AUDIT AND RISK COMMITTEE REPORT

ROLE OF THE AUDIT AND RISK COMMITTEE

The audit and risk committee has an independent role with accountability to the Board and shareholders. The committee's role is to assist the Board in carrying out its duties relating to accounting policies, internal controls, financial reporting practices and identification of significant risk exposure.

The main purpose of the audit and risk committee is to ensure the integrity of the financial statements and to oversee the effectiveness of the internal financial controls and the external and internal audit functions.

The audit and risk committee undertook a review of the audit function performed by the independent auditors of the Group. In terms of the Companies Act, The committee confirms that the same audit partner has not served as the designated auditor of the Company for more than five consecutive financial years.

The Group has internal controls and systems designed to provide assurance as to the reliability and integrity of the financial statements. The system of internal control is designed to manage, rather than eliminate, the risk of failure to achieve the Group's business objectives. It can only provide reasonable and not absolute assurance against material misstatement or loss and to safeguard, verify and maintain accountability adequately for its assets. (– *Principles 2, 4, 10, 11, 12, 13 and 15*)

The external and internal auditors had unrestricted access to the audit and risk committee and attended all the committee meetings by invitation during the year ended 31 August 2019. Detailed reports were presented by the internal and external auditors. The chairman of the audit and risk committee reported on the findings at the Board meetings.

The external auditors can communicate with the chairman of the audit and risk committee and all its members throughout the year. The chairman of the committee is also available at the AGM to answer questions about the committee's activities.

For the reporting year under review, the committee is satisfied that is has fulfilled all its statutory duties assigned by the Board.
(– *Principles 2, 4, 5, 10, 11, 12, 13, 15 and 16*)

REPORT OF THE AUDIT AND RISK COMMITTEE

The audit and risk committee has a formal audit and risk charter with formal rules governing the services provided by the external auditors in terms of systems and processes.

The committee reviewed all significant risks and challenges and assessed the adequacy of internal controls and the combined assurance delivered over the identified risks. It monitored the effectiveness of the control environment through reviewing reports from management, the external auditors and internal audit and ensured the quality of financial reporting by reviewing the 2019 interim financial results and the 2019 annual financial statements.

The committee reviewed the impact of the Company's medium to long-term strategy against pertinent factors of technology and communication, including cybersecurity and governance compliance to ensure that risk management was applied appropriately.

The committee reviewed the following:

- After receiving the Competition Commission's approval due to the change in its network firm from BDO Cape Inc. to BDO South Africa Inc. BDO South Africa Inc. were the company's auditors for 22 years (PKF for 17 years and four years as Grant Thornton Cape Inc. and one year as BDO Cape Inc.).
- The performance, independence, appointment and remuneration of the external auditors and the audit process.
- Internal financial controls and systems are monitored through the internal auditors and external audit findings, and the action taken by management from the significant findings.
- The effectiveness of risk management and controls through the evaluation of the risk management report and group risk register.
- The quality and integrity of the integrated report, including the annual financial statements and public announcements in respect of the financial results.
- The effectiveness of the internal audit function by monitoring the scope and execution of its audit plan, independence, skills, staffing and overall performance.
- Sustainability and environmental issues.
- Governance compliance.

AUDIT AND RISK COMMITTEE REPORT - continued

In the conduct of its duties and in accordance with section 94 of the Companies Act, the committee:

- considered the separate information about BDO South Africa Inc., the receiving audit firm, as the Company is deemed to be appointing BDO South Africa for the first year;

- satisfied itself that the external auditor BDO South Africa Inc. is independent of AEEI, as set out in section 94(8) of the Companies Act and considering, *inter alia*, the information stated in paragraph 22.15(h) of the JSE Listings Requirements;

- ensured that the appointment of the external auditor complied with the Companies Act;

- BDO South Africa Inc have advised that they will not make themselves available for re-election at the next AGM.

- the company is in the process of appointing new auditors for election at the AGM.

- recommended to the Board, the interim and preliminary announcements of results, interim reports, trading statements and approved the restatement of the prior year's interim results;

- reviewed the annual financial statements of the Company, the Group and its subsidiaries and considered the audit report and findings, together with combined assurance from management and the external auditors and recommended it for approval by the Board;

- reviewed the disclosure within the integrated report and reports to shareholders, taking into account all factors and risks that may impact on the integrity of the integrated report, including factors that may predispose management to present a misleading picture, significant judgements and reporting decisions made, monitoring of enforcement actions by a regulatory body, any evidence that brings into question previously published information, forward-looking statements or information;

- considered concerns regarding accounting practices and internal audit matters;

- continued to oversee the Group's 10 risks and its strategy to ensure that the Group manages its risks in an optimal manner;

- approved, reviewed and evaluated the adequacy and efficacy of the risk policies, procedures and controls applied in the day-to-day management of the business;

- reviewed and approved the response to the JSE proactive monitoring letters related to the 2017 annual financial statements and considered the action taken by management from the findings recommended in the 2018 report;

- obtained assurance from the external auditors that

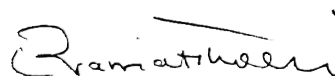adequate accounting records are being maintained;

- approved non-audit services when required for tax opinions and any independent internal quality assurance reviews related to the internal auditor's operational audits;

- evaluated the independence, effectiveness and performance of the internal auditor and compliance with its charter; and

- reviewed the appropriateness of the expertise and experience of the financial management team and reported these to be adequate.

For the purposes of determining the effectiveness of management systems and internal controls during the year, the committee reviewed the internal audit methodology and external audit plans and findings from the management reports.

Due to the restructure of the Board during the year, the audit and risk committee was affected and was seen to be non-compliant from 18 April to 23 September 2019.

The committee was reconstituted post year-end and fulfilled its statutory duties in terms of section 94(7) of the Companies Act and King IV™ compliance. As at the reporting date, the committee was compliant.

