

Risk Management

The telecommunications sector faces significant challenges, chiefly the diminishing demand for voice services juxtaposed with an exponential increase in data consumption, a trend hastened by the recent pandemic. This rapid digital transition, propelled by disruptive technologies, redefines traditional revenue models and necessitates swift innovation among telecom providers.

In an increasingly saturated market, differentiation through unmatched service offerings becomes paramount. Concurrently, significant investments in infrastructure, rigorous data protection protocols and adherence to regulatory frameworks are non-negotiable. Telecom enterprises must navigate this transformation by promptly adapting, broadening their service portfolios and delivering frictionless customer experiences to secure a sustainable competitive advantage. stc’s risk management is integral to its strategic framework, informing business planning and performance evaluation and embedding risk considerations into critical decision-making processes to maximize impact.

Enterprise risk management governance

The Board of Directors ensures the highest standard of corporate governance is maintained by regularly reviewing governance development best practices and making certain these are duly adopted. As a result, the Board has established the Board Risk Committee, which plays a key role in overseeing the implementation of the Enterprise Risk Management (ERM) framework, risk strategy and related risk management policies, as well as monitoring stc’s risk management system, reviewing the top risks and the management of those risks.

The risk management function is independent and separate from stc’s business groups and sectors; it has completed its first wave of measures this year as per the Board-approved risk strategy to uplift current practices and maturity.

Enterprise risk management framework


The ERM framework provides guiding principles for proactively managing business risks through a comprehensive and dynamic system designed to identify, assess, prioritize and mitigate risks effectively across stc operations. The ERM process is embedded within stc as this allows us to take a holistic approach and make meaningful comparisons to support the delivery of strategic objectives. Quarterly risk assessment is a core part of this process. The risk framework clearly defines roles and responsibilities and sets out a consistent end-to-end process for identifying and managing risks.


stc’s approach is continuously enhanced, enabling more dynamic risk detection, modeling of risk interconnectedness and leveraging data to improve risk visibility and responses. The attainment of ISO 31000 attestation further solidifies its commitment to industry-leading practices. A standard risk scoring methodology has been devised to provide context and ensure consistency in reporting and evaluating risks. The output from this process is consolidated to determine the principal risks and uncertainties for the organization.


The risk categories classify all risk source types that could affect stc into five main silos known as category 1 risks. For easier management and communication, Category 1 risks are broken down into Category 2 risk types and, in some instances, these are further sub-divided into Category 3 and 4 risk types. Furthermore, the ERM will be the custodian to the risk families and has the authority to add or reclassify them.


Risk family CAT1	Corporate risk >> 01	Operational risk >> 02	Technology risk >> 03	Financial risk >> 04	Legal and compliance risk >> 05
Risk family CAT2	Governance 1.1	Service delivery 2.1	Information technology 3.1	Market 4.1	Compliance 5.1
	Strategy 1.2	Sales and marketing 2.2	Network operations 3.2	Liquidity 4.2	Legal 5.2
	Program management 1.3	Supply chain 2.3	Cybersecurity 3.3	Foreign exchange 4.3	Regulatory 5.3
	Planning and resource allocation 1.4	People / human resources 2.4	Data privacy 3.4	Interest rate 4.4	
	Major initiatives 1.5	Revenue management 2.5	Data integrity 3.5	Investments 4.5	
	Mergers, acquisition and divestiture 1.6	Physical assets 2.6	Artificial intelligence 3.6	Credit 4.6	
	Market dynamics 1.7	Intangible assets 2.7		Accounting and reporting 4.7	
	Communication and investor relations 1.8	Project management 2.8		Tax and Zakat 4.8	
		Business continuity 2.9		Capital structure 4.9	
		Health and safety 2.10		Fraud 4.10	
				Revenue leakage 4.11	

Risk Management continued

	Impact: is the loss expected if a risk materializes ; the impact is generally tiered between 1 to 5 levels on an exponential scale. stc's impact rating scale is as follows:		
Rating	Qualitative measure	₪ value utilized for inherent risk calculation	Quantitative measure "monthly revenue"
5	Severe	Above ₪ 400M	>10%
4	Major	Between ₪ 200M and 400M	5% to 10%
3	Moderate	Between ₪ 40M and 200M	1% to 4.99%
2	Minor	Between ₪ 2M and 40M	0.05% to 0.99%
1	Insignificant	Below ₪ 2M	< 0.05%

