Risk Management Philosophy and Approach

Our Risk Framework

- Defines how risk management functions
- Aligns the Group's strategy with management of key risks
- Specifies role of the Board/ Management to fulfil risk appetite and tolerances
- Identifies risks and determines mitigation plans

THE BOARD

- Instils culture and approach for risk governance
- Provides oversight of risk management systems and internal controls
- Reviews key risks and mitigation plans
- Monitors exposure

AUDIT COMMITTEE

- Reviews adequacy and effectiveness of the Group's internal control framework
- Oversees financial reporting risk of the Group
- Oversees internal and external audit processes

BOARD RISK COMMITTEE

- Reviews and recommends risk strategy and policies
- Oversees design, implementation and monitoring of internal controls
- Reviews adequacy and effectiveness of the Group's risk framework
- Monitors the implementation of risk mitigation plans

MANAGEMENT COMMITTEE

- Responsible for effective implementation of risk management practices at functional levels

RISK MANAGEMENT COMMITTEE

- Reviews the risk assessments carried out by the Business Units
- Reviews and assesses risk management systems and tools
- Reviews efficiency and effectiveness of mitigations and coverage of risk exposures

Our Risk Philosophy

- Three key principles underpinning our Risk Management Approach

- **Risk Centric Culture**
- **Strong Corporate Governance**
- **Proactive Risk Management Process**

RISK MANAGEMENT FRAMEWORK

Review of risk management policies and processes on a regular basis

RISK REVIEW PROCESS

Continuous process of identification, monitoring, management and reporting of risk indicators

ALIGNMENT WITH GROUP STRATEGY

Risk assessment and mitigation strategies as integral parts of the Group's annual business planning and budgeting process

BUSINESS CONTINUITY MANAGEMENT

Business continuity, disaster recovery, crisis planning and management as key risk management activities

ASSURANCE

Self-assessment programme over risks and controls, together with internal and external audit to provide assurance to the Board

The identification and management of risks reduce the uncertainty associated with the execution of our business strategies and allow the Group to maximise opportunities that may arise. Risks take on many forms and can have material adverse impacts on the Group's ability to achieve our stated objectives by potentially impacting our reputation, operations, human resources and financial performance.

The Board is overall responsible for determining the Group's risk appetite and tolerance, and risk profile, overseeing the Group's risk management framework, reviewing the Group's key risks and mitigation strategies and ensuring the effectiveness of risk management policies and procedures. The Risk Committee (RC) and the Audit Committee (AC) review the management of these risks and effectiveness of mitigation strategies and controls. The Risk Management Committee (RMC) supports the Board and RC in terms of risk governance and oversight, and sets the direction and strategies for corporate risk management to be in line with the Goup's risk appetite and risk tolerance thresholds.

The Board has approved the following risk appetite statement:

The Group is committed to delivering value to our shareholders achieved through sustained profitable growth. However, the Group shall not compromise our integrity, values and reputation by risking brand damage, service delivery standards, severe network disruption or regulatory non-compliance.

The Group will defend our market leadership position in Singapore and strengthen our market position in Australia and in Asia Pacific through our regional mobile associates. The Group will continue to pursue business expansion in the emerging markets, including acquiring controlling stakes in the associates, and actively manage the risks.

The Group is prepared to take measured risks to seek new growth in the digital space by providing global platforms and enablers, targeted at a global footprint, while leveraging our current scale and core strengths.

The Group targets an investment grade credit rating and dividend payout policy consistent with our stated dividend policy and guidance.

The Management has the primary responsibility of identifying, managing and reporting the key risks faced by the Group to the Board. The Management is also responsible for ensuring that the risk management framework is effectively implemented within all areas of the respective business units. In addition, specialised areas such as Regulatory, Legal, Environment, Insurance, Treasury and Credit support the Group in the management of these risks.