The committee confirms that it has complied with its legal and regulatory responsibilities for the 2019 financial year. (🗎 – *Principles 10, 11, 12, 13 and 15*).

Advocate Dr Ngoako Ramatlhodi
Audit and risk committee chairman

EXPERTISE AND EXPERIENCE OF THE CHIEF FINANCIAL OFFICER AND THE FINANCE FUNCTION

The audit and risk committee satisfied itself in terms of paragraph 3.84(g)(i) of the JSE Listings Requirements that the Group CFO and the finance function have the appropriate expertise and experience and are adequately resourced.

RISK MANAGEMENT PROCESS

A key component of the audit and risk committee was to review the top 10 material matters that AEEI faces in order to respond to new and emerging risks and to ensure alignment with regulatory changes as well as best practice. In doing so, the committee took into account stakeholder needs, corporate governance principles, risk trends, global trends and external dynamics. Refer to page 28 for the full risk management report.

AUDIT AND RISK COMMITTEE REPORT - continued

COMPLIANCE

The audit and risk committee is responsible for reviewing the compliance with legal, regulatory, codes and other standards and continually monitors the implementation of the legal compliance processes. The audit and risk committee is satisfied that it has complied with all its legal, regulatory and other responsibilities during the year. (– *Principle 13*)

GROUP INTERNAL AUDIT

The Group internal auditor performs an independent assurance function. The Group internal auditor had unrestricted access to the Group CEO, the Group CFO and the chairman of the audit and risk committee.

The primary objective of the Group internal auditor during the year was to provide independent objective assurance and consulting activities on the adequacy and effectiveness of the Group's systems of governance, risk management and internal control. The Group internal auditor reports functionally to the audit and risk committee and administratively to the Group CFO. The audit and risk committee monitored the effectiveness of the internal audit function in terms of its scope, independence, skills, execution of its plan and overall performance.

The Group internal auditor recommended the annual internal audit plan for approval to the audit and risk committee. The committee approved the formal internal audit plan, which included risk-based operational and system audits on the Group's governance and business processes for 2019. The operational internal audit plan was reviewed by an independent external firm.

The system of internal control is designed to ensure that significant risks are appropriately identified, managed and provide reasonable assurance that:

- company assets and information are safeguarded;
- operations are efficient and effective; and
- applicable laws and regulations are complied with.

The Group internal auditor undertook the following during the year:

- Prepared and submitted a risk-based internal audit plan to the audit and risk committee for review and approval
- An independent review of the internal audit plan by Nexia SAB&T
- Implemented recommendations by Nexia SAB&T on quality improvement of the internal audit function
- Performed reviews on the Company's governance processes and ethics

- Systematically analysed and evaluated the business processes and associated controls
- Performed consulting activities requested by management
- Followed a risk-based approach
- Monitored and challenged, where appropriate, action taken by management with regard to the internal audit findings
- Monitored and reported on the risk management process to the audit and risk committee
- Liaised with the external auditors as part of the combined assurance process where internal audit followed up and ensured that management implemented the external auditors' recommendations from the prior year
- Provided a source of information on fraud, corruption, unethical behaviour and irregularities

The internal audit takes a risk-based approach to audit planning. Internal audits were performed at most subsidiaries during the year and no significant breakdowns in internal controls were identified. A formal quarterly report on the key findings of these audits was submitted to the audit and risk committee summarising the results of the internal audit activity and management's progress in addressing the control measures. This enabled the audit and risk committee to ensure that action was taken to address areas of concern. (*King IV™ – Principles 11 and 15*)

The chairman of the audit and risk committee reported to the Board on the activities of the committee at each Board meeting.

EXTERNAL AUDIT

The scope, independence and objectivity of the external auditors, BDO South Africa Inc., were reviewed. The committee considered the annual audit plan and related scope of work, determined the terms of engagement and fees of the external auditors. In the committee's opinion, the audit firm, BDO South Africa Inc., and the audit partner are independent of the Company and the Group.

BDO South Africa Inc. provided an audit opinion in accordance with the Companies Act, the JSE Listings Requirements and King IV™. Under company law, their responsibility is to the shareholders of the Group. In addition, they have professional responsibilities to report reportable irregularities in terms of section 45(1) of the Auditing Profession Act, 2005, and key audit matters in their audit report to the committee.

AUDIT AND RISK COMMITTEE REPORT - continued

AUDIT PROCESS

The audit process included:

PHASE I	PHASE II	PHASE III	PHASE IV	PHASE V
Planning	Assessing risk	Testing internal controls	Substantive testing	Concluding and reporting

AUDIT OBJECTIVES

The audit was conducted in accordance with International Standards on Auditing and the auditors' objective was to provide a comprehensive service to the Group.

The primary objective as independent auditors is to form an opinion as to whether or not the annual financial statements:

