

Our Value Creation Outcome 5: Embedding Responsible Business Practices

Mapping
against
SDGs



OUR INTEGRITY & GOVERNANCE

Upheld ethical business practices through robust integrity governance

Maxis has a zero-tolerance policy against bribery and corruption and is committed to the highest ethical standards and compliance with anti-corruption local laws, regulations and policies. Our Integrity and Governance Unit (IGU) implements, monitors, strengthens, and evaluates anti-corruption controls in Maxis through the Maxis Integrity & Compliance framework (MICF) and Anti-Money Laundering/Countering Financial Terrorism (AML/CFT) framework.

Maxis developed the MICF by adhering to T.R.U.S.T Principles to promote integrity and compliance within the Group while protecting against corporate liability. The MICF includes the MABC System, an anti-bribery management system complying with ISO37001:2016 Anti-Bribery Management (ABMS) requirements, and subject to periodic reviews.

MAXIS ANTI-BRIBERY MANAGEMENT (MABC) SYSTEM

Maxis effectively implements the MABC System across the organisation, governing the ethical conduct of its directors, employees and representatives. This system strictly prohibits bribery, money laundering, sponsorships, donations, and facilitation payments in all business transactions.

Number of employees who were disciplined or dismissed due to non-compliance with MABC Policies*

2020	2021	2022
0	18	2

* All non-compliances with and violations of the MABC System will lead to consequential management.

CORRUPTION RISK MANAGEMENT (CRM)

Maxis uses a CRM approach to address Group-wide bribery risks, which includes assessing related risks, policies and procedures, and implementing anti-bribery controls. The CRM process also identifies structural weaknesses that may lead to corruption, and staff participation is encouraged in identifying risk factors and mitigations.

Percentage of operations assessed for corruption-related risks

	2020	2021	2022
Total number of operations (divisions)	11	11	11
Total number of operations assessed for corruption-related risks (divisions)	11	11	11
Percentage of operations assessed for corruption-related risks (%)	100%	100%	100%

STRONG CULTURE OF INTEGRITY

To reinforce a strong ethical culture, we ensure that all employees participate in mandatory training programmes on Maxis' Code of Business Practice (CoBP) and Anti-Bribery and Corruption policies.

Number of employees who received training on Maxis' CoBP via Maxis Academy*

Year	2020	2021	2022
Total	5,219	5,379	5,473

Our Value Creation Outcome 5: Embedding Responsible Business Practices

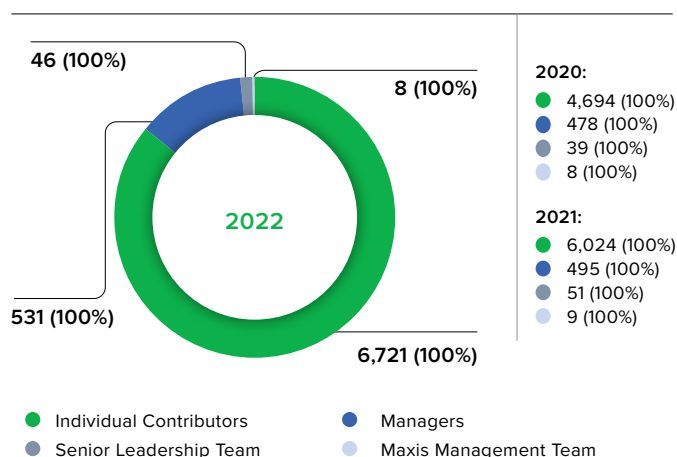
Number of employees who received training related to Anti-Corruption and Bribery

Year	2020	2021	2022
Total	5,219	6,579	7,306

Note:

* Employee training included all current Maxis employees and Third Party Contract Staff, at the point of rollout

Percentage of employees who received training on Anti-Corruption and Bribery by Employee Category



RECOGNITION OF MAXIS' COMMITMENT TO INTEGRITY AND GOVERNANCE

Maxis was awarded multiple ISO 37001:2016 ABMS certifications by SIRIM QAS International and IQNET (International Certification Network) in November 2022. This achievement is a testament to Maxis' steadfast commitment to conducting business with the highest levels of integrity and governance, in line with our Sustainability Strategy.

MAXIS INTEGRITY CORPORATE ADVOCACY PROGRAMME (MICAP)

In December 2022, Maxis celebrated International Anti-Corruption Day as part of its MICAP initiative, hosting a webinar on the theme 'Building A World United Against Corruption'. This webinar was held in collaboration with the Association of Certified Integrity Officer Malaysia (ACEIO), MACC and Inland Revenue Board of Malaysia (IRBM). The webinar, attended by approximately 500 participants including Maxis employees, Compliance Champions, and Integrity Officers, featured panel discussions on 'Corporate Liability: Keys to Corruption-free Business in Malaysia' and 'Corruption Prevention Activities Through Tax Incentives: Benefits for Commercial Organisations'. We also shared Maxis' Integrity Journey with all participants, advocating our stance against bribery and corruption and our compliance with ISO 37001:2016 ABMS.

