Risk Management Philosophy and Approach

We identify and manage risks to reduce the uncertainty associated with executing our business strategies and to maximise opportunities that may arise. Risks can take various forms and can have material adverse impact on our reputation, operations, human resources and financial performance.

We have established a comprehensive risk management framework approved by our Risk Committee. The risk management framework sets out the governance structure for managing risks, our risk philosophy, risk appetite and tolerance levels, our risk management approach as well as risk factors.

In addition, our risk assessment and mitigation strategy is aligned with our Group strategy and an integral part of the annual business planning and budgeting process.

Governance Structure for Managing Risks

THE BOARD

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

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

AUDIT COMMITTEE

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

MANAGEMENT COMMITTEE

- Implements risk management practices within all business units and functions

RISK MANAGEMENT COMMITTEE

- Supports the Board and Risk Committee in terms of risk governance and oversight
- Sets the direction and strategies to align risk management and monitoring with the Group's risk appetite and tolerance
- Reviews the risk assessments carried out by the business units
- Reviews and assesses risk management systems and tools
- Reviews efficiency and effectiveness of mitigation and coverage of risk exposure

Our Risk Philosophy

Our risk philosophy and risk management approach are based on three key principles:

RISK-CENTRIC CULTURE

- Set the appropriate tone at the top
- Promote awareness, ownership and productive management of key risks
- Promote accountability

STRONG CORPORATE GOVERNANCE STRUCTURE

- Promote good corporate governance
- Provide proper segregation of duties
- Clearly define risk-taking responsibility and authority
- Promote ownership and accountability for risk-taking

PROACTIVE RISK MANAGEMENT PROCESS

- Robust processes and systems to identify, quantify, monitor, mitigate and manage risks
- Benchmark against global best practices

Risk Appetite

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, we 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 the Pacific through our regional associates. We will continue to pursue business expansion in the emerging markets, including acquiring controlling stakes in the associates, and actively managing 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.

Risk Management

We have established a rigorous and systematic risk review process to identify, monitor, manage and report risks throughout the organisation based on our risk philosophy. Management has the primary responsibility for identifying, managing and reporting to the Board the key risks faced by the Group. Management is also responsible for ensuring that the risk management framework is effectively implemented within the business units. The business units are supported by specialised functions such as Regulatory, Legal, Tax, Cyber Resilience, Environment and Sustainability, Insurance, Treasury and Credit Management in the management of risks. In addition, through stakeholder engagement and materiality assessments, we regularly review and assess the environmental, social and governance (ESG) risks that exist or emerge in our broader value chain, and we address them with various corporate sustainability initiatives. Our corporate sustainability initiatives are discussed further on page 111 and in our Group Sustainability Report.

Risk Management Philosophy and Approach

Our key risk management activities also include scenario planning, business continuity/disaster recovery management and crisis planning and management. Close monitoring and control processes, including the use of appropriate key risk and key performance indicators, are implemented to ensure the risk profiles are managed within policy limits.

In addition, we have in place a formal programme of risk and control self-assessment where line personnel are involved in the ongoing assessment and improvement of risk management and controls. The effectiveness of our 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 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. Overall, the risk management processes facilitate alignment of our strategy and annual operating plan with the management of key risks.

Singtel's Internal Audit (IA) carries out reviews and internal control advisory activities aligned to the key risks in our businesses. This provides independent assurance to the Audit Committee (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 our business units submit an annual report on the key risks and mitigation strategies for their respective businesses to the Risk Committee. Our Group CEO and Group CFO, with assurance from the Management Committee members, provide an annual 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, external auditors review our material internal controls to the extent of the scope laid out in their audit plans. Any material non-compliance and internal control weaknesses, together with their recommendations to address them, are reported to the AC. Our Management, with the assistance of Singtel IA, follows up on the auditors' recommendations as part of their role in reviewing our 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

Our financial performance and operations are influenced by a vast range of risk factors. Many of these affect not just our businesses, but also other businesses in and outside 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 exposure through appropriate risk management strategies and internal controls.

The section below sets out the principal risk types, which are not listed in the order of significance.