- fairly represent the financial position of the Company;
- fairly represent the results of operations and cash flows for the Company and the Group for the year;
- comply with statutory and regulatory requirements, including the JSE Listings Requirements; and
- have been prepared in terms of the Company's accounting policies, applied on a consistent basis in terms of IFRS and conform to the JSE Listings Requirements.
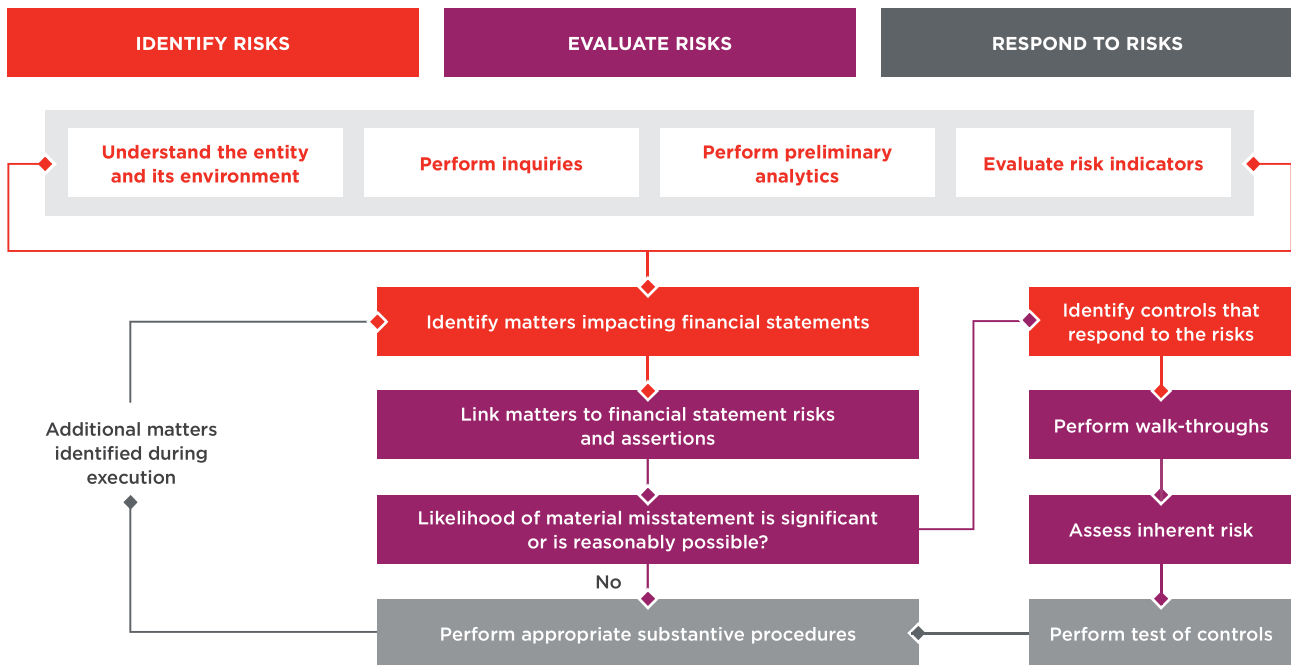
The audit was directed at delivering assurance at three levels:

1. For shareholders and other stakeholders
2. Independent opinions and reports that added credibility to the financial information released by the Company
3. Compliance with the requirements of the various regulatory bodies and legislation, including IFRS, the Companies Act and the JSE Listings Requirements

They assisted the audit and risk committee in discharging their corporate governance and compliance responsibilities. They provided advice on financial reporting and business issues and made recommendations to management to improve internal controls and business efficiencies to add further value to the Company.

AUDIT AND RISK COMMITTEE REPORT - continued

AUDIT METHODOLOGY

IDENTIFY RISKS	EVALUATE RISKS	RESPOND TO RISKS

Understand the entity and its environment	Perform inquiries	Perform preliminary analytics	Evaluate risk indicators

Identify matters impacting financial statements

Identify controls that respond to the risks

Additional matters identified during execution

Link matters to financial statement risks and assertions

Perform walk-throughs

Likelihood of material misstatement is significant or is reasonably possible?

Assess inherent risk

No

Perform appropriate substantive procedures

Perform test of controls

The audit involved performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depended on the auditors' judgement, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditors considered internal controls relevant to the Company's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Company's internal control. The audit included evaluating the appropriateness of accounting policies used and the reasonableness of accounting estimates made by management, as well as evaluating the overall presentation of the financial statements. (– *Principles 15 and 16*)

As the auditors of a public interest company, the same individual has not served as audit partner of the engagement for more than five consecutive financial years. BDO South Africa Inc. has been the Company's auditors for the past twenty-two years, with Mr Imtiaaz Hashim serving as audit partner.

The external auditors liaised with the Group internal auditor and attended the audit and risk committee meetings by invitation. As the auditors of the Company, they attend every AGM where the annual financial statements of the Company for the financial year are presented, in order to respond accordingly and to answer any questions relevant to the audit of the financial statements.

JSE'S PROACTIVE MONITORING

The Company's audit and risk committee considered the findings recommended by the JSE's proactive monitoring report and reviewed and approved the appropriate action taken by executive management to increase the resources and improve on the review process to improve the presentation of the annual financial statements.

The audit and risk committee members were made aware of the numerous letters presented by the JSE's Proactive Monitoring process. They reviewed the appropriate action taken by executive management to include additional disclosure in the interim reports and to disclose the prior period error in the 2019 interim results related to the investment in associate.

The proactive monitoring process has brought about a more assertive approach to improve the quality of financial reporting to stakeholders and investors. The committee has considered the areas that are highlighted in the proactive monitoring process that commenced in October 2018 and have actively reviewed the focused areas which will impact the 2019 annual financial statements.

RISK MANAGEMENT REPORT

The Board has delegated the management of risk to the audit and risk committee. The Board is committed to effective risk management in pursuit of the Group's strategic objectives with the aim of growing shareholder value sustainably. The Board understands that proactive risk management is both an essential element of good corporate governance and an enabler in realising opportunities and continues to enhance its capabilities to anticipate risks and manage them.

OUR APPROACH TO RISK MANAGEMENT

The Group's risk management approach continues to evolve. The audit and risk committee continued to assess, manage and report on all significant risks, the impact on the business and the mitigation of the risks.

The audit and risk committee also assessed whether the risk management process is effective in identifying and evaluating risks to determine whether the business operations have managed the risks in line with the Group's strategy and to consider the impact on the sustainability of the business, the external and internal environments in order to identify key developments related to our risks, implications and our responses.

The responsibility for monitoring the management of each of these risks is assigned to the executive committee of each business unit. The risks are then considered at a Group level through the monitoring process of the audit and risk committee.

Risk registers are tabled at each subsidiary Board meeting under the categories of financial, operational, strategic, legal, human resources and other risks. Action plans are monitored and discussed to reduce the risks to acceptable levels as per the risk appetite and tolerance levels. From the risk evaluation in the risk register, significant risks are reported to the audit and risk committee, who in turn reports these risks to the Board.

