# STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

Pursuant to Paragraph 15.26(b) of the Main Listing Requirements (LR) of Bursa Malaysia Securities Berhad (Bursa Securities), the Board of Directors of listed issuers is required to include in their annual report, a 'statement about the state of risk management and internal controls of the listed issuer as a group'. Accordingly, the Board is pleased to provide the following statement that was prepared in accordance with the 'Statement of Risk Management and Internal Control: Guidelines for Directors of Listed Issuers' as endorsed by Bursa Securities, which outlines the nature and scope of risk management and internal control of the Group during the financial year under review.

**Board's Responsibility**

The Board is responsible and accountable for maintaining sound processes of risk management and internal control practices to safeguard shareholders' investments and the Group's assets. Such processes cover not only financial control but also operational and compliance controls. In view of the limitations inherent in any process, the risk management and internal control processes and procedures put in place can only manage risks within tolerable levels, rather than eliminate the risk of failure to achieve the Group's business objectives.

The Board Audit Committee (BAC) assists the Board in evaluating the adequacy of risk management and internal control framework. The BAC, via the Axiata Group Risk Management Committee (GRMC), has put in place a systematic risk management framework and process to identify, evaluate and monitor principal risks; and implement appropriate internal control processes and procedures to manage these risks across the Group, excluding Associate Companies and joint ventures which are not within the Group's control.

Following the written assurance from the President and Group Chief Executive Officer (GCEO) and Group Chief Financial Officer (GCFO), that the Group's risk management processes and internal controls are operating effectively, the Board is of the view that processes covering risk management and internal control in place for the year under review and up to the date of issuance of the financial statements is sound and sufficient to safeguard shareholders' investments and the Group's assets.

**Risk Management and Internal Control Framework**

**1. Axiata Enterprise Risk Management Framework**

The Group adopts the Axiata Enterprise Risk Management (ERM) Framework as a standardised approach for timely identification, reporting and management of principal risks and ensures implementation, tracking and review of effectiveness of mitigation actions for the risks identified. The framework, benchmarked against ISO31000:2009, is adopted by all risk management teams across the subsidiaries. It stresses the importance of balancing between risk and reward in making strategic business decisions, a tool in managing both existing and potential risks with the objective of protecting key stakeholders' interests, and compliance with statutory and legal requirements. At the same time, the framework promotes an effective risk culture whilst embedding risk management in our daily business decisions.

**2. Risk Governance Structure**

The Group is committed towards continuous improvement of risk management processes and ensures that the processes remain relevant to the operating environment. The GRMC, which consists of all the members of Axiata Group Senior Leadership Team (SLT) and chaired by the Axiata Group BAC Chairman plays a key role in driving Axiata's ERM Framework. With the assistance of the Group Risk Management Department (GRMD), they ensure systematic implementation and monitoring of the effectiveness of risk management culture and processes across the Group. The committee meets on a quarterly basis to review existing, new and evolving risks and where necessary, evaluate effectiveness of mitigation plans and improve existing risk practises, where necessary. The following depicts the key parties within the Group's Risk Governance Structure and their principal risk management roles and responsibilities:

| | |
|---|---|
| **Board of Directors** | • Maintaining a sound system of risk management & internal controls<br>• Approves risk management policy and framework, governance structure and sets the risk appetite<br>• Receives, deliberate and endorses BAC reports on risk governance and internal controls |
| **Board Audit Committee** | • Assist the Board in evaluating the adequacy of risk management & internal control framework<br>• Reviews and endorses the Group Risk Profile<br>• Receives and reviews reports from the Risk Committee and recommend them to the Board for approval |
| **Group Risk Management Committee** | • Assist in identifying principal risks at Group level and providing assurance that the ERM is implemented group-wide<br>• Review and recommend frameworks and policies specifically to address enterprise risk inherent in all business operations<br>• Promote cross-functional sharing of risk information<br>• Monitor compliance to ERM Framework, regulatory requirements and status of action plans for both Group and subsidiaries<br>• Coordinate and promote risk management culture and implementation |
| **Group Risk Management Department** | • Establish, formulate, recommend and manage sound and best practice ERM program for Axiata Group<br>• Inculcate risk awareness within the Group<br>• Assist Axiata OpCos and Business Units in establishing their internal risk policy and structures, including business continuity programme for the Group<br>• Identification and consolidation of risk matters<br>• Secretariat for the GRMC<br>• Consolidated risk reports from Axiata OpCos and Business Units for the GRMC's review<br>• Encourages & recommend the adoption of mitigation actions where appropriate |
| **Risk Focals at Axiata CC and Opcos** | • Primarily responsible for managing risks on a day-to-day basis<br>• Promoting risk awareness within their operations and introduce risk management objectives into their business and operations<br>• Coordinate with Axiata Group Risk Management Department on Implementation of risk management policy and practices |