	Likelihood: The likelihood is the probability that a risk may cause a loss for the stc before considering the effectiveness of controls The likelihood rating scale is as follows:		
Rating	Qualitative measure	Qualitative chance of risk occurring in time period	Probability
5	Almost certain	Once in 3 months or less	90%-100%
4	Likely	Once in 6 months	60%-89%
3	Moderate	Once in a year	41%-59%
2	Unlikely	Once in 2 years	5%-39%
1	Remote	Once in 4 years or more	Less than 5%

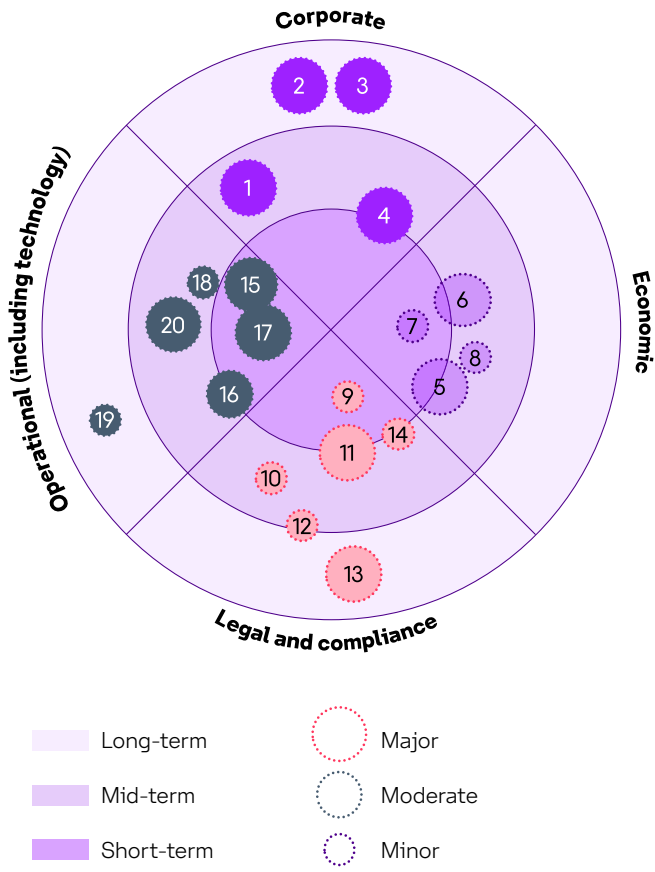
<div></div> Risk scoring: quantifies the potential impact and likelihood of risks using inherent risk ratings, which assume no controls, and residual risk ratings, which consider the mitigating effects of existing controls. The calculated inherent and residual scores result in an attention score or index:							
Action attention index							
Impact rating	Severe	256	16	36	64	144	256
	Major	81	9	20	36	81	144
	Moderate	16	4	9	16	36	64
	Minor	5	2	5	9	20	36
	Insignificant	1	1	2	4	9	16
			1	5	16	81	256
			Remote	Unlikely	Possible	Likely	Almost certain
Likelihood rating							

	The inherent and residual risk scores assists in assessing the risks on the following attention index:	
Risk rating	Risk matrix score	Risk appetite baseline
Negligible	< 9	Below appetite
Marginal	>= 9 to < 20	Within appetite
Manageable	>= 20 to < 51	Above appetite
Substantial	>= 51 to < 101	Greatly above appetite
Critical	>=101	Beyond appetite

Emerging risks are considered part of the risk assessment process and identified through horizon scanning, continual dialogue with the business and keeping abreast of market and industry changes. A summary of identified emerging risks is presented to the Board Risk Committee and Board for assessment, and these risks are consistently monitored as part of stc's ongoing risk management processes.

This year, stc placed greater emphasis on sustainability and ESG risks, reflecting its commitment to aligning with global best practices and stakeholder expectations. Significant progress was made in identifying, assessing and managing these risks, ensuring they are integrated into stc's broader risk management framework and strategic decision-making processes.