There were no specific risk incidents which resulted in significant financial loss or which may have negatively impacted our stakeholders during the 2019 financial year.

GOVERNANCE OF RISK MANAGEMENT THE THREE LINES OF DEFENCE

AEEI realises the importance of the three lines of defence in managing risk and has assigned the responsibilities and accountability in line with the three lines of defence.

FIRST LINE OF DEFENCE

Management is responsible for the implementation of the business strategy and the identification of risks and the design of related controls. It is the responsibility of management to monitor the controls implemented to mitigate the risks.

SECOND LINE OF DEFENCE

Risk management is the second line of defence where risks are assessed, evaluated and measured. The residual risk is measured against the risk appetite and tolerance levels set by the Board.

THIRD LINE OF DEFENCE

The internal and external assurance providers are the third line of defence. During the year, the audit and risk committee appointed an independent external audit firm to perform a strategic and operation risk assessment on the listed subsidiary. The results of those risk assessments were communicated to the audit and risk committee.

RISK MANAGEMENT REPORT - continued

BOARD		
STRATEGY, RISK APPETITE AND POLICY		
RISK OWNERSHIP	**RISK CONTROL AND MONITORING**	**INDEPENDENT ASSURANCE AND VALIDATION**
CEO AND EXECUTIVE COMMITTEE	AUDIT AND RISK COMMITTEE	INTERNAL AND EXTERNAL ASSURANCE
DOING AND RECORDING	**INTERNAL VERIFICATION**	**INDEPENDENT VERIFICATION**
Delegated Board authority to: • develop and implement the business strategy; • measure and manage performance; and • implement internal control and risk management framework within agreed appetite.	Objective oversight of risks Key activities include: • designing and deploying the overall risk management framework; • developing and monitoring policies and procedures; and • monitoring adherence to risk framework and strategy.	• assurance that the risk management process is functioning as designed and identifies improvement opportunities; and • independent and objective assurance of the effectiveness of corporate governance standards and business compliance.
MANAGEMENT-BASED ASSURANCE	**AUDIT AND RISK COMMITTEE ASSURANCE**	**INDEPENDENT-BASED ASSURANCE**

As part of Vision 2020 Vision, AEEI identified 10 material matters with each material matter having strategic objective/s. The material risks that are identified are linked to the strategic objectives in these material matters.

The executive committee of the divisional subsidiaries are accountable and responsible for managing risks within their business units and may delegate specific responsibilities appropriately. This process is evaluated by the Group Internal Audit who provides the audit and risk committee with assurance that significant business risks are systematically identified, assessed and reduced to acceptable levels in line with the Board's risk appetite and risk tolerance levels.

During the financial year, the audit and risk committee:

• assisted the directors in fulfilling their responsibilities for ensuring there is an effective risk management process in place throughout the Group;
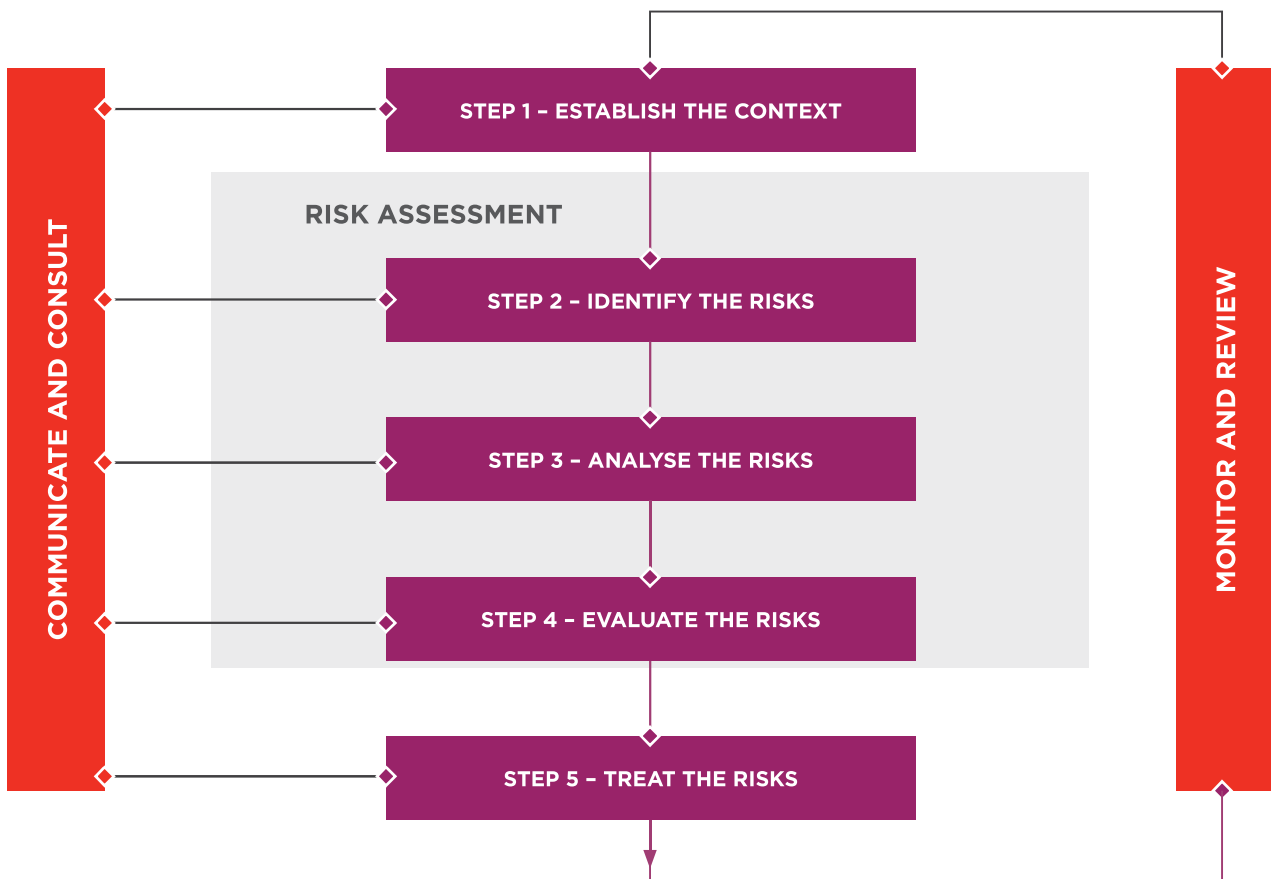
• assessed reports from management concerning the Group's risk management and compliance processes and controls in order to oversee their effectiveness;

