
Chusen Aun
CVM Analytics
XL Axiata
I love teaching others
how to grow their own food.
#ItBeginsWithMe

GOVERNANCE

WHAT YOU'LL FIND IN THIS SECTION

Governance

We continue to place emphasis on the strictest standards of corporate governance as a function of the creation of sustainable, long-term value for all our stakeholders.

It is also imperative that good corporate governance is ingrained from the highest levels of our organisation, with our Board of Directors responsible for establishing clear policies and procedures to lead prudent decision-making and ensure discipline and accountability. The Board remains guided by its governance framework to ensure the best interests of the Group, its shareholders and other stakeholders are prioritised in the decision-making process. The governance framework is also continuously enhanced to ensure its relevance to current developments and regulatory requirements.

Business Ethics And Compliance

Key Highlights:

- Achieved a Group-wide completion rate of over 90% for our Anti-Bribery and Anti-Corruption mandatory training module for our employees
- Continued accessibility of our whistleblowing channel
- Contributed USD1.3 billion in taxes to the governments of all countries where we operate

78 Strengthening Risk Governance Structure and Risk Management
78 Anti-Bribery And Anti-Corruption
79 Whistleblowing (Speak Up) Channel
79 Tax Transparency

Data Privacy

Key Highlights:

- Implemented Group-wide Privacy Programme
- Published Group Data Privacy Policy and updated Privacy Notices for customers
- Rolled out and completed 90% of our mandatory training and awareness programme for the Group's employees and vendors processing critical assets and personal data
- Transitioning our cyber security strategy from Digital Trust 2020 to Digital Trust and Resilience 2023