- Pandemic Risks/COVID-19
- Economic Risks
- Political Risks
- Regulatory and Litigation Risks
- Competitive Risks
- Expansion Risks
- Project Risks
- New Business Risks
- Technology Risks
- Vendor/Supply Chain Risks
- Information Technology Risks
- Data Protection and Privacy Risks
- Cyber Security Risks
- Network Failure and Catastrophic Risks
- Financial Risks
- Talent Management Risks
- Electromagnetic Energy Risks
- Climate Change Risks

PANDEMIC RISKS/COVID-19

The Group could be adversely impacted by global pandemics, and the Group's business and operations have been affected by the unprecedented disruption caused by the COVID-19 pandemic, which has shaken governments, health systems, economies and societies around the world. Since its outbreak, COVID-19 has spread with alarming speed across various countries and territories, and resulted in a significant number of infections and fatalities. The economic consequences of the outbreak are yet to

unfold although governments in many countries are implementing budgetary interventions and economic stimulus programmes. The outbreak of such infectious diseases together with the restrictions on travel and imposition of quarantine and/or lockdown measures may have an adverse effect on various aspects of our business and operations, impacting mobile roaming revenue and business continuity. The disruptions of such pandemic outbreaks to global supply chains of network systems, equipment, handsets, devices and content, could impact or lead to delays in the deployment, installation, upgrading, operation and maintenance of network infrastructure, and/or delivery of equipment, handsets, devices and content. The imposition of movement restriction measures on a nationwide or at a city level in the countries that we operate in, could lead to access and workforce constraints and impede our ability to operate and serve our customers, resulting in deterioration in service levels and/or quality, delays to projects and deliverables to customers, inability to meet contractual obligations and/or failure to comply with regulatory requirements. Such measures could significantly dampen both consumer and enterprise spending, and adversely affect revenues. Decline in revenues and delay in payments or non-payments from customers' default may lead to funding constraints for the Group.

A prolonged and widespread pandemic outbreak may result in a global recession with severe impact to various sectors such as telecommunication, aviation, travel, retail, tourism, auto, manufacturing and oil and gas; reduced investment and spending; and severe unemployment. An economic downturn of this scale, coupled with the uncertainties around disruption to business models posed by technology, changes in enterprise and consumer behaviours, and government and regulatory actions, may pose significant challenges to the management of capital investments, working capital and business changes.

As the COVID-19 situation develops, the consequences of the COVID-19 outbreak or any future outbreak of infectious disease are unpredictable and there can be no assurance that any precautionary or other measures taken against such infectious diseases would be effective. The effectiveness of the measures adopted by various governments in response to the COVID-19 outbreak and the extent to which these can mitigate the adverse economic impacts from the pandemic remain uncertain. There can be no assurance that the business environment and/or customer demand will fully recover post-COVID. However, we will continue to monitor the impact on our business, financial condition, results of operations and prospects, and institute the necessary measures to protect the health and safety of our workforce, and to mitigate the risks to our business. We will also plan and adjust our strategies to adapt to the post-COVID scenario, as telecommuting and digitalisation accelerate, and telecommunications infrastructure becomes even more critical.

ECONOMIC RISKS

Changes in domestic, regional and global economic conditions may have a material adverse effect on the demand for telecommunications, information technology (IT) and related services, digital services, and hence, on our financial performance and operations. Global headwinds such as trade tensions and the COVID-19 pandemic outbreak have resulted in significant uncertainty in the macroeconomic environment and this could have an adverse effect on our overall Group strategy and growth.

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, on consumer and business demand for telecommunications, IT and related services, and digital services.

Our planning and management review processes involve keeping abreast of the economic and market developments and periodic monitoring of budgets and expenditures to optimise the allocation of capital among the various businesses in our Group. Each of the business units in our Group has continuing cost management and transformation programmes to drive improvements in their cost structures and/or changes in their business model.

POLITICAL RISKS

Our business is geographically diversified with operations in Singapore, Australia and the emerging markets. Some of the countries in which we operate 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 on the ownership, control and condition of our assets in those areas.

We work closely with the Management and our partners in the countries where we operate, to leverage the local expertise, knowledge and ability to manage the local and socio-economic conditions and risks.

