Enterprise Risk Management

Saudi Tadawul Group's comprehensive and robust approach to enterprise risk management (ERM) is designed to safeguard the Group, its assets, and the Stakeholders' interests.

In line with the Group's governance model, framework, and culture, it is the responsibility of every individual across the Group to cooperate in identifying any potential risks and setting proper plans to avoid and mitigate any risks that might limit the Group's ability to execute its strategy to create sustainable value for its Stakeholders.

The Group operates within a complex environment that subjugates it to several types of risks, such as operational, technology, corporate, financial, business continuity, information security, and business environment risks. To mitigate such risks, the Group's ERM department implements the ERM policy and framework, which govern the process to which risk identification, assessment, treatment, monitoring, and reporting is carried out.

The ERM department supports the Group in conducting the risk and control self-assessment process to identify key risks and define appropriate treatment plans. Risk identification is carried out in accordance with the aforementioned type of risks. A process of periodic follow-up is in place to ensure treatment plans are implemented, and when necessary, enhanced.

Key risks are reported regularly to Executive Management and the Group's Governance, Risk, and Compliance Board Committee, which oversees and monitors these risks in line with the Group's risk appetite and tolerance levels. Risk assurance is carried out by the internal audit function which, as per the plan, conducts risk-based audits upon the Group's operations and services. In addition, the ERM department carries out additional risk assessment processes, such as projects risk assessment, assessment of key risk indicators, assessment of incidents and loss events.

Enterprise Risk Management Governance and Framework

The Group's ERM framework provides the appropriate methodology for implementing the risk management process, which includes identifying and measuring risks, as well as identifying risk treatment plans to reduce the likelihood and impact of risks for the Group.

Risk management strategy

The risk management strategy helps align risk management efforts with the Group's overall objectives, improves decision-making, and enhances the Group's ability to navigate uncertainties and achieve sustainable success.

Risk governance

The Group implements the Three Lines Model, which aims to outline the structures, processes and responsibilities to facilitate strong governance of risk management.

Risk culture

Risk culture is the set of values, beliefs, and understanding about risk shared by employees of the Group.

Risk management process

The risk management process includes risk identification, measurement, treatment, and continuous monitoring and reporting. Each step encompasses various tools and techniques that supports its completion. The output of the risk management process is the risk register, a log of all information related to risks and their treatment.

Risk universe

The Group's risk universe classifies risks into seven principal categories: operational risks, technology risks, corporate risks, financial risks, information security risks, business continuity risks, and business environment risks.

Risk appetite and tolerance

Established 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.

