10 Enterprise Risk Management

The security landscape continues to grow in complexity as technology evolves at an unprecedented pace. Recognizing this, Zain remains steadfast in strengthening its ability to anticipate and respond to emerging threats such as ransomware, phishing, and zero-day exploits. Zain's Risk Management Framework is designed to be both proactive and adaptable, ensuring that risks are managed effectively in a constantly shifting environment.

At the heart of this framework lies the Enterprise Risk Management (ERM) department, which plays a pivotal role in identifying, assessing, and prioritizing risks across all operations. By maintaining a forward-looking approach, ERM supports informed strategic decision-making and helps safeguard the organization's resilience. Continuous assessments including the annual review of information security controls ensure that the defenses evolve in line with new and emerging threats.

Oversight of the ERM function is provided by the Board Risk Committee (BRC). The committee reviews and approves the Risk Management Framework annually and monitors key risk trends on a quarterly basis. This process is reinforced through close collaboration with Internal Audit, Corporate Compliance, Corporate Governance, and Group Risk Management, ensuring that risk oversight remains robust and comprehensive.

In parallel, Zain's risk management activities are aligned with the Corporate Sustainability strategy, the ERM team evaluates social, economic, and environmental risks through ongoing research and stakeholder engagement, integrating sustainability considerations into Zain's broader risk outlook. Since 2019, particular emphasis has been placed on understanding the material impact of climate change — identifying both risks and opportunities to enable early mitigation planning across Zain's markets.

Through this integrated and evolving approach, Zain continues to strengthen its capacity to navigate uncertainty and maintain resilience in an increasingly dynamic risk environment.

Climate-Related Risks and Opportunities are explained in depth in the Task Force on Climate-Related Financial Disclosures (TFCD) report on page 120.

Membership Associations from a Risk Perspective

Zain's active participation in global telecommunications organizations underscores its commitment to responsible industry collaboration and continuous improvement in risk management and connectivity standards. As a member of both the GSMA and the International Telecommunication Union (ITU), Zain engages in international initiatives that drive innovation, promote interoperability, and strengthen the security and resilience of communication networks.

Through its GSMA membership, Zain takes part in global industry dialogues such as the Mobile World Congress, where collaboration with peers helps advance shared priorities including roaming, interconnectivity, and cybersecurity. These engagements enable us to remain aligned with emerging industry trends and best practices that support operational and strategic risk management.

Within the ITU, Zain contributes to initiatives focused on developing international standards, managing global radio spectrum resources, and expanding access to information and communication technologies (ICTs), particularly in underserved regions. This involvement reflects Zain's broader commitment to supporting a secure, inclusive, and sustainable digital ecosystem across its markets.

Risk Management Framework

In alignment with our established Risk Management Framework, Zain continues to maintain a consistent and disciplined approach to assessing and managing risks across all operations. As in previous years, this methodology has proven effective in ensuring that security-related events are analyzed systematically and in a manner that supports sound governance and informed decision-making.

Each security event is evaluated using a standardized risk rating process that applies an impact-likelihood matrix across Zain's operations. The assessment considers a comprehensive range of potential impact factors including financial, reputational, market, customer, employee, and climate-related dimensions to provide a balanced and forward-looking view of Zain's risk exposure.

Both inherent and residual risk levels are determined through the evaluation of pre- and post-mitigation conditions. This structured approach enables the company to maintain visibility over the effectiveness of its controls and to monitor changes in its overall risk profile, ensuring continuity, transparency, and accountability in the management of enterprise risks.

Figure 1: Zain Risk Management Framework (alignment to ISO 31000)

Figure 2: Zain Risk Management Framework (alignment to Committee of Sponsoring Organizations Framework)

Precautionary Principle

Zain applies the precautionary principle across its operations, from the design of products and delivery of services to the implementation of internal security technologies by integrating environmental considerations into every stage of decision-making. Zain remains mindful of the potential impacts of rapid technological advancements, with key risks monitored closely by the Board, the Board Risk Committee (BRC), and the Climate Action Committee.

In line with its sustainability objectives, Zain prioritizes the development and deployment of low-carbon products and services that meet customer needs while supporting environmental responsibility. Climate-related factors such as energy efficiency, heat dissipation, and end-of-life disassembly for repair or reuse are central to the Waste Management Policy Framework and embedded within our product and service design checklist to ensure that sustainability is an integral part of innovation.

Collaboration with suppliers further reinforces this approach. Zain's product design and procurement teams work closely with partners to encourage the creation of solutions with reduced environmental footprints. In the case of internal security technologies, vendor selection criteria include sustainability parameters such as energy consumption and heat management, ensuring that environmental performance contributes to overall evaluation and final decision-making.

Data Protection and Privacy

Zain Group continued to strengthen its data governance maturity through the establishment of the Group Data Office, reinforcing its commitment to responsible, secure, and innovative data management across all markets. The Data Office assumed full ownership of the Group Data Management and Privacy Frameworks, ensuring a unified and future-ready approach aligned with international best practices. Major enhancements to the Group's data privacy policies were approved by the Board, strengthening safeguards for personal data and ensuring full compliance across all Zain entities.