Risk Management Philosophy and Approach

This way, we ensure compliance with the laws and are better able to implement risk mitigation measures.

As our Enterprise and Digital Life businesses expand their business operations across the region and around the world, exposure to similar political and socio-economic risks may increase in the future.

REGULATORY AND LITIGATION RISKS

Regulatory Risks

Our businesses depend on licences issued by government authorities. Failure to meet regulatory requirements could result in fines or other sanctions including ultimately, the revocation of licences. Our 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, multimedia and related industries, as well as the regulatory environment (including taxation) in which we operate. Such changes could have a material adverse effect on our financial performance and operations.

Our overseas investments are also 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. Furthermore, judicial developments in various jurisdictions can be unpredictable. Any of these factors can materially and adversely affect our overseas investments.

Consumer Australia, Consumer Singapore and Group Enterprise are impacted by the implementation of national broadband networks in both Australia and Singapore.

In Singapore, the Infocomm Media Development Authority (IMDA) has, in its implementation of the Next Generation Nationwide Broadband Network (Next Gen NBN), designed a structure to level the playing field to make the benefits of the Next Gen NBN available to all industry players. This Next Gen NBN structure has significantly altered the existing cost model of the industry and increased the level of competition in the broadband market.

In Australia, the government has implemented a significant reform of the fixed line telecommunications sector, including the rollout of a national broadband network by the government-owned entity, NBN Co, operated on a wholesale-only open access basis. It is possible that the Australian government's policy decisions relating to the national broadband network or commercial decisions taken by NBN Co could ultimately lead to a sub-optimal or negative outcome for Optus.

Our operations are also subject to various other laws and regulations such as those relating to customer data privacy and protection, payment services and anti-money laundering, anti-bribery and corruption, workplace safety and health, public order and safety, cyber security, online falsehoods and national security. The regulatory landscape for the media and telecommunications industry has seen changes with recent developments applicable to cyber security and consumer protection. These changes, together with increasing scrutiny and regulators inclined to strong enforcement actions, may lead to additional compliance costs to the business. Failure to meet regulations may adversely affect our businesses.

In Australia, the government has adopted security legislation and made decisions which have affected the industry. In particular, equipment vendors from countries with certain legal structures or power have been excluded from participating in the supply of equipment for 5G infrastructure.

We have access to appropriate regulatory expertise and staffing resources in Singapore and Australia and we work closely with the various stakeholders and our partners in the countries we operate in. We monitor new developments closely and participate regularly 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. In addition to instituting measures and processes to ensure regulatory compliances, we conduct training and refresher sessions for staff and management.

Access to Spectrum

Access to spectrum is critically important for supporting our business of providing mobile voice, data and other connectivity services. The use of spectrum in most countries where we operate is regulated by government authorities and requires licences. Failure to acquire access to spectrum, or new or additional spectrum, on reasonable commercial terms, or at all, could have a material adverse effect on our core communications business, financial performance and growth plans.

Taxation Risks

Our Group has operations across a large number of jurisdictions, and we are subject to the tax regulations, or changes in regulations, in the

respective jurisdictions in which we operate. The tax legislations or changes may increase our compliance obligations and business costs.

We are committed to comply with applicable tax laws in countries where we operate. We have skilled staff in taxation matters and work with external tax advisors where necessary. Material tax disputes and risks are escalated in accordance with the risk management framework, and appropriate disclosures are made in our financial statements.

Litigation Risks
We are exposed to the risk of regulatory and litigation action by regulators and other parties. Such regulatory matters and litigation actions may have a material effect on our financial condition and results of operations. Examples of such litigation are disclosed as contingent liabilities in the Notes to the Financial Statements.

We have put in place master supply agreements with key vendors, master services agreements with key customers, and implemented contract policies to manage contractual arrangements with our vendors and customers. The policies also set out the necessary risk empowerment framework and principles for the Management Committee, CEOs, and Management to approve deviations from the standard terms.

COMPETITIVE RISKS

We face competitive risks in all markets and business segments in which we operate.