OUR SUPPLY CHAIN

Improved supply chain management with responsible procurement

RESPONSIBLE PROCUREMENT PRACTICES

Maxis strives to protect our brand's reputation with responsible procurement practices through robust risk management to identify gaps. As such, Maxis is governed by robust policies and procedures that provide guidelines in the process of sourcing, vendor selection, assessment and performance-monitoring of our suppliers.

As part of our commitment to ethical procurement practices, we assess and select suppliers based on their compliance with our technical and commercial requirements that align with Maxis' standards. This approach promotes healthy supplier competition, as procurement is based on suppliers' capability and experience, creating growth opportunities for new businesses.

Our potential suppliers are required to go through our vendor onboarding process, due diligence evaluation and submission of business and financial documentation for assessment and the signing of our MCOBP.

OPTIMISING SUPPLIER MANAGEMENT

We strive to ensure our suppliers meet and exceed our expectations in terms of quality, delivery and cost. We

do this by assessing our suppliers' performance, setting expectations for quality and delivery and maintaining good relationships with our suppliers.

In addition, our MCOBP contains guidelines that enable third parties to conform to the business conduct that is adopted by Maxis in all our business transactions with third parties. This means that third parties who conduct business with the Group must read, understand and pledge to comply with the MCOBP upon commencing work with the Group. We also have an annual Vendor Integrity Programme conducted by Maxis' IGU which increases awareness of our zero-tolerance for bribery and corruption among external parties.

Third Party Training on Anti-Bribery and Corruption

Year	2021	2022
Vendor Integrity Programme	8 sessions	14 sessions

Our Vendor Management team also carries out regular assessments on key suppliers to assess vendor performance, identify improvements and ensure corrective actions are implemented. Apart from that, existing suppliers are required to acknowledge the MCOBP on an annual basis.

Our Value Creation Outcome 5: Embedding Responsible Business Practices

We make every effort to provide timely delivery and sufficient supplies through constant communication with our suppliers, advance planning on business needs and, exploring and securing alternative supplies when necessary. We have improved our processes and technology tools in our Source to Contract framework, which allows online supplier interaction throughout onboarding, tendering and contracting, to ensure transparency and facilitate proper audit trials.

OUTLOOK

In our efforts to improve supply chain management, Maxis will continue to leverage technology and automation to provide the procurement team with better insights and understanding regarding spend patterns and trends. We are also committed to creating an efficient Supplier Relationship Management Framework to standardise our vendors' roles and responsibilities, ensuring successful partnerships and consistent delivery of quality products and services. Maxis will continue to strive for efficiency while maintaining strict controls and oversight. Furthermore, we will continually optimise our expenditure on low-spend, low-volume suppliers.

In the medium term, we aim to empower employees and drive greater productivity through AI and predictive technology. We will also move towards strategic partnerships with suppliers to establish closer relationships and enable further discussions on performance, issues and value-adding activities.

Our Priorities

Our priorities within the next one to two years:

- Automation and digitalisation, such as chatbots and spend analytics. Process simplification through technology enablement and data to provide greater knowledge and insights.
- Establishing a framework for Supplier Relationship Management that is efficient, with defined roles and responsibilities, including risk management. To enhance contractual benefits and minimise opportunity loss, strategic contracts and suppliers are monitored in a standardised manner.
- Ongoing process improvements with zero tolerance for misconduct. We will maintain controls and have good governance in place while balancing the requirements for more efficient procedures to meet current business needs.
- Conduct a review of long-tail spend to identify cost optimisation opportunities, increase resource productivity, improve compliance and reduce risks.

Our medium-term plans over the next two to five years:

- AI and predictive technology enablement (extreme automation) through which administrative tasks will be reduced, allowing workers to focus on more strategic initiatives.
- Moving towards strategic category and supplier management, with channels established to address performance, challenges and value-added activities such as innovation and sustainability.

OUR CYBERSECURITY

Strengthened cybersecurity to support digital transformation, ensuring cyber resiliency and responsible digital citizenship

As technology continues to advance and businesses become more digital, the risk of cybersecurity threats becomes increasingly prevalent. With customer data at stake, protecting our network and ensuring the security of customer information is a key priority. We continue to focus on a holistic approach in addressing these risks through our three strategic cybersecurity pillars: Protecting the Brand and Ensuring Compliance; Embedding Security in DNA; and Strengthening Cyber Resilience and Supporting Digitalisation. By taking a comprehensive approach to cybersecurity, we are able to Always Be Ahead™ of threats and do our best to ensure our network, applications and customers' data remain secure.