Management Approach to Protecting Personal Data

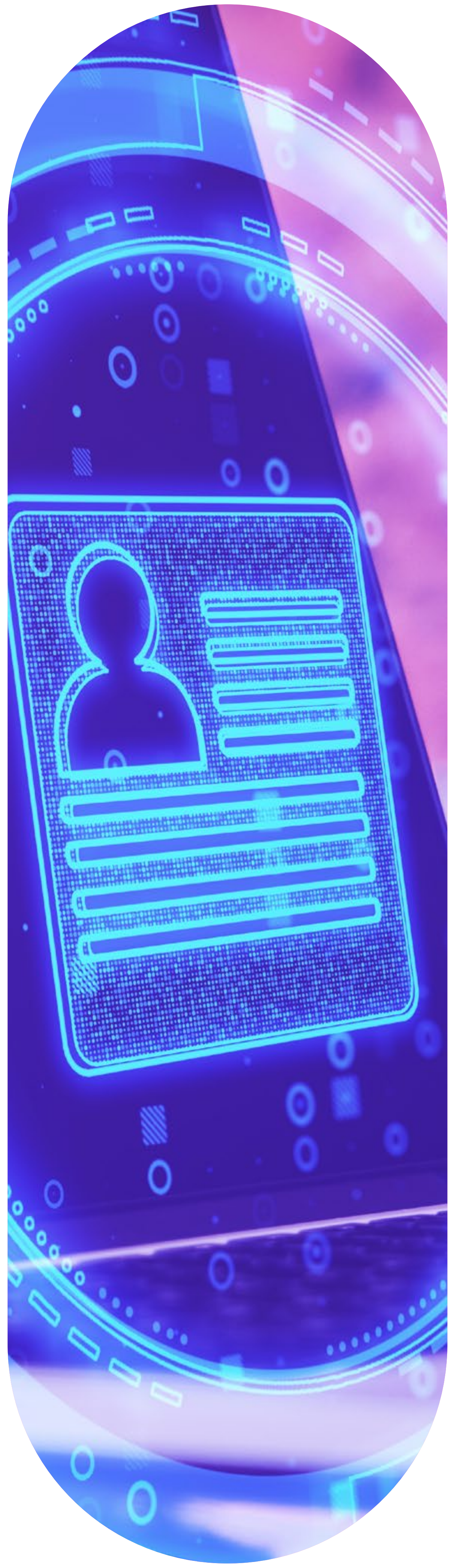
The Zain Group Data Privacy Framework serves as the Group's unified and binding governance model for managing personal and sensitive data across subsidiaries, affiliates, and operating companies. It outlines clear principles and mandatory controls for how data is collected, used, stored, shared, transferred, retained, and disposed of throughout its lifecycle. The Framework consolidates legal requirements, international standards, and internal governance practices into a single reference applicable to all business functions, technologies, and third parties.

Built around twelve core Domains, the Framework translates the Group's privacy commitments into actionable, measurable, and auditable requirements. Each Domain is structured into Sub-Domains, Executable Controls, and Evidence Deliverables, enabling consistent implementation and verifiable compliance across the Group. As part of this rollout, operating companies and subsidiaries are designating qualified Data Protection Officers, adopting the updated policy, and integrating its controls within their systems and processes. This Group-wide alignment strengthens privacy governance and harmonizes protection practices across all Zain operations.

Through this Framework, Zain embeds privacy into corporate governance, system design, and operational processes, ensuring that digital and technological initiatives including analytics, artificial intelligence, and cloud-based services apply the privacy-by-design principle. This positions data protection as both a regulatory requirement and a strategic enabler of trust, innovation, and sustainable digital transformation.

Zain operates within a rapidly evolving regulatory environment across Kuwait, the GCC, and global jurisdictions. Kuwait continues to advance national privacy and cybersecurity requirements through directives from the National Cyber Security Centre and the Communications and Information Technology Regulatory Authority. Across the GCC, countries including Saudi Arabia, the UAE, Qatar, Bahrain, and Oman have enacted comprehensive data protection and cybersecurity laws. Internationally, regulations such as the EU GDPR, the UK Data Protection Act, and sector-specific standards increasingly shape expectations for accountability, cross-border data transfers, and data subject rights.

To remain agile within this dynamic landscape, the Group Data Privacy Framework embeds continuous regulatory monitoring, compliance alignment, and periodic enhancement. This proactive approach mitigates legal and reputational risks while reinforcing Zain's commitment to maintaining global best practices and delivering secure, transparent, and responsible digital services.



Strategic Blueprint of the Zain Group Data Privacy Policy

The unified Zain's Data Privacy Policy is the Group's formal statement of commitment to protecting the personal data of all individuals who interact with its services across the Middle East and Africa. The Policy establishes the principles, legal bases, governance structures, and operational requirements that apply to the collection, processing, storage, sharing, transfer, retention, and deletion of personal data across all Zain entities, subsidiaries, and digital channels.