Group Consumer Business
The telecommunications market in Singapore is highly competitive. As competition further intensifies with the entry of a fourth mobile network operator and mobile virtual network operators (MVNOs), industry revenue may decrease further and our market share may decline. Singapore's Next Gen NBN allows Retail Service Providers (RSPs) equal and open access to Netlink Trust's fibre network and in turn, has increased competitive pressure in fixed broadband and home services.

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. We are, 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 further as new operators enter the market. With the impending merger of two existing operators, mobile competition is expected to further intensify.

The operations of our regional associates' businesses are also subject to highly competitive market conditions. Their growth depends in part on the adoption of mobile data services in their markets. Some of these markets have and could continue to experience intensifying price competition for mobile data services from new competitors and/or smaller scale competitors, leading to lower profitability and potential loss of market share for our associates.

Our business models and profits are also challenged by disintermediation in the telecommunications industry by handset providers and other digital service providers and non-traditional telecommunications service providers, including social media networks and over-the-top (OTT) players which provide multimedia and video content, applications and services directly on demand.

We continue to invest in our networks to ensure that they have the coverage, capacity and speed that will provide our customers with the best network and connectivity experience. Group Consumer is focused on driving efficiencies and innovation via new technologies, products, services, processes and business models to meet evolving customer needs and enhance customer experiences.

Group Enterprise Business
Business customers enjoy a wide range of choices for many of our services, including fixed, mobile, cloud, managed services and hosting, IT services and consulting. Competitors include multinational IT and telecommunications companies, technology companies that introduce new communication services, as well as other non-traditional players, while the enterprise market in Australia 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, technology innovations and price competition. Such price declines are expected to continue.

Group Enterprise continues to focus on offering companies

Risk Management Philosophy and Approach

comprehensive and integrated infocomm technology (ICT) solutions and initiatives to strengthen customer engagement. This includes broadening our solution portfolio to cover new areas of customer needs, such as cloud computing, cyber security and digital solutions for smart cities and enterprises.

Group Digital Life Business
The digital products and services we offer are primarily in the areas of digital marketing and data analytics. Competition is intense, with many OTT operators offering these services and facing low barriers to entry.

Group Digital Life aspires to become a significant global player in these areas by delivering distinctive products and services in the target markets and launching them quickly to capture market share. We will continue to scale our digital businesses, leveraging our valuable assets, such as extensive customer knowledge, touch points, intelligent networks and our customer base.

EXPANSION RISKS

Given the size of the Singapore and Australia markets, our future growth depends, to a large extent, on our ability to grow our overseas operations in both core communications 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 partners. There is no guarantee that we will be able to maintain these relationships or that our partners will remain committed to the partnerships.

Acquisition Risks
We continually look for investment opportunities that can contribute to our expansion strategy and develop new revenue streams. Our efforts are challenged by the limited availability of opportunities, competition from other potential investors, foreign ownership restrictions, government and regulatory policies, political considerations and the specific preferences of sellers. We face challenges arising from integrating newly acquired businesses with our own operations, managing these businesses and talent in markets where we have limited experience and/or resources and financing these acquisitions. We also risk not being able to generate synergies from these acquisitions, and the acquisitions becoming a drain on our management and capital resources.

The business strategies of some of our regional associates involve expanding operations outside their home countries, as well as in-country mergers and acquisitions. 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 guarantee that the regional associates can generate synergies and successfully build a competitive regional footprint.

We adopt a disciplined approach in our investment evaluation and decision-making process. Members of our management team are also directors on the boards of our associates and joint ventures. In addition to sharing network expertise, product innovation and development, and commercial experience, best practices in the areas of corporate governance and financial reporting are shared across the Group.

PROJECT RISKS

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

The projects that we undertake as contractors to operate and maintain 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 or service levels.

Group Enterprise is a major IT service provider to governments and large enterprises in the region. We face potential project execution risks such as effort estimation or technical complexities which can result in cost overruns, project delays and losses.

We have a risk management framework in place for systematic assessment, monitoring and reporting of project risks. Risk profiling of the projects is performed from bid qualification and participation and reviewed throughout project execution. This is to ensure that appropriate attention and quality assurance and focus are given by management to high risk projects.

