Risk management

The telecommunications sector continues to undergo a structural shift, with demand for traditional voice services maturing while data traffic and digital usage grow at pace. This evolution is supported by accelerating adoption of advanced connectivity, cloud-enabled services and digital platforms, which is reshaping customer expectations and business models and increasing the need for continuous innovation across the industry.

In an increasingly competitive market, differentiation depends on delivering reliable connectivity, compelling digital services, and seamless customer experiences. At the same time, sustained investment in resilient infrastructure, strong data protection, and consistent compliance with regulatory requirements remain essential. stc group's enterprise risk management (ERM) is embedded in its strategic framework, informing planning and performance evaluation and integrating risk considerations into key decisions to protect value, support disciplined execution, and enhance long term resilience.

At the forefront of stc group's commitment to trust and integrity, the Board of Directors provides active sponsorship and oversight of privacy and data security initiatives. This governance helps ensure that risk informed strategies, effective controls, and ongoing assurance practices protect stakeholders and reinforce stc group's position as a trusted leader in responsible data management.

Enterprise risk management

Enterprise risk management governance

The Board of Directors is committed to maintaining strong corporate governance through ongoing review of relevant best practices and their appropriate implementation. The Board Risk Committee provides dedicated oversight of the enterprise risk management framework, related strategies and policies and the effectiveness of stc group's risk management system. As part of its mandate, the Committee reviews stc group's risk families across a wide range of exposures, assesses the principal risks and evaluates management's approach to monitoring, controls and risk treatment.

During the year, stc group further elevated and enhanced its risk appetite to ensure it remains aligned with stc group strategic direction and decision making. The updated approach strengthens consistency across stc group by cascading risk appetite principles and metrics to subsidiaries and enabling a consolidated group view of risk capacity and tolerance. This supports clearer accountability, more consistent risk-based decisions and improved oversight across stc group and its subsidiaries.

The risk management function operates independently of business groups and sectors and continues to refine its strategic roadmap in line with the Board approved risk strategy, strengthening capabilities and advancing risk management maturity across stc group.

stc group risk appetite

	L2 risk category		stc group risk attitude	Type of cascade
Corporate risk	1.1	Governance	Averse	Direct cascade
	1.2	Strategy	Neutral	Direct cascade
	1.3	Program management	Neutral	Direct cascade
	1.4	Planning and resource allocation	Neutral	Flexibility permitted
	1.5	Major initiatives	Seeking	Direct cascade
	1.6	Mergers, acquisition and divestiture	Neutral	Direct cascade
	1.7	Market dynamics	Neutral	Flexibility permitted
	1.8	Communication and investor relations	Neutral	Direct cascade

	L2 risk category		stc group risk attitude	Type of cascade
Operational risk	2.1	Service delivery	Averse	Direct cascade
	2.2	Sales and marketing	Tolerant	Flexibility permitted
	2.3	Supply chain	Averse	Direct cascade
	2.4	People/human resources	Neutral	Flexibility permitted
	2.5	Revenue management	Neutral	Flexibility permitted
	2.6	Physical assets	Neutral	Flexibility permitted
	2.7	Intangible assets	Neutral	Flexibility permitted
	2.8	Project management	Neutral	Flexibility permitted
	2.9	Business continuity	Averse	Direct cascade
	2.10	Health and safety	Intolerance	Direct cascade

	L2 risk category		stc group risk attitude	Type of cascade
Technology risk	3.1	Information technology	Neutral	Direct cascade
	3.2	Network operations	Averse	Direct cascade
	3.3	Cybersecurity	Averse	Direct cascade
	3.4	Data privacy	Intolerance	Direct cascade
	3.5	Data integrity	Intolerance	Direct cascade
	3.6	Artificial intelligence	Averse	Direct cascade

	L2 risk category		stc group risk attitude	Type of cascade
Legal risk	5.1	Corporate compliance	Intolerance	Direct cascade
	5.2	Legal	Intolerance	Direct cascade
	5.3	Regulatory	Averse	Direct cascade

	L2 risk category		stc group risk attitude	Type of cascade
Financial risk	4.1	Market	Tolerant	Flexibility permitted
	4.2	Liquidity	Neutral	Flexibility permitted
	4.3	Foreign exchange	Tolerant	Flexibility permitted
	4.4	Interest rate	Tolerant	Flexibility permitted
	4.5	Investments	Seeking	Flexibility permitted
	4.6	Credit	Neutral	Flexibility permitted
	4.7	Accounting and reporting	Intolerance	Direct cascade
	4.8	Tax and zakat	Averse	Direct cascade
	4.9	Capital structure	Neutral	Flexibility permitted
	4.10	Fraud	Intolerance	Direct cascade
	4.11	Revenue leakage	Neutral	Flexibility permitted

stc group risk attitude

- Intolerance
- Tolerant
- Averse
- Seeking
- Neutral

Type of cascade

- Direct cascade
- Flexibility permitted

Risk management continued

Enterprise risk management framework

The ERM framework defines the principles and governance that guide proactive risk management across stc group through a comprehensive and dynamic approach. It enables stc group to identify, assess, prioritize and manage risks consistently across operations, supporting a holistic view of risk and enabling meaningful comparisons that inform decision making and delivery of strategic objectives.

Quarterly risk assessments are a core part of the cycle, underpinned by clear roles and responsibilities and a consistent end to end process for risk identification, evaluation, treatment and reporting. The methodology and key steps of stc group's ERM process are illustrated below.