The Group's philosophy and approach towards effective risk management are underpinned by three key principles:

- **Culture**
  We seek to build a strong risk management and control culture by setting the appropriate tone at the top, promoting awareness, ownership and proactive management of key risks, and promoting accountability. In short, we seek to promote a risk-conscious workforce across the Group.
- **Structure**
  We seek to put in place an appropriate organisational structure that promotes good corporate governance, provides for proper segregation of duties, clearly defines risk-taking responsibility and authority, and promotes ownership and accountability for risk taking.
- **Process**
  We seek to implement robust processes and systems for effective identification, quantification, monitoring, mitigation and management of risks. We seek to improve our risk management as well as internal control policies and procedures on an ongoing basis to ensure that they remain sound and relevant by benchmarking against global best practices.

Based on the above principles, the Group undertakes a continuous process of risk identification, monitoring, management and reporting of risks throughout the organisation to provide assurance to the Board and relevant stakeholders. The effectiveness of risk management policies and processes is reviewed on a regular basis and, where necessary, improved. Independent reviews are conducted by third-party consultants regularly to ensure the appropriateness of the Group's risk management framework. The consultants also report key risks to the Board, as well as provide periodic support and input when undertaking specific risk assessments. Furthermore, the risk management processes facilitate alignment of the Group's strategy and annual operating plan with the management of key risks.

Risk Management Philosophy and Approach

Risk assessment and mitigation strategy is an integral part of the Group's annual business planning and budgeting process. The key risk management activities include scenario planning, business continuity/disaster recovery management and crisis planning and management. Close monitoring and control processes, including the establishment of appropriate key risk indicators and key performance indicators, are put in place to ensure that risk profiles are managed within policy limits. The Group has in place a formal programme of risk and control self-assessment whereby line personnel are involved in the ongoing assessment and improvement of risk management and controls. Additionally, independent specialist consultants are engaged from time to time to review the Group's risk management framework and processes.

SingTel Internal Audit carries out reviews and internal control advisory activities aligned to the key risks in the Group's business. This provides independent assurance to the AC on the adequacy and effectiveness of our risk management, financial reporting processes, and internal control and compliance systems. In order to provide assurance to the Board, the CEOs of the business groups submit a report on the key risks and mitigation strategies for their respective businesses to the RC on a semi-annual basis. Annually, the Group CEO and Group CFO provide a written certification to the Board confirming the integrity of financial reporting, and the efficiency and effectiveness of the risk management, internal control and compliance systems.

In the course of their statutory audit, SingTel's external auditors carry out a review of the Group's material internal controls to the extent of the scope as laid out in their audit plans. Any material non-compliance and internal control weaknesses, together with the external auditors' recommendations to address them, are reported to the AC. SingTel's Management, with the assistance of SingTel Internal Audit, follows up on the external auditors' recommendations as part of their role in reviewing the Group's system of internal controls.

The systems that are in place are intended to provide reasonable but not absolute assurance against material misstatements or loss, as well as to ensure the safeguarding of assets, the maintenance of proper accounting records, the reliability of financial information, compliance with applicable legislation, regulations and best practices, and the identification and management of business risks.

RISK FACTORS

The Group's financial performance and operations are influenced by a vast range of risk factors. Many of these risk factors affect not just our businesses but also other businesses in and outside of the telecommunications industry. These risks vary widely and many are beyond the Group's control. There may also be risks that are either presently unknown or not currently assessed as significant, which may later prove to be material. However, we aim to mitigate the exposures through appropriate risk management strategies and internal controls.

The section below sets out the principal risk types.

ECONOMIC RISKS

Changes in domestic, regional and global economic conditions may have a material adverse effect on the demand for telecommunications, IT and related services, digital services, and hence, on the Group's financial performance and operations.

The global credit and equity markets have experienced substantial dislocations, liquidity disruptions and market corrections. These and other related events have had a significant impact on economic growth as a whole and consequently, consumer and business demand for telecommunications, IT and related services, and digital services.

Our planning and management review processes involve the periodic monitoring of budgets and expenditures to minimise the risk of over-investment. Each of the business units in the Group has continuing cost management programmes to drive improvements in their cost structures.

POLITICAL RISKS

Some of the countries in which Group Consumer operates have experienced or continue to experience political instability. The continuation or re-emergence of such political instability in the future could have a material adverse effect on economic or social conditions in those countries, as well as the ownership, control and condition of our assets in those areas.

