

PEACE

EMBODYING GOOD GOVERNANCE

At the core of everything we do, and the way that we do it, lies our commitment to the highest standards of governance excellence. It is not enough for us to deliver world class assets; we must do so while upholding standards of integrity and ensuring risks are managed at acceptable levels.

OUR ALIGNMENT TO THE UNSDGs



MATERIAL SUSTAINABILITY MATTERS

- Corporate Governance
- Business Ethics
- Cyber Security and Data Privacy

MAPPED TO OUR CAPITALS



RELATED PRINCIPAL RISKS

- Market
- Finance
- Asset Management
- Security

In this section

Corporate Governance

- Corporate Governance and Compliance
- Risk and Crisis Management
- Board Diversity

Business Ethics

- Integrity and Corruption Management

Cyber Security and Data Privacy

OUR APPROACH

Sound corporate governance underpins our values, culture, processes, functions and organisational structure.

We have a strong culture of entrenched values, which form the cornerstone of our behaviour towards stakeholders and against which, we measure practices and activities to assess the characteristics of good governance. Directors and employees are required to conduct themselves with integrity, consistently and uncompromisingly displaying moral strength and behaviour that promote trust.

This commitment to good corporate governance is reflected in the CoBE, our foundation in fulfilling our business obligations with utmost integrity and transparency. Our culture of openness, transparency and accountability are strengthened with the adoption of the No Gift Policy and Whistle Blowing Policy and our adherence to the Anti-Bribery and Corruption Policy and Guidelines (ABC manual).

In managing the risk, the Group has a robust KLCC Resiliency Model which provides an integrated view on our overall strategy in managing risks.

FOCUS FOR THE YEAR

Surveillance Audit by SIRIM to evaluate compliance of the Group's **Anti-Bribery Management System** to the requirements of ISO 37001:2016

Review of the **Risk Appetite** to provide comprehensiveness to the current risk appetite statement in ensuring the risk exposure and type of risk to be pursued or retained by KLCCP Stapled Group in achieving its strategic objectives are properly defined



CORPORATE GOVERNANCE

Corporate Governance and Compliance

At the highest governance level, the Boards have the ultimate responsibility to monitor that the Group is operating as a responsible organisation. This includes considerations around climate-related risks and opportunities when reviewing the group's strategy. Principal and emerging risks are identified through robust assessments by the Boards and the various sub-committees. The Boards recognise that a balanced board is vital for sustainable value creation and that competency skills are adequately represented within the Board Committees. The Boards composition is both qualitatively and quantitatively balanced in terms of skills, gender, experience, tenure and independence. The Boards regularly review its own effectiveness and therefore undertakes a formal evaluation of its performance and that of its committees and individual directors once in three years.

The Boards of KLCCP and KLCCRM reconstituted their respective board composition with **63%** independent directors

INITIATIVES FOR THE YEAR

Representation of women directors on the Boards achieved **50%**

Undertook the **ISO 37001 SURVEILLANCE** Audit exercise to evaluate continued compliance of the Group's Anti-Bribery management system to the requirements of the standards

PEACE

PEACE

Stakeholder Engagement

Our Board is committed to continuous improvement in our corporate governance principles, policies and practices, and does so by remaining abreast of evolving regulations and best practices. This is further enhanced through engagement with regulators and industry bodies, and through seeking regular feedback from other stakeholders.