80 Data Privacy Strengthened Through Our Privacy Commitment
81 Strengthening Cyber Security Programmes And Technologies

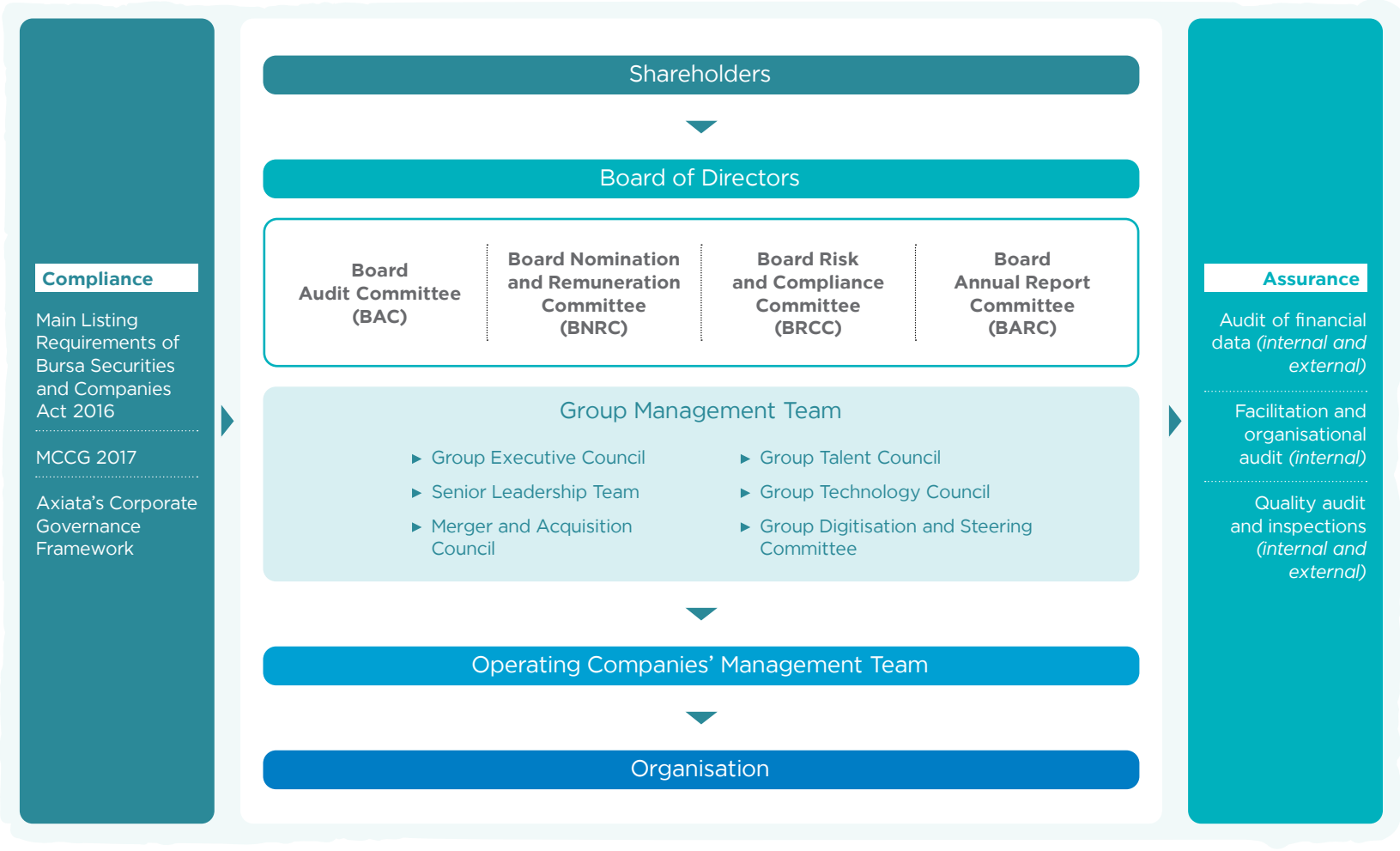
Regulatory and Political Risk

- Established a regulatory compliance framework to monitor regulatory compliance at the Group level and across OpCos in a more structured way
- Appointed subject matter experts at the Group level and OpCos to monitor regulatory compliance
- Strengthened political risk mitigation to enable better monitoring processes of key political and geopolitical events as well as anticipate emerging risks

Our Corporate Governance

At Axiata, we continue to uphold the strictest corporate governance standards as part of our sustainable and long-term value proposition for all our stakeholders. In this regard, the Board of Directors is responsible for establishing clear policies, standards, and ensuring that the decisions are guided by our Corporate Governance Framework. The Framework is continuously enhanced to ensure its applicability to current developments and evolving regulatory requirements.

The Board continues to ensure that Axiata's corporate governance is in accordance with the Malaysian Code on Corporate Governance (MCCG) 2017. We have adopted an iterative process of transparent reporting and disclosure, as well as rigorous risk and performance management, underlined by transparency, ethical and effective leadership. Furthermore, we leverage on the Board's diversity in gender, race, and professional backgrounds to achieve constructive deliberations which take into account the interests of our equally diverse stakeholders. Collectively, these corporate governance measures provide safeguards to our company strategy and contribute to value creation for our business and for all our stakeholders in the short-, medium-, and long-term.



IAR More details on our Corporate Governance can be found on page 80-103 of IAR 2020

Business Ethics And Compliance

Ethics and compliance management ensure that the Group remains compliant with all applicable laws, regulatory requirements, and policies. Our culture of ethics and compliance, underpinned by our Uncompromising Integrity value, is embedded in our daily operations and engagement with all our stakeholders. Our Policies and Standards define a set of minimum requirements and practices that ensure the same level of professionalism, ethics and integrity is applied consistently with all stakeholders.

We have zero-tolerance for any bribery and corruption. All stakeholders are mandated to avoid any activity that might constitute, lead to, or be perceived as, bribery and/or corruption activities and/or breach of any laws and regulations. The prevention, detection and reporting of any forms of bribery and corruption are the responsibility of all stakeholders across the Group.

APPROACH

Our Board Risk and Compliance Committee oversees the Group's risk and compliance related matters to safeguard our shareholders' interests and Group's assets. Following changes in the governance structure in early 2020, the compliance culture in Axiata was further strengthened by implementing guidance in the form of policies, standards, and procedures with reinforcement of these concepts through training and awareness programmes.

We ensure good governance is upheld through our risk and compliance governance structure, ensuring compliance to all aspects of the laws, regulations, and international standards applicable to our operations throughout the countries we operate.

Axiata's standardised Enterprise Risk Management (ERM) Framework governs our risk management and governance process. Although we appreciate that some autonomy is necessary within the local jurisdictions in each of our regions, our Group Risk Management department ensures consistency in the approach to managing risk across the Group. To this end, we have started to align the risk management practices among our OpCos, with full support from the Board Risk and Compliance Committee (BRCC) and the Group's Senior Management.