The implementation of risk management activities encompasses both corporate and subsidiary (at Operating Company or "OpCo") levels where OpCos have similar risk structures within their jurisdiction. To ensure the operationalisation of risk management processes and clear accountability at the OpCo level, risk committees comprising of their Chief Executive Officer (CEO) as Chair, and selected senior management members are set up in each OpCo. At the same time, a risk focal person ("Risk Champion") is appointed to provide timely risk updates and act as the key liaison with GRMD. Events which may materially impact the Group's financial position and reputation will be escalated to the GRMD for appropriate action. At the same time, the Risk Champion would provide recommendation on the adoption of appropriate mitigation steps and provide quarterly updates to their respective OpCo BAC on the action taken. To further strengthen accountability at the management level, the CEO or Chief Financial Officer (CFO) of each OpCo is required to present their risk profile at the GRMC on a rotational basis. This structure provides the Group with the necessary detailed knowledge from OpCos, thus allowing the Board to have a comprehensive view of principal risks and mitigation activities across the board and ensure accountability by OpCos in managing their risks. As and when new OpCos are established, GRMD will work closely with the new management team in the set-up of the risk function.

The Group faces many risks and uncertainties which we mitigate and manage through various risk management strategies, actions and controls. These risks vary widely with some threatening our business model, future performance and financial standing of the business. There may be risks that are beyond the Group's control, or presently unknown or currently assessed as insignificant, which may later prove to be material. Nonetheless, we aim to mitigate the exposures through appropriate risk management strategies and internal controls as much as possible.

Principally, the Group's key risk factors are categorised into the following eleven categories:

- Financial Risk
- Market Risk
- Regulatory Risk
- Cyber Risk
- Operational Risk
- Geo Political Risk
- Strategic Risk
- Investment Risk
- People Risk
- Technology Risk
- Governance and Integrity Risk

A write-up of the key risks faced by the Group are listed in Appendix 1 of this statement.

The following key internal control structures are in place to assist the Board to maintain a proper internal control system.

**Key Internal Control Structures of the Group**

**1.0 Control Environment**

The control environment sets the tone for the Group by providing fundamental discipline and structure. Key elements of the Group's internal control systems include:

**1.1 Integrity and Ethical Values**

- **Code of Conduct and Practice**

  The Senior Management and Board set the tone at the top for corporate behaviour and corporate governance. All employees of the Group shall adhere to the policies and guidelines as set out in the Code of Conduct of the Group which sets out the principles to guide employees in carrying out their duties and responsibilities to the highest standards of personal and corporate integrity when dealing within the Group and with external parties. The Group's Code of Conduct covers areas such as compliance with respect to local laws and regulations, integrity, conduct in the workplace, business conduct, protection of the Group's assets, confidentiality, conflict of interest and anti-competition practices. In 2016, various initiatives including ongoing enforcement of the Gift Policy, consequence management on violation of integrity and values and Group Recognition Event to inculcate and encourage the appropriate behaviours continued.

- **Guidelines on Misconduct and Discipline**

  Guidelines are in place for handling misconduct and disciplinary matters. These guidelines govern the actions to be taken in managing the misconduct of employees who breach the Code of Conduct and Practice or do not comply with the expressed and implied terms and conditions of employment. The Code of Conduct and Practice has also been extended to contractors and suppliers of the subsidiaries.

**1.2 Board Committees**

**(a) Board**

Clear roles of the Board are stated under the Statement of Corporate Governance section of this Annual Report.

**(b) Board Committees**

To promote corporate governance and transparency, in addition to the Board, the Group has the BAC, Board Nomination Committee (BNC) and Board Remuneration Committee (BRC) collectively 'Board Committees' in place. These Board Committees have been established to assist the Board in overseeing internal control, Board effectiveness, and nomination and remuneration of the Group's key positions and directors. The responsibilities and authority of the Board and Board Committees are governed by a clearly defined Terms of Reference (ToR).

**(c) BAC**

The primary function of the BAC is to assist the Board in fulfilling its statutory and fiduciary responsibilities. The BAC will review the financial statements and financial reporting process, the system of internal controls, management of enterprise risk, the audit process and the process for monitoring compliance with law and regulations including Bursa Securities requirements and the company's Code of Conduct.

It has direct access to the internal and external auditors and full discretion to invite any Director to attend its meetings. Further details of the BAC are stated under the BAC Report section of this Annual Report.

In 2016, the Cyber Security Steering Committee ("CSSC") was established as a sub-committee of the BAC focusing on the accelerated implementation of cybersecurity initiatives, for example, the establishment of the Cyber Security Operation Centre ("CSOC") and Cyber Security Posture Assessment in the Group and ensuring a standardised and aligned implementation across the Group.