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 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	40%-59%
2	Unlikely	Once in 2 years	5%-39%
1	Remote	Once in 4 years or more	Less than 5%

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 assist 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

Risk management continued

stc group continues to enhance risk visibility and responsiveness by strengthening data driven detection and better understanding interconnected risks. ISO 31000 attestation reinforces alignment with recognized practices. A standardized risk scoring methodology supports consistent evaluation and reporting, enabling consolidated results and clearer identification of stc group's principal risks and uncertainties.

To ensure comprehensive coverage, stc group structures its risk universe into risk families that capture the full range of exposures across stc group. These families provide a consistent way to categorize risks across five core domains and their related sub-families, supporting clear ownership, oversight and aggregation of risk information. The risk families and sub-families are illustrated below.

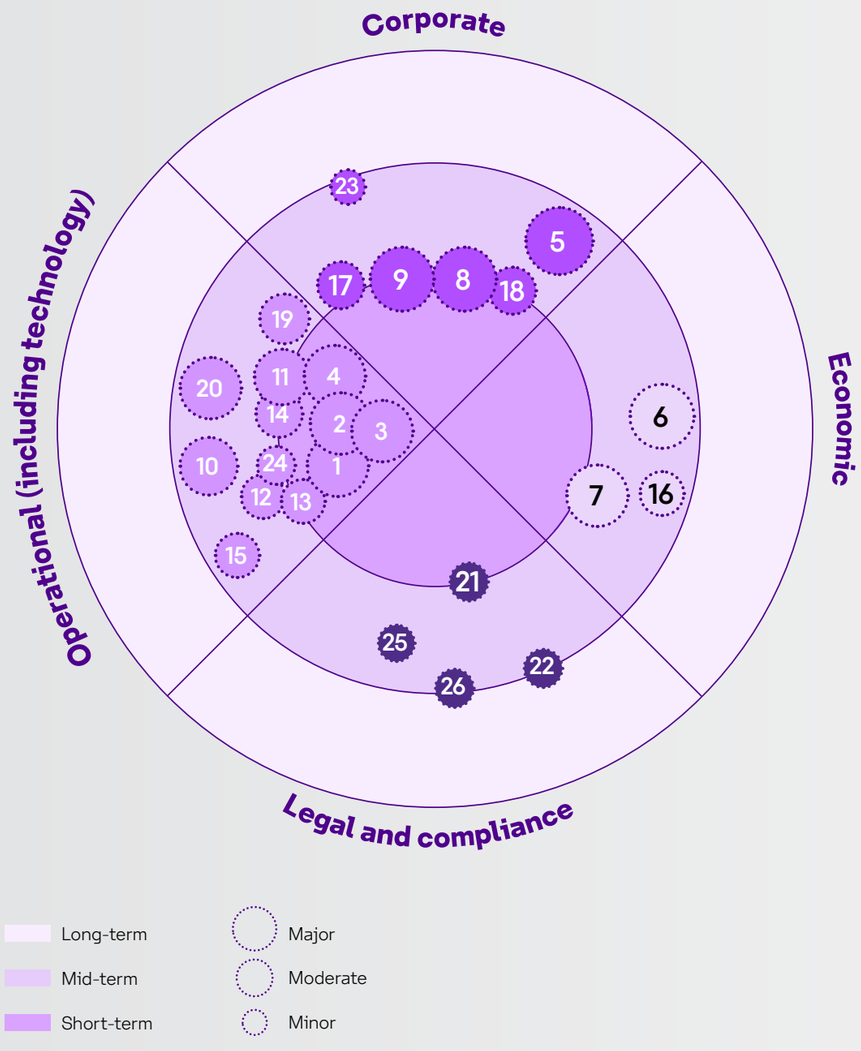
The risk categories classify all risk source types that could affect stc group into five main silos known as category 1 risks. For easier management and communication, category 1 risks are broken down into category 2 risk types and, in some instances, these are further sub-divided into category 3 and 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

Emerging risks are addressed through the risk assessment process and identified through horizon scanning, ongoing engagement with the business and monitoring market and industry developments. A summary of emerging risks is presented to the Board Risk Committee and the Board for review, and these risks are monitored on an ongoing basis through established risk management processes.

Global emerging risk landscape



No.	Category	Name
1	Major	Cyber security heterogeneous landscape
2	Major	Autonomous AI-powered attacks
3	Major	AI-powered disinformation and deepfake
4	Major	Shadow AI-agents
5	Major	Domain-specific language models (DSLMs)
6	Major	Economic slowdown and credit tightening
7	Major	Digital currency and currency valuation
8	Major	International tensions and economic relations
9	Major	Supply chain interruption
10	Major	In-orbit data centers and global connectivity
11	Major	Direct to device satellite connectivity
12	Moderate	Smart city IoT distributed denial of service (DDoS) surges
13	Moderate	5G network slicing

No.	Category	Name
14	Moderate	6G and next-gen spectrum
15	Moderate	AI-RAN and network automation reliability
16	Moderate	Capital requirements for network infrastructure
17	Moderate	Data center power scarcity
18	Moderate	Talent scarcity in telco and AI-skills
19	Moderate	Environmental interface climate events
20	Major	Post-quantum cryptography
21	Minor	5G coverage and performance
22	Minor	Disputes over spectrum access, pricing and deployment
23	Minor	Growth of private computing
24	Minor	Wafer-scale and analog AI chip disruption
25	Minor	Stringent national and trans-national regulations
26	Minor	Expansion of sovereign control

Corporate Operational Economic Legal and Compliance

This year, stc group placed greater emphasis on sustainability and adopting the GSMA humanitarian connectivity charter (HCC), 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 group's broader risk management framework and strategic decision-making processes.