Core Policy Pillars

Compilance Framework

Unified framwork for compilance with national data protection laws across Kuwait, Saudi Arabia, Jordan, Bahrain, Iraq, South Sudan, and UAE

Data Categories

Clear definitions of personal and sensitive data categories, lawful processin bases, consent requirements, and special rules for children's data

Governance Model

Comprehensive internal governance led by Data Protection Officers at Group and Entity levels overseeing compliance and risk management

The Policy sets out a unified framework for compliance with national data protection laws in all Zain markets, including Kuwait, Saudi Arabia, Jordan, Bahrain, Iraq, Sudan, South Sudan, and the United Arab Emirates. It ensures that Zain processes personal data lawfully, fairly, and transparently, and that data subjects are informed of their rights and the ways in which their information is used.

Data Privacy Policy Architecture

Principles

- Lawful processing
- Fair & transparent
- Purpose limitation
- Data minimization

Data Subject Rights

- Access & correction
- Erasure & objection
- Consent withdrawal
- Data portability

Security Safegurads

- Technical controls
- Organizational measures
- Access restrictions
- Encryption standards

DPO Structure

- Group-level DPO
- Entity-level DPOs
- Compliance oversight
- Risk assessment

Retention & Deletion

- Defined retention periods
- Secure deletion of protocols
- Lifecycle management
- Audit trails

Breach Notification

- Mandatory timelines
- Regulator reporting
- Individual notification
- Incident documentation

The Policy outlines the lawful bases under which personal data is processed, and explains the circumstances where consent is required. It provides clear rules for processing children's data, explains the legitimate purposes for which Zain uses customer and employee information, and describes when and how Zain may share or transfer data to third parties or across borders.

Collection → **Processing** → **Storage** → **Sharing**

Collection	Processing	Storage	Sharing
Lawful & Transparent Gathering	Purpose-limited use	Secure retention	Controlled transfer

Data subjects are provided with detailed rights, including access, correction, erasure, objection, and withdrawal of consent. The Policy also outlines Zain's procedures for breach notification, including mandatory timelines for reporting incidents to regulators and affected individuals.

Overall, the Policy functions as the Group's binding rulebook for ethical, transparent, and compliant data handling. It ensures that privacy risks are managed, regulatory obligations are met, and trust is maintained across all operations, services, and jurisdictions in which Zain operates.

Policy Outcomes

Ensuring trust, compliance, and ethical data stewardship

Regulatory Compliance

Full adherence to national data protection laws across all markets

Trust Maintenance

Building and sustaining customer confidence through transparency

Risk Management

Proactive identification and mitigation of privacy risks

Data Exposure and Vulnerability Assessment

During the current year, Zain continued its efforts to strengthen its capabilities for identifying, assessing, and managing personal data exposure risks across all operations. Through coordinated efforts between the Zain Data Office, Group Cybersecurity, and the OPCO data and privacy functions, exposure points were identified earlier and addressed with greater consistency. No major incidents or confirmed data breaches occurred during the reporting period. The exposure points identified represent risk conditions rather than any confirmed loss, misuse, or unauthorized disclosure of personal data.

Telecom operators globally face similar exposure risks due to large volumes of customer data spread across complex systems where older platforms sit alongside newer digital environments. These conditions lead to inconsistent access controls, uneven encryption, manual data handling, and rapid growth of APIs and third-party integrations that demand stronger oversight. Zain Group made these risks a priority within its broader privacy and data governance transformation, introducing a unified Data Privacy Framework and standardized policies to reduce inconsistencies across all operating companies, strengthening access governance, improved retention and disposal practices, clarified accountability for data protection, and tightened oversight of vendors, processors, and high exposure systems.

Zain may process customer information for clearly defined secondary purposes, consistent with the Sustainability Accounting Standards Board definition of secondary use and aligned with the data protection laws in all jurisdictions where Zain operates. Secondary purposes refer to the lawful and proportionate use of customer information beyond the delivery of core telecommunications services. These purposes include service quality enhancement, product and network development, fraud prevention, customer experience improvement, and analytical activities that support operational efficiency and strategic planning.

The newly introduced Group Data Privacy Framework and the aligned privacy policies are currently being rolled out across all Opcos. As this work progresses, these documents will establish a unified structure for purpose limitation, data minimization, and transparency, and will serve as the central reference for how secondary processing is governed. Once fully implemented, the framework and policies will create a more consistent and accountable approach across the Group. Their adoption will allow Zain to demonstrate clearer improvement in the next reporting cycle, supported by measurable indicators and aligned practices across all markets.

Zain currently applies the principle of collecting and using only the minimum amount of information required for service improvement, analytics, or product development, and uses anonymization or pseudonymization techniques wherever feasible to reduce the risk of re-identification. As the framework becomes fully operational, adherence to these requirements will be monitored in a more structured and comparable manner across Opcos, enabling the Group to validate progress and identify areas requiring further enhancement.

Secondary processing related to analytics, research, or new service development continues to take place within controlled environments. These environments follow safeguards such as access restrictions, encryption, comprehensive logging, and oversight by the Zain Data Office and the designated Entities data protection officers. As the new framework and unified policies are embedded, future assessments will reflect stronger privacy governance, more consistent implementation across markets, and clearer evidence of improvement in the responsible management of customer information.

Data Security

Zain remains steadfast in its commitment to strengthening the security of its operations through the continuous adoption of advanced technologies and the enhancement of its overall security posture. As part of this ongoing effort, regular assessments are conducted to identify potential vulnerabilities and validate the effectiveness of existing controls, ensuring that its defenses remain resilient against evolving threats.