**(d) BNC**

Please refer to the Statement on Corporate Governance section of this Annual Report.

**(e) BRC**

Please refer to the Statement on Corporate Governance section of this Annual Report.

**1.3 Senior Leadership Team (SLT)**

The SLT is committed to the identification, monitoring and management of risks associated with its business activities. The GCEO and Management are ultimately responsible to the Board for the Group's system of internal control and risk management. Each business unit is responsible and accountable for implementing procedures and controls to manage risks within its business.

**1.4 Organisation Structure**

- **Clear Organisation Structure**

The Group has an appropriate organisational structure led by functional SLT members who have clear roles of responsibility and lines of reporting. The proper segregation of duties promotes ownership and accountability for risk taking and defines lines of accountability and delegated authority for planning, executing, controlling and monitoring of business operations. Competent and professional individuals have been selected as part of our SLT to ensure we manage our business well and to deliver business results. Regular reviews of the organisational structure are held to address the changes in the business environment as well as to keep abreast of current and future trending of new technologies, products and services.

- **Corporate Centre**

The Corporate Centre plays an advisory role to add value to the subsidiaries at varying engagement levels. The broad roles of the Corporate Centre are as follows:

1. Supporting role to Axiata Board Representatives at OpCos and OpCos' management; and
2. Supporting role to OpCos' Functional Heads.

Besides engaging in regular communication between the OpCos and the Group functions, the Corporate Centre also gives appropriate inputs and steers the Group on best practices through sharing of the Group's guidelines and strategies to minimise risk exposure and to increase the efficiency and effectiveness of business operations.

The Corporate Centre is also responsible for key processes and functions including strategic planning, mergers and acquisitions, joint development projects, capital raising and allocation, leadership, talent development, group accounts and reporting, procurement, treasury, technology including cybersecurity and network.

The Corporate Centre is also involved in leading Group initiatives to address current and future challenges of the Group.

**1.5 Assignment of Authority and Responsibility**

- **Policies and Procedures**

Documented policies and procedures are now in place for all major aspects of the Group's business and these are regularly reviewed and updated to ensure that they remain effective and continue to support the organisation's business activities at all times as the organisation continues to grow.

These policies and procedures are supported by clearly defined delegation of authorities for amongst others, spending on operating and capital expenditures, authority to enter into contracts and commitments, business plans and budget, and procurement of goods and services.

- **Limits of Authority (LoA)**

The Board has approved a clearly defined and documented LoA which is to be used consistently throughout the Group. These are regularly updated to reflect changing risks or to resolve operational deficiencies. It establishes a sound framework of authority and accountability within the Group, including segregation of duties which facilitates timely, effective and quality decision making at the appropriate levels in the Group's hierarchy.

Axiata's LoA document clearly sets out the matters reserved for the Board's consideration and decision making, the authority delegated to the President and GCEO and other SLT members, including the limits to which the President and GCEO can execute the authority, and provides guidance on the division of responsibilities between the Board and Management.

### 1.6 Commitment to Competency

- **Competency Framework**

  The Group appoints employees of the necessary competencies to ensure that the personnel driving key operations are sufficiently skilled and exert the required qualities of professional integrity in their conduct.

- **Performance Management**

  The Group is committed to attract and retain competent, dedicated and loyal employees. Programmes and initiatives have been established to ensure that the Group's human capital is equipped with the qualities and skills to drive the Group to become a world class company through ongoing emphasis on performance management and employee development.

  The Group has in place a Key Performance Indicators (KPI) performance measurement process as prescribed under the Government-Linked Company Transformation (GLCT) programme to link performance and compensation in order to create a high performance work culture. This process also seeks to provide clarity, transparency and consistency in planning, reviewing, evaluating and aligning employees' actions and behaviours to that of the Group's vision and mission.

- **Training and Development Framework**

  It is the Group's policy to train employees at all levels so that they would be able to perform well in their present jobs and also to develop employees who are considered to have the potential to perform duties with wider responsibilities so that they may be ready to assume them when needed. Programmes are also implemented to ensure that employees receive continuous training in various areas of work such as knowledge, health and safety, technical training, leadership and new product development.

- **Talent Development and Succession Planning**

  There is a Group Talent Management Framework in place to identify and develop a group talent pipeline within the organisation as a supply for future leadership demands. In this respect, the Group has met its target of identifying C-suite potentials that provides a cover ratio of 2:1, from within the organisation and has been intensifying its efforts in making these talent ready to succeed the current top management across the Group. This is done via structured leadership development programmes, mentoring and coaching, regular leadership readiness assessments, as well as cross-functional and cross-country assignments.