Global emerging risk landscape



Source : BCG and Gartner

	Category	Name
1	Corporate	Evolving dynamics of the digital currency from China and US
2	Corporate	Increased competition with OTT and DC providers
3	Corporate	Carriers in smart city infrastructure
4	Corporate	International tensions and economic relations
5	Economic	Credit crunch widens
6	Economic	Market effect from higher borrowing costs
7	Economic	Erosion of ARPU for IoT and consumer customers
8	Economic	Increased capital requirements for core network construction and operations
9	Legal and compliance	Potential expectation gap on 5G coverage and performance
10	Legal and compliance	Compliance to Deep Packet Inspection or network access
11	Legal and compliance	Legal framework for the development, marketing and use of AI
12	Legal and compliance	Disputes over spectrum access, pricing and deployment
13	Legal and compliance	Complex and stringent national and trans-national cyber security regulations
14	Legal and compliance	Personal data regulatory fragmentation
15	Operational	AI and LLM threats and misinformation
16	Operational	Quantum computing and encryption
17	Operational	Cyber security incident management in heterogeneous technology landscape
18	Operational	ORAN and the exposure of the attach surface
19	Operational	Early development of 6G technology
20	Operational	Low orbit satellite advancements

Risk Management continued

Identifying risks

All stc entities identify and assess their own risks, which could potentially affect their strategy and operations. A consolidated list of these risks is presented to senior leaders and executives, along with the outputs from an external environment scan and related benchmarks. Applying a Group-wide perspective, these executives evaluate and determine critical risks and which emerging threats warrant further exploration. These are defined and agreed upon by the Risk Management Committee before being submitted to the Board Risk Committee and the Board for final review and approval.

Managing risks

Establishing the context and having a clear understanding of the environment in which it operates is important. Therefore, stc assigns each of its risks to a specific category (i.e. corporate, technology, operational, financial and compliance) and identifies whether the source of the threat is internal or external. This approach enables a better understanding of how it should treat the risk and ensures the right level of oversight and assurance are provided.

The assigned executive risk owners are accountable for ensuring that adequate controls are in place and implementing the necessary treatment plans to bring the risk within acceptable tolerance levels. stc continues to monitor the status of risk treatment strategies across the year and hold in-depth reviews of its risks. stc also develops a comprehensive assessment of the related scenarios for each of the top risks, providing additional insight into possible threats and enabling a better risk treatment strategy.

Monitoring risks

stc’s risk report, which presents the main risks, is prepared for the Board of Director on a quarterly basis. The Board Risk Committee also examines this report at its meetings. In addition, the emerging risks are presented once a year as part of the risk report. Among other benefits, stc risk report ensures transparent monitoring of the development of individual risks, as well as the overall risk situation. It informs the Board Risk Committee about all of the latest developments and/or changes in the risk management system.

With the aim of managing and supervising risks, stc is enhancing its risk management technology tools, which facilitate the reporting, analysis, assessment and management of risk information. These are continuous improvements developed in risk management tools to improve or expand their functionalities. As part of ongoing enhancements, stc has improved its risk management technology tools to support better reporting, analysis, assessment and management of risk information. Additionally, stc has refined its existing Key Risk Indicators (KRIs) as a key measure to strengthen risk monitoring practices, ensuring more robust oversight and proactive management of risks.

Risk mindset and culture

stc engenders a set of behaviors and expectations that drive risk awareness throughout its business activities. It is driven by the tone from the top and supported by its people management systems. It promotes timely and sensible risk interventions and actions that improve operational integrity and help employees make smart choices about risks. It communicates expected behaviors to every colleague to weave risk awareness into the fabric of its culture. It has an ongoing program of training and communication and has defined roles to formalize risk management and continuously integrate risk management procedures into key areas of decision-making.

Business continuity

stc’s unwavering commitment to Business Continuity Management (BCM) reflects its strategic focus on safeguarding national resilience, operational integrity and the trust of its stakeholders. As a key enabler of Saudi Arabia’s Vision 2030, stc continues to prioritize the resilience of its critical infrastructure, the protection of its assets and the safety of its people, ensuring it remains a cornerstone of the nation’s digital and communication backbone.