Management approach to identifying and addressing data security risks

Zain continues to adopt a proactive and comprehensive approach to managing data security risks in response to the evolving threat landscape. Building upon established security policies and procedures, Zain conducts regular risk assessments and implements robust data protection controls to safeguard the confidentiality, integrity, and availability of information across its operations.

Given the sensitivity of the data stored and processed, periodic evaluations are carried out to identify vulnerabilities, emerging risks, and evolving attack vectors. Each year, the scope of these assessments is expanded to encompass new technologies, processes, and operational areas, ensuring comprehensive coverage of Zain's evolving digital landscape. This ongoing assessment ensures that Zain's defenses remain up to date and aligned with industry best practices.

Zain employs a defense-in-depth strategy designed to establish multiple layers of protection against unauthorized access and potential data breaches. This includes a combination of preventive, detective, and responsive security controls that safeguard information assets across all operations. Continuous monitoring and incident response mechanisms further enhance preparedness and ensure rapid action in the event of a security incident.

The following is an illustration of a framework referenced in Zain's cyber resilience strategy.

Identify	Protect	Detect	Respond	Recover
Threat vectors, assets, data, and actors	Install technology controls, i.e. point solutions	Monitoring infrastructure	Incident response and management plans	Resilience to resume from 'normal state' at the earliest
Cross validate with risk assessment studies	System/device hardening	Analytics & threat hunting		Crisis management protocols
	Access control mechanisms	External subscriptions		

Below are some initiatives undertaken by Zain across the operations.

- Vulnerability assessments
- Penetration testing
- Telecom signaling security assessment
- Regular security awareness on relevant topics
- Incident and breach handling and notification to related authorities
- ISO 27001 Information Security Management System certification
- New security solutions implemented and enhancements to existing solutions

Managing Systemic Risks from Technology Disruptions

Mission-critical services demand uninterrupted availability, as any downtime is unacceptable and can lead to immediate and severe consequences. Zain actively monitors its key systems to detect and address any disruptions.

Zain Bahrain

System	Availability
Core	100%
Charging	100%
Website	100%

Zain Iraq

System	Availability
Core	100%
Charging	100%
Website	100%

Zain Jordan

System	Availability
Core	99.67%
Charging	100%
Website	99.63%

Zain Kuwait

System	Availability
Core	100%
Charging	100%
Website	100%

Zain Saudi Arabia

System	Availability
Core	100%
Charging	100%
Website	100%

Zain Sudan

System	Availability
Core	100%
Charging	100%
Website	100%

Zain South Sudan

System	Availability
Core	100%
Charging	100%
Website	100%

Zain Group

System	Availability
ERP	100%
Oracle Hyperion	100%
Zain Group Website	100%

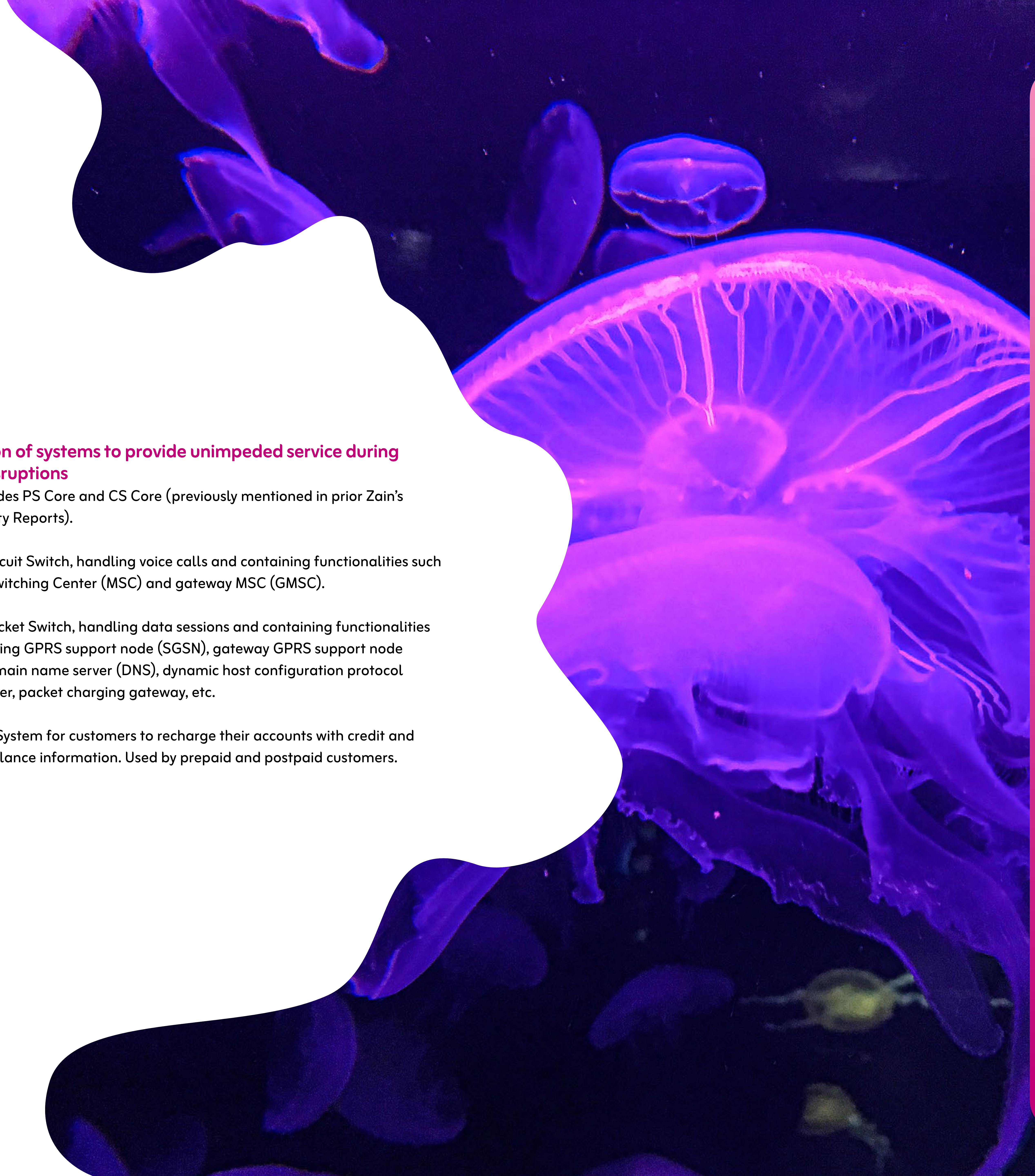
Description of systems to provide unimpeded service during service disruptions