  This leadership talent pipeline is also regularly reviewed via the Group Talent Council and assessed as potential successors for key positions in the Group, via internal and external benchmarks.

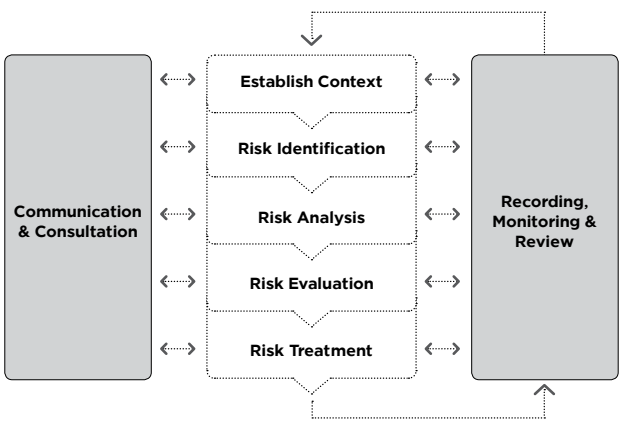
  Succession plans and the robustness of the talent pipeline are regularly reviewed by the Board. The talent pipeline includes fresh graduates and middle management levels so as to ensure a continuous supply of talent. As of 31 December 2016, eleven (11) internal successors have been at placed top positions across the Group.

### 2.0 Risk Assessment

Axiata's risk management process is guided and principally aligned to ISO31000:2009 where risk is managed to ensure the achievement and implementation of strategic objectives. The Group's risk management process typically involves identifying particular events or circumstances relevant to our objectives and risk appetite, assessing them in terms of likelihood and magnitude of impact, determining a response strategy, evaluation of adequacy of existing controls, and monitoring the implementation of the response. The objective is to protect and create value for our key stakeholders.

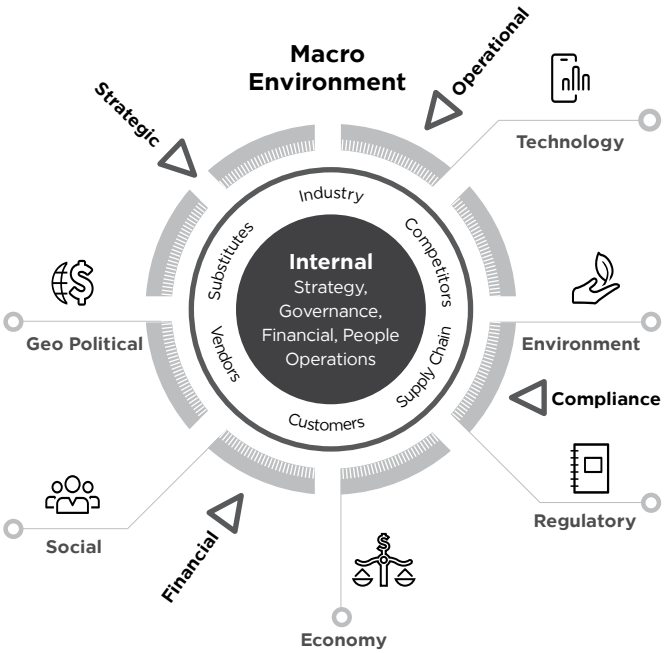
Axiata's Risk Assessment Process is depicted in the following diagram:

**Process for Managing Risk**



# STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

The risk identification process, which is done on an ongoing basis entails scanning all key factors within Axiata's business context from an 'outside-in' perspective, i.e. from macro-environment (external) to industry and internal risks. Risks are generally classified into distinct categories, i.e. strategic, financial, operational and compliance, representing the challenges to the Group's business operations, as depicted below:




Risk information and treatment plans are captured and updated into a risk register which is maintained by the respective OpCos and the Group. The information is then consolidated to provide an enterprise overview of material risks faced by the Group and the associated risk mitigation plans, which is tracked and reviewed from time to time.

- **Control Self-Assessment (CSA)**

  CSA is an effective process used by the Group for improving business internal controls and processes. It allows employees of the Group to identify the risks involved in achieving the business objectives, to evaluate the adequacy and effectiveness of the controls in place and activities designed to manage those risks. CSA was performed on selected areas in XL and Robi in 2016.

## 3.0 Control Activities

Control activities are the policies, procedures and practices that ensure management objectives are achieved and risk mitigation strategies are carried out. Key activities within the Group are as follows:

### 3.1 Policies and Procedures

- **Financial and Operational Policies and Procedures**

  The Group currently maintains two policies, i.e. Limits of Authority (LoA) and Group Policies encompassing both the Group and OpCo levels, which sets the framework for the development of the respective procedures covering financials and controls. The documented procedures include management accounting, financial reporting, procurement, information systems security, compliance, risk management and business continuity management.