Risk management continued

Identifying risks

All stc group entities identify and assess risks that could affect strategy and operations. These inputs are consolidated and presented to senior leadership alongside outputs from external environmental scanning and relevant benchmarks.

Taking a Group wide view, executives evaluate the consolidated risk landscape to determine critical risks and identify emerging threats that warrant further analysis. The resulting set of risks is reviewed and agreed by the Risk Management and Compliance Committee, then submitted to the Board Risk Committee and the Board for final review and approval.

Managing risks

Understanding the environment in which it operates is central to stc group's risk management approach. Accordingly, stc group classifies each risk across defined categories such as corporate, technology, operational, financial, and compliance, and determines whether key drivers are internal or external. This structure supports consistent evaluation, appropriate treatment, and the right level of oversight and assurance.

Executive risk owners are accountable for maintaining effective controls and implementing treatment plans to keep risks within approved tolerance levels. Progress is monitored throughout the year through ongoing tracking and in-depth risk reviews. For the most significant risks, stc group also develops scenario assessments to provide additional insight into potential developments and to strengthen risk treatment strategies.

stc group has also integrated loss management within business continuity management by introducing a framework that consolidates operational, financial, and technology loss information into a single view. This enables earlier detection, standardized reporting, and structured analysis of loss events, supporting clearer root cause identification and targeted corrective actions. The framework is designed to strengthen controls, reduce recurrence, improve response effectiveness, and protect organizational value.

Monitoring risks

stc group prepares a quarterly risk report presenting the principal risks for submission to the Board of Directors, with the Board Risk Committee reviewing it as part of its regular agenda. Emerging risks are presented annually within the risk reporting cycle. This supports transparent monitoring of individual risk developments and the overall risk profile and provides timely updates on material changes and enhancements to the risk management system.

To further strengthen risk supervision and decision-making, stc group continues to enhance its risk management technology tools to improve more effective reporting, analysis, assessment and management of risk information. In parallel, stc group has refined its key risk indicators (KRI) to improve risk monitoring, support earlier detection of changes in exposure and enable more proactive risk management.

As part of elevating its monitoring capabilities, stc group has launched an enhanced risk management system that brings together a wide range of models and features to support greater automation and consistency across the ERM function. The platform is designed to strengthen end-to-end risk processes by enabling streamlined risk assessments, structured capture and tracking of KRIs, risk control self-assessment activities and standardized management reporting. This supports improved timeliness, data quality and transparency, while enabling more efficient analysis and oversight of risk information across stc group.

Risk management continued

Risk mindset and culture

stc group promotes a set of behaviors and expectations that embed risk awareness across day-to-day business activities. This is driven by tone from the top and reinforced through people management systems, encouraging timely and proportionate risk interventions that support operational integrity and informed decision making. Expected behaviors are communicated consistently to colleagues to integrate risk awareness into the Group's culture. This is supported by ongoing training and communications, defined roles and responsibilities, and the continuous integration of risk management practices into key decision-making processes.

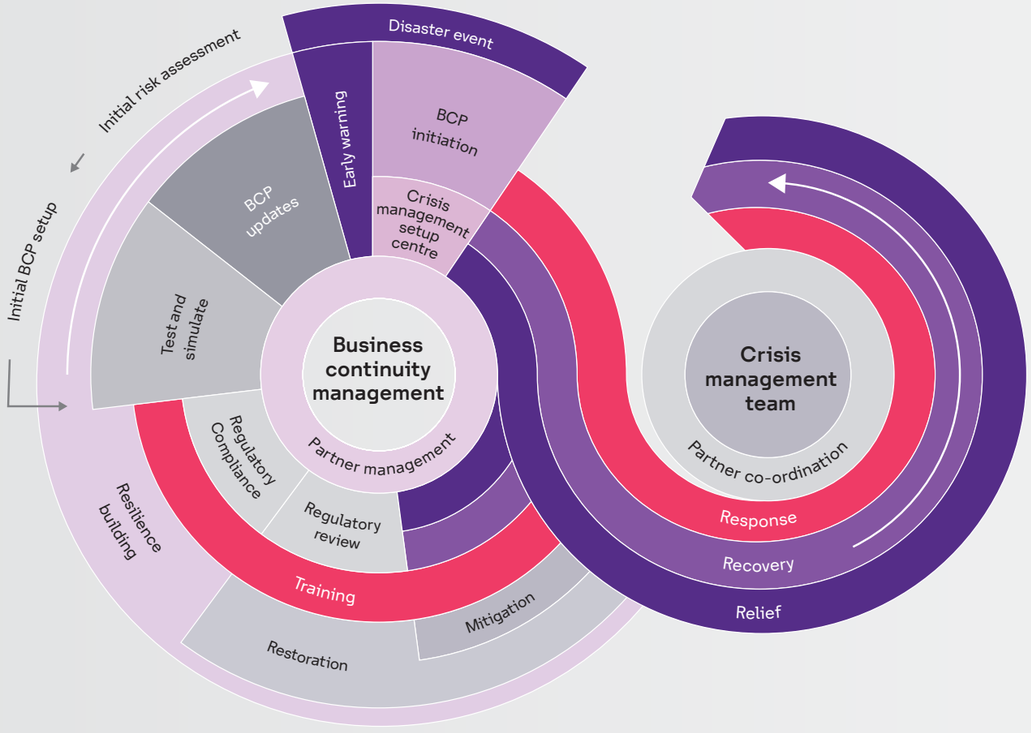
During the year, more than 1,000 colleagues participated in crisis and continuity workshops and supporting awareness initiatives, and stc group plans to sustain an annual cadence of workshops integrated with leadership and talent development programs. In collaboration with the Ministry of Communications and Information Technology, stc group delivered business continuity and risk management training for technology sector professionals to support resilience across the digital ecosystem. stc group also strengthened its control environment through training on internal controls.