Core - Includes PS Core and CS Core (previously mentioned in prior Zain's Sustainability Reports).

CS Core: Circuit Switch, handling voice calls and containing functionalities such as mobile switching Center (MSC) and gateway MSC (GMSC).

PS Core: Packet Switch, handling data sessions and containing functionalities such as Serving GPRS support node (SGSN), gateway GPRS support node (GGSN), domain name server (DNS), dynamic host configuration protocol (DHCP) server, packet charging gateway, etc.

Charging - System for customers to recharge their accounts with credit and maintain balance information. Used by prepaid and postpaid customers.



Security Risk Training

Since its launch in 2020, Zain's *PAUSE.THINK.ACT* Cybersecurity Awareness Program has continued to strengthen employees' ability to recognize, prevent, and respond to potential security threats. The program equips all Zainers with the knowledge needed to identify phishing attempts, apply secure digital practices, and understand their critical role in safeguarding the company's information assets.

Awareness is promoted through a variety of engagement channels, including email campaigns, SMS alerts, in-person and virtual training sessions, onboarding programs, and awareness workshops conducted across operations. By embedding cybersecurity awareness into the organizational culture, Zain reinforces a shared sense of responsibility and accountability, thereby reducing risk exposure and further enhancing the company's overall security posture.

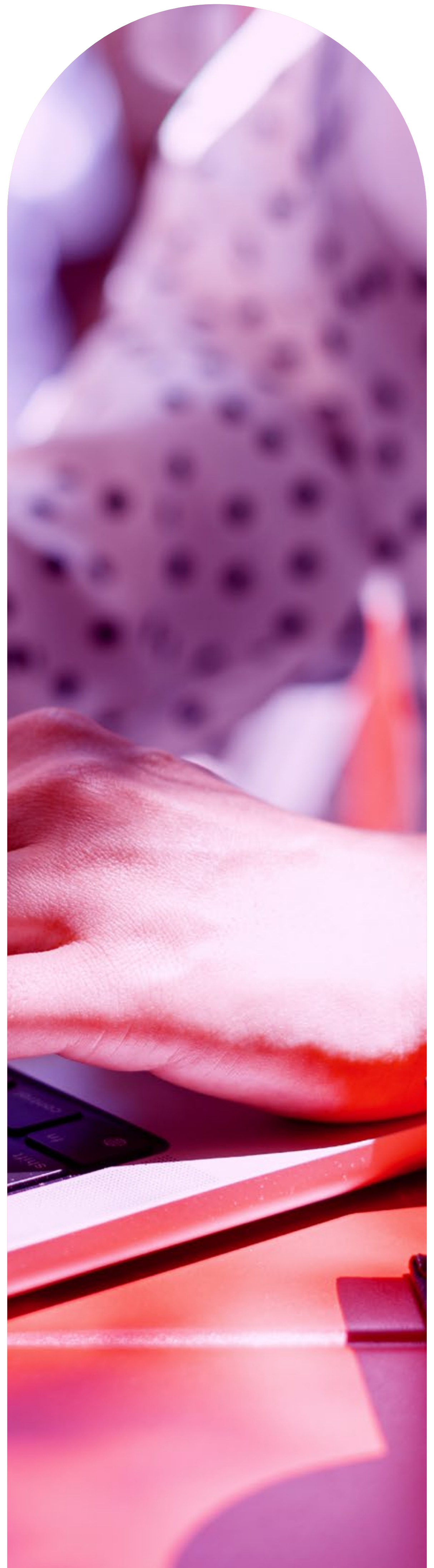
Information security topics covered in 2025

- Phishing Emails
- Physical Security
- Social Media Best Practices
- Safe Remote Work Practices
- Email Security Best Practices
- Ransomware Threat