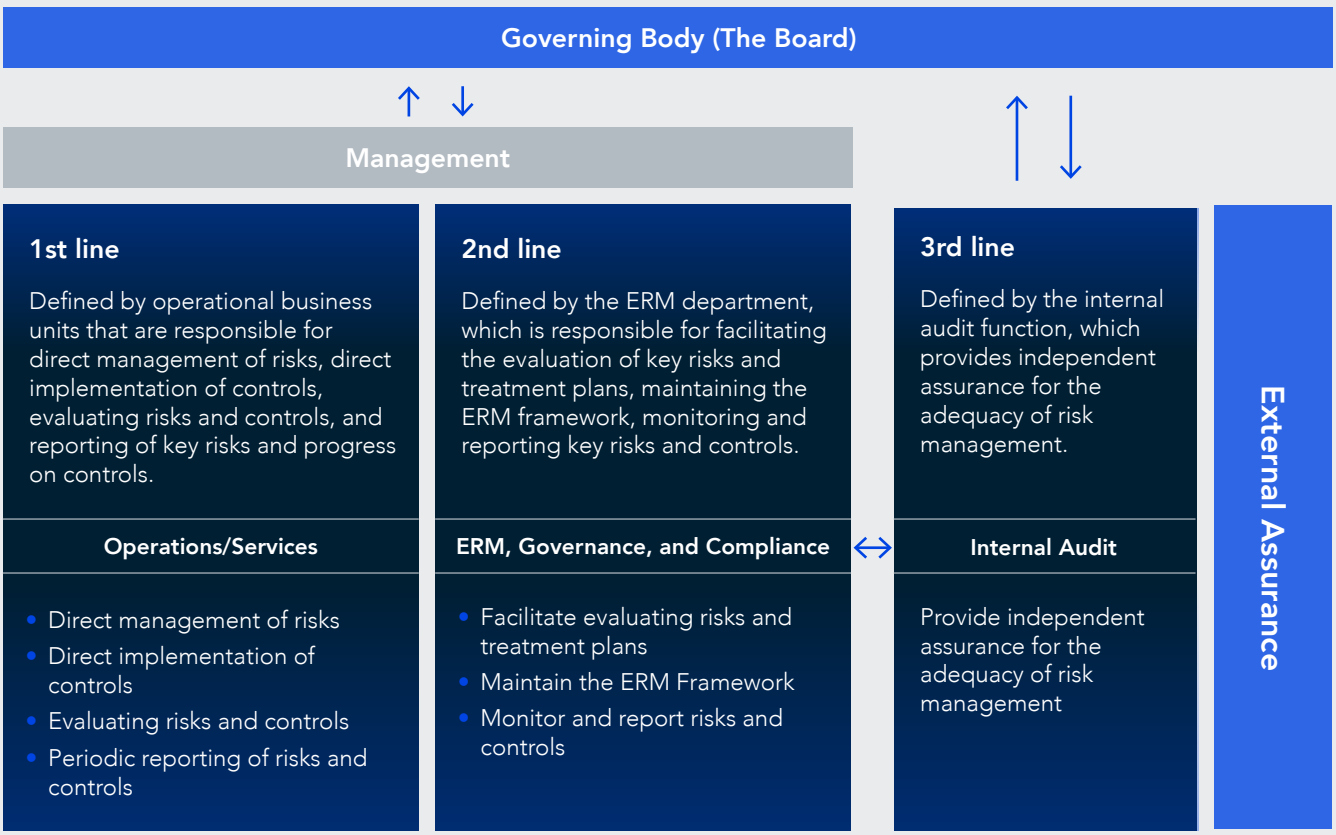
ERM policies and procedures

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

Enterprise Risk Management (continued)

The Three Lines Model

Governed and overseen by the Group's Board of Directors, the Group applies the Three Lines Model.



ERM Department

The ERM department's main purpose is to manage activities required to identify, evaluate, and prioritize risks that could affect services, infrastructure, assets, and resilience of the Group and the execution of its strategy, by developing and maintaining a comprehensive, systematic, and proactive approach aligned with the objectives and long-term initiatives of the Group.

The ERM department is responsible for the following:

- Develops and maintains the ERM policy and framework, which outline the principles, procedures, and responsibilities for managing risks across the Group. This includes defining risk categories, and outlining the overall approach to risk management.
- Works with Senior Management and the Board of Directors to define the Group's risk appetite and tolerance levels, which establish guidelines to ensure risks are managed within acceptable limits and aligned with the Group's strategic objectives.
- Conducts comprehensive risk assessments to identify and evaluate key risks across the Group. The department implements risk assessment methodologies, such as qualitative and quantitative analyses, to determine the potential impact and likelihood of risks. These assessments help prioritize risks and allocate resources effectively.

- Establishes and monitors key risk indicators (KRI), which are measurable metrics that provide early warning signs of potential risks. The department defines relevant KRIs for different risk categories and implement monitoring systems to track and report on the status of these indicators. Monitoring KRIs helps in identifying emerging risks and trigger appropriate risk responses.
- Collaborates with project managers and Stakeholders to conduct risk assessments for the Group's programs, projects, and initiatives. The department identifies and evaluates risks specific to each project, considering factors such as project scope, objectives, timelines, and resource allocation. The department provides guidance on risk mitigation strategies and ensures project risks are appropriately managed within the overall ERM framework of the Group.
- Fosters a risk-aware culture throughout the Group by developing and delivering training programs to enhance risk awareness and understanding among employees. The department promotes the integration of risk considerations into decision-making processes and encourages open communication about risks across all levels of the Group.
- Prepares and presents regular risk reports to Senior Management and the Board of Directors. These reports provide an overview of the risk landscape, highlight key risks, and assess the effectiveness of risk mitigation strategies. Effective communication of risk-related information helps Stakeholders make informed decisions and take appropriate actions.