In alignment with the directives of the National Risk Committee (NRC); Communications, Space and Technology Commission (CST); and the newly introduced National Emergency Management Authority (NEMA), stc has fully integrated national guidelines into its BCM framework. These efforts affirm its leadership in crisis management, organizational resilience and business continuity, setting an example for the sector while engaging with top-tier experts globally to adopt best practices and innovative solutions.

stc’s BCM strategy is underpinned by adherence to international standards, such as ISO 22301, with comprehensive training programs for its teams in DRI and BCI standards. This equips stc with cutting-edge capabilities to ensure readiness and response excellence.

Over the past year, it has achieved significant milestones, including successfully executing over 200 BCM exercises, spanning all critical functions and incorporating interdepartmental collaboration. These rigorous tests have strengthened its recovery strategies, validated its Business Continuity Plans (BCPs) and reinforced its ability to maintain seamless operations under any circumstance.

To ensure measurable and transparent performance, stc employs strict Key Performance Indicators (KPIs) across all BCM activities, underscoring its disciplined approach to maintaining the highest levels of preparedness and reliability. Through continuous Business Impact Analyses (BIAs) and iterative improvement cycles, it has elevated its BCM maturity, ensuring alignment with national and international resilience mandates. Moreover, stc has harnessed the power of digital transformation to enhance the agility, scalability and efficiency of its Business Continuity Management System (BCMS). These initiatives have modernized its operations and fortified its capacity to adapt swiftly to evolving challenges.

Recognizing the importance of a skilled workforce, stc has invested in extensive training and professional development programs in BCM, Crisis Management, Incident Response, and Disaster Recovery. This ensures that its employees remain at the forefront of resilience disciplines, empowering them to respond effectively to crises and disruptions. This year’s accomplishments reflect stc’s steadfast commitment to supporting national resilience frameworks, maintaining operational continuity and safeguarding the interests of its shareholders, stakeholders and the nation. These efforts reassure its leadership and citizens that stc remains a trusted partner in pursuing a secure and resilient future for Saudi Arabia.

Internal control

stc’s Board of Directors declares that the accounting records have been prepared correctly and that the internal control system and procedures have been properly prepared and effectively implemented without material observations or concerns raised and asserts that nothing exists to impede the company from continuing its operations and activities.

The Audit Committee oversees the compliance and internal and external audits, and regularly reviews the adequacy and effectiveness of the internal control system.

One of the objectives of the Board is to obtain reasonable assurance about the soundness of the design and the effectiveness of stc’s internal control system. In this regard, during the fiscal year 2024, the Audit Committee held 8 meetings and discussed a number of topics falling under its competencies, including reviewing financial statements, investments and business units, as well as strategic and organizational affairs, human resources, procurement and IT systems. This meeting is attended by Executive Management and members of the Internal Audit team.

Risk management highlights

In the past year, stc has achieved significant milestones in its journey toward excellence in risk management, reinforcing its position as a forward-looking and resilient organization. A key achievement was the comprehensive review and re-assessment of stc’s risk appetite. This effort ensured alignment with evolving strategic priorities and established a robust foundation for governing risk-taking activities, enabling more informed and balanced decision-making at all levels.

To strengthen risk oversight, stc introduced automated monitoring indicators across all key risks. This advanced mechanism provides real-time insight into risk status, allowing the organization to anticipate potential threats and respond proactively to emerging challenges. Complementing these efforts, stc obtained ISO 31000 certification for enterprise risk management and ISO 27001 certification for information security, highlighting its adherence to international best practices and its dedication to maintaining the highest standards of governance and security.

Risk Management continued

Recognizing the critical role of a strong risk culture, stc conducted extensive training sessions and awareness events across the organization. These initiatives have fostered a heightened understanding of risk management principles and have begun to deliver tangible improvements in internal processes, enhancing collaboration and accountability.