NEW BUSINESS RISKS

Beyond our traditional carriage business in Singapore and Australia, we are venturing into new growth areas to create additional revenue streams, including 5G, regional premium OTT video, mobile payment and remittance services, gaming and content, managed services, cloud services, cyber security, ICT, data analytics and digital marketing. There is no assurance that we will be successful in these ventures and gain market share, and these businesses may require substantial capital,

new expertise, considerable process or system changes, as well as organisational, cultural and mindset changes. These businesses may also expose us to regulatory and IT security risks, along with the risks associated with industries like cyber security, media, online content, such as media regulation, brand safety, intellectual property infringement, content rights disputes, online falsehood, and data protection regulations and legislation.

As new businesses place new demands on people, processes and systems, we respond by continually updating our organisation structure, talent management and development programmes, reviewing our policies and processes, and investing in new technologies to meet changing needs. We will constantly stay abreast of new trends and build strategic partnerships with market players to stay competitive.

5G Risks
In Singapore, IMDA has announced Singtel Mobile Singapore Pte Ltd as one of the winners of its 5G Call-For-Proposal and will allocate radio frequency spectrum for us to deploy nationwide 5G networks. In Australia, new spectrum licences for the 26GHz band are likely to be auctioned in late 2020. Failure to acquire the licences in Australia could have an adverse effect on our core communications business and our competitiveness. The business case for investment in 5G network and related systems has risks of uncertainty and may be earnings dilutive. There may also be a long payback period as 5G use cases and revenue and monetisation opportunities are not yet fully developed. The existing high quality 4G networks may also limit the perceived value of 5G and impact its monetisation potential.

In addition, the Australian government has implemented security legislation to restrict vendors from certain countries from participating in the supply of 5G network equipment to mobile network operators. This limits the available vendor sources and may lead to higher investment costs.

With 5G, as with the deployment of our various networks, we will continue to monitor health and safety concerns around exposure to electromagnetic energy emissions (EME), ensure full compliance with government mandated standards and institute the necessary precautionary measures to safeguard the health and safety of the public and our customers.

Digital Banking Risks
In June 2019, the Monetary Authority of Singapore (MAS) announced that it will issue up to two digital full bank (DFB) licences and three digital wholesale bank (DWB) licences. The digital bank licences will allow companies (including non-bank players) to conduct digital banking businesses in Singapore and this marks a new chapter in the liberalisation of Singapore's banking industry. We have formed a consortium with Grab Holdings Inc. to apply for a DFB licence, which will allow the digital bank to take deposits from and provide banking services to retail and non-retail customer segments.

Should our consortium be awarded the licence, there is no assurance that the consortium will be successful in its digital banking venture. The digital bank requires substantial capital outlay and could be subjected to investment and/or financial losses arising from failure to scale and acquire customers and/or the failure to manage the various risk exposure related to the digital banking business, including credit risks, market risks, liquidity risks, technology risks and/or other operational risks. The business is also exposed to the regulatory risks associated with the banking industry, including compliance with existing and/or new laws and regulations, and associated increased cost of compliance. The digital bank may not be able to attract, integrate and retain the right talent with the appropriate skillsets and expertise to develop and/or execute the bank's business strategies and plans, or effectively manage risks arising from the bank's activities. The digital bank may lose its licence to continue operations if its financial performance does not meet expectations or deteriorates. There could also be a misalignment of interests, goals and cultures between the members of the consortium, and/or with the management of the digital bank, resulting in an inability to resolve disputes in an effective and timely manner.

We will collaborate with our partners and the digital bank to drive synergies from the combined strengths, digital assets and know-how, and other resources of the Group and partners. We will have appropriate board representation and shareholders' agreement to ensure governance and rights protection and oversee the establishment of sound risk management principles, policies and procedures and sustainable business practices.

TECHNOLOGY RISKS

Rapid and significant technological changes are typical in the telecommunications and ICT industry. Technological changes may reduce costs, expand the capacity of new infrastructure, bring new sources of revenue, and/or result in shorter periods for investment recovery, all of which present both opportunities aswell as disruptions and challenges. These changes may materially affect the Group's capital expenditure and operating costs, as well as thedemand for products and services offered by our business divisions.