Business continuity

At stc group, business continuity management (BCM) is a core part of how stc group protect service reliability, operational integrity and stakeholder trust, supporting the Kingdom's digital resilience and Vision 2030 objectives. stc group's BCM system is aligned with relevant national directives and regulatory expectations, including those issued by the NRC, CST and NEMA, and is designed to anticipate and manage disruption while safeguarding critical services, people and assets. stc group maintained ISO 22301 certification, reinforcing alignment with recognized best practices through regular testing and exercises to validate readiness and recovery capabilities. The resilience model applies clear decision rights and structured escalation to enable timely response and coordinated recovery. A dedicated crisis communications plan supports consistent, transparent engagement with employees, regulators, customers and partners and is periodically reviewed and tested to maintain effectiveness.

Enterprise governance in business continuity and crisis management

stc group operates under a mature governance structure led by a dedicated Crisis Management Organization, Business Recovery Team, Technical Recovery Team and Emergency Response Team. This structure supports the rapid restoration of services, the safeguarding of lives and assets and the continued operability of critical technology systems under adverse conditions. The tiered model provides holistic oversight and clear lines of authority for managing physical, cyber and operational threats across the enterprise. Policies are aligned with global best practice frameworks for BCM, including ISO 22301 for Business Continuity, ISO 22320 for Emergency Management, ISO 27031 for ICT Readiness for Business continuity and ISO 22361 for Crisis Management. This alignment is reviewed continuously to ensure compliance with local and international standards. In addition, each sector within stc group maintains detailed Business Continuity Plans validated through a rigorous testing program, including simulation exercises, technical failover testing and tabletop crisis drills, to ensure business critical functions from customer care to the network control center can operate during emergencies.



Preparation (pre-disaster): This is where data concerning identified disaster scenarios is gathered and based on the output of the analysis of the data relevant plans are drawn up (such as BCP).

Response (post-disaster): This is triggered by the disaster, the conditions for triggering a response are one of the areas which need to be pre-agreed in the preparation along with degrees of severity so that affected organizations like MNOs can map and initiate the relevant action plans (from the BCP) to the scenario.

Recovery (post-disaster): This phase follows on from the initial response phase and looks to rebuild any damage infrastructure, capacity, processes, skills, etc., back to the point they were prior to the disaster (or better). It is often hard to define an obvious transition point from response to recovery.

Mitigation (post/pre-disaster): This is where learnings from the disaster are taken to update infrastructure, processes, etc. to not just improve the business but also increase resilience to future disasters thus adding to a higher level of protection for the business. This will often be tied to national objectives, programs and regulation looking to improve resilience to future events.

Risk management continued

Integrated national response and readiness model

stc group is embedded within the Kingdom's national emergency readiness model and regularly aligns disaster preparedness protocols with national regulatory authorities; chief among them the Communications, Space and Technology Commission. Disaster playbooks are designed to support coordinated response and resource deployment during major events. In support of national public safety, stc group's network is configured to support the national early warning system by using cell broadcast service, as mandated by the Communications, Space and Technology Commission, to disseminate geo-targeted alerts to the public without congesting mobile networks. stc group's network also supports Advanced Mobile Location (AML), which automatically provides precise location data from a caller's handset directly to emergency services to reduce response times. Teams remain on standby to assist with reconnecting remote locations and responding to extreme surges in network usage during major national events, including the Hajj pilgrimage.

Human life and asset protection as a strategic priority

stc group regards communication as a critical lifeline in times of crisis. Protocols are designed not only to restore technical operations, but also to help ensure families can reach one another, first responders can coordinate rescue missions, and critical national infrastructure such as hospitals, airports and government institutions remain connected. stc group proactively deploys field engineers to risk prone areas to inspect and reinforce equipment, and is prepared to install temporary mobile base stations and satellite uplinks to maintain service. Monitoring centers, including the security operations center, the network operation center and the business continuity cell, provide 24/7 surveillance using real-time analytics to detect degradation, intrusion or anomalies across infrastructure.

Tactical field response and proactive resilience

stc group's tactical field response is underpinned by a continued commitment to preparedness and resilience. Investment focuses on strengthening network infrastructure, including building redundancies, installing backup power supplies and generators at cell sites and maintaining rigorous cybersecurity protocols. This supports rapid service restoration. Network disaster recovery plans are regularly tested and portable network assets are pre-positioned alongside a fleet of emergency mobile base stations, including cells on wheels and cells on light trucks, with teams on standby for immediate deployment. These truck mounted mobile towers can be dispatched within hours and are self-sufficient, using satellite backhaul connectivity to restore mobile and data services rapidly, including where terrestrial fiber links are affected. Preparedness is reinforced through regular emergency drills and tabletop exercises so crisis management, technical and customer service teams are trained to respond effectively. Customer awareness campaigns are also used to support readiness, such as guidance on maintaining battery life or accessing emergency alerts.

stc group maintains collaboration with government agencies such as Saudi Civil Defense and relevant humanitarian organizations to integrate support with broader response efforts. The approach is supported by continuous improvement to anticipate emerging risks and explore innovations such as advanced early warning capabilities and satellite enabled coverage.