Group Consumer is geographically diversified with operations in Singapore, Australia and the emerging markets. We work closely with the Management and our partners in the countries where we operate to leverage the local expertise, knowledge and ability. In this way, we ensure compliance with the laws and are able to implement risk mitigation measures.

As Group Enterprise and Group Digital L!fe expand their products and services across the region and around the world, exposure to similar political risks may increase in the future.

REGULATORY RISKS AND LITIGATION RISKS

Regulatory Risks

The Group's global operations are subject to extensive government regulations, which may impact or limit our flexibility to respond to market conditions, competition, new technologies or changes in cost structures. Governments may alter their policies relating to the telecommunications, IT and related industries as well as the regulatory environment (including taxation) in which we operate. Such changes could have a material adverse effect on the Group's financial performance and operations.

Group Consumer and Group Enterprise are impacted by the implementation of national broadband networks in both Australia and Singapore. In Singapore, the Infocomm Development Authority of Singapore (IDA) has, in its implementation of the Next Generation Nationwide Broadband Network (Next Gen NBN), designed a structure aimed at levelling the playing field to allow the benefits of the Next Gen NBN to be available to all industry players. This has significantly altered the existing cost model of the industry and increased the level of competition in the market with new entrants.

In Australia, the government is currently undertaking a significant reform of the fixed-line telecommunications sector, including the rollout of a national broadband network to be operated on a wholesale-only open-access basis. It is possible that the Australian government's regulatory reforms, including legislation and the deployed national broadband network and commercial transactions relating to the national broadband network, could ultimately lead to a sub-optimal or negative outcome for Optus. Our businesses depend on statutory licences issued by governmental authorities. Failure to meet regulatory requirements could result in fines or other sanctions including, ultimately, the revocation of licences.

In Singapore, the Personal Data Protection Act 2012 (PDPA), which came into effect in January 2013, regulates the collection, use, disclosure, transfer and security of personal data. The Act will be enforced in phases, with the provisions relating to the Do-Not-Call Registry coming into force in early 2014 and the provisions relating to the main data protection coming into force in July 2014. In Australia, The Privacy Act introduced changes with effect from March 2014 on a new set of Australian Privacy Principles that will regulate handling of personal information by Australian government agencies and some businesses. The Group has access to appropriate regulatory expertise and staffing resources in Singapore and Australia. We regularly participate in discussions and consultations with the respective regulatory authorities and the industry to propose changes and provide feedback on regulatory reforms and developments in the telecommunications and media industry.

Our overseas investments are subject to the risk of imposition of laws and regulations restricting the level, percentage and manner of foreign ownership and investment, as well as the risk of nationalisation, any of which could materially and adversely affect our overseas investments.

With regards to personal data protection, the Group has established a PDPA Steering Committee and Working Committee to put in place PDPA policies and procedures in Singapore to ensure compliance. Similarly, in Australia, most of the recent changes to the Privacy Law existed under the previous Act, and there are well-established mechanisms in place to ensure compliance. The inclusion of a new Australian Privacy Principle – Direct Marketing – has meant some change to ensure prevalent opt-out mechanisms are in place. Overall, the Group has also increased resources and improved the support infrastructure around information security.

Access to Spectrum

The Group may need to access additional spectrum to support both organic growth and the development of new services. Access to spectrum is of critical importance to us in order to support our business of providing mobile voice and broadband services. The use of spectrum in most countries that we operate in is regulated by governmental authorities and requires licences. Failure to acquire access to spectrum or new or additional spectrum on reasonable terms or at all could have a material adverse effect on the core communications business, financial performance and growth plans.

Risk Management Philosophy and Approach

Litigation Risks
We are exposed to the risk of regulatory or litigation action by regulators or other parties. Such regulatory matters or litigation actions may have a material effect on our financial condition and results of operations. Examples of such actions which the Group is exposed to are disclosed in Notes to the Financial Statements under "Contingent Liabilities".

The Group has put in place standard master supply agreements with vendors and implemented contract policies to manage contractual arrangements with customers. The policies provide the necessary empowerment framework for the CEOs, the Management Committee and the Board Committees to approve any deviations from the standard policies.

COMPETITIVE RISKS

The Group faces competitive risks in all the markets and business segments in which we operate.