Board of Directors	Sets the tone and culture towards effective risk management, internal control in all aspects of the Company's activities and decides on Board's acceptable risk appetite whilst maintaining a proper balance between risks incurred and potential returns to shareholders.
Board Risk and Compliance Committee	Responsible and accountable for maintaining sound processes of risk management and internal control practices to safeguard shareholders' investments and the Group's assets. The BRCC also monitors Axiata's ERM framework and risks relating to cyber security, data privacy, as well as compliance, ethics and integrity.
Risk and Compliance Management Committee	The primary function of the Risk and Compliance Management Committee (RCMC) is to support the BRCC in fulfilling its responsibilities on risk management and compliance.
Group Chief Risk and Compliance Officer	Leads the Group Risk and Compliance Department.
Group Risk and Compliance Department	Executes and implements the strategies for risk and compliance at Group and across OpCos, including establishing and monitoring ERM Programmes, strengthening risk and compliance policies, implementing adequate procedures in line with Section 17A of the Malaysian Anti-Corruption Commission (Amendment) Act 2018, identifying key risks and mitigating actions, and inculcating culture of risk and compliance within the Group.
Risk and Compliance function (OpCos) and Business units (Axiata Corporate Centre)	Responsible for risk and compliance related matters in their respective OpCos and business units and coordinating with Group Risk and Compliance Department on implementation of risk and compliance related initiatives, policies and procedures.

OUTLOOK

With the introduction of Section 17A (S.17A) of the Malaysian Anti-Corruption Commission (Amendment) Act 2018 that came into effect in June 2020, the Group has established adequate procedures to ensure full compliance with this section. Further, in view of the current COVID-19 pandemic which has dominated the risk landscape since 2020, the Group continues to demonstrate agility, supply chain risk oversight with technology and network resilience.

Business Ethics And Compliance

Strengthening Risk Governance Structure and Risk Management

In 2020, the evolution of the Board Risk Management Committee (BRMC) into the BRCC, the establishment of the Group Risk and Compliance Department and the appointment of the Group Chief Risk and Compliance Officer (GCRCO), resulted in the strengthening of our risk governance for risk management and reinforced the implementation and review of risk programmes, policies, and procedures.

Value of strengthening the risk governance across organisation	▶ The BRCC was established to assist the Group in fulfilling its responsibilities on risk management and compliance, which includes ensuring that there are robust processes in place to identify, assess, and monitor key business risks to safeguard our shareholders' investment ▶ The BRCC is also established at all OpCos to ensure that risk and compliance management is prioritised
Strengthening and establishing a new Compliance Framework	▶ In view of S.17A, the existing Compliance Framework was reviewed and a new Compliance Framework was established. A Compliance Maturity Model that encompasses six critical components from the top, risk assessment, undertaking control measures, monitoring and detection, response and remediation, and training and communication was introduced across the Group ▶ Adoption of No Gift Policy across the Group and our clear stance of zero-tolerance towards any form of bribery and corruption was instituted as part of additional or strengthened policies and procedures ▶ Introduced mandatory ABAC clauses in contracts, revised governance instruments, strengthened our Supplier Code of Conduct and the Supplier Declaration process to minimise any third-party risks

To date, our corporate compliance has successfully attained a Level 3-Established Rating in 10 of the 24 components of the Compliance Maturity Framework. For 2021, we are targeting to attain Level 3-Established Rating for all 24 components.

Anti-Bribery and Anti-Corruption

In line with our UI.EP values, we have adopted a Zero Tolerance Policy towards bribery and corruption and a No Gift Policy. This is reflected in our Group-wide Anti-Bribery and Anti-Corruption (ABAC) and Gifts, Donations and Sponsorships Policies respectively.

ABAC Policies

Axiata's ABAC Policy governs the Group's internal and external stakeholders' practices in conducting business for and on behalf of the Group. The Policy addresses:

- Gifts, entertainment and corporate hospitality
- Donations and sponsorships
- Corporate Social Responsibility (CSR)
- Facilitation Payments
- Conflicts of Interest
- Third-party and business partner dealings
- Interactions with public/government officials and politically exposed persons
- Political contributions and donations
- Mergers, acquisitions and investments
- Avoiding nepotism
- Anti-money laundering/ counter-terrorism financing
- Record keeping and documentation
- Our Speak Up channel
- Training and communication

Training & Awareness

As part of fostering a strong risk and compliance culture, the Group carried out several interactive initiatives and training and awareness sessions to engage and inform the staff throughout the year:

- Townhall sessions reinforcing our UI.EP values, whistleblowing and consequence management
- ABAC Introductory Training Module mandatory for all employees Group-wide
- Banners, posters and regular email messages to increase awareness among staff on ABAC Policies and our Zero Tolerance Policy

We have achieved over 90% Group-wide completion rate for the ABAC Mandatory training module.

