As the security threat landscape grows increasingly complex, it is characterized by rapid technological advancements. Zain recognizes the need to remain adaptable and vigilant as emerging threats such as ransomware, phishing, and zero-day exploits demand a dynamic approach to risk management. To navigate these challenges, Zain employs a proactive, relevant, and agile Risk Management Framework capable of addressing current and future risks.

The Enterprise Risk Management (ERM) department plays a critical role in this Framework by identifying, assessing, prioritizing, and managing risks proactively. This approach enables the organization to make informed strategic decisions while staying ahead of evolving threats. A key example is the annual evaluation of information security controls to ensure they remain effective in countering the fast-evolving security landscape. This continuous adaptation strengthens Zain's ability to safeguard its operations and maintain resilience in an increasingly volatile environment.

The ERM function reports directly to the Board Risk Committee (BRC), which supervises the adherence to risk management policies and procedures and the effectiveness of the Risk Management Framework. The BRC reviews and approves the Framework on an annual basis, and risk trends are reviewed on a quarterly basis. Other functions such as Internal Audit and Corporate Governance departments, and their respective Board committees, along with Group Risk Management, assist the BRC in its oversight.

Zain's ERM function, in close alignment with the company's Corporate Sustainability strategy, evaluates the company's social, economic, and environmental impacts from a risk standpoint through proactive research and extensive engagement with stakeholders. Since 2019, the key considerations have been the risks and opportunities associated with climate change and its material impact, allowing for early-stage planning of mitigation strategies across Zain's operating markets.

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

## Membership Associations from a Risk Perspective

As a member of both the GSMA and the International Telecommunication Union (ITU), Zain actively engages with global initiatives to foster innovation and enhance connectivity. Through its GSMA membership, Zain participates in key events like the Mobile World Congress, collaborating with industry peers and exchanging insights on topics such as roaming, interconnectivity, and security.

In its role within the ITU, Zain contributes to global efforts to facilitate seamless international communication by supporting the development of technical standards, global radio spectrum management, and initiatives aimed at improving access to ICTs for underserved communities worldwide.