• assessed reports from divisional management concerning business, operational and compliance risk in order to oversee their risks and assess their impact on the Group;

• assessed reports from management concerning the risk implications of new and emerging risks, legislative or regulatory initiatives and changes in order to ensure the risk is held at an acceptable level;

• received reports from management concerning resolution of significant risk exposure and risk events, in order to monitor them in accordance with the Board's risk appetite;

RISK MANAGEMENT REPORT - continued

- assessed whether all significant new business opportunities have been appropriately considered from a risk perspective;
- monitored the Group's compliance with applicable external and regulatory obligations, and significant internal policies relating to the operation of its business units;

- facilitated communication of risk issues to all management; and
- evaluated the results of the risk assessments performed by the external independent firm and plan of action by management.

The Company complies with the principles of King IV™ related to risk management.

RISK MANAGEMENT PROCESS

The structure of our risk management process is set out below. This structure was rolled out across the entire Group and is in line with industry standards.

COMMUNICATE AND CONSULT

MONITOR AND REVIEW

STEP 1 – ESTABLISH THE CONTEXT

RISK ASSESSMENT

STEP 2 – IDENTIFY THE RISKS

STEP 3 – ANALYSE THE RISKS

STEP 4 – EVALUATE THE RISKS

STEP 5 – TREAT THE RISKS

RISK MANAGEMENT REPORT - continued

COMMUNICATE AND CONSULT	Communicate and consult with those who are involved in the assessment of the risks and engage those who will be involved in treating, monitoring and reviewing the risks
ESTABLISH THE CONTEXT	Consider the environment internally and externally within which the risks are present
IDENTIFY THE RISKS	Identify all possible uncertainties (risks) that may impact and prevent the organisation from achieving its objectives
ANALYSE THE RISKS	Analyse and assess the risks in terms of likelihood and impact
EVALUATE THE RISKS	Compare the level of risk found during the analysis process and decide whether these risks are acceptable or require treatment
TREAT THE RISKS	Identify actions and controls to manage the inherent risks to an acceptable residual level, and then assess the effectiveness of the actions and controls
MONITOR AND REVIEW	Monitor risks and review the effectiveness of the treatment plan, strategies and management system

STRATEGIC OBJECTIVE	Apply risk management process	**OUTCOME** Risk mitigating and implementation choices	**STRATEGY EXECUTION** Manage risk exposure Risk control and measurement	**RISK MANAGED OUTCOMES**

RISK MANAGEMENT REPORT - continued

Financial	Human Capital	Business Operations	Macroeconomic	The environment	Social and relationship capital

MATERIAL RISKS

	RISK AND RATIONALE	MITIGATION	OPPORTUNITY	LINK TO MATERIAL MATTER/ STRATEGY
1	Reallocation of the long-term fishing rights may impact the profitability of the fishing segment.	Active engagement with communities for outside quota holders Monitoring government policy and processes on requirements for reallocation Diversification into other products to reduce the impact on growth strategy Expansion in the aquaculture division to minimise impact	Favourable quota allocation by the Department of Agriculture, Forestry and Fisheries will substantially increase revenue, resulting in better financial performance by the Group, which will also present an opportunity for more spend on SMMEs as well as socio and economic investments.	
2	The loss of major customers could result in a potential reduction in revenue in the information and communications technology (ICT) sector.	Pursue and extend client base, underpinned by long-term support and maintenance agreements	Gain business confidence from stakeholders resulting in long-term relations	
3	Compliance with the CIPC and JSE Listings Requirements; and all legislation and regulations require the Group to constantly adapt to keep abreast of the latest changes	Training and awareness is continuously assessed and provided across the Group. Policies and procedures are updated to adapt to all new regulations and legislative requirements on a regular basis. King IV™ compliance review.	Compliance with the applicable laws and regulations governing the Group, results in the Group being seen as a good corporate citizen	

RISK MANAGEMENT REPORT - continued

MATERIAL RISKS - continued

|	RISK AND RATIONALE	MITIGATION	OPPORTUNITY	LINK TO MATERIAL MATTER/ STRATEGY
4	Environmental pressures have an impact on the production and consumption of our products: • Adverse weather conditions affect landings of fish stocks • Water temperature variables and disease affect the location • Uncertainty in the distribution and availability of certain marine resources due to changes in sea variables	Mitigation of these risks comes from constant monitoring of these environmental variables to allow flexibility in our response to these external factors	Products of good quality will be produced and offered to the market, which can increase revenue and the Group's reputation in the market	
5	Business interruptions in the Group's ICT systems by malicious software and increasing advances in cyber and ransomware attacks could result in loss of information and increased fraud.	Restricted access to the Group's ICT systems. Constant monitoring of systems for any possible infections and intrusions. Rollout and implementation of new ICT system. Backups performed daily and stored in different external servers.	The Group can maintain data integrity and decrease downtime on secure IT systems. Uninterrupted business practices will lead to efficiency and maximise profits.	
6	Exchange rate volatility may have both a negative and positive impact on business performance.	Exchange control is monitored regularly with efficient management of overhead and cost structures in place to ensure that all volatile environments have a minimal effect on the operations.	A positive exchange rate, i.e. a weak rand value compared to major international currencies increases revenue for the Group.	