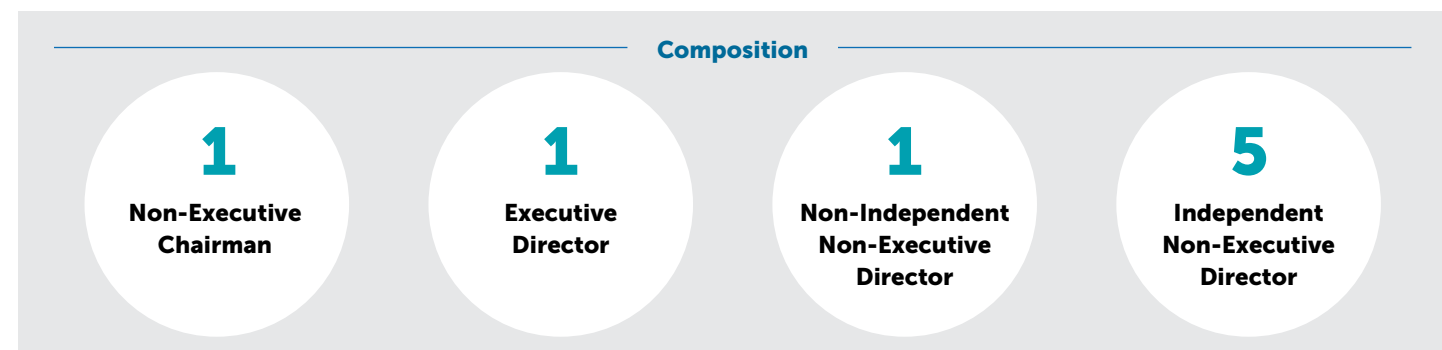
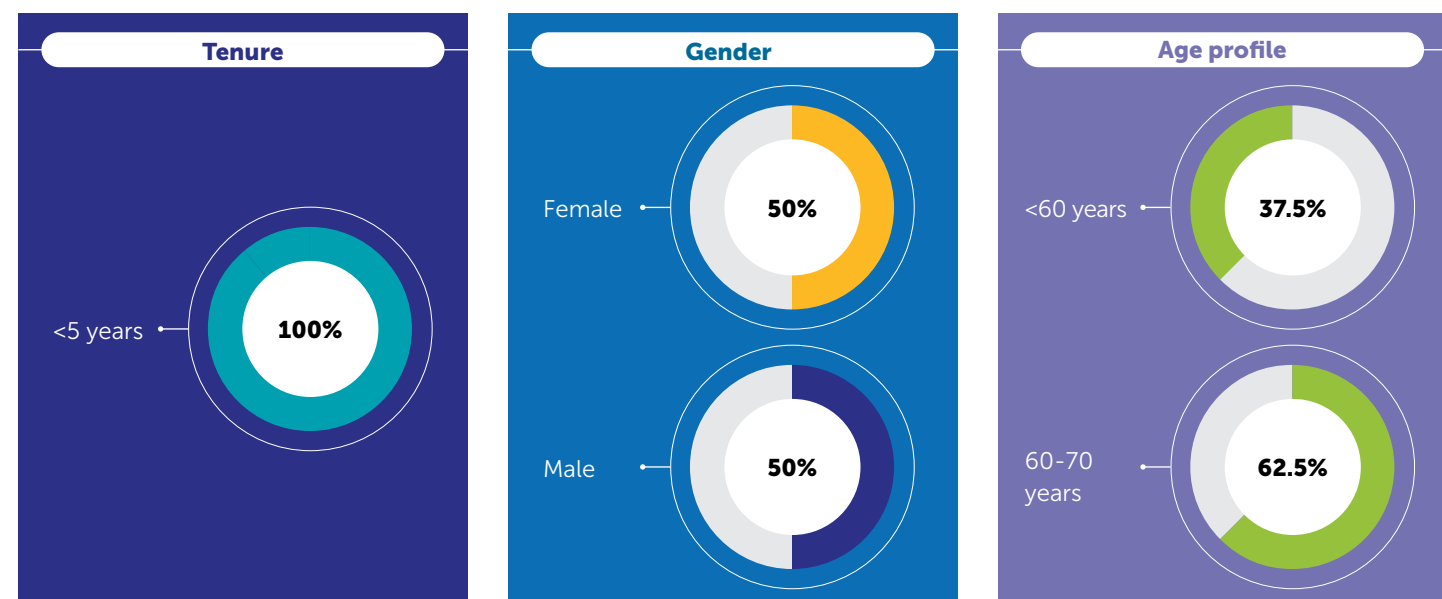
We establish and maintain proactive dialogue with all our stakeholders and recognise that stakeholder needs are dynamic and that we need to be responsive to the evolving stakeholder

landscape. We manage our stakeholders' needs and expectations by taking into consideration their viewpoints towards more tangible business value creation.

Our Stakeholder Management framework, as set out on page 16 to 17 of this report demonstrate how we engage and create values for our diverse group of stakeholders. Communication with stakeholders is imperative in understanding and managing their expectations and provide new perspectives in generating positive impact to the organisation.



Board Diversity



RISK AND CRISIS MANAGEMENT

Risk management is an integral part of KLCCP Stapled Group's business at both strategic and operational levels. An effective and sound risk management system is important for the Group to achieve its business strategies and objectives. The Group leverages on the KLCC Group Enterprise Risk Management Framework (the ERM Framework) which sets out the risk policy, risk governance and structure, risk measurement, risk operations and system. The ERM Framework is central to ensure the Group's strategic and operational activities are within strategic mandates, risk appetites and corporate objectives.