Risk Management Philosophy and Approach

The rapid advancements in wireless communications and new digital technologies such as 5G, AI, Application Programming Interfaces, cloud and blockchain are driving the development of entirely new ecosystems and business models. This may leave us with infrastructure and systems that are technically obsolete before the end of their expected useful life and may require us to replace and upgrade our network and systems to remain competitive, and as a result, incur additional capital expenditure.

On the other hand, these changes also present opportunities for us to build upon our connectivity advantage, depending on our ability to apply these technologies to relevant services. In the emerging markets in which our associates operate, regulatory practices, including spectrum availability, may also not necessarily synchronise with the technology progression path and the market demand for new technologies.

Each business unit faces the ongoing 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. Our business may also incur substantial development expenditure to gain access to related or enabling technologies to pursue new growth opportunities in the business, e.g. the ICT industry. The challenge is to modify our existing infrastructure and processes in a timely and cost-effective manner to facilitate such implementation, failing which, this could adversely affect our quality of service, financial condition and operational performance.

We continue to invest in upgrading, modernising through digital transformation initiatives and equipping our people and systems with new capabilities to ensure we are able to deliver innovative and relevant services to our customers.

VENDOR/SUPPLY CHAIN RISKS

We rely on third-party vendors and service providers and their extended supply chain in many aspects of our business for various purposes, including, but not limited to, the construction, operations and maintenance of our network, the supply of handsets and equipment, systems and application development services, customer service operations, content provision and customer acquisition. Accordingly, our operations and reputation may be affected by third-party vendors or their supply chains failing to perform their obligations or failing to operate in line with increased expectations of key stakeholders such as government, regulators and customers on a broadening set of ESG issues. In addition, the industry is dominated by a few key vendors for such services, handsets and equipment. Any severe delays, failure or refusal by a key vendor to provide such services, handsets or equipment arising from disruptions caused by global pandemics including the COVID-19 situation, government-imposed bans on vendors and/or sanctions due to security and other concerns, or any consolidation of the industry, may significantly affect our business and operations.

We monitor new legislation introduced such as the recent Australian Modern Slavery Act, as well as the developments and restrictions by governments and regulators on various vendors to ensure our key vendors comply with the relevant laws and regulations. We also monitor our relationships with key vendors closely and develop new relationships to mitigate supply risks. We have in place a Sustainable Supply Chain Management strategy and approach, including a Supplier Code of Conduct, which is regularly updated to manage risks that may exist in our supply chain (Refer to the Singtel Group Sustainability Report for more details on how we address these risks and issues).

INFORMATION TECHNOLOGY RISKS

Our businesses and operations rely heavily on information technology and we have established the Cyber Security Resiliency Committee to provide oversight of all IT and network security risks, including cyber security threats and data privacy breaches. The committee is chaired by CEO, Group Enterprise and comprises senior members from the businesses, various IT and network domains, and meets on a regular basis. The committee develops appropriate policies and frameworks to ensure information system security, reviews the projects and initiatives on IT and network security, reviews IT security incidents, and establishes overall governance by performing audits and cyber security drills.

We have established a Group Cyber Security Policy for managing risks associated with information security. The policy is developed based on industry best practices and is aligned with international standards such as ISO 27001. The policy covers holistically 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.

We have also established a Project Management Methodology to ensure that new systems are developed with appropriate IT security controls and are subject to rigorous acceptance tests, including penetration testing, prior to implementation.

DATA PROTECTION AND PRIVACY RISKS

We seek to protect the data privacy of our customers in our networks and systems. Significant failure of security measures or lapses in established processes may undermine customer confidence and result in litigation actions from customers and/or regulatory fines and penalties. We may also be subject to the imposition of additional regulatory measures relating to the security and privacy of customer data, which may impact the way we conduct our business and/or market our products and services to customers.

Regulators in various countries have strengthened existing legislation and introduced new laws to protect consumer privacy. In Australia, regulators are increasingly active in enforcing existing laws and are examining options to extend these laws to address public concern over data breaches and the activities of social media platforms. In the United States, regulators in California have implemented new legislation governing consumer data and privacy.