  Internal control is embedded into these policies to ensure consistent application throughout the Group. This serves as a preventive control mechanism whilst allowing the Group to promptly identify and respond to any significant control failures.

- **Budgeting Process**

  A comprehensive annual budgeting process is in place to evaluate the feasibility and viability of the Group's businesses and to ensure that the Group's OpCos business plans are in line with the Group's future strategic plans. Annual budgets are prepared by the OpCos and deliberated with their respective Boards. They are then presented and discussed during the Axiata Board Retreat for approval before the commencement of a new financial year.

  Upon approval of the budget, the Group's performance is periodically monitored and measured against the approved budget and ongoing business forecast, which is cleared by the President and GCEO and supported by the SLT. The Group's performance is also reported to the BAC and the Board. Reporting systems which highlight significant variances against the plan are in place to track and monitor performance. The results are reviewed on a quarterly basis by the Board to enable them to gauge the Group's overall performance, compared to the approved budget and prior periods, and to take remedial action where necessary. Similar performance reviews at OpCos Board level take place on a monthly or quarterly basis.

- **Whistleblower Policy and Procedures**

  The Group has a Whistleblower Policy which enables employees to raise matters in an independent and unbiased manner. As part of this Whistleblower Policy and procedures, there is an anonymous ethics and fraud e-mail, under the administration of the Group Chief Internal Auditor (GCIA), as a mechanism for internal and external parties to channel their complaints or to provide information in confidence on fraud, corruption, dishonest practices or other similar matters by employees of the Group. The objective of such an arrangement is to encourage the reporting of such matters in good faith, with the confidence that employees or any parties making such reports will be treated fairly, their identity remains anonymous and are protected from reprisal.

- **Insurance and Physical Safeguard**

  The Group maintains an insurance programme to ensure that its assets and businesses are sufficiently covered against any damage that will result in material losses. At the same time, we also ensure that our major assets are physically safeguarded and review the adequacy and type of insurance cover at regular intervals to ensure alignment against the Group's risk exposure and appetite.

### 3.2 Security (Application and IT Network)

- **Business Continuity Management**

  The Board is committed to safeguard the interest of our stakeholders by ensuring the ability of business operations to continue during a crisis and to have speedier recovery from a crisis through the implementation of Business Continuity Management (BCM) across the Group. The BCM programme provides a framework for the Group in building organisational resilience in the face of a crisis. The programme created is sufficiently robust in catering for enhancement due to technological evolution or organisational changes.

  The Group BCM framework, aligned against international standards of ISO 22301 Business Continuity Management have been formalised and standardised across the Corporate Headquarters and selected OpCos. At the same time, our versatile framework allows for customisation in accordance to each OpCo's requirements and operating environment. Business recovery plans have been documented for mission critical processes, tested and rehearsed regularly to ensure effective coordination, familiarity and awareness among employees. The Group Risk Management department, which is led by the Group Chief Risk Officer, is responsible in ensuring effective implementation and coordination of business continuity efforts across the Group. As at end 2016, BCM has been implemented for all OpCos including Corporate Centre.

- **Information Technology (IT)**

  IT modernization and digital enablement for superior customer experience is identified as one of the Group's key strategies. All OpCos have been focusing in line with this strategy undertaking various initiatives which include the ground work for inducting Digital IT Stack, application rationalization, enhancing Application Programme Interface (API) strategy, modernising Business Support Systems (BSS) and Operations Support Systems (OSS) in order to meet evolving business requirements and achieve competitive positioning. Cybersecurity is an essential and underlying part of our digital strategy and risk mitigation. In 2016, the Cyber Security Operations Center (CSOC) was established across the majority of OpCos to improve incident monitoring capability. In addition, relentless focus continues on strengthening cybersecurity resilience through various initiatives, for example, periodic Cyber Security Posture Assessment (CSPA) etc. With business continuity being another critical area, continued focus and investments are being ensured in disaster recovery for key IT systems.

### 3.3 Regulatory and Compliance

- **Group Regulatory Affairs (GRA)**

  The approach used is to pro-actively shape the landscape (external environment) at each OpCo market thus enabling proper and effective management of regulatory issues confronting the OpCos. The regulatory issues are those identified and monitored via regular reviews of the Group's risk matrix and managed as part of the Enterprise Risk Management process.

  This approach encompasses:

  **1. Regulatory Strategy:**

  a. Constant monitoring of regulatory developments and identification of regulatory issues for each OpCo based on issues of highest strategic, financial and/or reputational impact;
  b. Periodic review of national OpCo annual regulatory strategies which addresses these issues. This would translate into an advocacy plan engaging regulators and other authorities through formal and informal submissions and where appropriate, joint advocacy with international partners such as GSMA; and
  c. Development of Group-wide positions on key issues such as availability of new spectrum bands, review of spectrum strategy, same service same rules for 'Over-The-Top' (OTT) providers, net neutrality, competition, digital services regulations and the ASEAN Digital Revolution Framework.