Business Ethics And Compliance

Whistleblowing (Speak Up) Channel

We are committed to upholding the highest standards of lawful and ethical conduct, by demonstrating honesty, fairness and accountability in all our conduct and dealings. In this regard, our Whistleblowing Policy enables all our employees, vendors and stakeholders to speak up in an independent and unbiased manner through our Speak Up Channel without the fear of reprisal to alert the Group of any breaches, suspected misconduct or violation of any of our policies, procedures or applicable laws and regulations by the Group's employees. The Speak Up Channel is accessible by internal and external parties to raise their complaints or provide information in confidence.

Speak Up Channel

- A central, unified platform across the Group and OpCos to enhance **governance, transparency, integrity and management** of whistleblowing cases
- Available in all **local languages** of our operating markets
- **Anonymous** channel managed by an independent **third-party service provider**, under the administration of the **Group Chief Internal Auditor**

Tax Transparency

As a Group, we contribute to the nation-building efforts and socioeconomic development of the jurisdictions in which we operate. We achieve this both directly through our investments in local communities (refer to the Society section in the Social chapter of this Report) as well as indirectly through taxes paid whereby these funds can be utilised by the Government in their initiatives to help local communities.

We have tax teams in each of the countries where we operate to ensure taxes are paid in accordance with local laws and regulations. The team reports its annual tax contributions in our National Contribution Report and our Group Financial Statements. The Audit Committee of the Board deliberates and approves Axiata's financial reporting, including the review of tax matters that are material to the financial statements.

In 2020, Axiata paid USD1.3 billion direct and indirect taxes and fees to the governments of all countries where we operate.

SNCR For further disclosure on our country-by-country tax contributions, refer to our National Contribution Report 2020 on page 85

Data Privacy

As a digital company, we recognise that our customers, employees, and other stakeholders' data privacy is paramount, and we ensure it is handled with the highest level of respect, due care and diligence in line with our robust Group-wide data privacy practices.

APPROACH

In view of the heightened risks of data breach, we continue to strengthen and ensure due care and diligence when dealing with personal data. Data privacy is overseen by the Board Risk and Compliance Committee, supported by the Risk and Compliance Department. Each of our OpCos has also appointed a Data Privacy Officer (DPO) responsible for enhancing their respective data privacy capabilities.

OUTLOOK

With the completion of Phase One, we will continue to execute Phase Two of the Privacy Programme with focus on implementing automated privacy solutions to improve our business operations and maintain the strictest vigilance, enhance our monitoring activities, and strengthen oversight of vendors' data-handling activities.

The Cyber Security Programme focused on building a strong foundation and implementing common standards and processes in DT2020. The next three-year strategy from 2021 will focus on evolving our security programme - a value creation function by ensuring we are right-sized, collaborative, future-fit, cost-conscious and making data-driven decisions on enabling business agility.

GAFS More details can be found in the "Building Digital Trust Through Data Privacy and Cyber Security" section on page 37 of GAFS 2020

Impact of COVID-19 on Industry Digital Risk Management

The spike in cyber risks globally demanded enhanced identification and remediation of external threats and cyber security capabilities. Digital users are required to be more vigilant to phishing attacks, fraud, and scams surrounding pandemic information and assistance, requiring a mindset change towards stronger cyber resilience and privacy awareness.

Data Privacy Strengthened Through Our Privacy Commitment

Our Privacy Commitment is based on the principles of T.R.U.S.T, a commitment that emphasises the Group's standing as a trusted regional digital telecommunications and digital services provider. These principles articulate Axiata's Privacy Commitment to embed strong security and privacy governance in our technology, processes, and people.

TRANSPARENT

We are **TRANSPARENT** about what, why and how we collect and protect **YOUR PERSONAL DATA** so that **YOU** can make informed decisions.

RIGHTS

We respect **YOUR RIGHTS** as individuals, so **YOU** are in control of **YOUR PERSONAL DATA**.

USE

We **USE YOUR PERSONAL DATA** for specific and stated purposes, and keep it for only as long as required.

SECURITY

We have established robust **CYBER SECURITY PRACTICES** in line with leading industry standards to protect **YOUR PERSONAL DATA** that **YOU** have shared with us.