Scenario training and team level resilience building

To maintain a high level of preparedness, stc group conducts frequent scenario-based training and simulations. As recommended by the GSM association, these drills help ensure plans remain fit for purpose and that teams understand their roles in high-pressure environments. The drill program includes simulations of data center outages with restoration service level agreements, complex cyberattack scenarios involving multiple service platforms and simulations of critical application outages. Each training cycle encompasses real-time coordination between executive crisis response teams, customer care escalation leads, regional engineering units and external stakeholders. stc group also conducts multi agency simulations with emergency agencies and infrastructure regulators to support a unified national response capability.

Corporate social responsibility during crises

stc group's crisis response framework is anchored in a commitment to social responsibility, aligned with the GSMA humanitarian connectivity charter, which treats connectivity as a vital form of humanitarian support. During disruptive events, the objective is to preserve the digital lifeline for those most at risk. stc group prioritizes network uptime and quality of service for first responders, healthcare facilities and civil defense agencies, deploying temporary cellular assets where needed. Access to national emergency numbers is maintained as universally available and free, enabling customers to reach emergency services or family without barriers.

Recognizing that crises can create immediate economic strain, stc group may activate financial relief protocols to support customers, including the suspension of billing and collection activities, the waiver of late fees and the provision of emergency voice and data packages to impacted areas. Where appropriate, stc group is also prepared to support access to critical national services, including government emergency portals, health applications and remote learning platforms to help ensure essential information remains accessible.

Beyond network operations, stc group may extend support through physical and logistical assistance, including emergency connectivity solutions such as free public Wi-Fi hotspots and portable charging hubs at critical locations such as shelters and hospitals. Working with national humanitarian agencies, stc group can facilitate community support through trusted SMS text to donate campaigns. Throughout disruptive events, stc group provides proactive updates on network status and restoration efforts to support transparency, manage expectations and maintain trust.

Internal control

The Board of Directors maintains an unwavering commitment to a robust system of internal control, recognizing it as the bedrock of stc group's operational resilience and strategic success. By adhering to the globally recognized COSO Internal Control Integrated Framework, the Group ensures its governance structures are not merely compliant, but are designed to drive operational efficiency, safeguard assets and guarantee the absolute integrity of financial reporting. While acknowledging inherent limitations, this sophisticated framework provides stakeholders with reasonable assurance regarding the mitigation of material risks.

Following a year of rigorous self-assessments and a professional opinion from an independent accounting and consultancy firm providing assurance and advisory services and comply with related requirements for conducting assurance services, the Board confirms that stc group's internal controls were effectively implemented and operating robustly as of year-end, with no material weaknesses identified that could compromise stc group's financial standing or continuity.

The Audit Committee exercises active and vigilant oversight over this control environment, serving as a critical bridge between Executive Management and the Board. In fiscal year 2025, the Committee deepened its engagement through eight focused sessions, scrutinizing high-impact areas, including financial reporting integrity, investment portfolio health, strategic organizational developments and the resilience of IT infrastructure. These deliberations were supported by direct dialogue with Executive Management and the Internal Audit team, ensuring stc group's control mechanisms remain agile and responsive to emerging global trends and industry-specific challenges. This rigorous oversight model provides shareholders with confidence that the governance bodies are actively challenging management to maintain the highest standards of control.

Risk management continued

Throughout the year, the Internal Control function transitioned the organization from reactive compliance to proactive risk intelligence. By executing comprehensive risk and control self-assessments (RCSA) across all critical business units, stc group successfully embedded risk ownership into the first line of defense, ensuring potential threats are identified and mitigated at the source. This was validated by an independent internal control review (ICR) program, which confirmed the design and operating effectiveness of key controls. Crucially, management demonstrated exceptional responsiveness in addressing identified opportunities for improvement, maintaining a high velocity of remediation that aligns strictly with stc group's risk appetite. This proactive stance signals to stakeholders that stc group is capable of navigating complex operational landscapes with minimal disruption.

Enterprise risk management highlights

Over the past year, stc group advanced its risk management capabilities to support resilience and informed decision making. A key milestone was the review and re assessment of stc group's risk appetite to ensure alignment with strategic priorities and provide a clearer basis for governing risk taking activities.

stc group also strengthened oversight by introducing automated monitoring indicators across key risks, improving visibility and enabling more proactive management. In addition, stc group attained ISO 31000 certification for enterprise risk management and ISO 27001 certification for information security, reinforcing alignment with recognized practices.

To further embed a strong risk culture, stc group delivered training and awareness initiatives across the organization, supporting improved accountability. stc group also continued to broaden risk coverage, strengthen controls and enhance mitigation strategies to address a dynamic risk environment.

Principle risks

As a leading telecommunications and information technology group, stc group operates in a fast-changing environment with inherent uncertainty. Sustained performance depends on proactively anticipating developments and systematically identifying, assessing and managing related risks and opportunities. stc group considers effective risk and opportunity management an integral part of value focused corporate governance. Risks are evaluated and categorized across corporate, technology, operational, financial and compliance domains, supporting clearer understanding and proportionate oversight and assurance.

The principal risks remain broadly consistent with the prior year, with some additional risks identified and minor refinements to existing ones. Material risks, including environmental and social exposures, are summarized in the following table, together with the approaches used to manage them. The process continues to emphasize the most significant entity level risks, reflecting ongoing operating conditions. As the below will reflect what are the top risks that the organization are monitoring based on management reports.