Group Consumer Business
The telecommunications market in Singapore is highly competitive. As new players enter the market and regulation requires SingTel in Singapore to allow our competitors to have access to our networks, our market share in some segments and prices for certain products and services have declined. These trends may continue and intensify for SingTel in Singapore.

In the Australian mobile market, in addition to the incumbent operator, a number of participants are subsidiaries of international groups and operators, and have made large investments which are now sunk costs. The Group is, therefore, exposed to the risk of irrational pricing being introduced by such competitors. The consumer fixed-line services market continues to be dominated by the incumbent provider, which can leverage its scale and market position to restrict the development of competition. With the deployment of the Australian National Broadband Network, competition is expected to increase as new entrants enter the market.

The operations of our international associates' businesses are also subject to highly competitive market conditions. The growth of our associates depends in part on increases in the mobile penetration rate in the markets where they operate. Some of these overseas markets, including India and Indonesia, have experienced and could continue to experience an increase in the number of competitors, leading to intense price competition and potential loss of market share for our associates. As these markets mature, the pace of subscriber growth may slow and new customers may not be as profitable as existing customers.

Our business models and profits are also challenged by disintermediation in the telecommunications industry by handset providers and non-traditional telecommunications service providers who provide multimedia content, applications and services directly on demand.

Group Consumer continues to work with Group Digital L!fe to invest in innovation, technologies, new products and services, transformational initiatives in processes, new business models and customer experience to meet evolving customer needs and strengthen customer loyalty.

Group Digital L!fe Business
The digital products and services offered by the Group face competition from both traditional and non-traditional competitors globally. The proliferation of mobile applications and other content delivered over the internet threaten to disintermediate the relationships between telcos and their customers. The over-the-top operators which provide these services are seeking to grow scale through mergers and acquisitions, which will allow them to exert a stronger influence in customers' usage of our services.

Against this environment, the Group plans to leverage valuable assets we already have, such as our extensive customer knowledge, touchpoints, intelligent networks and the scale of the Group's customer base, to create relevant and personalised services for our customers, such as digital advertising, mCommerce and content.

Group Enterprise Business
Business customers enjoy a wide range of choices for many of the services that we provide, particularly international voice and data communications. Competitors include multinational IT and telecommunications companies, while in Australia, the enterprise market is dominated by the incumbent. The quality and prices of these services can influence a potential business customer's decision. Prices for some of these services have declined significantly in recent years as a result of capacity additions and price competition. Such price declines are expected to continue.

Group Enterprise continues to focus on offering companies comprehensive and integrated infocomm technology (ICT) solutions and initiatives to strengthen customer engagement.

REGIONAL EXPANSION RISKS

Given the size of the Singapore and Australian markets, the future growth of the Group depends, to a large extent, on our ability to grow our overseas operations in both traditional and new digital services. This comes with considerable risks.

Partnership Relations
The success of our strategic investments depends, to a large extent, on our relationships with, and the strength of our investment partners. There is no assurance that the Group will be able to maintain these relationships or that our investment partners will remain committed to their partnerships with the Group.

Acquisition Risks
In acquisitions, the Group faces challenges arising from integrating newly acquired businesses with our own operations, managing these businesses in markets where we have limited experience and financing these acquisitions. The Group risks not being able to generate synergies from these acquisitions, and the acquisitions become a drain on the Group's management and capital resources.

We continually look for investment opportunities that can contribute to our regional expansion strategy and for the development of new revenue streams. Our efforts are challenged by the limited availability of opportunities, competition for the available opportunities from other potential investors, foreign ownership restrictions, government and regulatory policies, political considerations and the specific preferences of sellers.

In addition, the business strategy of some of our regional mobile associates involves the expansion of operations outside their home countries. These associates may enter into joint ventures and other arrangements with other parties. Such joint ventures and other arrangements involve risks, including but not limited to the possibility that the joint venture or investment partner may have economic or business interests or goals that are not consistent with those of the associates. There is no assurance that the regional mobile associates can fully generate synergies and successfully achieve their aims of regional competitiveness and building a competitive regional footprint.