RISK MANAGEMENT REPORT - continued

MATERIAL RISKS - continued

	RISK AND RATIONALE	MITIGATION	OPPORTUNITY	LINK TO MATERIAL MATTER/ STRATEGY
7	Negative reputational perceptions of the ICT business by shareholders could result in lost growth opportunities.	Pursuing strategic investments and ensuring new opportunities and ventures are adopted in line with the guiding principles of our acquisition strategy.	Resilience from the impact of the external environment and continued growth by acquisition.	
8	Limited access to funding may slow down the ability to capitalise on the various niche growth initiatives in the biotech companies.	The sources of available funding have been allocated to each project based on an approved business plan and this is monitored by the team to ensure that it meets the Group's strategic objectives. Management is actively engaging potential investors.	The success of these projects can result in groundbreaking medical treatment developed and manufactured in South Africa.	
9	Environmental challenges include carbon emissions, waste management, climate change and marine coastal management – and must be reviewed constantly.	Adhere to marine management policies from the Marine and Coastal Management to ensure no overfishing takes place. Recycling and better waste removal techniques are being employed across the Group.	There is an opportunity for the Group to maintain a clean, safe environment and reduce carbon emissions, and be seen as a good corporate citizen.	
10	The inability to recruit and retain key skilled employees, hence skills retention and succession planning remain a constant challenge for all divisions.	Better recruitment policies have been implemented to recruit and retain high-calibre personnel. A continuous review of employee training, development and succession planning occurs annually to ensure that it is in line with the Group's strategy.	Retention of key skilled employees ensuring efficiency and effectiveness of business processes.	

RISK MANAGEMENT REPORT - continued

RISK METRICS
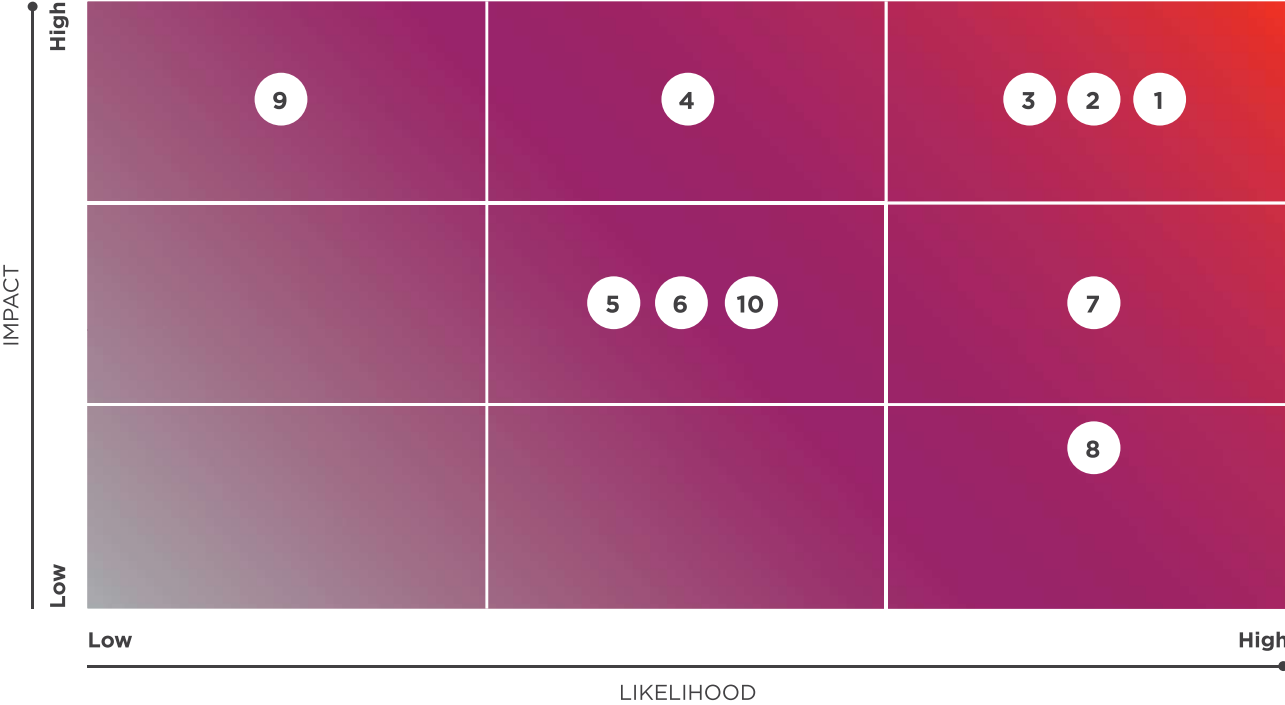
TECHNOLOGY AND INFORMATION

The Board is responsible for technology and information governance in the Group and delegated the management of technology and information governance to the audit and risk committee to ensure the promotion of an ethical technology and information governance culture and awareness.

The audit and risk committee governs technology and information in a way that supports the organisation in setting and achieving its strategic objectives and has delegated this responsibility to management to implement and execute effective technology and information management. Management is accountable for operational governance of technology and information management.

What the future looks like will be largely determined by the Group's investment into the technologies that will help drive it to lead its people and its businesses into the fourth industrial revolution and beyond. With this in mind, AEEI has embarked on a strategic investment drive to ensure the sustainability of its various businesses, unlocking stakeholder value in the process.

King IV™ refers to advances in technology and digitisation as the fourth industrial revolution and stresses what a big impact it has on all organisations.

As business leaders, we are finding it difficult to keep pace with the rapid rate of change and to understand all the new technology-driven opportunities. Information technology (IT) security can no longer be an afterthought as the digital economy accelerates and both consumers and organisations become increasingly inter-connected. At AEEI, cybersecurity is the foundation on which solutions are built.