## Risk Management Framework

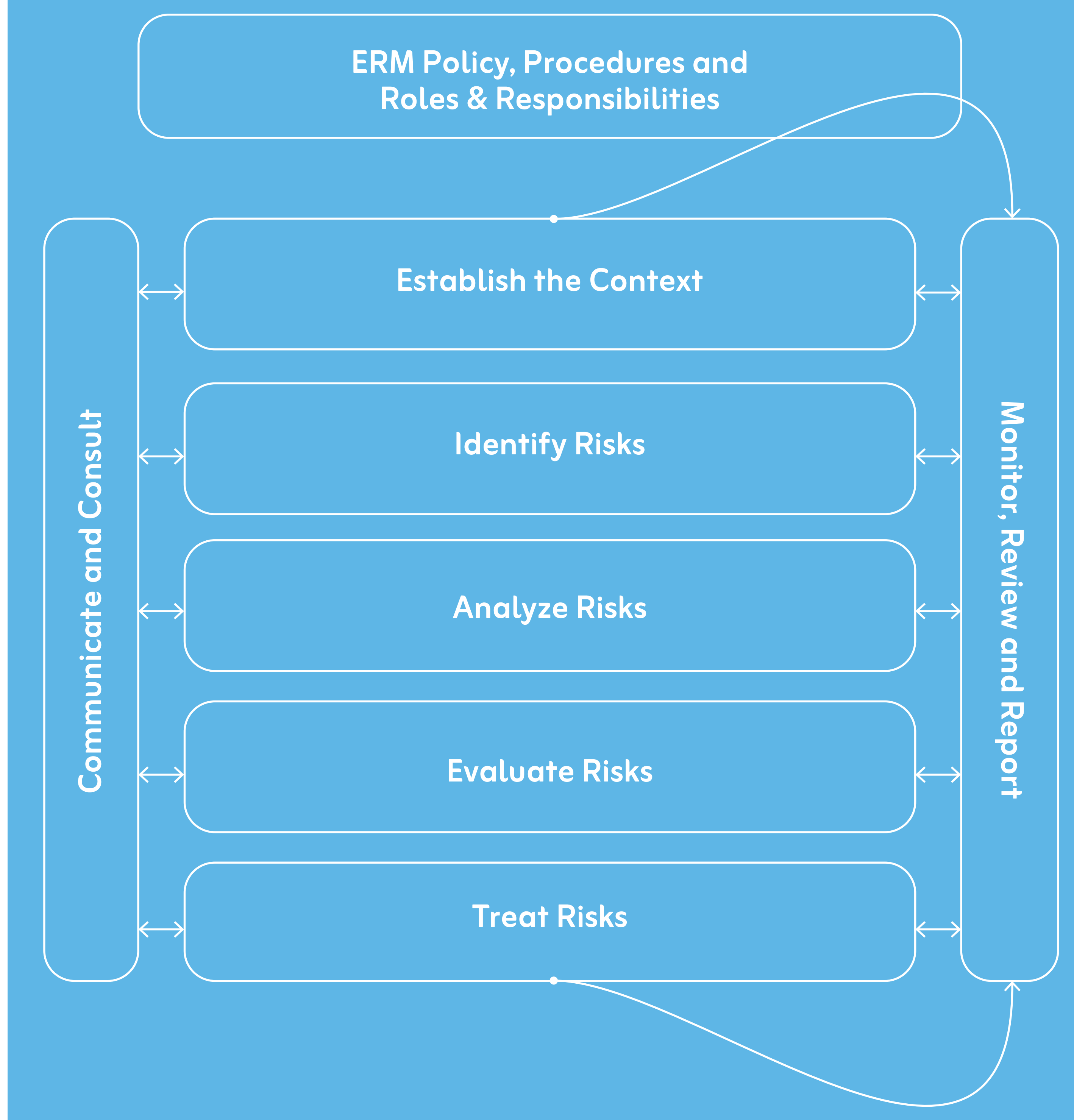



Figure 1: Zain Risk Management Framework (alignment to ISO 31000)

All security events that affect Zain are analyzed based on the risk rating. The risk rating is determined by an impact-likelihood matrix across Zain's operations. The various factors that are assessed to determine the impact include financial, reputational, climate change, markets, customers, employees, and others. The rating also takes into consideration the pre- and post-mitigated status of the risks, providing information on both the inherent and residual risk status of the organization.