Finally, stc has continued to focus on expanding its coverage of risks, ensuring a comprehensive understanding of exposures across its operations. Rigorous efforts were made to strengthen existing controls and implement robust mitigation strategies, further securing the organization against an increasingly complex and dynamic risk environment. These achievements collectively reflect stc’s unwavering commitment to safeguarding its future while driving sustainable growth.

Principal risks

As a leading entity in the global telecommunications and information technology arena, stc navigates a landscape rife with uncertainties and rapid

change. Success in this dynamic environment is predicated on its proactive anticipation of potential developments and the systematic identification, evaluation and management of the consequent risks and opportunities. stc regards an efficacious risk and opportunity management system as an indispensable component of its value-driven corporate governance. In the risk evaluation phase, it categorizes risks into corporate, technology, operational, financial, and legal and compliance domains. This classification enhances its comprehension of each risk’s unique characteristics and informs its management approach, allowing it to craft tailored oversight and assurance strategies.

The key risks affecting stc remain largely unchanged from last year, with only 1 additional risk identified and minor updates to existing risks. The material risks, including environmental and social exposures, are detailed below, along with the strategies employed to manage them. The risk management process continues to highlight the most significant risks at the entity level, reflecting ongoing challenges rather than new developments.



Category	Risks	Mitigation measures
Technology	Cybersecurity threats The rise of advanced malware and DDOS botnets is reshaping the threat landscape and forcing enterprises to reassess how they protect themselves. This threat exists not only within stc, but upstream through vulnerabilities in its vendors and suppliers; and downstream, where vulnerabilities in stc may be leveraged by cyber-criminals to attack its customers. Third-party access management is a significant matter as it relies heavily on third-party contractors with multiple incidents reported by stc.	stc continues to strengthen the cybersecurity. Internal systems and policies are developed, levels of security procedures are raised, awareness is intensified, and the effectiveness of information security plans is tested. stc has established robust cyber assurance practices for information protection and asset management and stc has established advanced penetration testing and vulnerability management capabilities.
Technology	Data privacy One of the biggest challenges faced by any organization is managing privacy as data volumes continue to grow and regulatory and customer scrutiny increases. It is more important than ever to be clear on the privacy risks it faces to handle PII, or an individual's right to determine what kind of data can be collected, stored, protected and can be shared with third parties.	stc has established a privacy framework containing policies and procedures relating to the privacy of personal information address data classification, record management, retention and destruction, that is also aligned with the PDPL regulations established by the government, as well as implemented technical solutions to set different permission levels for employees based on what PII they need to access, such as public, private, and restricted access.
Technology	Resilience following disaster, crisis or events impacting business continuity In the rapidly evolving landscape of telecommunications sector, stc's network has faced unprecedented demand surges, compelling us to confront the specter of partial or complete service interruptions. The resilience of Information and Communication Technology (ICT) services is pivotal to maintaining its operational integrity and is, consequently, a focal point of its risk mitigation strategies. The potential for network disruptions stemming from failures within telecom networks poses a persistent challenge that demands its undivided attention and proactive solutions to ensure business continuity and provide reliable services to our customers.	stc has established entity-wide written programs that address and validate the continuity of the institution's mission-critical operations. It has recertified the organization against ISO 22301:2019 and taken all required steps to comply with any relevant regulatory requirements. stc has worked on additional projects to strengthen disaster recovery (DR) systems to ensure business and services continuity, taking into account various possibilities. The Emergency Response team oversees major contingency planning work and periodically conducts virtual experiments. Additionally, stc intends to work closely with the National Emergency Management Authority (NEMA) recently established to ensure resiliency of the Kingdom.
Legal and compliance	Unfavorable regulatory changes impacting its current business model Regulations over its current obligations are increasing, both in number, frequency and impact, and are evolving in their nature. The potential impact of these new regulations could have serious negative implications for stc's profitability, market position and include penalties or financial liabilities.	stc studies the regulatory legislation on an ongoing basis, coordinates efforts with sectors related to it, inside and outside stc, and applies the best standards to ensure the provision of the best services to its clients in a manner that achieves the objectives of the national plans. A dedicated administrative structure is established for the regulatory affairs sector to contribute to enhancing stc's capabilities in the regulatory field.
Operational	Supply chain disruptions Material shortages and supply risks to rare earth minerals and other key components for chip manufacturing may have far-reaching consequences for continued stc technology leadership, including its ability to provide essential services and next-generation mobility, and to meet the demands of infrastructure projects upon which it has engaged.	stc diversifies its supply chains so that it does not depend on limited numbers of suppliers, and it emphasizes in its contracts that the systems are compatible with each other regardless of the supplier. It also reviews the conditions of contracted companies and sets legislation to ensure their financial and operational suitability for stc's requirements, in line with technological development and the integrity of their business plans. Additionally, stc keeps track of the geopolitical aspect ensuring it stays ahead of predicting and supply chain disruptions due to such reasons.
Corporate	Strategy implementation in a dynamic market In order to succeed in this highly competitive and dynamic environment, it is essential to have agile strategic development, maintenance and implementation processes capable of providing stc with a strategy for success and carrying sufficient agility to meet the demands on the markets in which it operates.	stc's strategy is updated on a 3-year basis and refreshed annually to ensure it remains current and relevant for the labor market. The timing of the annual refresh and 3-year updates is flexible in line with context, dynamics and stakeholders' inputs. It has also conducted a 360-degree environmental scan (i.e. competition, industry trends, regulation, socio-economic and stc performance). ERM sector has developed its own 3-year strategy, which is aligned with stc's strategy to support achieving all strategic objectives.