KLCCP Stapled Group is committed to provide overall reasonable level of confidence that risks and their associated controls are adequately, effectively, and safely managed through assurance programs.

To support the above, there is an established Risk Management Oversight Structure encompassing the Boards, Board Risk Committee (BRC), and the Risk Management Committee (RMC). This structure assigns responsibility for risk management whilst facilitating the assessment and communications of risk matters from the operational levels to the Boards. The KLCCP and KLCCRM Boards developed the KLCC Resiliency Model that essentially covers the following three key areas to provide an integrated view on the overall strategy.

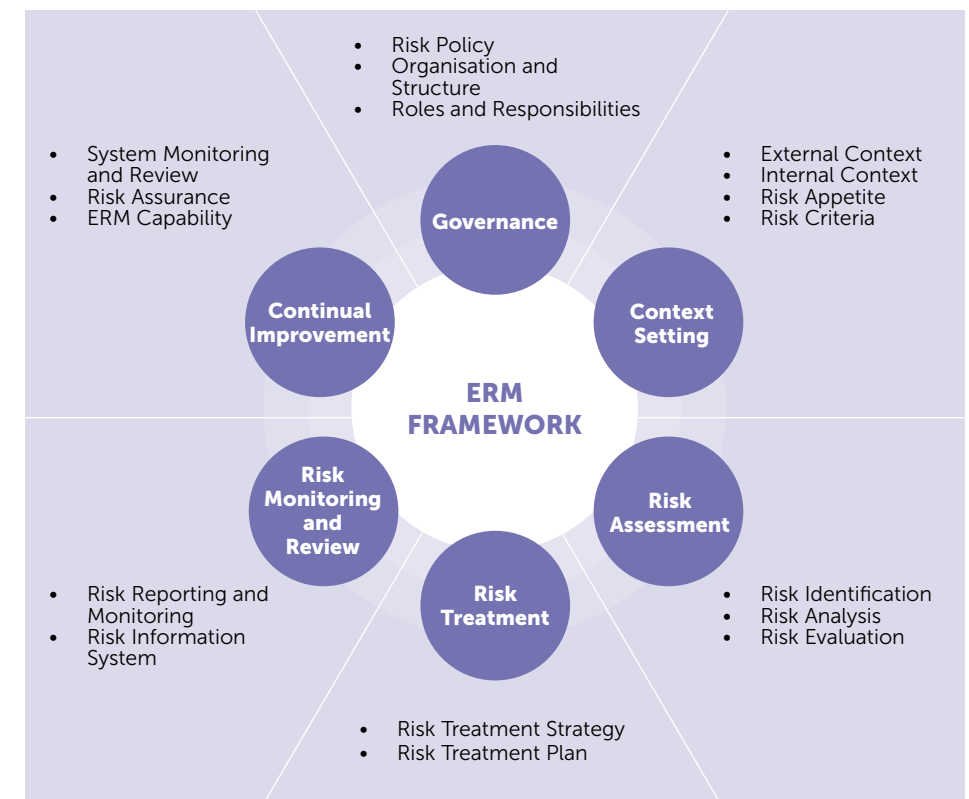


Enterprise Risk Management

The application of the ERM Framework is a structured and holistic approach to identify, assess, treat, and monitor risk aimed to reduce the likelihood and impact of all identified risks to enhance ability to achieve strategic objectives.

The ERM Framework is aligned to the ISO 31000 and is designed to manage risks in an integrated, systematic, and consistent manner. The ERM Framework sets out the six key elements comprising Governance, Context Setting, Risk Assessment, Risk Treatment, Risk Monitoring and Review and Continual Improvement.