TRANSFER

With **YOUR CONSENT** or in accordance with **APPLICABLE LAWS** we may **TRANSFER YOUR PERSONAL DATA** and will take appropriate steps to ensure it is adequately protected.

Data Privacy

Data Privacy Strengthened Through Our Privacy Commitment (cont'd)

Our position reaffirms our utmost commitment to developing a more resilient data privacy ecosystem that protects and respects customers, employees, and other stakeholders' privacy. In 2020, Axiata published the Group Data Privacy Policy and Privacy Notices for customers on its website to raise their awareness of data privacy issues.

In 2020, we embarked on the Privacy Programme's implementation phase to enhance data protection capabilities across our operations. We continuously embed privacy across all the Group's business facets. We built on our capabilities to further improve our privacy posture by strengthening our governance policies and monitoring activities, ensuring efficient oversight and privacy risk management.

This phase of the programme also saw the successful roll out of a mandatory training and awareness programme Group-wide to all employees as well as vendors processing critical assets and personal data. As we maintained our standards and best practices, we achieved a 90% overall completion rate. We successfully upskilled our Privacy Community members through an annual certification training of the Certified Information Privacy Manager (CIPM) Certification.

To ensure regulatory compliance is upheld throughout the Group's business processes, we will continue to demonstrate the strictest vigilance and conduct due diligence exercises over our vendors' data-handling processes and activities.

Our employees, vendors, and business partners must comply with data privacy and cyber security compliance standards and adopt our Code of Conduct.

Employee Code of Conduct

Updated our Employee Code of Conduct details, Axiata's cyber security and data privacy requirements, and underlined the Group's commitment to these areas

Supplier Code of Conduct

To further enhance third-party data processing by our vendors, we reviewed our Supplier Code of Conduct to include the Group's expectations on vendor obligations in processing stakeholders' data and information

In our continuous path to inspire digital confidence and trust, we have plans that will further enhance our data governance. In markets with Data Protection Laws, the aim is to ensure that the relevant OpCos are in full compliance with prevalent laws and regulations. While in those OpCos where Data Protection Bills are being drafted into laws, the focus is on ensuring adequate compliance readiness is in place. We will further employ automated privacy solutions to support our business operations.

Strengthening Cyber Security Programmes and Technologies

While technology advancements continue to breed cyber risks, we have also leveraged advanced technology to elevate our cyber capabilities. Through advanced technology tools such as Machine Learning and Artificial Intelligence (AI), we have ensured that we remain relevant and agile in measuring our risks. We have also improved our cyber capabilities and agility by adopting Robotic Process Automation to enhance and expand operational tasks to cover vendor resources' shortfall during the pandemic. Furthermore, we have adopted more automation and data driven analytics in our activities to improve our response time, reduce cost, maintain consistency and repeatability of common activities.

As part of our efforts to detect cyber threats, we have also expanded our Group Security Operations Centre (GSOC) capabilities. GSOC has been effective in providing consistent monitoring and timely updates on internal and external threats. Additionally, we have established internal teams of professional white hat hackers and conducted several crisis simulation exercises across the Group to test and improve our incident response.

Data Privacy

Strengthening Cyber Security Programmes and Technologies (cont'd)

Cyber security training and awareness for our employees

Working From Home	Cyber assessments were conducted across all OpCos during the work from home implementation to ensure our network adjustments for the new norm maintained the level of security for our networks and services. The assessment resulted in improvements to controls, better awareness among staff, and tightening of remote access systems. We also increased employee awareness on securing home WiFi access, cautioned the use of public WiFi, and provided guidelines for conducting virtual meetings securely.
Phishing, Malware and Ransomware	Conducted phishing, malware and ransomware related awareness to appraise employees on trends of attackers during the pandemic, including malicious links on topics dealing with COVID-19 recovery, statistics, and medical news. Furthermore, we conducted phishing simulation exercises to test the effectiveness of these programmes, the results showed an overall improvement in employee awareness.

Training and awareness initiatives have improved in 2020 with the adoption of a Group-wide training platform with curated material for cyber security based on internal policies and standards with current best practices to build an informed workforce. The coverage and completion of training modules across the Group stood at greater than 90% for the year.

Cyber security awareness for our digital telcos customers

General Security Awareness for customer/ subscribers	We published awareness information on our digital telcos websites to help raise and build awareness with our customer on cyber threats (phishing, financial and commercial scams, fake online shopping scams, and social engineering scams on their mobile services).