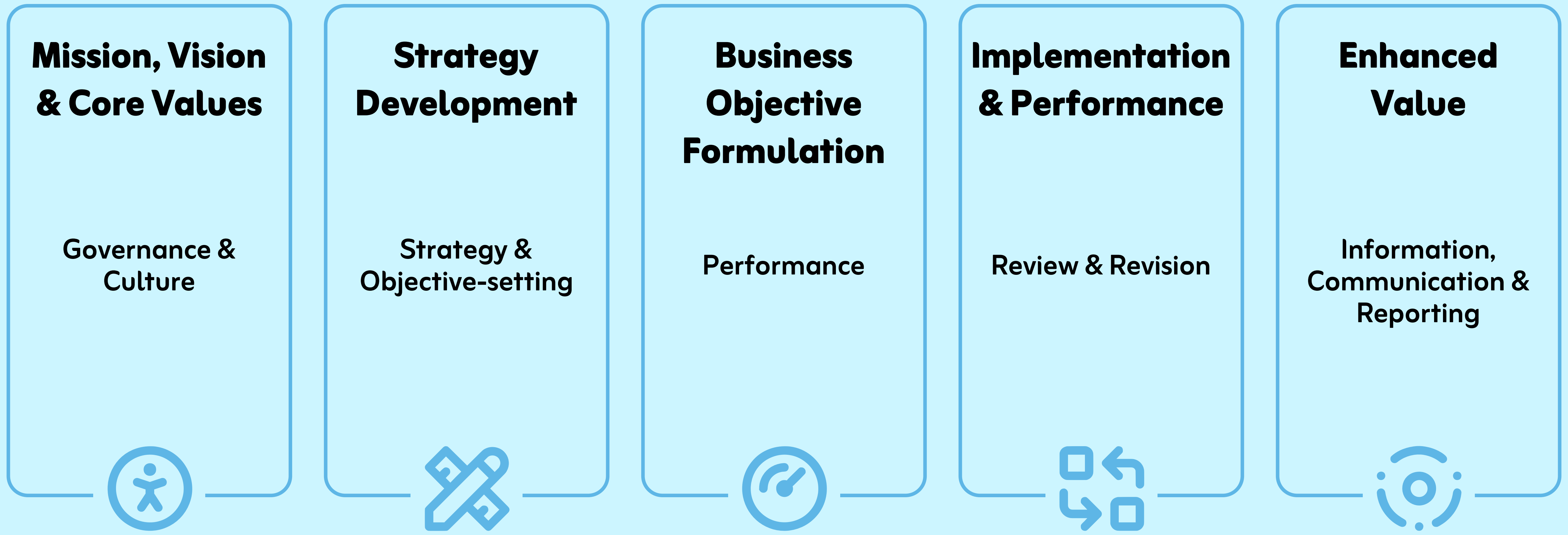



Figure 2: Zain Risk Management Framework (alignment to Committee of Sponsoring Organizations Framework)

## Precautionary Principle

When Zain designs its products, delivers services, or even implements internal security technologies, it follows a precautionary principle by considering all relevant environmental requirements. Key risks, such as rapid technological advancements, are closely monitored by the BRC, the Climate Action Committee, and the Board. Zain's business prioritizes the development and delivery of low-carbon products and services to meet customer needs. Zain also ensures that when a specific security solution is selected for implementation internally, climate-related factors, including energy consumption, heat dissipation and end-of-life disassembly for repair or reuse are taken into consideration and are integral to the product and service design checklist.

The company's product design and procurement teams engage with suppliers to develop products with lower eco footprints. The checklist used as part of the design process includes climate-related considerations such as energy use and end-of-life disassembly for repair or reuse. For security solutions implemented internally, vendor selection takes into consideration the heat dissipation and power consumption values in the final scoring.

## Data Protection and Privacy

Zain considers data privacy as a vital control to prevent data leakage. To comply with applicable laws and regulations, the company is committed to safeguarding the 'personally identifiable information' (PII) entrusted by its customers, employees, suppliers, and other stakeholders, including the processes involved in collecting, using, retaining, and securing this information.

In 2023, Zain introduced a new Data Protection and Privacy Policy to uphold the highest standards of data protection and privacy for all stakeholders. Approved by the Board, this policy ensures Zain's compliance with relevant data protection and privacy laws and regulations. The updated policy outlines the principles and guidelines for collecting, using, and storing personal data, as well as the rights of individuals to access and control their data. Zain is dedicated to protecting and respecting the privacy of all data subjects who engage with the company, maintaining security and transparency. Data protection and privacy principles are embedded across our operations Group-wide to prevent misuse that could harm stakeholder interests or the company's reputation.

The policy can be found on this link.

**Policies and practices related to collection, usage, and retention of customer information and PII for each Zain operating company:**

### Zain Bahrain

Please refer to the link below for more details:

https://www.bh.zain.com/en/copyright/privacy-policy

### Zain Iraq

Zain Iraq does not use any customer data gained from website for Behavioral Advertising.

### Zain Jordan

A new law for data protection was introduced in Jordan, where Zain is still in the process of assessing the risk for PII data and is to set policies and corrective actions accordingly.

### Zain Kuwait

CITRA's data privacy protection regulation is applicable to both public and private sectors that collect, process and store PII. Zain appointed a Data Privacy Officer responsible for overseeing appropriate technical and regulatory controls to comply with the regulations.

CITRA's data privacy protection regulation is applicable to both public and private sectors that collect, process and store personally identifiable information (PII).

### Zain Saudi Arabia

Zain has a data privacy policy that is established and approved by the Saudi Data and AI Authority (regulating authority).

### Zain Sudan

Zain ensures customer information and PII is protected through policies such as its Code of Conduct and customer care process guidelines.