Elements of the ERM Framework



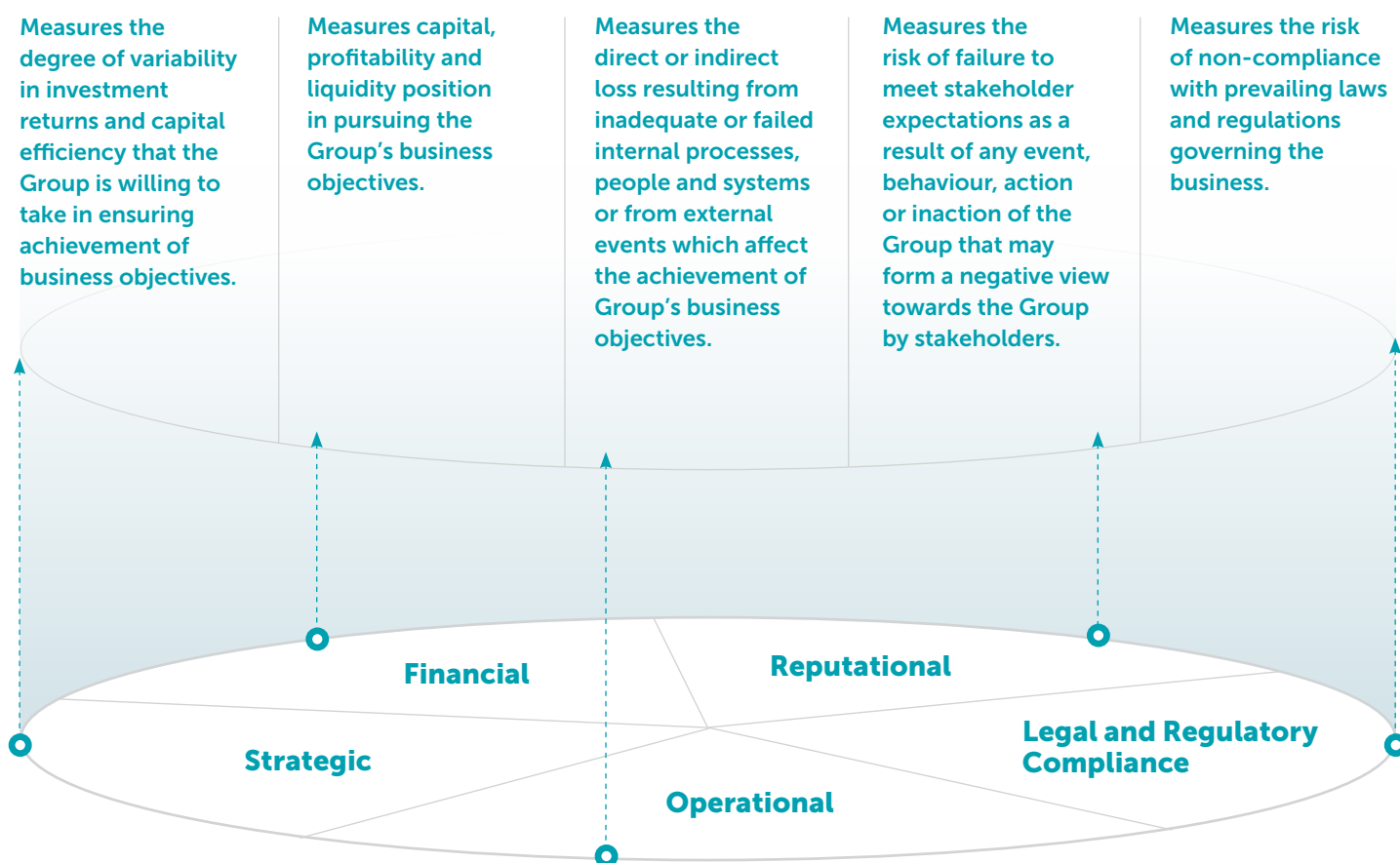
The risk profiling exercise is carried out to provide a balanced view for informed decision making through richer risk conversations and considerations of risk reward trade-offs.



KLCCP Stapled Group utilises the INTERISK system as a risk tool to effectively manage and monitor risk profiles. It embeds the industry standard risk management process of ISO 31000. The INTERISK system drives active risk conversation/analysis monitoring through a dashboard, reinforces effective risk governance and assurance practices and provides a seamless flow of information and processes along the risk management value chain.

Annual Review of Risk Appetite

- Governance, Risk and Assurance Department reviewed the risk appetite to provide comprehensiveness to the current risk appetite statement in ensuring the financial and non-financial risk exposure and type of risk to be pursued or retained by KLCCP Stapled Group in achieving its strategic objectives are properly defined. The annual review is crucial to reflect the threshold during this transitional period to the endemic phase.
- The updated risk appetite statement, risk tolerances and risk threshold were presented to the Risk Management Committee, Board Risk Committee and the KLCCP and KLCCRM Boards.
- The risk appetite covers five main areas:



Annual Review of Risk Profile

- Governance, Risk and Assurance Department facilitates and coordinates the risk profiling exercise to review, assess and update the principal risks to safeguard KLCCP Stapled Group's investment and key business activities. This is to ensure the risk exposures are relevant and up to date taking into account emerging risks and transitional period to the endemic phase.
- The updated risk profiles were presented to the RMC, BRC and the KLCCP and KLCCRM Boards.