  **2. Stakeholder Engagement:**

  a. Engagement plan covering key government and political stakeholders in each OpCo market including key agencies such as the National Regulatory Agencies with effective messages based on the regulatory strategy; and
  b. Engagement plan covering international and regional regulatory bodies, inter-governmental agencies and trade bodies with effective messages based on the regulatory strategy.

  **3. Regulatory Compliance Framework:**

  a. Forms an essential part of the Corporate Governance Framework of the Group and states the principles and the tone by which regulatory compliance is to be approached and implemented;

  b. Objectives of the Regulatory Compliance Framework:

     i. Set baseline expectation in relation to regulatory compliance;
     ii. Place Axiata and OpCos in the best position to comply with regulatory obligations;
     iii. Manage exposure to unacceptable compliance risk; and
     iv. Avoid surprises on regulatory compliance and action from regulatory authorities.

  In addition, GRA constantly embarks on ensuring a group-wide baseline of best practice regulatory skills and knowledge, through the development of industry collaterals, position papers and regular capacity building programmes.

  The Group Regulatory Policy outlined in the Group Policy document provides guidance and establishes internal policies and procedures that attempt to manage the risk and impact of adverse regulatory decisions.

# STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

Underpinning the Group Regulatory Policy is the understanding that the Group shall comply with all applicable laws and regulations, regulatory obligations and governmental policies in the jurisdictions in which it operates, and that regulatory advice should be obtained in an efficient and cost effective manner as and when required.

It should be noted that the regulatory risks faced by Axiata in most markets are typical of those faced by telecommunications operators in emerging markets, where regulatory frameworks may be incomplete, there may be insufficient consultation with stakeholders, or political influence may materially affect the operations of mobile markets. Current regulatory risks which affect Axiata in multiple national communications markets include but not limited to: spectrum refarming, availability of new spectrum and associated acquisition costs, timely renewal of key operating licenses and spectrum allocations, levels of sector-specific taxation, quality of service, subscriber registration, competition, level playing field challenges from OTT providers, network security, digital services regulations, universal service obligations and periodic review of legal and regulatory frameworks.

**4.0 Information and Communications**

Information and communications support all other control components by communicating control responsibilities to employees and by providing information in a form and time frame that allows employees to carry out their duties. The key activities within the Group are as follows:

**4.1 Corporate Communication Policy**

There is a Corporate Communications Policy in place to ensure that communication across the Group and to investors inside and outside of Malaysia are effectively managed and meets the diverse needs of the organisation.

The Board recognises the need for a robust reporting framework given the growth of the Group's international investments and is working towards further strengthening that element of the internal control system. The Board also recognises the need for more dialogue with investors and analysts as well as with the media moving forward. Details of investor relations activities are listed within the Statement on Corporate Governance section of this Annual Report.

**4.2 Business Control Incident (BCI) Reporting**

The Group has in place BCI Reporting aimed at capturing and disseminating the lessons learnt from internal control incidents with the objective of preventing similar incidents from occurring in other OpCos within the Group and to enable monitoring of internal control incidents that have caused significant losses. Twelve (12) such incident reporting were shared with all OpCos in 2016.

**5.0 Monitoring**

Monitoring covers the oversight of internal control by management or other parties outside the process or the application of independent methodologies, such as customised procedures or standard checklists, by employees within a process. Key monitoring activities within the Group are as follows:

**5.1 Performance Reporting**

- **SLT Meetings**

  The SLT meets monthly and as and when required, to deliberate on business performance, financial and operating risks and issues which include reviewing, resolving and approving all key business strategic measures and policies. Progress, exceptions and variations are also fully discussed and appropriate action taken. In 2016, there were 13 SLT meetings held at Group level. Similar meetings were held regularly at OpCo level.

  Significant matters identified during these meetings are highlighted on a timely basis to the Board, which is responsible for setting the business direction and for overseeing the conduct of the Group's operations. Through these mechanisms, the Board is informed of all major control issues pertaining to internal control, regulatory compliance and risk taking. This ensures that business objectives stay on course.

- **Major Control Issues**

  Quarterly reports on financial and operational control issues are tabled and subsequently reviewed by the BAC.

- **Headline Performance KPIs**

  Headline Performance KPIs have been set and agreed upon by the Board as part of the broader KPI framework that the Group has in place, as prescribed under the GLCT programme.

  The headline KPIs represent the main corporate performance measurement targets for the year and are announced publicly as a transparent performance management practice.