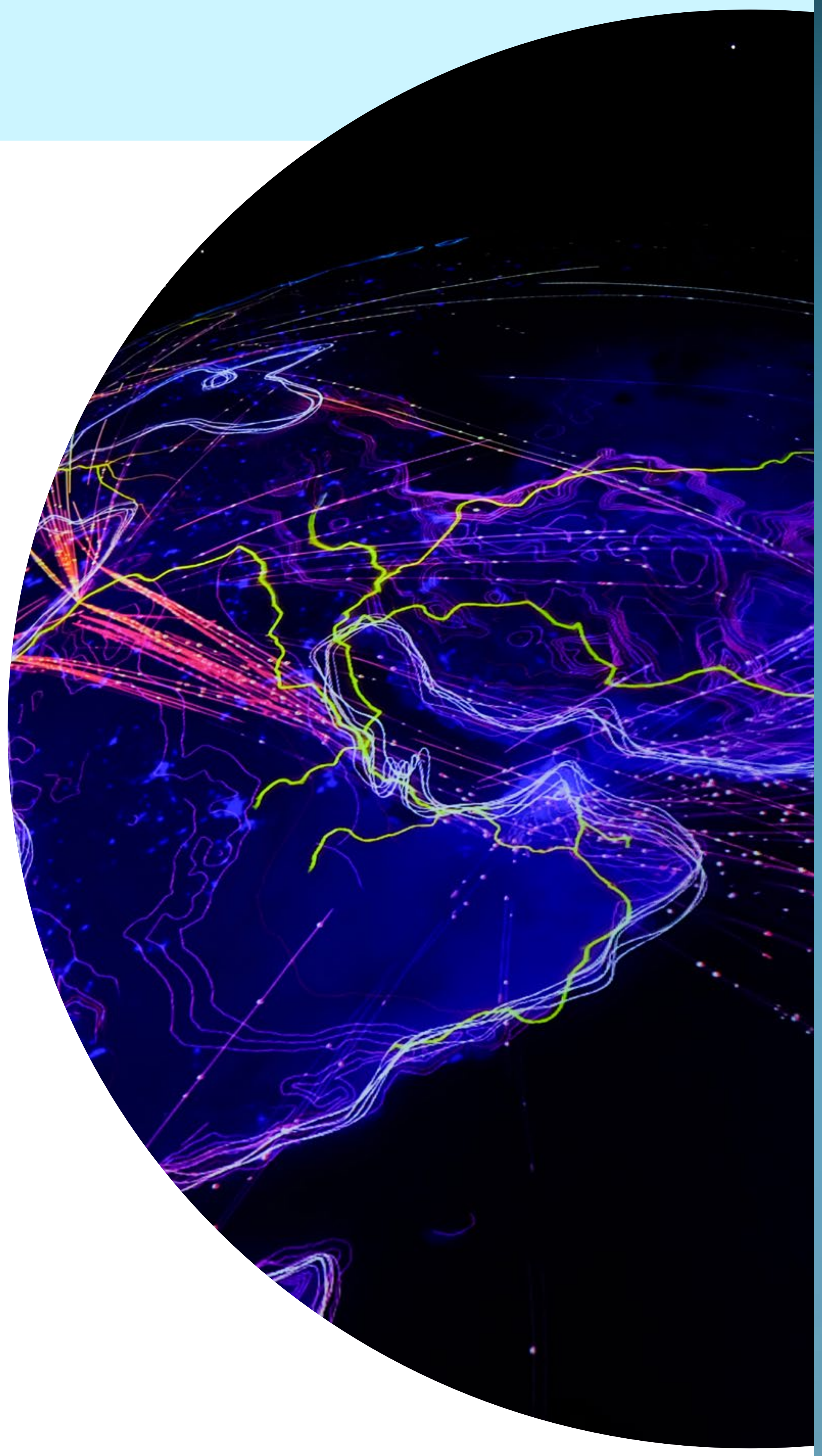
### Zain South Sudan

South Sudan is following best practices and security controls are enhanced year-on-year to improve its maturity and protect data.

### Customer Information for Secondary Purposes

As per the Sustainability Accounting Standards Board's (SASB) definition of secondary purpose, Zain's operations process data for designing products to enhance the quality of services offered to customers. However, customer information and the usage of data is not transferred or shared to third-parties unless requested by law enforcement, in which case it takes place via a judicial order.

As of 2024, there have been no reports or complaints from third-parties or regulatory bodies, or the identification of leaks or losses of customer data.