Crisis Management

KLCCP Stapled Group has in place a comprehensive set of processes towards preparing the organisation to respond and manage a crisis event in order to protect and save people, environment, assets, and reputation.

The Crisis Management Plan (CMP) encompasses:

- ▶ Objective and scope of emergency/crisis management plan
- ▶ Emergency/crisis team structure with roles and responsibilities
- ▶ Activation thresholds and protocols
- ▶ Communication process with updated contact numbers and integration with relevant parties - government authorities and relevant stakeholders
- ▶ Strategies and actions for responding to pre, during and post emergency/crisis
- ▶ Work flow and process for escalating relevant emergency/crisis information to potential impacted parties within KLCCP Stapled Group and resource requirement during emergency/crisis

The CMP addressed the credible scenario in HSE and areas beyond HSE which are Finance, Human Capital, Digital, Facility Management, Legal and Regulatory in managing crisis.

The testing and exercising for CMP is conducted annually to ensure the readiness and effectiveness of the communication process and the recovery action plan in responding to the crisis. From this exercise, risk owners are aware of their roles and response preparedness in the event of emergency/crisis.

Testing and Exercising for Crisis Management Plan

During the year under review, KLCCP Stapled Group conducted the following activities to ensure readiness in responding to crisis:

- Tabletop incident command structure exercise at Menara 3 PETRONAS for tenants, floor safety managers and emergency management team.
- Emergency evacuation and fire drill exercise with floor safety managers and tenants at Kompleks Dayabumi and Menara Exxonmobil.
- Communication of Initial Action Plan on natural disaster namely flood to Hotel operator's HSE team.
- Basic First Aid, Cardiopulmonary Resuscitation (CPR) and Automated External Defibrillator awareness with floor safety managers and tenants at PETRONAS Twin Towers.
- Testing and exercising for all identified credible scenarios other than HSE, via walk through sessions with all risk owners in KLCCP Stapled Group.

Based on the above exercises, employees and tenants were trained for their respective roles and responsibilities in the event of crisis.



Crisis Management

KLCC Stapled Group has established a Business Continuity Plan (BCP) as part of its Business Continuity Management to manage any interruptions arising from any incidents affecting ICT, business supply chain, assets and people. The BCP is designed to provide guidance in resuming key business functions in the event the CMP is unable to contain a crisis event that may have a major or catastrophic impact on the business in terms of financial, operation and reputation.

The BCP is reviewed annually to meet changing needs by conducting Business Impact Analysis (BIA) for all divisions, departments and OPIs in accordance with BCM framework. Results are presented to the Risk Management Committee and the Approving Authority. The BIA ensures that critical business functions are identified, the impact of unavailability of the functions over time are ascertained, as well as prioritisation of timelines for resumption of activities and specifying Minimum Resources Requirements. People, equipment, assets, facilities, technology, vital record, interdependencies are to be allocated to recover and resume these functions following prolonged business disruptions.

The testing and exercising for Call Tree Verification exercise to validate that phone numbers and contact lists of relevant personnel and stakeholders are accurate and up to date, was conducted twice this year to ensure the effectiveness of communication to Critical Business Function (CBF) staff upon activation of BCP. This is to ensure that the CBF staff are contactable to carry out their designated roles accordingly. Based on the call tree verification exercises, CBF staff were trained to respond promptly to the activation of BCP.

BUSINESS ETHICS

Anti-Bribery Management System (ABMS) KLCC (Holdings) Sdn Bhd KLCC Property Holdings Berhad

Integrity and Corruption Management

KLCCP Stapled Group is mindful of the threats of corruption and bribery to its operations. The risks vary across different landscapes including jurisdictions, business sectors, people and transactions.

The Group's continuous effort in managing integrity risks within the organisation reflects our commitment to conduct business with high integrity and in support of the Group's zero tolerance against all forms of bribery and corruption.

