Risk management policy and control

The Risk and Security Division of Saudi Stock Exchange (Tadawul) follows the "Three Lines of Defence" methodology, which is in accordance with international standards. It also helps to define the responsibilities of each of the Company's Divisions, Executive Management and the Board Committees of the Council in a precise and effective manner with regard to risks. The important roles of Management are to approve and develop the standards and requirements of information security and business continuity for all Exchange members and data providers or vendors, in line with the ongoing changes within and relating to the market. This includes risk awareness, security and business continuity in line with market changes and the Company's vision.

The following types of risks are defined and approved by Tadawul:

Type 1: Operational risk
These risks arise due to poor efficiency or failure of internal and external processes, individuals, systems, or external events. These include risks due to issuances, clearing companies' transactions, market transactions, asset and deposit transactions, market regulation, HR and material assets. The Risk and Security Division reviews all operational risk sources in collaboration with the concerned Departments with a view to develop suitable policies to minimize these risks.

Type 2: Technical risks
These are the risks associated with IT resulting from the possibility of a defect in information systems, technical structure errors, or communications. IT risk management is concerned with understanding the ongoing operations and processes, identifying the potential risks, and assessing the possible impact of any failures to processes or the information to be derived from them. Prevention and damage mitigation strategies have to take into account human factors, especially the possibility of intentional damage, in addition to accidental damage. Such strategies include reducing the Company's responsibility for any risks, avoiding them, mitigating their adverse effects, or accommodating their consequences wholly or partially.

Type 3: Regulatory risks
These are the risks arising from improper decisions by the Company's Management, erroneous regulatory decisions, improper implementation of regulatory decisions or lack of timely decision-making, which may result in direct loss or loss of alternative opportunities. These risks may arise out of the Company violating laws and standards established by the regulatory authorities; they may be also due to the lack of a suitable strategy to achieve short-term and long-term goals.

Type 4: Financial risks
Financial risks are current or future risks that may affect the Company's revenues or reduce the efficiency of operating expenses. An example is the variable nature of trading commission which constitutes a large percentage of revenue. Other risks include variability in interest rates, exchange rates and the market value of stocks that may affect the return on investment. These are in addition to the liquidity, investment, insurance and financial analysis risks. A key risk mitigation strategy is to increase income not related to trading, in order to mitigate the risks arising from market variations. Also within the ambit of financial risks are procurement and support services risks for which an approved strategy has been put in place to reduce the potential impact.

Type 5: Information security risks
These are risks arising from technical shortcomings and threats to information assets used by the Company that affect the achievement of business objectives. Such risks include internal threats and external threats to information security, threats to privacy, confidentiality and integrity of data, and risks to availability of information. The Risk and Security Division defines the level of data classification in order to ascertain the tools, processes and controls required to grant access to it. The Division also evaluates the ability of the Company to protect classified data considering the threat posed by any unauthorized disclosure or access.

Type 6: Business continuity risk:
This is the risk that the Company's operations are affected by catastrophic and disruptive events, resulting in significant losses in the technical structure and level of services provided. These include risks due to infrastructure breakdowns, natural disasters, logistic support providers, and threats to personnel.

The Risk and Security Division determines the requirements for restoring the services after major disruptive events and ensures the Company's ability to maintain the services provided to retain the credibility of the Exchange with the market and investors. The Division also works to establish controls and plans to reduce the risk of disruption of the system or public facilities to ensure the continuity of business commensurate with the requirements of raising the efficiency of the market.

Type 7: External risks
These are the potential risks or losses resulting from a number of external factors that constitute the external environment and affect the performance and business of the Company such as economic, political and environmental conditions, which create risks to market members, legal risks, risks to data providers and the risks to vendors and suppliers.