Risk Management continued

Financial risk management

Credit risk management

stc has approved guidelines and policies that allow it to only deal with creditworthy counterparties and limits counterparty exposure. The guidelines and policies allow stc to invest only with those counterparties that high have investment grade credit ratings issued by international credit rating agencies and limits the exposure to a single counterparty by stipulation that the exposure should not exceed 30% of the counterparty’s shareholders’ equity. Further, stc’s credit risk is monitored on a quarterly basis.

Other than the concentration of credit risk disclosed in Note 18 in the consolidated annual financial statements, concentration of credit risk with respect to trade receivables is limited given that stc’s customers consist of a large number of unrelated customers. Payment terms and credit limits are set in accordance with industry norms.

Ongoing evaluation is performed on the financial condition of trade receivables, and management believes there is no further credit risk provision required in excess of the normal provision for impairment loss (for more details, see note 18 in the consolidated annual financial statements).

In addition, stc is exposed to credit risk in relation to financial guarantees given to some subsidiaries with regard to financing arrangements. stc’s maximum exposure in this respect is the maximum amount stc may have to pay if the guarantee is called on. There is no indication that stc will incur any loss with respect to its financial guarantees as the date of the preparation of these consolidated financial statements (for more details, see note 45 in the consolidated annual financial statements).

Cash balances and short term investments are deposited in banks with credit rating ranging from Baa1 and above, while investments made with local banks had an investment grade credit rating of Baa3 and above.

The credit rating of the Company’s investments in government Sukuk and Binariang GSM Sdn Bhd (“BGSM”) Sukuk are A and Aa3, respectively as at 31 December 2024 (2023: A and Aa3, respectively) (for more details, see note 16.1 in the consolidated annual financial statements).

The carrying value of financial assets represent the maximum exposure to credit risk.

Foreign currency risk management

Saudi Riyal is considered as the functional currency of stc which is pegged against the United States Dollar. Therefore, stc is only exposed to exchange rate fluctuations from transactions denominated in foreign currencies other than United States dollar. The fluctuation in exchange rates against currencies, which are not pegged with Saudi Riyal, are monitored on a continuous basis and risk is assessed via the Value-at-Risk (VaR) measure. stc’s exposure to foreign currency changes for all other currencies is not material. The sensitivity of the changes of SAR/EUR exchange rates by 1% would have impacted equity by ₪ 25 million (2023: ₪ 88 million).

Liquidity risk management

stc has established a comprehensive liquidity risk management framework for the management of stc’s short, medium and long-term funding and liquidity requirements under the approved guidelines.

stc ensures its liquidity by maintaining cash reserves, short-term investments and committed undrawn credit facilities with high credit rated local and international banks. stc determines its liquidity requirements by continuously monitoring short and long-term cash forecasts in comparison to actual cash flows.