## Data Security

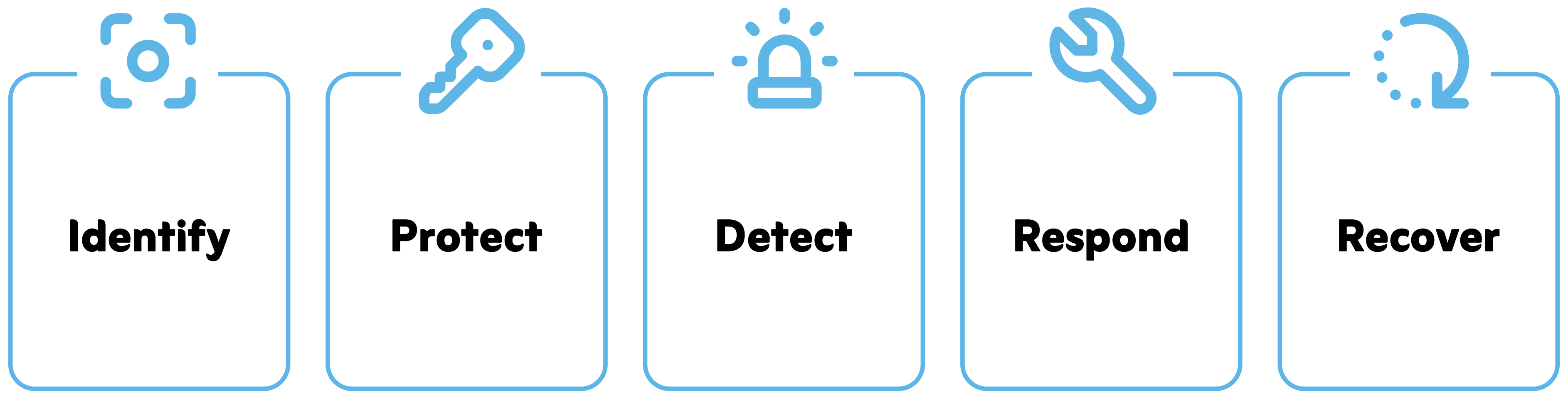
Zain remains committed to enhancing the security of its operations by continuously implementing new security technologies, improving its overall security posture. As part of this effort, the company conducts multiple assessments to identify vulnerabilities and ensure defenses remain robust.

### Management approach to identifying and addressing data security risks

To address evolving security threats, Zain adopts a proactive approach through risk assessments and the implementation of robust data security controls in addition to the existing security policies and procedures. Moreover, as Zain stores and processes confidential information, regular assessments are conducted to identify vulnerabilities, emerging risks, and evolving attack vectors, ensuring that our defenses remain current.

By deploying layered security controls such as firewalls, encryption, intrusion detection systems, and access management, we create multiple barriers against unauthorized access. Monitoring tools and incident response plans further enhance our security by enabling early detection and prepare for potential breaches.

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




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

## 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.

**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.

**Zain Group**

| System | Availability |
|---|---|
| ERP | 99.99% |
| Oracle Hyperion | 100% |
| Zain Group Website | 100% |

**Zain Bahrain**

| System | Availability |
|---|---|
| Core | 99.85% |
| Charging | 100% |
| Website | 98.74% |

**Zain Iraq**

| System | Availability |
|---|---|
| Core | 100% |
| Charging | 100% |
| Website | 100% |

**Zain Jordan**

| System | Availability |
|---|---|
| Core | 99.99% |
| Charging | 100% |
| Website | 99.72% |

**Zain Kuwait**

| System | Availability |
|---|---|
| Core | 100% |
| Charging | 100% |
| Website | 100% |

**Zain Saudi Arabia**

| System | Availability |
|---|---|
| Core | 100% |
| Charging | 99.82% |
| Website | 99.72% |

**Zain South Sudan**

| System | Availability |
|---|---|
| Core | 100% |
| Charging | 99.99% |
| Website | 100% |

**Zain Sudan**

| System | Availability |
|---|---|
| Core | 86.53% |
| Charging | 99.80% |
| Website | 63.52% |

## Security Risk Training

Since 2020, Zain's PAUSE.THINK.ACT Cyber security Awareness Program has equipped Zainers with the knowledge and skills needed to recognize and respond to potential threats. Through this program, employees learn to identify phishing attempts, follow secure practices, and understand their role in protecting the company. Various channels are used by operations such as email newsletters, SMS, in-person and online training, and induction meetings and workshops. By fostering a culture of vigilance and accountability, information security becomes a shared responsibility, reducing risks and enhancing Zain's overall security posture.