2025 Awareness Updates	Kuwait	Saudi Arabia	Bahrain	Iraq	Jordan	Sudan	South Sudan
Total Staff	1,638	1792	578	1903	1284	793	155
Total Number of Staff that received awareness content	1,638	1792	578	1903	1284	793	155
Total number of channels utilized	5	3	4	2	4	2	5
Channels utilized	Emails Induction Workshop SMS	Workshops Awareness Campaign Emails SMS	Learning Platform Emails Workshops In-Person Session Digital Learning	Emails Instagram	Emails Social Media Digital Screens Workshops Gamification	Corporate Email Newsletter Social Media	Emails Workshops

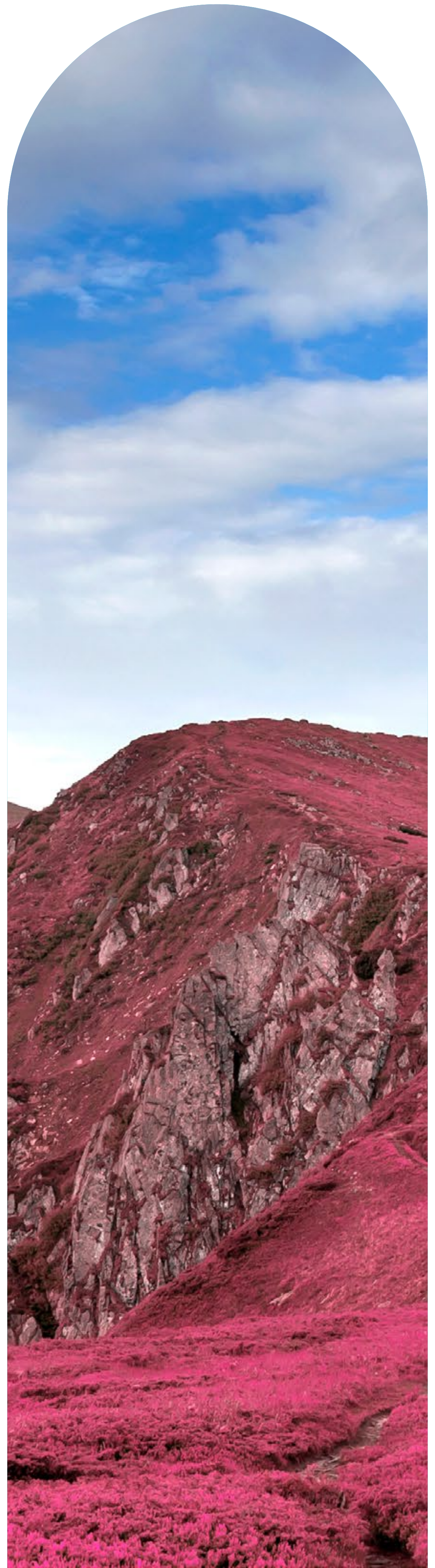
The following list consists of the cyber security training courses undertaken by Enterprise Risk Management employees across Zain's operations.

- SEC401: SANS Security Essentials – Network, Endpoint, and Cloud
- Decoding MITRE D3FEND for Building Strategy for Cyber Resilience
- COMPTIA Security+
- Network XDR Training
- Defcon Security Testing & Defense
- National Cybersecurity Crisis Management



Initiatives with External Stakeholders

Initiative	Date of Adoption	Opcos in Scope	Nature of Initiative (Binding/Voluntary)	Range of Stakeholders Involved
Information Security Management System ISO 2700	10-Jan-24	Zain Bahrain	Binding	Telecommunication Regulatory Authority
	22-Nov-23	Zain Iraq	Voluntary	AQC
	02-Feb-24	Zain Kuwait	Voluntary	DNV-GL
	21-Jun-23	Zain Jordan	Voluntary	SGS
	30-Aug-23	Zain KSA	Voluntary	Intertek
Business Continuity Management System ISO 22301	29-Jan-23	Zain Kuwait	Voluntary	DNV-GL
	13-Jan-2025	Zain Iraq	Voluntary	AQC
	01-Apr-24	Zain Jordan	Voluntary	SGS
	30-Aug-23	Zain KSA	Voluntary	Intertek
Quality Management System ISO 9001:2015	29-Jul-2024	Zain Bahrain	Voluntary	DNV-GL
	03-Feb-2024	Zain Kuwait	Voluntary	DNV
Environmental Management System ISO 14001:2015	03-Feb-2024	Zain Kuwait	Voluntary	DNV
IT Service Management System ISO 20000-1	31-Jan-23	Zain Kuwait	Voluntary	DNV



Sustainability Risks Impacting Risk Management

Physical risks: Increase in energy costs due to additional cooling caused by temperature increases

Each Zain operation monitors the pattern of fuel and electricity consumption and reports to the Group on a quarterly basis. Fuel and electricity consumption patterns are analyzed to assess variations.

In case energy consumption increases more than 10% quarter-on-quarter, the concerned opcos are required to provide details and justifications for such changes. We took the reference of Coupled Model Intercomparison Project, Phase 6 (CMIP6) models included in the IPCC's Sixth Assessment Report (AR6).