KLCCP's Policy Statement on Anti-bribery and Corruption has been reviewed and endorsed by the CEO. The policy states our commitment to comply with applicable laws and regulations, which include the CoBE, the Anti-Bribery and Corruption Manual. Consequence Management will be implemented on employees who failed to comply. The Group provides channels for employees and public to disclose improper conduct in the Group.

Anti-Bribery Management System

KLCC Property Holdings Bhd and its subsidiaries, are certified to ISO 37001:2016 Standard. The Group passed the surveillance audit conducted by SIRIM in November this year. The Surveillance Audit assures the adequacy and effectiveness of the Group's management systems.

The Group governs its ABMS through a structure which encompasses:

- i. Governing Body (the Boards) who has the ultimate responsibility and oversight of the ABMS
- ii. Top Management, comprising Chief Executive Officer and Head Divisions, who ensure that the ABMS is implemented adequately to address the Group's bribery & corruption risks, and
- iii. Compliance Function, who is dedicated to oversee the implementation of ABMS, review and report the ABMS performance to the Governing Body and Top Management

We implement our ABMS based on the MACC Act 694 T.R.U.S.T. Principles i.e. Top Level Commitment, Risk Assessment, Undertake Control Measures, Systematic Review, Monitoring & Enforcement, and Training & Communication.

TONE FROM THE TOP

"Integrity must always reside within ourselves. Having the right system does not make the organization invulnerable. It should come together with a strong commitment in upholding the highest standards of integrity, transparency and accountability in all our actions and communications. It is about delivering the 'Amanah' entrusted to us without fear or favor and without sacrificing our moral values"
- Yilgh, Datuk Md. Shah Mahmood, Group Chief Executive Officer

"Being honest and true. Leading by example is best."
- Mohainee Tahir, Group Strategy & Sustainability

"Integrity is about honesty, moral commitments and willingness to do what is right. It should be embedded in one's life and is demonstrated through conducts whether one is alone or in a crowd."
- Hassan Ramadi, Group Commercial

"Integrity is being honest, acting morally and having strong ethical principles."
- Rohizal Kadir, Strategic Finance

"Being honest, authentic and real in doing what is right and good regardless of the setting or situation."
- Ho Mei Ling, Group Governance, Risk & Assurance

"Integrity is the quality of being honest with having strong moral principles in doing the right thing without other people knowing"
- Mummat Hilme Hassan, Project Delivery

"Being truthful and congruent in thinking, action and being in upholding the company values."
- Saiba Ahmad Dahlan, Human Capital

"I must do things correctly because I will ultimately be accountable to Allah and He knows whatever I am doing openly and secretly"
- Ahmad Zahid Zainal Abidin, Legal and Company Secretariat

"Practicing integrity through honesty."
- Shabuddin Ahmad, Group Health, Safety & Environment

"Integrity is the foundation on which co-workers build relationships and trust, and it is one of the fundamental values that employers seek in the employees that they hire."
- Norhayani Mohd Khalid, Group Procurement

"Doing the right thing all the time."
- Norfaizi A Samad, Group Security

"Integrity is about putting both hands on the table, not one underneath and being true to yourself even when there is no one around. You will never know that spirit lurking behind the cabinet which can see you"
- Fadzul Harris Mohd Kamal, Group Digital

What INTEGRITY means to YOU?

T . R . U . S . T

Principle

T

Top Level Commitment

R

Risk Assessment

U

Undertake Control Measures

S

Systematic Review, Monitoring and Enforcement

T

Training and Communication

Actions taken in 2022

T

- Endorsed the Policy Statement on Anti-bribery and Corruption in September 2022
- Reinforced importance of integrity with Head of Divisions and operating units setting Tone from the Top during 'Leaders' Time Out' with respective constituents

R

- Conducted risk assessment on bribery and corruption
- Endorsed the Bribery and Corruption Risk Profiles for all entities
- Risk Mitigation Owners are responsible to implement the controls

U

- Continued implementing the No Gift Policy
- Continued implementing the Whistleblowing Policy
- Conducted the due diligence check during pre-employment for high-risk/sensitive positions
- Obtained Integrity Pledge by all employees
- Conducted due diligence on business associates
- Obtained asset Declaration by employees
- Continued implementing Limit of Authority

