Risk Management

The Group's Risk and Security Division plays a pivotal role in governing and managing processes that identify, evaluate and prioritize key risks and cybersecurity threats that could impact the Group's operational resilience and strategic objectives. With its strong governance model and deeply embedded culture of risk and cybersecurity awareness, the division ensures a coordinated approach across its 3 departments: Enterprise Risk Management, Cybersecurity and Business Continuity and Environmental Security.

By proactively addressing both existing and emerging challenges, the division enables the Group to mitigate threats, enhance adaptability in a dynamic environment and protect its assets. Whether through strengthening cybersecurity defenses, ensuring business continuity during disruptions or integrating environmental security considerations, the division's work underpins the Group's ability to execute its corporate strategy and maintain Stakeholder confidence.

Through a holistic and collaborative approach, the Risk and Security Division ensures that risk management and cybersecurity considerations are embedded into decision-making. This not only fortifies operational resilience but also supports sustainable growth, positioning the Group to create long-term value for its Stakeholders while achieving its strategic vision.

Enterprise Risk Management

The Enterprise Risk Management (ERM) Department ensures the Group is prepared to navigate a complex environment by proactively identifying, evaluating and mitigating risks across the Group, including operational, technology, strategy, compliance, financial, business continuity, cybersecurity and business environment risks.

Core activities include:

- Developing and maintaining the ERM policy and framework, which outlines principles, responsibilities and methodologies for managing risks across the Group.
- Collaborating with Senior Management and the Board of Directors to establish risk appetite and tolerance levels that align with the Group's strategic objectives.
- Conducting qualitative and quantitative risk assessments to evaluate key risks, prioritize them and allocate resources effectively.
- Establishing measurable metrics to monitor emerging risks and enable timely responses.
- Collaborating with project managers to assess risks associated with projects and initiatives, providing guidance on mitigation strategies.
- Promoting a risk-aware culture by delivering training programs that integrate risk considerations into decision-making processes.
- Preparing regular risk reports for Senior Management and the Board, summarizing the risk landscape, key risks and mitigation effectiveness.

ERM Framework

The Group's ERM framework provides a systematic process for identifying, assessing, treating, monitoring and reporting risks. It includes:

Risk Strategy and Culture

The ERM strategy aligns risk management with the Group's objectives to enhance decision-making and foster sustainable success. A strong risk culture ensures shared values and practices that prioritize risk awareness at all levels of the organization.

Risk Governance (Three Lines Model)

The Three Lines Model aims to outline the structures, processes and responsibilities to facilitate strong governance of risk management:

1st Line

Business and operational units manage risks and controls directly

2nd Line

The ERM Department supports risk management efforts

3rd Line

Internal Audit provides independent assurance of risk management effectiveness

ERM Policy and Procedure

The ERM policies and procedures provide a structured framework for identifying, assessing, monitoring and controlling risks across the Group.

Risk Appetite and Tolerance

The risk appetite and tolerance levels help the Group make decisions that contribute to achieving its strategic objectives. Risk appetite and risk tolerance levels are determined on the basis of the Group's direction, objectives, culture and external environment.

Risk Management Process

A structured process encompassing risk identification, measurement, treatment and continuous monitoring and reporting. The output is a risk register that logs all identified risks and their treatments.

Principal Risks and Categories

The Group's Risk Universe encompasses 7 principal risk categories: operational risks, technology risks, corporate risks, financial risks, cybersecurity risks, business continuity risks and business environment risks.

Risk Management continued

Cybersecurity

The Cybersecurity Department ensures the confidentiality, integrity and availability of the Group's data, systems and networks, enabling business objectives while mitigating security risks. Comprising Cybersecurity Governance and Cybersecurity Operations, the department safeguards assets without disrupting business operations through proactive threat management and regulatory compliance.

Core activities include:

- Deploying robust security measures to protect the Group from potential threats and vulnerabilities.
- Continuously monitoring for vulnerabilities and promptly responding to incidents.
- Ensuring alignment with all relevant cybersecurity regulations and standards.

Compliance with NCA Frameworks

The department adheres to the National Cybersecurity Authority (NCA) frameworks, ensuring high standards of cybersecurity across the Group. These include:

- Essential Cybersecurity Controls (ECC)
- Critical Systems Cybersecurity Controls (CSCC)
- Cloud Cybersecurity Controls (CCC)
- Telework Cybersecurity Controls (TCC)
- Organization Social Media Accounts Cybersecurity Controls (OSMACC)
- Data Cybersecurity Controls (DCC)

Through proactive threat management and regulatory compliance, we are committed to safeguarding assets without disrupting the Group's business operations.

Business Continuity and Environmental Security

The Business Continuity and Environmental Security Department ensures the Group maintains critical functions during and after disruptive events while promoting sustainability and resilience against environmental challenges.

Core activities include:

Policy and Framework Development

- Establishing the Business Continuity Management framework and strategy for approval by the relevant committee.
- Developing and implementing strategies, sub-policies and standards required for policy execution.
- Maintaining and communicating the latest versions of the Business Continuity policy and framework to all relevant parties.

Business Continuity Management Plan

- Coordinating with Business Continuity Champions to implement the policy and framework.
- Ensuring regular testing and exercising of continuity plans, incorporating lessons learned to enhance effectiveness.
- Conducting exhaustive assessments of new initiatives or major service/system changes to ensure proper continuity plans are developed.

Risk and Impact Assessments

- Collaborating with the ERM Department to identify potential threats and assess their operational impacts.
- Analyzing business impact and risk data to develop resilient strategies, including alternative operating methods, relocation plans and dependency solutions.

Incident Review and Continuous Improvement

- Reviewing post-incident and management reports, applying lessons learned to strengthen continuity measures.
- Evaluating business continuity capabilities of members, suppliers and service providers based on the nature of their businesses.

Stakeholder Collaboration

- Planning, scheduling and developing exercise objectives, scope and scenarios in partnership with Stakeholders.
- Ensuring alignment with organizational priorities, reducing risks to acceptable levels for unmitigated disruptions.

Business Continuity Strategy

The Group's Business Continuity strategy ensures prioritized activities and services continue following disruptions. It leverages insights from business impact analyses, risk assessments and Stakeholder evaluations to develop robust, scalable and resilient continuity measures.

Risk and Security Highlights and Achievements

The Risk and Security Division achieved significant milestones this year, reflecting its comprehensive approach to safeguarding the Group's resilience and strategic goals. Key highlights and achievements include:

- Reviewed and updated Enterprise Risk Management, Cybersecurity and Businesses Continuity Management policies, methodologies and processes to align with evolving industry standards and strategic objectives of the Group.
- Ensured continuous evaluation of the Key Risk Indicators (KRIs) to reflect the strategic changes and ensuring proactive risk monitoring and identification of emerging risks.
- Ensured continuous support and evaluation of the Group's projects and initiatives through identifying, assessing and mitigating risks throughout their lifecycle.
- Achieved ISO 27001 certification and maintained high compliance with all national cybersecurity regulations, including NCA controls across applicable frameworks.
- The cybersecurity program excelled in monitoring assessments, increasing awareness and enhancing overall effectiveness. These efforts resulted in no critical or high cybersecurity incidents.
- Enhanced the Business Continuity framework to ensure the continuous maintenance of a robust, enterprise-wide framework that supports all aspects of the Group's core operations and projects.