Liquidity is reviewed periodically for stc and stress tested using various assumptions relating to capital expenditure, dividends, trade receivable collections and repayment of loans without refinancing (for more details, see note 6-43 in the consolidated annual financial statements).

Profit rate risk

stc’s main profit rate risk arises from borrowings with variable profit margin rates.

The sensitivity analyses below have been determined based on the exposure to profit rates for non-derivative instruments at the end of the financial year. These analyses show the effects of changes in market profit rates on profit and loss. For floating rate liabilities, the analysis is prepared assuming the amounts outstanding at the end of the year were outstanding for the whole year. A 100-basis point increase or (decrease) represents management’s assessment of the reasonably possible change in profit rates. If profit rates had been 100 basis points higher (lower) and all other variables were held constant, the impact on the profit of stc would have been higher (lower) by ₪ 26 million (2023: the impact on the profit of stc would have been higher (lower) by ₪ 155 million). This hypothetical effect on profit of stc primarily arises from potential effect of variable profit financial liabilities.

stc periodically monitors the impact of the incremental changes in profit rates and assesses the impact on stc’s profitability.

Market risk

Market risk is the risk that the fair value or future cash flows of a financial instrument will fluctuate because of changes in market prices. Market risk comprises different types of risk: interest rate risk, currency risk and price risk. Financial instruments affected by market risk include loans and borrowings, deposits, debt and equity.

stc is exposed to changes in the value of equity investments and derivatives associated with such investments. To reduce the risk associated with variations in fair value and share price, stc acquires derivative instruments that hedge the risk profile of such investments.

The hedge ratio for each designation is established by comparing the quantity of the hedging instrument and the quantity of the hedged item to determine their relative weighting; for Group’s existing hedge relationships, the hedge ratio has been determined as 1:1.

Hedge effectiveness is determined at the inception of the hedge relationship and through periodic prospective effectiveness assessments to ensure that an economic relationship exists between the hedged item and hedging instrument. To test the hedge effectiveness, stc compares the changes in the fair value of the hedging instrument against the changes in fair value of the hedged item attributable to the hedged risk.

The hedge ineffectiveness can arise from a change in the credit risk of the counterparty with the hedging instrument.

Fair value of financial instruments

stc uses valuation techniques appropriate to current circumstances that provide sufficient data to measure fair value. In addition for financial reporting purposes, fair value measurements are categorized into Level 1, 2 or 3 based on the degree to which the inputs to the fair value measurements are observable and the significance of the inputs to the fair value measurement in its entirety (for more details, see note 20-4 in the consolidated annual financial statements).

The fair values of financial instruments represented in trade and other receivables, short-term murabaha, cash and cash equivalents, and trade and other credit payables closely approximate their book value due to their short maturity (for more details, see note 2-43 in the consolidated annual financial statements).

Capital management

stc manages its capital, which includes share capital, statutory reserves, other reserves and retained earnings attributable to the equity holders of the parent company, to ensure that:

- It will be able to operate as a going concern.
- It efficiently finances its working capital and strategic investment requirements at optimal terms.
- It provides a long-term dividend policy and maintains a stable dividend pay-out.
- It maximizes the total return to its shareholders.
- It maintains an appropriate mix of debt and equity capital.

Risk Management continued

stc reviews its capital structure in light of strategic investment decisions, changing economic environment, and assesses the impact of these changes on cost of capital and risk associated to capital.

stc is not subject to any externally imposed capital requirements. stc did not introduce any amendments to the capital management objectives and procedures during the year ended 31 December 2024.

stc reviews the capital structure on an annual basis to evaluate the cost of capital and the risks associated with capital (for more details, see note 1-43 in the consolidated annual financial statements).

Compliance

stc is committed to fostering a culture of compliance across the organization. This is achieved through a comprehensive compliance program, led by experts and supported by integrated policies and technology, ensuring consistent adherence to regulatory standards and best practices.

stc’s compliance program is built on strong governance principles, ensuring the independence and effectiveness of the compliance sector. The sector engages with two key committees – the Audit Committee and the Risk and Compliance Committee – to maintain transparency and accountability in all operations. There is a constant effort to ensure stc’s compliance with all regulatory requirements, with periodic reports provided to the relevant committees.