Risk management continued

Category	Risks	Mitigation measures
Technology	**Cybersecurity threats** stc group operates in an environment of evolving cyber threats, including ransomware, malware, distributed denial-of-service attacks, credential theft, and social engineering, which may target stc group, its customers, or third-party providers. Emerging technologies such as AI-enabled tools, and advances in computing including quantum computing, may increase the sophistication, speed, and scale of attacks. Over time, sufficiently capable quantum computers could weaken certain widely used public-key cryptographic methods that support secure communications, authentication, and data protection. This creates the risk that data encrypted today could be retained and decrypted in the future ("harvest now, decrypt later"). Transitioning to quantum-resistant cryptography may require significant investment and coordination across stc group's systems and suppliers. A successful incident could disrupt services, compromise data, increase costs, and harm confidence and reputation.	stc group strengthens cybersecurity through a dedicated security unit, clear accountability, and continual enhancement of policies and controls. Capabilities span prevention, detection, response, and recovery, supported by centralized monitoring and incident management. Control effectiveness is validated through assurance activities, vulnerability management, and penetration testing, including oversight of key third-parties. Awareness programs reinforce secure behaviors. stc group also advances readiness for new computing developments through cryptography reviews and planning for transition to quantum resilient approaches where appropriate. Threat intelligence informs control priorities.
Technology	**Data privacy** stc group manages significant volumes of customer and business information across multiple systems, channels, and partners. Regulatory requirements and customer expectations for lawful processing, confidentiality, retention, cross border transfers, and third-party sharing continue to evolve. As data ecosystems become more complex, strong governance, including clear accountability, disciplined approvals, well configured access controls, and ongoing monitoring, helps reduce the likelihood of unauthorized access, leakage, or misuse. If a privacy incident or compliance gap were to occur, it could lead to regulatory engagement, remediation activities, contractual considerations, and reputational effects.	stc group manages privacy through an enterprise framework aligned with applicable requirements. Policies support data classification, retention, and secure handling, with defined ownership and approvals. Role based access controls and periodic reviews support least privilege, while monitoring helps identify unusual activity. Privacy by design is embedded in initiatives and partner engagements, supported by training and compliance oversight. Third-party sharing and cross border transfers are governed through assessments and contractual safeguards, with incident processes to support timely response and continuous improvement.
Operational	**Business continuity** Telecommunications services rely on resilient networks, core platforms and critical ICT infrastructure. Like other operators, stc group may from time-to-time experience service degradation or interruptions resulting from equipment or software issues, demand surges, power disruptions, physical incidents, reliance on third-parties or impacts to terrestrial and subsea connectivity. Extreme weather and other climate-related events can also influence network availability and restoration timelines. If such events occur, they may affect customer experience, revenues, operating costs and the ability to meet service obligations.	stc group maintains an entity-wide business continuity and disaster recovery program to support mission critical services. Resilience is enhanced through network redundancy, diversified routing, capacity planning, spares readiness and proactive monitoring. Recovery capabilities are validated through periodic exercises and testing, with lessons used to improve restoration performance. Dependencies on suppliers and partners are addressed through continuity expectations and coordinated response arrangements. The entity-wide written programs that address and validate the continuity of the institution's mission-critical operations is governed againststandards and regulatory requirements, including alignment with ISO 22301 and engagement with national stakeholders.
Compliance	**Regulations** stc group operates in a regulatory landscape that can evolve in scope, interpretation and enforcement. Obligations relating to spectrum, licensing, coverage, network performance, consumer protection, cybersecurity, data governance and reporting may require ongoing investment and refinement. Mandated targets for speed and coverage, together with spectrum pricing and potential new entrants can influence how capital is allocated between network expansion and new digital use cases. Government procurement and tendering frameworks promote transparency and value for money but can affect contract timing, pricing and revenue visibility, including at renewal.	stc group manages regulatory obligations through governance, ongoing monitoring of legislative developments and coordinated implementation across stc group. Engagement with regulators and stakeholders supports alignment with national objectives and expectations for licensing, spectrum, coverage, performance, consumer protection, cybersecurity and reporting. Compliance controls and assurance practices support transparency and audit readiness. Strategic and capital planning incorporate scenarios to maintain flexibility under changing requirements. Public procurement participation is supported by bid and contract governance to promote consistency, value delivery and continuity of service.