Global warming of 1.5C relative to 1850–1900 would be exceeded during the 21st Century under the intermediate, high, and very high greenhouse gas (GHG) emissions scenarios considered in this report (SSP2-4.5, SSP3-7.0 and SSP5-8.5, respectively).

For our analysis, we selected the following SSP scenarios: SSP1 2.6 2039: Kuwait (1.012), KSA (1), Bahrain (0.971), Iraq (1.113), Jordan (1.086), Sudan (0.863) and South Sudan (0.702).

SSP5 8.5 2039 and 2059: Kuwait (1.2222.492), Saudi Arabia (1.18, 2.453), Bahrain (1.158, 2.244), Iraq (1.302, 2.538), Jordan (1.258, 2.362), Sudan (0.923, 2.047), South Sudan (0.688, 1.643).

SSP2 4.5 2039 and 2050: Kuwait (1.018, 1.813), Saudi Arabia (1.035, 1.8), Bahrain (0.979, 1.688), Iraq (1.11, 1.854), Jordan (1.082, 1.731), Sudan (0.858, 1.496), South Sudan (0.628, 1.268).

The timeframes mentioned are the ones covering our net-zero timeline, but our analysis went beyond 2050 to provide an understanding of the extent to which our business could be impacted in the long-run.

Transition Risk: Increases in energy tariffs will lead to an increase of energy costs for the operation of our telecom/IT sites

During the assessment of climate-related risks for our core site, offices, and base station facilities, we identified that there could be an increase in operational expenditure due to fuel tariff hikes and grid power units in our areas of operation.

Zain’s total energy consumption in 2025 was **128.4M Liters** and **1,240.39 GWh** across seven operations. The 2025 overall energy cost was **USD 195.3m** from the 2024 overall energy cost which was based at **USD 155.26M.** Overall energy costs including diesel in 2025 was **USD 195.34M.** With Zain’s long-term planning process of 14 years, it estimates that energy operating costs could **increase by over 60% to USD 314.57M in 2039.** Overall energy costs including diesel in 2025 was USD 149.07 M. With Zain’s long-term planning process of 14 years, it estimates that energy operating costs could increase by over 60% to USD 249 million in 2039.

Opportunities

The availability of a reliable universal grid supply is essential for economic growth and the alleviation of poverty. While the South Sudanese government’s desire to modernize and extend on-grid coverage and introduce additional generation capacity is commendable, until such time when a stable political and conflict-free environment exists in the country, the current challenging state of the nation’s main utility supply is likely to persist for the foreseeable future.

Zain implemented a range of green energy solutions, including battery-hybrid systems, solar installations, outdoor equipment modernization, grid connections for base station sites, and site-sharing arrangements with other mobile network operators. Zain’s strategic approach focuses on converting identified physical and transition risks into opportunities by adopting solutions that reduce operating costs while ensuring payback periods do not exceed six years. The deployment of 140 outdoor cabinets featuring substantially higher energy efficiency compared to traditional telecom shelters incurred a total opex savings of **USD 1.21m**. Collectively, these initiatives resulted in a reduction of **806 metric tons of CO_2 emissions**, with additional emission reductions expected to continue for at least the next five years, aligned with the operational lifetime of the installed equipment. While the opportunity extends across Zain’s wider operations, Iraq, Sudan, and South Sudan represent the primary beneficiaries due to their grid availability constraints and the elevated cost of diesel driven by local currency devaluation.

The opportunity also refers to Zain’s broader operations. We highlighted Iraq, Sudan, and South Sudan as these opcos are the major beneficiaries of this opportunity due to grid availability and cost of diesel in the face of devaluation of the local currencies.

To mitigate the increase in energy consumption associated with heightened cooling requirements, Zain implemented a series of initiatives under its strategic pillar of operational effectiveness.In 2025:

- 41 infrastructure sharing sites for a cost of USD 184,900
- The deployment of 140 outdoor sites in Bahrain for a cost of USD 1,531,188
- Installation of 81 inverter-based cooling systems in Kuwait for USD 115,830
- The deployment of smaller size diesel generators in Kuwait for USD 61,201
- The installation of 218 DG hybrid solutions in Iraq and Saudi Arabia for USD 3,775,000
- The installation of additional 433 DG-Battery Hybrid solutions Bahrain, Iraq, and Saudi Arabia through our TowerCo Partners.
- Implemented 158 solar hybrid solutions in Iraq, Saudi Arabia, and South Sudan for USD 2,725,000
- Connected 330 sites to the grid in all operations, except Iraq, for USD 710,812

Risk Management Value Creation from Climate Change Perspective

Zain’s Risk Management practices have a positive impact and creates value in the below mentioned areas:

Business: Long-Term (5+ years)

Information security assessments, strict risk management policies, and robust security solutions enhance Zain’s business operations by safeguarding critical data, ensuring compliance, and minimizing disruptions. These proactive measures build trust with stakeholders, protect intellectual property, and support seamless operations, driving business continuity and growth. Additionally, by preventing breaches and mitigating risks from threat actors, Zain avoids costly incidents, legal penalties, and downtime, achieving cost optimization through reduced financial losses and efficient resource allocation. This is a long-term impact as security threats will continue to exist and evolve, meaning Zain’s security posture will continue to mature.