Members of our management team are also directors on the boards of our associates. In addition to the sharing of network and commercial experience, best practices in the areas of corporate governance and financial reporting are also shared across the Group.

The Group adopts a disciplined approach in our investment evaluation and decision-making process.

PROJECT RISKS

The Group incurs substantial capital expenditure in constructing and maintaining our networks and systems infrastructure. These projects are subject to risks associated with the construction, supply, installation and operation of equipment and systems.

Project Management
The projects the Group undertake as contractors to roll out infrastructure are subject to the risks of increased project costs, disputes and unexpected implementation delays, any of which can result in an inability to meet projected completion dates.

Group Enterprise is also a major IT services provider to governments and large enterprises in the region. We face potential project execution risks when projects are not accurately scoped or the quality of service performance is not up to customers' specifications, resulting in over-commitments to customers, as well as inadequate resource allocation and scheduling. These can lead to cost overruns, project delays and losses.

The Group has a project risk management framework in place, with processes for regular risk assessment, performance monitoring and reporting of key projects.

Satellite Business
The launch and operation of any satellite is subject to the risk of launch delays, cost overruns and the occurrence of other unforeseeable events such as satellite launch failures, satellite failure to enter into designated orbital locations, in-orbit failure or any other events beyond the control of the Group. We maintain and regularly review our business continuity programme, including restoration plans, for implementation in the event of a catastrophic loss of all or part of a satellite.

A key capital project undertaken by Optus is the planned launch of a new satellite, Optus 10. The build and launch plan of Optus 10 is closely monitored by the Management. The satellite will be launched in mid-2014 and will also be part of the Group's business continuity plans.

NEW BUSINESS RISKS

From a traditional carriage business in Singapore and Australia, the Group is now venturing into new growth areas to create new revenue streams,

Risk Management Philosophy and Approach

including mobile applications and services, pay TV, managed services, cloud services, content, ICT, and new digital services such as digital advertising. There is no assurance that the Group will be successful in these ventures, which may require substantial capital, new expertise, substantial process or systems changes, as well as organisational cultural and mindset changes. These businesses may also expose the Group to new areas of risks associated with the media and online industries such as content rights disputes and customer data privacy and protection.

The Group's organisation structure, talent management and development programme seeks to respond to changing needs and new business strategies. We continue to update our policies and invest in processes and technologies to support the requirements of new businesses.

BREACH OF PRIVACY RISKS

The Group seeks to protect the privacy of voice and information on networks and systems infrastructure. Significant failure of encryption and security measures may result in customer confidence being undermined and materially impact our businesses. The Group may also be subject to the imposition of additional regulatory measures relating to the security and privacy of customer data.

The Group has in place security mechanisms such as firewalls and encryption algorithms designed to minimise the risk of privacy breaches. We also implement and test antivirus or intrusion prevention systems, based on established security standards. Aside from cyber security practices, the Group has also established an escalation process for major incidents, which includes security breaches, to ensure timely response, internally and externally, to minimise impact.

INFRASTRUCTURE AND TECHNOLOGY RISKS

Rapid and significant technological changes are typical in the telecommunications and ICT industry, and these changes may materially affect Group Consumer and Group Enterprise's capital expenditure and operating costs, as well as the demand for the products and services offered by all of our business divisions.

We have invested substantial capital and other resources in the development and modernisation of our networks and systems. Technological changes continue to reduce costs and expand the capacities of new infrastructure able to deliver competing products and services. Moreover, our associates operate predominantly in emerging markets, where the regulatory practices, including spectrum availability, may not synchronise with the technology progression path and the market demand for new technologies.

Such rapid advancements in technology may leave the Group stranded with investments that are technologically obsolete before the end of their expected useful life. These changes may require us to replace and upgrade our network infrastructure to remain competitive and as a result, incur additional capital expenditure.

Each of the business groups face the continuing risk of market entry by new operators and service providers (including non-telecommunications players) that, by using newer or lower-cost technologies, may succeed in rapidly attracting customers away from established market participants.

Group Enterprise may have to incur substantial development expenditure to gain access to related or enabling technologies so that we may pursue new growth opportunities in the ICT industry. The challenge is to modify our network infrastructure in a timely and cost-effective manner to facilitate such implementation, failing which this could adversely affect our quality of service, financial condition and results of operations.