Category	Risks	Mitigation measures
Operational	**Supply chain** stc group sources network equipment, devices, software, spares and specialist services from a global supplier base. Industry-wide supply conditions can be influenced by factors such as geopolitical developments, trade requirements, transportation capacity, commodity and rare earth availability, semiconductor production and the level of concentration among key vendors. In addition, the resilience and cybersecurity practices of suppliers can affect product quality and operational reliability. Changes in availability or delivery schedules may require adjustments to project sequencing, procurement planning or cost assumptions, particularly for large scale programs and upgrades.	stc group supports continuity of supply through supplier governance that considers resilience, financial health, security assurance and performance. Procurement practices emphasize diversification and qualification of alternatives where feasible and encourage interoperability to reduce dependency on single vendors. Demand forecasting, inventory management and logistics planning support availability of critical equipment and spares. Contractual safeguards and service expectations are maintained for key suppliers. External developments, including geopolitical and market conditions, are monitored to inform contingency planning and support delivery of programs and upgrades.
Corporate	**Strategy** Telecommunications and digital markets are dynamic, influenced by technology developments, changing customer expectations and evolving competition. Demand patterns continue to shift, with some legacy services maturing while adjacent areas such as cloud, fintech, IoT, and digital platforms offer growth opportunities. These trends may require timely strategic choices, disciplined capital allocation and continued capability development. Competitive intensity can also be shaped by new entrants, global technology providers and emerging connectivity models such as satellite direct to device solutions, which may influence pricing, coverage economics and customer behavior. Some initiatives may be pursued through partnerships and joint ventures, which require clear governance and effective coordination.	stc group manages strategic and competitive dynamics through a structured planning cycle with periodic multi-year updates and annual refreshes. Market intelligence and scanning track technology trends, customer needs and competitive developments. Portfolio governance and capital allocation support balanced investment across core connectivity and adjacent digital opportunities. Execution is supported through program governance and performance monitoring. Partnerships and joint ventures are managed through clear decision rights, aligned objectives and oversight, supported by enterprise risk management to strengthen delivery discipline and agility.
Financial	**Credit and collections** stc group is exposed to credit, collection and liquidity risks linked to the timing and recoverability of receivables, billing matters, economic conditions and customer credit profiles, including large accounts. Payment patterns may vary over time and could influence cash flows, working capital and reported results.	stc group manages credit, collection and liquidity through governance that segments counterparties, monitors receivables and applies collection practices. Expected credit loss methodologies and provisioning use historical experience and forward-looking information, with reviews of key accounts. Billing matters are addressed through resolution and ongoing engagement. A significant portion of collections relates to government entities and is managed through established processes aligned to public sector requirements. Liquidity is supported through cash reserves, committed facilities and forecasting and stress testing to maintain resilience.
Technology	**Artificial intelligence (AI)** AI adoption can enhance customer experience, network operations and productivity, while requiring disciplined governance to manage associated considerations. Key areas include data quality, privacy, model reliability, fairness, cybersecurity, integration with existing systems and the need for ongoing monitoring and updates. Generative AI can also raise intellectual property and copyright considerations related to training data, third-party content and generated outputs, alongside evolving regulatory expectations. Increased automation may call for workforce planning, skills development and effective change management to support adoption.	stc group approaches AI adoption through governance that sets accountability and risk assessment for material use cases. Data governance and privacy controls support appropriate sourcing and use of information, while human oversight helps maintain reliability and fairness. Security controls cover access management and monitoring. Third-party solutions are subject to vendor due diligence and performance review. Legal and regulatory expectations, including intellectual property considerations, are monitored and reflected in policies. Training and change management support responsible adoption and value realization consistently.
Operational	**Human resources** stc group's performance and transformation are supported by its ability to attract, develop and retain skilled talent across telecommunications, technology, cybersecurity, data and digital businesses. Market demand for these capabilities continues to evolve and workforce expectations are changing, including for specialist and leadership roles. Growth in digital services and increased automation also require ongoing reskilling, succession planning and effective change management to sustain delivery. Variations in talent availability can influence the pace and cost of executing strategic programs and maintaining service quality.	stc group supports sustainable performance through workforce planning aligned with priorities across telecommunications, technology, cybersecurity, data and digital businesses. Talent development is reinforced through learning pathways, leadership programs and capability building, complemented by succession planning for critical roles. Engagement initiatives and rewards support attraction and retention. Reskilling and change management help enable new operating models and increased automation. Localization and capability building programs aligned with national priorities support a pipeline of skills and leadership depth, sustaining service quality and organizational resilience.

Risk management continued

Financial risk management

Credit risk management

stc group has approved guidelines and policies that allows it to only deal with creditworthy counterparties and limits counterparty exposure. The guidelines and policies allow stc group to invest only with those counterparties that have high 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 group 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 are limited given that stc group customer consists 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 contract assets. Management believes there is no further credit risk provision required in excess of the normal provision for impairment loss (for more details, see note 15,18 in the consolidated annual financial statements).

In addition, stc group is exposed to credit risk in relation to financial guarantees given to some subsidiaries with regard to financing arrangements. stc group maximum exposure in this respect is the maximum amount stc group may have to pay if the guarantee is called on. There is no indication that stc group 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 44 in the consolidated annual financial statements).

The majority of the stc group cash balances and short-term investments are deposited in: international banks with credit rating ranging from Baa1 and above and local banks with an investment grade credit rating of Baa3 and above.

The credit rating of the stc's investments in the Government Sukuk is Aa3 and A+ respectively from Moodys and Fitch as at 31 December 2025 (2024: Aa3 and A+), respectively (for more details, see note 16-1 in the consolidated annual financial statements). In addition, stc group has investment in BGSM Sukuk, which currently does not have a credit rating.

Foreign currency risk management

Saudi Riyal is considered as the functional currency of stc group which is pegged against the United States Dollar. Therefore, stc group 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. The sensitivity of the changes of ﷼ /EUR exchange rates by 1% would have impacted equity by ﷼ 22 million (2024: ﷼ 25 million).

Liquidity risk management

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

stc group ensures its liquidity by maintaining cash reserves, short-term investments and committed undrawn credit facilities with high credit rated local and international banks. stc group 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 group 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 42-6 in the consolidated annual financial statements).

Profit rate risk

stc group 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 group would have been (lower) higher by ﷼ 29 million (2024: the impact on the profit of stc group would have been (lower) higher by ﷼ 26 million). This hypothetical effect on profit of stc group primarily arises from potential effect of variable profit financial liabilities.