We continue to ensure data privacy by protecting the personal data of our customers and staff. We also ensure compliance with applicable privacy laws, and perform regular reviews in order to refine our practices. We have implemented security policies, procedures, technologies and tools designed to minimise the risk of privacy breaches. We have also established an escalation process for incident management, which includes security breaches to ensure timely response, internally and externally, to minimise impact.

CYBER SECURITY RISKS

The scale and level of sophistication of cyber security threats have increased with the changing tactics and tools by cyber attackers, ranging from terrorist attacks, state-sponsored hacking, black-hat hacking or even internal threats and ransomware. As our business is heavily dependent on the resiliency of our network infrastructure, and supporting systems, we are exposed to cyber security threats which can result in disruptions to our network and services provided to customers, and leakage of sensitive and/or confidential information. The exposure is further intensified with the growing dependency on connectivity and smart devices by our customers, and can lead to impact on our reputation, litigation actions from customers and/or regulatory fines and penalties.

Group Enterprise is growing our cyber security business globally. The failure to keep up with and counteract increasing cyber security threats can materially and adversely affect our reputation, cyber security business and growth strategy.

We adopt a holistic approach in managing and addressing risks of cyber threats and attacks by keeping abreast of the threat landscape and business environment as well as implementing a multi-layered security framework to ensure there are relevant preventive, detective and recovery measures. This includes training our people to adopt a security-first mindset and security by design principle, being vigilant to existing and new cyber threats, deploying the tools and resources to mitigate risks and ensuring compliance reviews on third-party service providers are conducted.

We have been building our capabilities organically, as well as partnerships with best-of-breed technology partners. We have approximately 1,800 cyber security professionals, global security operations and engineering centres and a specialised team of ethical hackers and forensic experts assisting the businesses to manage vulnerabilities and threats, achieve regulatory compliance and implement secure solutions. The Group's Cyber Security Institute conducts regular training programmes to enhance the cyber security skills and preparedness of our staff as well as our customers, including businesses and governments in the Asia Pacific. The Group also invested in a research and development lab to drive innovation in this area.

NETWORK FAILURE AND CATASTROPHIC RISKS

The telecommunications industry faces a continuous challenge of providing fast, secure and reliable networks to an increasingly digital and connected world. The provision of our services depends on the quality, stability, resilience and robustness of our networks and systems. We face the risk of malfunction of, loss of, or damage to, network infrastructure from natural or other uncontrollable events such as acts of terrorism.

Risk Management Philosophy and Approach

Some of the countries in which we and/or our regional associates operate have experienced a number of major natural catastrophes over the years, including typhoons, droughts, floods, fires and earthquakes. Some of these catastrophes have also increased in intensity and frequency due to climate change factors, causing prolonged and exacerbated impact on our infrastructure and operations.

In addition, other events that are/are not within our control and/or our regional associates' control, such as fire, deliberate acts of sabotage, vendor failure/negligence, pandemic shutdowns, industrial accidents, blackouts, terrorist attacks, criminal acts or large scale cyber attacks on our network and systems, could damage, cause operational interruptions or otherwise adversely affect any of the facilities and activities, as well as potentially cause injury or death to personnel. Such losses or damages may significantly disrupt our operations, which may have a materially adverse effect on our ability to deliver services to customers. Sustained or significant disruption to our services can also significantly impact our reputation with our customers. Our inability to operate our networks or customer support systems may have a material impact on our business.

We continue to make our networks robust and resilient, and continually review our processes to prevent any network disruptions and to have an effective communication process for timely updates to our stakeholders during any incident and/or crisis. There is a defined crisis management and escalation process for our CEOs and senior management to respond to emergencies and catastrophic events. In addition to key network infrastructure, we have business continuity plans and insurance programmes and policies in place.

FINANCIAL RISKS

The main risks arising from our 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 with the unprecedented global recessionary impacts arising from the uncertainties posed by the COVID-19 situation, may heighten execution risk for funding activities and increase credit risk premiums for market participants.