Society: Long-Term (5+ years)

Zain’s Risk Management practices create societal value by promoting a safer digital environment through comprehensive information security assessments, well-defined policies, and robust procedures. These efforts not only protect the company’s data but also contribute to safeguarding customers' information, fostering trust and reliability. Through security awareness programs and sessions, Zain empowers employees and stakeholders with the knowledge to mitigate risks, reducing the impact of cyber threats beyond the organization. This proactive approach helps build a more secure community, encouraging responsible digital behavior and supporting overall societal resilience against cybercrime.

Environment: Zain’s Risk Management practices take a short-term, medium-term and long-term approach.

Short-Term – (1-3 years)

We analyze the operational risks arising due to climate change events that need to be addressed to enhance our services to remain competitive in our markets. The normal lifetime of some of our assets such as diesel generators used on off-grid sites is approximately three years. Hence, we consider three years to be a reasonable period for assessing the impact of physical risks on such assets. From a financial and strategic perspective, our short-term horizon is focused on development and achievement of revenue forecasts, cost targets and profitability targets based on existing consumer and enterprise business portfolios.

Medium-Term – (3-5 years)

Our medium-term time horizon is aligned to our business planning process that uses a five-year horizon for the operational risks arising due to climate change events. This period is also in line with the lifetime of other assets such as deep cycling batteries, which are used to mitigate the factors associated with some of the physical and transition risks. Our five-year business plan is updated annually, while monitoring the progress of the plan from the previous year. The business plan is updated with actuals of the first year and the revised forecast for four years, and subsequently an incremental year is added.

Long-Term – (5+ years)

Our long-term business financial planning process is planned over 5 and 15 years to align with our goals for climate change initiatives. This is the timeframe that gathers a large portion of the company’s assets such as the cooling systems, DC power systems, the radio systems, and other active equipment in transmission and core sections. The impact of physical risks on such assets is evaluated and mitigated to ensure that the company remains competitive in its markets of operation. From a strategic perspective, our strategic business plan entails the long-term horizon and is focused on a forecast of cashflows and revenue potential from the initiatives that we identify as part of our organization’s strategy.

The following table demonstrates the company's risks and opportunities in relation to the six integrated thinking capitals. It provides insights on such topics are impacting the business holistically.

MATERIAL TOPIC
Business Model, Resilience and Physical and Sociopolitical Risks

SUB-TOPIC
Risk Management

RISK

Inability to anticipate emerging threats, fragmented controls, operational disruptions, and inconsistent risk governance.

OPPORTUNITY

Strengthening enterprise-wide risk management improves resilience, supports informed decisions, and ensures continuity across operations.

IMPACT ON THE SIX INTEGRATED THINKING CAPITALS

Strengthened risk management enhances intellectual, human, and social capital by improving preparedness, decision-making, and stakeholder confidence. However, it requires upfront investments that place short-term pressure on financial capital.

- (+) Intellectual Capital
- (+) Human Capital
- (+) Social & Relationship Capital
- (−) Financial Capital

MATERIAL TOPIC
Customer Privacy & Data Security

SUB-TOPIC
Data Protection & Privacy

RISK

Data exposure from legacy systems, inconsistent access controls, non-compliance with privacy laws, and weaknesses in data handling.

OPPORTUNITY

Unified Group Data Privacy Framework enhances trust, transparency, and regulatory compliance across all markets.

IMPACT ON THE SIX INTEGRATED THINKING CAPITALS

Effective data privacy governance increases social and relationship capital by building trust and strengthening human and intellectual capital through better practices and accountability. These improvements, however, come with additional compliance and system-upgrade costs that impact financial capital.

- (+) Social & Relationship Capital
- (+) Human Capital
- (+) Intellectual Capital
- (−) Financial Capital

MATERIAL TOPIC
Customer Privacy & Data Security

SUB-TOPIC
Data Security

RISK

Cyberattacks, ransomware, API vulnerabilities, weak monitoring, and risks from third-party systems.

OPPORTUNITY

Continuous monitoring and stronger cyber controls strengthen security posture.

IMPACT ON THE SIX INTEGRATED THINKING CAPITALS

Robust cybersecurity measures enhance intellectual and manufactured capital by reinforcing system resilience and technical capability, while also boosting social capital through greater customer confidence. The required technology and training investments, however, reduce financial capital in the short term.

- (+) Intellectual Capital
- (+) Social & Relationship Capital
- (+) Manufactured Capital
- (−) Financial Capital

MATERIAL TOPIC
Natural Capital, Climate Change, and Biodiversity and Nature Impacts

SUB-TOPIC
Climate-Related Risk

RISK

Physical risks (heat, storms), rising cooling demand, grid instability, fuel price volatility, and increased Opex.

OPPORTUNITY

Energy-efficient systems, solar/battery solutions, grid upgrades, and site-sharing reduce long-term Opex and emissions.

IMPACT ON THE SIX INTEGRATED THINKING CAPITALS

Actions to mitigate climate-related risks strengthen natural and manufactured capital by improving energy efficiency and infrastructure resilience and elevate intellectual capital through improved climate scenario planning. Nonetheless, these initiatives require initial capital outlays that affect financial performance.

- (+) Natural Capital
- (+) Intellectual Capital
- (+) Manufactured Capital
- (−) Financial Capital