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

Equity price risk

stc group is exposed to changes in the fair value of equity investments and derivatives associated with such investments. To reduce the risk associated with variations in fair value and share price, stc group has acquired 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 stc group 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 group 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 group 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 4-20 in the consolidated annual financial statements).

The fair values of financial instruments represented in trade and other receivables, short-term murabahas, cash and cash equivalents from banking and non-banking operations, and trade and other credit payables closely approximate their book value due to their short maturity (for more details, see note 42-2 in the consolidated annual financial statements).

Capital management

stc group manages its capital which includes share capital, 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.

stc group 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 group is not subject to any externally imposed capital requirements. stc group did not introduce any amendments to the capital management objectives and procedures during the year 2025 and comparative year.

stc group 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 42-1 in the consolidated annual financial statements).

Risk management continued

Compliance

Toward a sustainable culture of compliance

stc group continues to foster a strong culture of compliance across its business ecosystem through a comprehensive program built on well-defined policies and compliance frameworks, supported by advanced digital technologies. This program aims to ensure continuous adherence to regulatory requirements, in alignment with globally recognized best practices.

stc group's compliance approach is founded on the principles of independence, transparency and integration with all relevant sectors/units and committees, ensuring:

- Clear definition of roles and effective policy implementation.
- Increased trust and accountability at all organizational levels.
- Ongoing coordination and periodic reporting to both the Board Audit Committee and the Risk Management and Compliance Committee, ensuring alignment of activities with governance, risk and compliance requirements.

In 2025, stc group continued to enhance its compliance organization by updating policies, procedures and expanding digital transformation initiatives that enabled greater automation of monitoring and compliance reviews, improved data quality and faster response times. As part of its ongoing efforts to reinforce a culture of ethics and professional conduct, the compliance team continued to conduct training and awareness programs aimed at embedding the values of integrity and responsibility among employees. These efforts were crowned by stc group's achievement of the ISO 37301:2021 certification for Compliance Management Systems, confirming the efficiency of its compliance organization and sustainability of its operations.

stc group reaffirms its commitment to nurturing a corporate culture of compliance that embodies the values of trust and accountability, supporting its operations through the integration of institutional development and digital transformation and reinforcing its position as a leader in governance excellence and sustainable performance.

Business integrity

In its pursuit to enhance stakeholder trust, stc group has placed significant emphasis on embedding integrity values and combating illicit practices. Following the Board of Directors' adoption of the initiative to establish the organizational structure for the general department of business integrity, the following departments were established:

- Whistleblowing department.
- Anti-fraud and corruption department.
- Anti-financial crimes department.
- Forensic department.
- Investigations department.

To further develop business integrity efforts, a comprehensive three-year strategy has been approved, focusing on several core pillars:

- Strengthening oversight of business integrity activities within stc group.
- Leveraging proactive detection and prevention measures.
- Adopting cutting-edge digital technologies.

stc group is investing in this direction to lead the telecommunications sector in establishing a business model that covers all aspects of integrity, thereby boosting stakeholder confidence and creating an attractive investment environment. This includes the following key initiatives.

1. **Establishing a dedicated reporting department:** A specialized department has been created to receive all reports related to suspected fraud and corruption through stc group's reporting channels. Awareness campaigns have been conducted for all employees to educate them about various reporting channels, the mechanism for submitting reports and the protection afforded to good-faith whistleblowers. A dedicated icon labeled "Business Integrity Reports and Consultations" has been added to the employee portal for seamless reporting. A separate channel for business integrity consultations has also been developed.

2. **Automation:** The first phase of task automation has been completed at 100%, and stc group has progressed to the second phase, adopting a machine-learning model to deploy AI tools for proactive detection solutions. By mapping normal transaction patterns, these technologies identify unusual operations for further AI-driven analysis. This is expected to provide critical data for decision-makers and strengthen the first line of defense against threats.

3. **Awareness programs:** In collaboration with the Control and Anti-Corruption Authority (Nazaha), stc group has organized numerous training sessions, seminars and workshops. These initiatives have educated employees about prohibited practices, their risks and the importance of reporting them, positively enhancing trust in reporting channels and enabling corrective solutions for problematic transactions.

4. **Digital forensics:** Advanced electronic examination technologies have been deployed to improve the quality and accuracy of report outputs. Construction of a state-of-the-art digital forensics lab, adhering to the latest standards and technologies, is currently underway.

5. **Fraud and corruption prevention:** Following a partnership agreement with the risk sector, stc group has enhanced operational procedures, self-monitoring efforts, risk indicators and control mechanisms. This includes ongoing root-cause analysis of detected cases, coordinated corrective solutions with business sectors and strengthened controls.

6. **Anti-money laundering (AML) and counter-terrorist financing (CTF):** After bolstering the Financial Crimes Department with expert human resources and investing in technical monitoring tools, stc group has analyzed internal data sources to build controls for suspicious activity monitoring. These controls are continuously reviewed to enhance effectiveness, contributing to an improved sustainability rating for the company.

7. **Investigations management:** The Investigations Platform has been integrated with the electronic business integrity platform to minimize manual case processing. Technical linkages with stakeholders streamline workflows and database updates, improving the quality of examination, analysis and prediction outputs. Agreements with all subsidiaries ensure robust investigation processes, and maturity assessments of business integrity practices across stc group are conducted to drive continuous improvement.

8. **Governance:** stc group has reviewed and enhanced the Business Integrity Committee's charter, restructuring it to reinforce oversight, accountability and independence principles.

Through these measures, stc group continues to solidify its leadership in business integrity within the telecommunications industry.