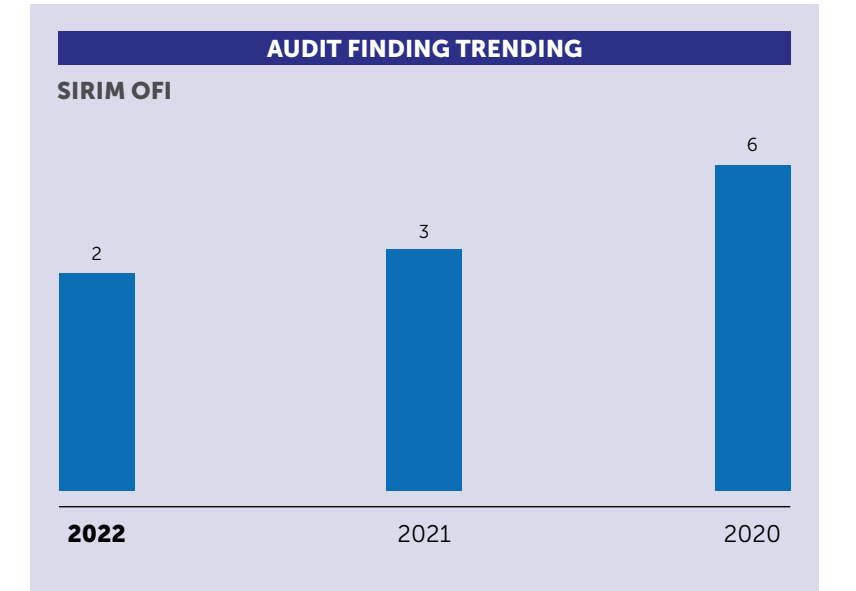
S

- Conducted Compliance Function Review
- Conducted internal audits in September
- Conducted Surveillance Audit by SIRIM in November
- Conducted Top Management Review in December
- Conducted Governing Body Review in November

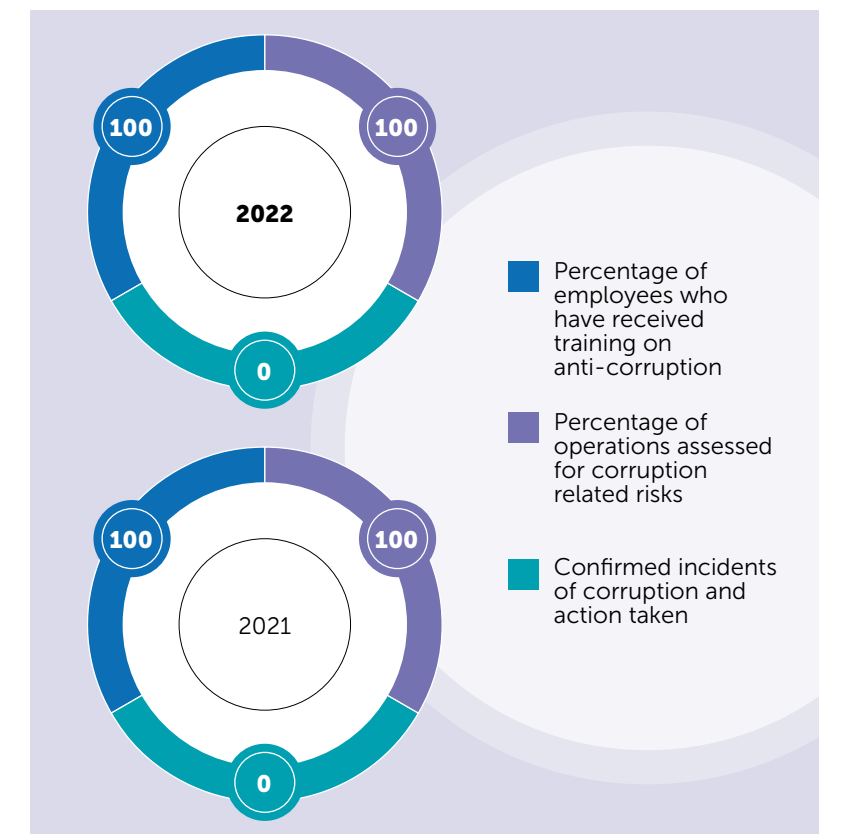
T

- Conducted engagement on Corporate Governance and Integrity for Governance Body
- Conducted integrity awareness induction for new employees
- Conducted internal audit training for ABMS internal auditors
- Conducted refreshers on ABMS for all employees
- Communicated ABMS and related policies to third parties and service providers
- Conducted competency training for Compliance Function
- Communicated monthly Integrity Message to all employees

ABMS performance has improved over the years, evidenced by the zero Non-Conformance Report (NCR) and the declining number of Opportunities for Improvement (OFI) from SIRIM audits.