**5.2 Ongoing Monitoring**

- **Financial and Operational Review**

  Quarterly financial statements and the Group's performance are reviewed by the BAC, which subsequently recommends them to the Board for their consideration and approval. Monthly management accounts containing key financial results, operational performance indicators and budget comparisons are also presented to the SLT to enable them to have regular and updated information of the Group's performance.

- **Internal Audit (IA)**

  The function of IA is highlighted within the BAC Report section of this Annual Report.

**APPENDIX 1 - Key Risks Faced by the Group**

**1. Financial Risk**

2016 was a volatile year for certain emerging markets currencies such as the Indonesian Rupiah and Malaysian Ringgit against US dollar. As a global player with presence across 10 countries, the Group is exposed to these volatilities which could adversely affect the Group's cash flow and financial performance. The Group has borrowings in foreign currencies and is cognisant of the foreign exchange and interest rates exposures. To mitigate this risk, Axiata Treasury Management Centre has been tasked to oversee and control the Group's treasury and funding matters, develop hedging strategies which are governed strictly by the treasury policies, taking into consideration current and future outlook of the relevant economies and foreign exchange markets with the ultimate objective of preserving the Group's profitability and sustainability.

**2. Market Risk**

The Group's key markets are predominantly emerging markets which are generally characterised as being economically less developed. These countries are also more prone to economic uncertainties and sensitive towards any changes in developed countries. The unexpected vote for Brexit in United Kingdom, the new American President and its policies, and the volatile price of oil have had an impact on the global economy. These developments have affected investor sentiment, lowered economic growth and hence resulting in lower levels of disposable income among customers. In addition, our OpCos are challenged by stiff price competition, from both incumbents, new players and smaller scale players, leading to lower profitability and a damaging price war in certain markets. It is imperative that the Group takes the necessary measures to drive efficiencies and innovations through investments in new technologies, establish strategic ties with 'Over-the-Top' (OTT) or other digital product developers in order to create products and services that meets evolving customer needs, increase the Group's share of customers' wallet and rebuild customer loyalty.

**3. Regulatory Risk**

The telecoms sector where the Group operates is subjected to a broad range of rules and regulations, put in place by various regulatory bodies. High tax rates, significant spectrum fees, levies, Value Added Taxes (VAT), call drop penalties, etc, are common challenges faced by the Group. In some countries, the Group is faced with prolonged tax litigations while others are challenged with a systematic increase in taxes and more favourable treatment accorded to the domestic operators. Such policies and regulations could disrupt the Group's business operations and impair its business returns and long-term growth prospects. These rules and regulations may also limit our flexibility to respond to market conditions, competition and new technologies. In responding to such a challenging environment, the Group advocates strict compliance, transparency and putting our case before the relevant authorities. We have instituted dedicated personnel and resources to constantly monitor all relevant developments and maintain regular contact and a courteous relationship with the governing authorities. The Group has also been at the forefront in engaging regulatory officials, participating in government consultations, and sharing knowledge and best practices in the development of healthy regimes for the telecoms sector.

Spectrum, a scare resource, remains critical for the Group's core business of providing mobile voice and broadband services and is often seen as means of raising funds by the local government as evident in previous spectrum auctions within the Asian region. The Group saw two spectrum renewal exercises in 2016 which, through prudent planning, we were able to obtain sufficient spectrum capacity within the confined budget approved by the Board.

**4. Cyber Risk**

The increase connectedness of many everyday goods and services via the Internet (digitisation) has meant that telecom operators are facing greater challenges of security breaches from such connections. Such breaches may result in the loss or compromise of sensitive information or interruption to services. The Group considers this as a heightened risk, following the increase in malicious and high profile attacks against major corporations around the world. As the Group relies heavily on information technology, the Group has to protect the privacy of our customers as well as company confidential information stored within our network and systems infrastructure. A successful cyber-attack will undermine customers' confidence in the Group and may materially impact our businesses and tarnish the Group's reputation. Such breaches are also costly to rectify and could result in criminal or civil action in addition to regulatory penalties. Mindful of the risk and repercussions, the Group has established a Cyber Security Steering Committee, which focuses on the accelerated implementation of security initiatives. The committee has been at the forefront of safeguarding the Group by ensuring strict compliance with security policies, procedures, and putting in place technologies and tools to minimise the risk of security breaches. Other technical action have also been instituted to monitor and detect security breaches.

**5. Operational Risk**

The Group relies on third party vendors in many aspects of our business. Their non-performance will have an impact on the Group's operations. The telecoms industry is dominated by a handful of vendors which means any failure or refusal by these key vendor to meet their agreed obligations may significantly affect our core business and operations. One of Axiata Procurement Centre's key role is to be on the lookout for ways to manage these risks, monitor the performance of the vendors and develop new relationships to reduce such dependencies.