We are exposed to foreign exchange fluctuations from our operations and through subsidiaries as well as associates and joint ventures operating in foreign countries. These relate to our dividend receipts and the translation of the foreign currency earnings and carrying values of our overseas operations. Additionally, a significant portion of associates and joint venture purchases and liabilities are denominated in foreign currencies, versus the local currency of the respective operations. This gives rise to changes in cost structures and fair value gains or losses when marked to market.

We have established policies, guidelines and control procedures to manage and report exposure to such risks. Our financial risk management is discussed further on page 239 in Note 37 to the Financial Statements.

TALENT MANAGEMENT RISKS

As we seek new avenues of growth, it is pertinent to be able to attract, develop and sustain talent with new skills and capabilities. We also identify, develop and build the next generation of leaders from both internal and external talent pools to ensure a robust succession pipeline. The loss of some or all of our key executives or the inability to attract, build and retain key talent and leaders, could materially and adversely affect our business.

We continue to invest in the skills of our existing workforce and build up our current and emerging capabilities through external professional hires and targeted recruitment. In order to develop and retain talent, we conduct regular skills assessment in the critical business areas and set out structured developmental roadmaps to fill new and emerging skills gaps. We have a targeted development approach to develop young, emerging and future technical and business leaders through formal learning activities, coaching and mentoring, as well as providing critical experiences such as international assignments, rotations and special projects.

Succession management is key to ensuring that the Group effectively manages the short-term and long-term risks associated with critical roles. A robust annual succession planning review by the businesses and the Management Committee, with the involvement of the Board for senior leadership roles, ensures that leadership succession plans are current and relevant to support the business strategies.

ELECTROMAGNETIC ENERGY RISKS

Health concerns have been raised globally about the potential exposure to EME emissions from using mobile handsets or being exposed to mobile transmission equipment. While there is no substantiated evidence of public health risks from exposure to the levels of EME typically emitted from mobile

phones, perceived health risks can be a concern for our customers, the community, and regulators. Perceived health risks in terms of environmental exposure from mobile base station equipment can impact and cause concern for the local communities on the implementation of new or upgrading of existing mobile base stations. This may impact the mobile coverage at that locality and also, our mobile business. In addition, government legislations and industry requirements may be introduced to address this perceived risk, affecting our ability to deploy the mobile communications infrastructure. These perceived health risks could result in reduced demand for mobile communications services and/or litigation actions against us.

We design and deploy our network to comply with the relevant government-mandated standards for exposure to EME. Our standards are based upon those recommended by the International Commission on Non-Ionizing Radiation Protection (ICNIRP), which is a related agency of the World Health Organisation. The ICNIRP standards are adopted by many countries around the world and are considered best practices. We continue to monitor research findings on EME, health risks and their implications on relevant standards and regulations.

CLIMATE CHANGE RISKS

Climate change is one of the key long-term global risks that has the potential to impact our operations, infrastructure and supply chain. Some of the countries in which we and/or our regional associates operate have experienced several extreme weather events, including typhoons, droughts, floods and bushfires, which have increased in intensity and frequency due to climate change factors. Apart from physical risk, damage to our networks and disruptions to our operations, there are also other energy security and regulatory risks associated with climate change, which could result in stricter greenhouse gas emission standards, 'carbon' taxes, and/or changes in energy prices or accompanying infrastructure investments for adaptation or mitigation. To address these concerns, we have adopted a two-pronged approach, an absolute greenhouse emissions reduction goal and the adaptation of our infrastructure to continue building resilience against climate change risks.

We have set absolute carbon reduction targets approved by the Science Based Target initiative in 2017 to address the continued impact of carbon and increasing temperatures. This approach progressively aligns our 2030 carbon contribution and reduction target with the agreements made at Paris COP 21 and the Intergovernmental Panel on Climate Change reports. Our aspiration is to meet the more aggressive 1.5°C target and net zero by 2050. We adapt our infrastructure design and standards progressively to long-term scenarios related to climate change, such as increased risk of inundation and stronger cyclonic activities, rising temperatures and higher frequency and severity of bushfires in Australia. We have also supported a global agreement for the ICT industry through our active participation at the GSM Association to align the efforts of this sector and we continue working with our stakeholders to prepare our disclosures on climate-related risks to align to the recommendations of the Task Force for Climate-Related Financial Disclosures.