Risk Assessment and Mitigation

Risk Assessment Methodology

The key attributes of the risk assessment methodology are assessing impact, likelihood, and the risk scoring defined below.

Impact assessment is the process of assessing the probabilities and consequences of the risk events in case they may materialize. Assigning an impact rating to the risk will be based on the rating for the highest impact anticipated, whether it is financial, reputational, strategical, customer-based, or legal.

Likelihood assessment is the probability that a risk may cause loss for Tadawul Group before considering the effectiveness of controls.

Risk score is calculated by multiplying the likelihood and impact ratings of each risk. Risk score addresses the inherent risk in case it is calculated without the consideration of the presence or the effectiveness of the related controls.

Risk Status categorizes risks into four ratings: from highest and most urgent risks, which may hinder the Group from achieving its goals; to lower and less urgent risks that have a minimal effect on the Group's efficiency.

After consideration of the presence and effectiveness of controls, the residual risk is determined using a similar methodology to that used for calculating the inherent score. The difference is that the likelihood score is reduced by the control effectiveness rating. When the impact of control effectiveness score is subtracted from the inherent risk, the remaining is the residual risk score.

Likelihood	1.Insignificant	2. Minor	3. Moderate	4. Major	5. Significant
5. Almost Certain	M (5)	H (10)	H (15)	C (20)	C (25)
4. Likely	L (4)	M (8)	H (12)	C (16)	C (20)
3. Possible	L (3)	M (6)	M (9)	H (12)	H (15)
2. Unlikely	L (2)	L (4)	M (6)	M (8)	H (10)
1. Remote	L (1)	L (2)	L (3)	L (4)	M (5)

Impact

Risk Status: C Critical risk | H High risk | M Medium risk | L Low risk

Enterprise Risk Management (continued)

Risk Mitigation

The ERM department remains proactive in mitigating risks by working collaboratively with all departments to identify and address key risks. The department's comprehensive ERM framework includes implementing robust internal controls, providing guidance to enhance operational efficiency and resilience, conducting periodic risk assessments, facilitating effective communication, and assisting in developing risk awareness throughout the Group.

The department monitors key risks and provides guidance on risk mitigation strategies while ensuring adherence to recognized standards and guidelines. The department collaborates with Stakeholders to minimize the risk of disruptions and maintain the integrity and credibility of the Group. Additionally, the ERM department monitors external factors such as economic, political, and environmental conditions to identify key risks that may impact the Group's performance and objectives and assists in developing contingency plans, engages with Stakeholders, and manages key risks.

Principal Risks

Risk	Description
Operational risks	Risks arising from poor efficiency or failure of internal and external processes, individuals, systems, or external events. These include issuer operations risks, member operations risks, market operations risks, human resources risks, and physical asset risks.
Technology risks	Technology failure that disrupt business operations. Technology risks include infrastructure failures, IT system failures, or telecommunications risks.
Corporate risks	Risks related with Group's strategic objectives, compliance and governance framework, projects, and communication.
Financial risks	Risks that may affect the Group's revenues or reduce the efficiency of operating expenses. Financial risks include liquidity risks, credit risks, investment risks, accounting and financial reporting risks, insurance risks, and fraud risks.
Information security risks	Risks arising from vulnerabilities and threats to information and system, which may affect the achievement of business objectives. Information security risks include internal threats, external threats, data privacy risks, and data integrity risks.
Business continuity risks	Risks that lead to a catastrophic disruption of the Group's operations, resulting in significant losses in the technology infrastructure and level of services provided. The ERM department oversees the requirements determined by business continuity management (BCM) for restoring the service and ensuring the Group's ability to maintain the services provided to ensure the integrity and credibility of the market and investors. The ERM department also supports the BCM to establish controls and plans to reduce the risk of disruption of the system or facilities to ensure the continuity of business commensurate with the requirements of raising the efficiency of the market.
Business environment risks	Risks arising from a number of external factors that form the business environment that affects the performance and objective of the Group, such as economic, political, and environmental conditions, which includes the risks of market members, legal risks, data vendor risks, and the risks of vendors and suppliers.