The telecoms network within our OpCos are subjected to risks of failures, some within our control while others are not. Repeated failures or service outages could disrupt services, resulting in revenue losses, damage to reputation and eventually customer churn. In some countries, the OpCo could be fined with stiff penalties for poor quality of services or drop calls. The IT systems are also crucial in running operations, from providing end-to-end customer services to running internal processes such as billing. The IT architecture changes regularly due to newer versions, upgrades and security patches. Failure to keep the architecture updated may result in a system crash or security breaches. Cognisant of the risks, the Group continuously address issues such as network congestions, drop calls, upgrades to network coverage, etc., to ensure better quality network and service delivery. Operating procedures with appropriate incident escalation procedures and adequate disaster recovery plans are in place at each OpCo to ensure seamless business continuity. In addition, the Group maintains a global insurance programme to mitigate business losses.

# STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

**6. Geo Political Risk**

2016 witnessed a rise in terrorist attacks globally. The Group operates in some countries that are the subject of such attacks and threats. In addition, they also continue to experience political instability and civil unrests. Such conditions, which are beyond the Group's control, may cause disruption to the business, undermining market sentiment and investor confidence towards the Group. To mitigate this risk, the Group work closely with the respective OpCo Management, leveraging on their local expertise, knowledge and ability to continually assess the political situation and have in place various measures to ensure a timely response in the event of such occurrences.

**7. Strategic Risk**

Evolution of the telecoms landscape, through the substitution of services by non-traditional OTT service providers, and entry of new operators, including Mobile Virtual Network Operators (MVNOs) has had a profound impact on the telecoms sector. There is a change in customer expectations away from simple connectivity to customers wanting better experience in Internet connection, network quality and competitive tariff rates. Increasingly, the ability to provide compelling digital content and lifestyle applications such as music and mobile money are equally important for mobile users. The entry of new players has also created pricing pressure eroding the Group's margin. Keeping pace with changing consumer expectations and competitive pricing has become a challenge across most of the key markets the Group operates in. To mitigate this risk, the Group closely monitors the competitive landscape, explores and makes appropriate investments to upgrade its technology and platform and reviews the relevance of its products and services offerings in order to stay in the game. Prudent cost management keeps our budget lean while maintaining strong strategic alliances with network vendors helps us to keep pace with technology shifts.

**8. Investment Risk**

Venturing into new growth areas remains as one of the Group's strategic initiatives to create additional revenue streams such as participating in digital and OTT initiatives and expanding into green field markets through strategic investments. Nonetheless, the Group recognises the risk and repercussions involved in poor investment decisions and the management of these new initiatives post-acquisition. To manage this risk, we have put in place a Mergers and Acquisition Committee that oversees all acquisitions and divestments and at the same time, maintain a robust due diligence process to evaluate and manage the potential risks involved. Post-acquisition, transition teams are put together to ensure that organisational, cultural and mind-set changes that are required are implemented appropriately.

**9. People Risk**

People are one of the key pillars of success for the Group as it underpins our ability to develop and deliver superior services to our customers. Hiring the right employee and loss of key talent remain a challenge in the emerging economies which the Group operates in. Failure to attract, develop and retain talented employees of the appropriate calibre will compromise our ability to execute our business strategies. Our Talent Management team is on a constant lookout for suitable employees, whilst developing our people through robust talent development programmes, attractive performance based rewards and providing a safe and healthy work environment. Employee engagement is also critical for the Group as a failure to motivate and keep employees engaged will reduce overall morale, increase attrition and ultimately affect our business.

**10. Technology Risk**

The Group constantly strives to be at the forefront of both technology and innovation in all our operating regions. Rapid technological advances may result in premature obsolescence of key technology and equipment before the end of their expected useful life. On the other hand, a lag in development and deployment of new technologies may also result in the Group falling behind its competitors. To remain relevant, it is imperative that the Group constantly reviews and refreshes its technology yet maintain financial prudence. Capex intensity remains a challenge given the persistent upward trend of spending to keep pace with competition. The Group has recently reviewed and revamped its capital expenditure (CAPEX) governance and business planning process, focusing on prudent cost management and capex productivity, whilst increasing Group's visibility of these expenditure across all OpCos.

**11. Governance and Integrity Risk**

The Group holds strongly to our key values of Uncompromising Integrity and Exceptional Performance (UIEP) to ensure high ethical standards and good corporate governance are maintained. We believe that sound corporate governance is a key success factor when conducting business in a global, highly competitive, regulated and changing market. The Group's Code of Conduct sets out rules and guidelines on how personnel acting for or on behalf of the Group are expected to conduct business. The Group will continue its focus on maintaining and further developing the strong ethical platform and corporate governance standard to support Axiata's business integrity and continuing strong performance.