Several strategic initiatives have been implemented to strengthen the compliance program, aligning stc with global best practices. These initiatives include the development of comprehensive policies and frameworks, alongside the continuous enhancement of integrated compliance risk management systems.

Aligned with stc’s digital transformation journey, an advanced digital model for compliance assurance is being adopted, leveraging process automation and innovative technologies to improve operational efficiency and transparency throughout the organization.

Efforts to unify compliance practices across stc are consolidated through the launch of specialized training programs aimed at developing professional skills and building a deeper understanding of regulatory requirements and ethical standards.

In its pursuit of excellence, stc is dedicated to advancing a culture of compliance through the ongoing enhancement of compliance programs, ensuring regulatory adherence, reinforcing internal monitoring frameworks, and prioritizing training and awareness initiatives across the organization.

Business integrity

stc has placed significant emphasis on promoting and instilling the values of integrity within the Company, earning the trust of its stakeholders. The Board of Directors adopted this initiative and strengthened it by implementing policies to combat fraud, corruption and financial crimes, making stc a pioneer in the telecommunications sector by adopting financial crime prevention measures that were previously limited to banking and financial institutions. stc recognized the need to allocate and support the General Department of Business Integrity with these specializations, and improved communication with regulatory authorities and law enforcement agencies by fostering an effective partnership with the Anti-Corruption Authority, “Nazaha” and the General Court of Audit.

stc has devolved the General Department of Business Integrity to include the following departments:

- Whistleblowing Department
- Anti-Fraud and Corruption Department
- Anti-Financial Crimes Department
- Forensic Department
- Investigations Department

stc established a dynamic integration process among these departments to achieve the desired goals and adopted a strategy focused on task automating and greater reliance more on advanced quantitative and data analysis techniques. By identifying unusual transactions patterns, advanced technologies are enabled to detect and prevent unusual activities, subjecting them to further analysis using artificial intelligence. This approach provides decision-makers with comprehensive data to support critical decisions and activates the first lines of defense, ensuring they are the first to address potential threats.

In this context, stc has completed the installation of a case management platform and provided various reporting channels for whistleblowers, accessible to employees and business partners involved in stc projects, which reinforces the values of integrity and responsibility.

In the area of anti-fraud and corruption awareness, stc has held number of courses, seminars and workshops in collaboration with the Anti-Corruption Authority “Nazaha”, these efforts had effectively educated employees about prohibited practices, raised awareness of their risk and emphasized the importance of reporting them.

Regarding digital detection, stc invested in automated systems that enable proactive prevention by leveraging machine learning and artificial intelligence technologies to perform advanced analysis and make predictions based on data inputs.

In the field of analyzing digital evidence related to cases under investigation, this task has been assigned to the Forensic Department. This department has been equipped with the best human and logistical resources to carry out this role, relying on the latest best practices in digital and information investigation, including the Nuix system to assist in digital evidence examination processes.

In the area of fraud and corruption prevention, a partnership agreement was finalized with the Risk Sector to conduct fraud risk assessments and update the risk registry in a reciprocal process. The General Department of Business Integrity conducts in-depth analyses of the root causes of detected cases and coordinate efforts with various business sectors to develop corrective solutions that reduce such incidents and strengthen regulatory controls.

In combating financial crimes, including anti-money laundering and terrorist financing as well as sanction management. The General Department of Business Integrity supported this effort by deploying experts human and investing in a monitoring and detection platform, leveraging the stc’s rich data sources to enhance control measures and implement the “Know Your Customer” principle, ensuring the safety of the work environment, products and services safe, which positively impacts stc’s sustainability ratings.

The Investigations Department handles investigations into suspected cases with relevant parties in detected incidents, utilizing examination and analysis outputs supported by discovered evidence, after which it proceeds with issuing final reports and collaborating with internal entities, including Legal Affairs, to achieve best practices.

Additionally, stc has established a Business Integrity Committee to oversee the General Department’s operations, provide the necessary support to achieve its objectives, address challenges and submit reports to the Group CEO and the Board’s Audit Committee.