The Group continues to invest in upgrading, modernising and equipping our systems with new capabilities to ensure that we continue to deliver innovative and relevant services to our customers.

VENDOR RISKS

The Group relies on third-party vendors in many aspects of our business for various purposes, including but not limited to the construction of our network, the supply of handsets and equipment, systems and applications development and services, content provision and customer acquisition. Accordingly, our operations may be affected by third-party vendors failing to perform their obligations. In addition, the industry is dominated by a few key vendors for such services and equipment, and any failure or refusal by a key vendor to provide such services or equipment, or any consolidation of the industry, may significantly affect our business and operations.

The Group monitors closely our relationships with strategic vendors and develops new relationships to mitigate supply risks.

INFORMATION TECHNOLOGY RISKS

As the Group's businesses and operations rely heavily on information technology, the Management has established the IT & Network Security Committee to provide oversight of all IT and network security risks, including cyber security threats and data privacy breaches. The committee comprises members from the various IT and network domains, meets bi-monthly and reports directly to the Risk Management Committee. The committee develops appropriate policies and frameworks to ensure information system security, reviews the projects and initiatives on IT and network security, and reviews any IT security incidents.

The Group has established the Group Information Security Policy for managing risks associated with information security in a holistic manner. The policy is developed based on industry best practices and is aligned with international standards such as ISO27001. The policy covers various aspects of IT risk governance including change management, user access management, database configuration standards and disaster recovery planning, and provides the cornerstone for driving robust IT security controls across the Group.

The Group has also established the Project Management Methodology to ensure that new systems are developed with appropriate IT security controls and are subjected to rigorous acceptance tests, including penetration testing, prior to implementation.

FINANCIAL RISKS

The main risks arising from the Group's financial assets and liabilities are foreign exchange, interest rate, market, liquidity, access to financing sources and increased credit risks. Financial markets continue to be volatile and this may heighten execution risk for funding activities and credit risk premiums for market participants.

The Group is exposed to foreign exchange fluctuations from our operations and through subsidiaries as well as associated and joint venture companies operating in foreign countries. These relate to the translation of the foreign currency earnings and carrying values of the overseas operation. Additionally, a significant portion of associated and joint venture company purchases and liabilities are denominated in foreign currencies, versus the local currency of the respective operations, thereby giving rise to changes in cost structures and fair value gains or losses when marked to market.

The Group has established policies, guidelines and control procedures to manage and report exposure to such risks. Our financial risk management is discussed in detail on page 187 in Note 37 to the Financial Statements.

ELECTROMAGNETIC ENERGY RISKS

Health concerns have been raised regarding the potential exposure to electromagnetic energy associated with the operation of mobile communications devices. While there is no substantiated evidence of public health risks from exposure to the levels of electromagnetic energy typically emitted from mobile communications devices, perceived health risks can result in reduced demand for mobile communications services or worse, litigation against the Group. In addition, government environment controls may be introduced to address this perceived risk, restricting our ability to deploy our mobile communications networks.

The Group is currently in compliance with the leading global standard, International Commission on Non-Ionizing Radiation Protection (ICNIRP) Electromagnetic Energy (EME), as well as relevant standards and regulations in Singapore and Australia on emission of electromagnetic energy. We continue to monitor research findings on electromagnetic energy health risks and their implications on relevant standards and regulations in Singapore and Australia, as well as the rest of the world.

NETWORK FAILURE AND CATASTROPHIC RISKS

The provision of our services depends on the quality, stability, resilience and robustness of our integrated networks. We face the risk of the malfunction of, loss of, or damage to network infrastructure from natural or man-made causes. Some of the countries in which we operate have experienced a number of major natural catastrophes over the years, including typhoons, droughts and earthquakes. Such losses or damage may significantly disrupt our operations, which may materially adversely affect our ability to deliver services to customers.

The Group has insurance policies as well as a defined crisis management and escalation process involving the CEOs and senior management to respond to emergencies and/or catastrophic events. However, our inability to operate our networks or customer support systems may have a material impact on our business.