Implementation of the ABMS action plan is monitored by the Governance, Risk and Assurance Department via a digital dashboard, the "TRUST-T". "TRUST-T" is a digital tool that track, monitor and automate reminders to the OPUs to implement their planned programs. TRUST-T dashboards create insights on the overall ABMS implementation status in the Group.



CYBER SECURITY AND DATA PRIVACY



Safeguarding the data within our stewardship throughout its lifecycle and ensuring ongoing compliance with data protection regulations globally remain a key priority for the Group. Our IT infrastructure is fully supported by Group Digital, PETRONAS. Through the cyber security alerts and other initiatives, we continue to educate and create awareness among employees on cyber threats.

As our employees are the first line of defence in keeping the organisation secure, it is important for them to understand the threats and be equipped with the necessary cyber security knowledge. We continue to create greater awareness and compliance on cyber security, via awareness training programmes. In dealing with external parties, we make transparent the Data Privacy Policy, requiring strict adherence such as incorporating Non-Disclosure Agreement (NDA) into Vendor Contract Agreements to prevent unauthorised usage

and leakage of confidential data. We have in place a series of system controls to provide further protection assurance, including robust validation of system access and obligations on external parties who may have the data access.

Our cyber security efforts are guided by the Enterprise Cyber Security Governance Framework (ECSGF) which aim to protect our systems and data from malicious attacks such as Ransomware and Phishing. The Enterprise Cyber Security Governance Framework, defines the guidelines, standards, policies and procedures required to ensure our risks are effectively managed and mitigated. In 2020, we developed the Cyber Security Action Plan in our effort to mitigate cyber security crime and to strengthen the existing system and procedures to address the root causes of cyber security issues resulting from poor enforcement, weak internal control, and acceptance culture.



CYBER SECURITY RISK MANAGEMENT INITIATIVES FOR THE YEAR

- Implemented PETRONAS Zscaler Internet Access (ZIA) to ensure secured browsing particularly by users on Work From Home (WFH) mode.
- Developed the Digital Project Management Framework (DPMF) that governs all IT and Operational Technology (OT) System processes for the Group's ICT Business As Usual (BAU) and Digital projects.
- Reviewed the KLCC Group Cyber Security Risk Profile to make it current and reflect latest cyber threats together with Group Risk Assurance team.
- Conducted Call Tree Testing to assess the effectiveness of communication amongst Division/Department Head, BCM Coordinator and CBF Staff in the event that a crisis occurred due to system disruption.
- Implemented Monthly Phishing Test and reported the Phishing Test Failure Rate to the Management.
- Conducted Cyber Security – Business Impact Analysis (CS-BIA) and Legal Regulatory Assessment (LRA) to assess the impact of system disruption in terms of Confidentiality, Integrity and Availability and Maximum Acceptable Outage (MAO). This is done during the Project Initiation stage of any ICT BAU and Digital Projects.
- Assessed on all critical Third Party vendors' applications to ensure Disaster Recovery (DR) and Backup Restore Procedure are incorporated into these applications.

CAPABILITY BUILDING FOR EMPLOYEES

- Organised the Global Cyber Security Month for the Group to raise cyber security awareness and adoption level to greater heights.
- Tracked and reported users' overall completion of cyber security training on SWITCH and MyLearningx PETRONAS e-Learning platforms.
- Conducted regular cyber security and Phishing Awareness Training for users (physically and virtually) targeted at users who failed the Phishing Test and not completed training materials on SWITCH and MyLearningx.

DATA SECURITY MANAGEMENT

- Enforced the Personal Data Protection Act (PDPA), General Data Protection Regulation (GDPR) and Payment Card Industry, and Data Security Standards (PCI DSS) to ensure compliance by vendors.
- 29 Enterprise Content Management System Representatives and Document Records Management Focals were upskilled on the best practices to support the principle of information Security and Risk Management;
 - Participants acquired the awareness on the importance of Enterprise Information Management in maintaining information Confidentiality, Integrity, and Availability.
 - Adherence to the Document Ownership Matrix and Information Classification Matrix will help the organisation prevent or reduce the likelihood of unauthorised access to data or record, and minimise the risk of critical data disclosure.