The fourth industrial revolution is being heralded as the answer to many of the continent's socio-economic woes but, understanding just what it is, and what positive and negative impacts it will have on the future of the world, has not been fully considered yet, but more importantly, it should be done responsibly.

Due consideration needs to be taken as to the impact it will have on the Group, well into the next millennia. What we do now will have everlasting consequences. We need to make sure that we use this new wave of technology as a positive force for good, and that requires us to not just look at the short-term financial interest, but to adopt a holistic approach to technology.

The fourth industrial revolution does have the power and potential to raise global income levels and improve the quality of life – for everyone, wherever in the world one is.

TECHNOLOGY AND INFORMATION GOVERNANCE

The objective of technology and information governance is to direct technology and information endeavours to ensure that technology and information's performance meets the following objectives:

- Alignment of technology and information with the Group and realisation of the promised benefits
- Use of technology and information to enable the Group by exploiting opportunities and maximising benefits
- Responsible use of technology and information resources
- Appropriate management of technology and information-related risks

Technology and information governance ensures that technology and information goals are met and risks are mitigated and that technology and information deliver value to sustain and grow the Group.

TECHNOLOGY AND INFORMATION - continued

TECHNOLOGY AND INFORMATION GOVERNANCE FRAMEWORK

Compliance for Technology Governance

King IV™ Principle 12: The Board should govern technology and information in a way that supports the organisation setting and achieving its strategic objectives

AEEI Governance Framework supports Principle 12 to achieve good governance outcomes

| Outcomes | Ethical Culture | Good Performance | Efficient Control | Legitimacy |

Technology and Information Governance Framework

| 1 | 2 | 3 | 4 | 5 | 6 |

| **Roles and responsibilities** | **Technology sustainability, strategy and business alignment** | **Technology and governance reporting** | **Technology investment monitoring and evaluation** | **Technology risk managemnet** | **Information asset management** |
| Includes well-defined roles and responsibilities and management structures | Includes value delivery, performance management, technology sustainability, technology strategy and business alignment | Includes technology project benefits realisation and technology governance reporting | Includes technology management | Includes technology risk management, information security and business continuity planning (including disaster recovery | Includes technology compliance, acquisitions and disposal and information management |

| Key technology decisions | Technology governance processes and procedures | Technology organisation structure (roles and responsibilties) | Technology strategy enablement | Communication and change management |

Technology Governance Enablers

The technology and information governance framework promotes an ethical technology and information governance culture and awareness by ensuring the following:

- The activities and functions of the technology and information strategy are aligned to the business strategy, and opportunities to improve the use of technology and information within the Group are identified and exploited.

- The investment made in technology and information, ensuring costs are managed and the return on investment is measured by the relevant divisional boards and committees. Where applicable, synergies between technology and information initiatives are enabled and technology and information choices are in the best interests of the Group as a whole.

- Technology and information risks are identified and adequately addressed in line with the Group's risk management framework. The Group ensures that it has adequate business resilience arrangements in place for disaster recovery and assurance has been provided to the Board.

- Technology and information resources are sourced optimally and legitimately, keeping core capabilities in-house.

- Processes and procedures are in place to ensure that the Group's IT assets are managed, maintained, replaced and disposed of effectively and in accordance with applicable policies.

- Infrastructure, systems and policies are in place for the management of information which includes information security and information privacy.

- The audit and risk committee considers technology and information as it relates to financial reporting and the going concern of the Company/Group through regular risk-based audit coverage.

- Technology and information use remains sustainable with respect to the environment.

TECHNOLOGY AND INFORMATION - continued

DIGITAL REVOLUTION

Simplified, technology defines how scientific knowledge is practically applied to advance industries, and the equipment and methods, using scientific means, to solve problems.

A core belief at AEEI, which contributes to the Group's enduring commercial sustainability, is that the 'digital dawn' (as we call it at AEEI) is the beginning of a true digital democracy for Africa, where this 'science' is made available to all. It is what propels AEEI to do good for people, ensuring that the enabling brought about by technology can be used to improve the lives of ordinary citizens in South Africa and beyond. The prospect for technology to change people's lives for the better is extraordinary and equally so for doing better business. AEEI looks to enhance its efficiencies and minimise the negative effects on environments and communities.

AEEI is incorporating technology into its everyday function to enable not just one person, but communities of people. While much of the emphasis of the fourth industrial revolution is placed on ensuring that the youth of today are a productive and skilled workforce of tomorrow, AEEI has not forgotten the pre fourth industrial revolution contingent. The Group is cognisant of the fact that many of the older generation possess immense experience and expertise, but lack the technological know-how to engage in a fully-connected ecosystem. The Group therefore also focuses on investing in skills upliftment and training to bridge the technological gap between millennials and the older generations.

By putting our workforce development at the forefront, employees may be more aligned and motivated to extend the influence of their newly developed skills.

REPORT OF THE COMMITTEE

It is clear we are witnessing an inflection point and a transition to the fourth generation of cyberattacks. We are now seeing threat factors effectively weaponising ransomware to cripple large institutions, affecting the health and lives of nation-states' populations, as well as causing pain to many businesses' bottom lines. Data breaches continued to take centre stage in the past year, with some shocking revelations about major customer data compromises.

We realised how the threat landscape, by entering the fourth generation of cybersecurity, now spans across countries and industries along multiple vectors of network, cloud and mobile and uses state-sponsored technologies to do so. By reviewing recent attacks, we can understand how 97% of organisations are not prepared for the fifth generation of cyberattacks.

Cybersecurity threats aren't just technical, but societal and political. The seven most critical threats to businesses in 2019 include:

- Phishing
- Ransomware
- The cloud
- General data protection regulation (Protection of Personal Information Act)
- Cryptocurrency mining
- Cyber intrusions
- Privacy violations

TECHNOLOGY TRENDS, INNOVATION AND TRANSFORMATION

The Group continues to consider the emerging technology trends to ensure that we remain abreast of change. The IT steering committee oversees new technologies and innovations that could assist in improving our network access, security, performance and efficiency and creating new ways of working and identifying opportunities.