In measuring our progress and effectiveness of programmes and initiatives, we apply these standards:

National Institute of Standards and Technology (NIST) Cyber Security Framework

- Internationally recognised cyber security maturity framework
- Identifies key cyber security functions and improves our ability to detect and respond to incidents. Axiata's 2020 aggregated NIST maturity index at 3.5 on a 5-point scale now exceeds the world average of 3.2

Minimum Baseline Security Standard (MBSS)

- Enforced Group-wide on all our IT and telecoms systems, our assets are hardened by default to a level that reduces the risk of attack and failure
- Improved to MBSS Version 2.0, inclusive of 91 standards and introduced automation to achieve scale and consistency

Axiata's cyber security strategy will leverage on, and evolve from, our existing DT2020, to Digital Trust and Resilience 2023 (DT&R2023) to provide a competitive differentiator that continues to build customer trust. DT&R2023 will be a coherent, defensible cyber security programme based on a clear vision and strategic goals.

DT&R2023

Our Vision: To inspire trust and confidence in Axiata as The Next Generation Digital Champion

Our Mandate: To secure information assets against cyber threats across the Group, in line with Axiata 5.0 Strategy

2021
Converge common capabilities and introduce a risk-based approach

2022
Enhance the capabilities by focusing on automation

2023
Scale those capabilities to monetise

The next three years will be focused on helping our businesses to address the impacts of the global pandemic and proactively transition to the next new normal by continuously discovering, assessing, and adapting to ever-changing risks and trust levels.

Regulatory And Political Risk

Operationally, we have long recognised the importance of regulatory and political risks in our business due to conditions in the markets where we are present, which have historically shown a propensity for uncertainties in their regulatory and political landscapes. In light of this, we took appropriate steps to improve our response to these risks. This has also been in response to feedback from our internal and external stakeholders who raised the need to strengthen our mitigation and enhance disclosure of our risks.

Regulatory Risk

The industry we operate in remains highly regulated by a broad range of telecom regulations. In some markets, these regulations may also be uncertain or subject to change as the markets mature. Major regulations that we are required to comply with include core operating licenses, spectrum usage, subscriber registration and tariff approvals. Additionally, we are subject to telco-related taxes and levies imposed across the Group by relevant telco regulatory bodies, which include service taxes, excise duties and Value Added Tax (VAT).

These regulations create uncertainties on our operations and may impair business returns and long-term growth prospects, in addition to limiting our flexibility to respond to market conditions, competition and new technologies.

To mitigate this risk, the Group Regulatory team has established a regulatory compliance framework to provide a more structured approach in monitoring regulatory compliance at Group level and across its subsidiaries. In addition to this, dedicated subject matter experts were appointed at Group level and across all OpCos to monitor regulatory compliance.

Externally, we collaborate with other telco industry players to represent one voice in advocating strict compliance, fair and transparent policies in addition to knowledge sharing of best practices. We also conduct close engagement and active participation in regulatory and government officials' dialogues to anticipate emerging regulations, address and highlight concerns/obstacles/challenges that telco players may face. Additionally, we engage with regulatory officials in implementing sustainable regulatory regimes that will lead to the development of healthy regimes for the telecoms sector and participate in government consultations and industry association events to foster collaboration and knowledge sharing for best industry policies and practices.

Supported by these measures, we were able to improve our regulatory compliance monitoring and insights during the year. This enabled greater agility in adopting and adapting to adverse changes in the regulatory landscape.

Political Risk

The markets we operate in are prone to political instabilities, civil unrest and other social tensions which may cause business disruption, exposure to adverse changes in the regulatory landscape, and uncertainty of policy making. These may undermine market sentiment and investor confidence.

Our mitigation of these risks focuses on collaborating with all our OpCos to track the development of risks, including geopolitical tensions which may arise, leveraging on their local expertise, local familiarity, and connections to assess changing scenarios continually. In ensuring business resilience amidst any instability, all OpCos are equipped with a comprehensive Business Continuity Plan (BCP) to be activated when a crisis is triggered.

To manage and maintain good relationships with the broader stakeholders, we adopt a neutral stance towards politics and foster healthy relations with the governments of the day. To further demonstrate our long-term commitment to the markets, we also contribute to the country's wellbeing through various CSR programmes that contribute to socioeconomic development.

For 2020, our efforts in political risk mitigation have resulted in better monitoring processes of key political and geopolitical events as well as improvements in anticipating emerging risks.