it had been passed at a meeting of the Committee. Any such resolution may be contained in a single document or may consist of several documents in like form each signed by one or more of the members of the Committee.

(d) Frequency of Meeting

The Committee shall meet not less than twice a year. It can be convened and held by attending in person, by telephone or video conference. Additional meetings may be held as and when the Committee considers necessary.

(e) Minutes of Meeting

Following approval of the minutes by the Chairman of the Committee, the minutes shall be circulated by the secretary of the Committee to all members of the Committee for their comments and record respectively, in both cases within a reasonable time after the Committee meeting is held.

4. Duties:

The duties of the Committee shall include the following:

- (a) To review the effectiveness of the Company's risk management function;
- (b) To review and assess the Company's risk appetite;
- (c) To review and monitor the Company's risk profiles taking into consideration the Company's risk appetite and the prevailing and forward-looking aspects of risk exposures and to ensure an appropriate risk control environment is enforced and maintained;
- (d) To review and assess the methodologies employed by management to identify, measure, manage and/or control risks that may have an impact on the business in accordance with the Company's risk appetite and risk management policy;

- (e) To enhance constructive discussion, effective communication and timely escalation of risks by adopting a common platform for risk management;
- (f) To review and assess the half-yearly Risk Management and Internal Control Checklist including confirmation from management of respective corporate departments and business units that risk management is properly in place and enforced, and those key risks escalated by them where appropriate;
- (g) To review and assess the Company's risk management policy from time to time;
- (h) To provide its recommendation in relation to the above matters, with a holistic view of the Group's material risk exposures and steps taken to manage and monitor such exposures, to the Audit Committee for consideration; and
- (i) To perform such other duties as may be delegated to the Committee by the Audit Committee.

5. Authority:

The Committee is authorized:

- (a) to have access to such information and advice, both from within the Company and externally, as it deems necessary in order to perform its duties;
- (b) to obtain, at the Company's expense, outside legal or other professional advice on any matter within its terms of reference; and
- (c) to be provided with sufficient resources to discharge its duties.

6. Reporting Procedures:

- (a) The Committee shall report directly to the Audit Committee on its findings, decisions and/or recommendations, if any.
- (b) The secretary of the Committee shall also circulate the minutes of meetings, reports and/or written resolutions of the Committee to all members of the Audit Committee if required.

- END -