We need to look closer at what 2020 and beyond may have in store and, most importantly, how best to prepare for it. The Group continues with its baseline principles with the development and implementation of a technology and information governance framework. These principles incorporate standards included in King IV™, Control Objectives for Information Technology (COBIT) and Information Technology Infrastructure Library. This started from the premise that technology and information need to deliver the information that the Group requires to achieve its objectives.

These governance baseline principles are as follows:

- Business alignment and enablement focused on ensuring the linkage of business and technology and information plans, defining, maintaining and validating the technology and information value proposition and aligning technology and information operations with the Group's operations.
- Responsible and adequate procurement of technology and information hardware and software and the correct selection of technology partners and suppliers.
- Accountability for operational performance in technology and information sits with the right people who are developed and empowered and so that optimal technology and information processes and measurements are deployed that result in:

TECHNOLOGY AND INFORMATION - continued

- integration of people, technologies, information and processes across the Group;
- integration of technology and information risks into the Group's risk management;
- arrangements to provide for business resilience;
- proactive monitoring of intelligence to identify and respond to incidents, including cyberattacks and adverse social media events;
- managing the performance of and the risks pertaining to third-party outsourced service providers;
- assessing the value delivered to the Group through significant investments in technology and information, including evaluation of projects throughout their life cycles and of significant operational expenditure;
- the responsible disposal of obsolete technology and information in a way that should have a minimal impact on environmental and information security;
- ethical and responsible use of technology and information;
- compliance with relevant laws;
- ongoing oversight of the management of information that resulted in the following:
    - The leveraging of information to sustain and enhance the Group's intellectual capital
    - An information architecture that supports confidentiality, integrity and availability of information
    - The protection of privacy of personal information
    - The continual monitoring of security information
- Management of technology that resulted in the following:
    - A technology architecture that enables the achievement of strategic and operational objectives
    - The management of risks pertaining to the sourcing of technology
    - Monitoring and appropriately responding to developments in technology, including capturing potential opportunities and managing disruptive effects on the Group and its business model
- Supplier performance management practices outlining the implementation and monitoring of service level agreements and commercial agreements.
- Business continuity/disaster recovery requirements and practices regarding the processes in terms of technology and information disruptions.
- Security regarding data privacy, cybersecurity and user access.
- Compliance in terms of internal monitoring and external assurance.
- Compliance with the Protection of Personal Information (PoPI) Act, 2013.

(– *Principle 12*)

TECHNOLOGY RISK AND CYBERSECURITY

The Group continues to monitor the evolving threat of cyberattacks in order to protect our systems, employees and customers. We continue to make progress with our security programmes, which include the proactive monitoring of our systems and networks to ensure that our IT controls are robust, and running awareness programmes with our employees so that the necessary steps can be taken to protect themselves and others against cyberattacks.

RISK MITIGATION

No significant risks were reported during the year. We are cognisant of cybersecurity and the implications thereof, taking into account the protection of our stakeholders, which remains a high priority. One aspect driving risks and security is our governance and internal audit to ensure that the Group's information assets are secure.

As the Group is dependent on IT to meet its business needs and sustainability objectives, all identified risks are monitored and reduced to an acceptable level by executive management. The Group encourages a high standard of security monitoring, data protection, business service availability and network reliability. It ensures that IT maintenance is performed and reviewed constantly through monthly reporting. The firewall protection is renewed annually and backup technology is checked continuously to ensure business continuity and an average of 99% server uptime.

We remain abreast of best practices, threats from phishing, ransomware and other cyber threats which could have an impact on business operations, financial statements, legal exposure and the Company's reputation. Greater user awareness and training was put in place in the current year to keep us updated on the threats and risks in the IT environment. (– *Principle 11*)

TECHNOLOGY AND INFORMATION - continued

THE CHANGING ROLE OF IT

In terms of our Vision 2020 Vision strategy, the Group continues to look into the technology landscape and systems, taking into account the current systems. A system was identified and rolled out in the Group with future additional benefits that could be implemented through a phased approach.

Key to considering the new technology was the multi-user environment and data being generated in a variety of options, thus reducing the risk of errors, audit trails, document management, improving workflow, multiple users and reviewers as well as the consolidation of information and maintenance costs.

The Group's current focus is on maintaining the existing traditional enterprise systems where operational reliability is paramount. The current systems have necessitated the need for enhancements within the Group's business units and consolidation for improved corporate controls and reporting.

Our technology subsidiary continues to provide technology-enabled solutions which add value to our customers.

The Board has oversight of the effectiveness of technology and information governance through the delivery of the integrated report and the approval of the governance framework and policy.

The Board oversees the following:

• The adoption of a governance framework and IT policies that detail the strategic direction on the use of technology and information.

• The report from management that contains

progress against the following objectives in terms of compliance:

– The IT administrator manages the IT investment to ensure the alignment and convergence of various IT tools and devices to improve communication within the business units.

– IT risks are identified and adequately addressed and assurance is obtained to ensure that the IT control framework is in place to address IT risks efficiently.

– IT resources are sourced within subsidiary companies or externally.

– Information, IT assets and intellectual property contained in the IT systems are protected and effectively managed and used.

– IT has adequate business resilience arrangements in place for disaster recovery.

– Information management is a joint IT and business responsibility.

– IT governance conforms to laws and related rules, codes and standards are considered.

– The use of IT is sustainable with respect to the environment and security.

– Synergies between IT initiatives and the benefits to the Group as a whole and individual business units are achieved.

(– *Principle 12*)

For the year, the audit and risk committee is satisfied that is has fulfilled all its statutory duties assigned by the Board. The chairman of the committee reports to the Board on the activities of the committee at each Board meeting.