2022 AND OUR COMMITMENT TO CONTINUOUS IMPROVEMENT



As part of our holistic approach, Maxis has attained several significant milestones to demonstrate our commitment to cybersecurity. Maxis is the first telecommunications provider in Malaysia to achieve ISO 27001 certification for our cloud infrastructure, audited by SIRIM. This accomplishment signifies that we have established a robust information security management system (ISMS) to safeguard our

Our Value Creation Outcome 5: Embedding Responsible Business Practices

cloud infrastructure and services. Notably, our ISO 27001 certification extends beyond our cloud infrastructure and also covers our Voice and Data Networks, Enterprise Managed Services and Data Centres giving Maxis customers the confidence that the Maxis Network is secure and that their data is being managed and stored securely in compliance with global standards.

PROTECTING OUR BRAND AND ENSURING COMPLIANCE

We recognise the importance of protecting our brand and reputation from cyber threats and have implemented various measures to achieve this goal. We invest in the latest technologies and processes to protect against cybersecurity attacks in areas such as data protection, cloud infrastructure, IoT, telecommunication and network security infrastructure. We are also implementing a partner or vendor risk management programme to assess the cybersecurity posture of selected vendors and suppliers. This helps us identify potential cyber risks in our supply chain and take proactive measures to mitigate them.

Maxis has also adopted a zero-trust security strategy that will be rolled out in phases that assumes all users and devices are untrusted and need to be verified before being granted access to resources. This approach minimises the risk of unauthorised access to sensitive data and applications. Additionally, our cybersecurity team takes an active role in participating in cybersecurity forums organised by regulators such as MTSFB and government agencies such as NACSA and MCMC to provide input on privacy and cybersecurity laws and regulations.

EMBEDDING SECURITY IN OUR DNA

Maxis recognises that cybersecurity is a shared responsibility and that our employees and partners play a critical role in protecting the Group's assets and reputation. To this end, Maxis provides cybersecurity training to employees and partners, and collaborates with vendors and/or academic institutions to develop cybersecurity training programmes. This approach not only helps to build a security-focused culture, but also helps to address the shortage of cybersecurity talent in the industry.

Maxis also partners with leading cloud service providers, such as Amazon Web Services (AWS), Google Cloud Platform (GCP) and Microsoft, to strengthen our technology stack and ensure that our cloud infrastructure is secure and compliant. These partnerships enable Maxis to leverage the expertise and resources of these cloud providers to build resilient and scalable cloud services that meet the needs of its customers.

STRENGTHENING CYBER RESILIENCE AND SUPPORTING DIGITALISATION

We take a comprehensive approach in addressing cybersecurity risks as part of our digitalisation programmes. This includes embedding security in the design and

implementation of all our products and services, including our network and our systems, as well as our people, for the benefit of our customers. We incorporate security assessments and testing at each stage of our development and also experiment with new technologies such as AI and ML to proactively identify and respond to potential security threats. Additionally, our partnerships with leading technology providers, such as CrowdStrike, Mandiant, Saviynt, Palo Alto, Splunk, Darktrace, Veracode, Tenable, Imperva, ServiceNow, AWS, Google Cloud and Microsoft, ensure that our digitalisation programmes are built on secure and trusted platforms. Through these efforts, we strive to enable digital transformation while maintaining the highest levels of security and resilience.

To ensure cyber resilience, secure our network and protect our customers' data, Maxis works with teams of internal and external partners. These teams are responsible for continuously testing, assessing vulnerabilities and proactively hunting for potential threats. Maxis has implemented various security measures such as breach and attack simulation tools, DevSecOps application security assessment tools and/or SOC automation tools. Additionally, we conduct regular audits, vulnerability assessments and penetration testing to identify weaknesses in our systems and mobile network and telecommunications infrastructure. Through these proactive measures, Maxis remains committed to mitigating cyber threats and maintaining our position as Malaysia's leading converged solutions provider.

OUTLOOK

Our long-term goal is to establish a fully automated, cyber resilient organisation that can withstand cyber incidents with minimal impact to business operations. We ensure the security and trustworthiness of our network, digital touchpoints, systems, infrastructure and data stores through a zero-trust architecture and a security-by-design approach. Our products, services and offerings all integrate cybersecurity measures, and we promote a shared responsibility model among our employees and partners. Compliance is also continually assessed, tracked and reported where we work closely with our regulators and the Government to ensure that our customers and Malaysia's critical infrastructure remain safe and secure.

To achieve this goal, we prioritise investments in key technologies for network security, data protection, cloud security, application security, IoT security and 5G security. We also have a strong risk management programme that regularly assesses organisational and partner cybersecurity risks. We empower our employees with digital literacy skills, including cybersecurity, to ensure appropriate implementation of cybersecurity controls across the organisation.