Enterprise Risk Management Highlights and Achievements

2023 was a year of significant ERM advances and achievements for Saudi Tadawul Group, including:

- Enhanced risk awareness across the Group by providing training programs that educate employees about the importance of risk management and their roles in identifying and mitigating risks. Fostered a risk-aware culture by promoting open communication, collaboration, and accountability for risk management.
- Established a risk appetite and tolerance framework that aligns with the Group's and subsidiaries' strategic objectives. This framework defines the acceptable level of risk the Group is willing to take and helps guide risk management decisions, ensuring risks are managed within predetermined boundaries.
- Conducted thorough risk assessments, utilizing appropriate methodologies and tools, and established appropriate risk treatment plans, implementing internal controls, and monitoring the effectiveness of risk mitigation measures.

- Established a structured risk reporting process, providing timely and accurate risk information to Management and the Board of Directors.
- Ensures alignment with applicable laws, regulations, and industry standards relevant to risk management. Proactively monitored regulatory changes and assessed their impact on the Group's risk profile.
- Implemented proactive monitoring systems and key risk indicators (KRI) to track changes in risk profiles and identify emerging risks.
- Regularly reviewed and evaluated the effectiveness of the ERM policy and framework by identifying areas for improvement and implementing lessons learned. Embraced a culture of continuous improvement by regularly reviewing and enhancing the ERM framework, methodologies, and processes. This includes soliciting feedback, conducting internal assessments, staying informed about evolving industry standards to ensure ongoing effectiveness and relevance and actively monitored the external environment for emerging risks that could impact the Group.
- Ensured that risk management is integrated into project management processes and new initiatives by conducting risk assessments and providing guidance on risk mitigation throughout the project lifecycle.

Cybersecurity

Saudi Tadawul Group's Cybersecurity department, which consists of cybersecurity governance and cybersecurity operations, is responsible for:

- Building, maintaining, and improving the cybersecurity policy and procedures.
- Handling cybersecurity compliance and risk.
- Operating and integrating relevant systems and processes with the Security Operations Center (SOC).
- Continually optimizing existing cybersecurity monitoring tools and processes to ensure protection of critical information assets.

The Department follows National Cybersecurity Authority (NCA) frameworks, such as:

- Essential cybersecurity controls (ECC).
- Critical systems cybersecurity controls (CSCC).
- Cloud cybersecurity controls (CCC).
- Telework cybersecurity controls (TCC).
- Organizations social media accounts cybersecurity controls (OSMACC).
- Data cybersecurity controls (DCC).

In 2023, it effectively monitored cybersecurity assessments, awareness, and the overall effectiveness of the Cybersecurity program. This contributed to ensuring no cybersecurity incidents, obtaining the ISO 27001 certification and ensuring the Group meets all relevant CMA requirements and improves the level of compliance with NCA's regulations.

Business Continuity

Saudi Tadawul Group's Business Continuity department, which follows ISO 22301:2019, is responsible for:

- Developing the appropriate business continuity policy, strategies, and framework.
- Developing, reviewing, and maintaining the Group and subsidiaries business impact analysis (BIA) and business continuity plans.
- Setting the minimum business continuity standards or guidelines for members or any authorized participants who utilize the Saudi Tadawul Group's trading platform or other core services.
- Assessing new initiatives or major changes or systems for business continuity aspects.
- Reviewing and maintaining business continuity risk assessments.
- Developing, reviewing, and maintaining Business Continuity program reports.
- Establishing, implementing, and maintaining an incident response plan to avoid any disruption to the organization's critical services.
- Preparing and managing appropriate testing and exercising plans annually.
- Preparing and maintaining the business continuity training and awareness program for various levels of employees across the Group and its subsidiaries.

In 2023, the Business Continuity department succeeded in evaluating the Group's resiliency by reviewing the Business Continuity program, which covers business continuity and disaster recovery plans, scenario testing, crisis management, and employee awareness, hence obtaining the ISO 22301:2019 certification. The department has supervised failover tests for all the Group's critical systems, including critical businesses, market members, and related third parties and service providers, to ensure the Group's capability and resilience against potential disruptions. Finally, the department also oversaw the Group's continuity by evaluating the resilience of its technical infrastructure and current strategies to optimize it in line with best practices and standards.