Information security topics covered in 2024

- Business Continuity
- Incident Handling
- Signs of Phishing
- Safe Internet Browsing
- Smishing & Vishing
- Malvertisements
- Malicious Downloads
- Social Engineering Red Flags
- Mobile Device Security

## 2024 Awareness Updates

| | Kuwait | Bahrain | Iraq | Jordan | Saudi Arabia | Sudan | South Sudan |
|---|---|---|---|---|---|---|---|
| **Total Staff** | 1,752 | 223 | 916 | 1,236 | 1,792 | 766 | 155 |
| **Total Number of Staff that received awareness content** | 1,752 | 223 | 916 | 1,236 | 1,792 | 766 | 155 |
| **Total number of channels utilized** | 4 | 4 | 2 | 4 | 3 | 2 | 5 |
| **Channels utilized** | Corporate email<br>Newsletter<br>SMS<br>Induction<br>Assessment program | Learning Platform<br>Instructor Lead Sessions<br>LinkedIn Learning<br>Digital Learning | In-Person Training<br>Online Training | Corporate Email<br>Instagram<br>Internal Learning System, Infographics<br>Phishing Simulation | Workshops<br>Awareness Campaign<br>Awareness Email | Corporate Email<br>Newsletter<br>Teams Sessions | Corporate Email Newsletter<br>WhatsApp<br>SMS<br>In-Person Sessions<br>Teams Meeting |

## 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 27001** | 10-Jan-24 | Zain Bahrain | Binding | Telecommunication Regulatory Authority |
| | 22-Nov-23 | Zain Iraq | Voluntary | AQC |
| | 29-Jan-23 | 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 |
| | 01-Apr-24 | Zain Jordan | Voluntary | SGS |
| | 30-Aug-23 | Zain Saudi Arabia | Voluntary | Intertek |
| **Quality Management System ISO 9001:2015** | 15-Jan-24 | Zain Bahrain | Voluntary | DNV-GL |
| **IT Service Management System ISO 20000-1** | 31-Jan-23 | Zain Kuwait | Voluntary | DNV |

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

- Fortinet Certified Professional Public Cloud Security
- Fortinet Certified Solution Specialist Security Operations
- Cybersecurity Foundations: Governance, Risk, and Compliance (GRC)
- IT Security Foundations: Network Security
- Security Incident Response and Digital Forensics
- Security Operations and Management

# Sustainability Risks Impacting Risk Management

**Physical risks:** As we progress as an organization, we are continuously evolving and changing the way we address climate-related risks and opportunities to ensure the sustainability of our operations. Below highlights the physical and transition risks associated with rising energy costs and global warming, along with our strategies to mitigate these challenges.

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 operations 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 – 1.9: Sustainability Road, SSP2 – 4.5: Middle of the Road, SSP5 – 8.5: Fossil fuel development. We have taken the following estimations per opco: SSP1 1.9 2039 and 2050: Kuwait (0.38, 0.43), KSA (0.27, 0.40), Bahrain (0.38, 0.38), Iraq (0.25, 0.26), Jordan (0.16, 0.17), Sudan (0.14, 0.18) and South Sudan (0.22, 0.33).

SSP5 8.5 2039 and 2050: Kuwait (1.06,2.33), Saudi Arabia (1.1, 2.41), Bahrain (0.99, 2.15), Iraq (1.18, 2.52), Jordan (1.06, 2.3), Sudan (0.9, 2.03), South Sudan (0.68, 1.59). SSP2 4.5 2039 and 2050: Kuwait (0.98, 1.76), Saudi Arabia (1.02, 1.79), Bahrain (0.86, 1.55), Iraq (1.1, 1.86), Jordan (1.02, 1.71), Sudan (0.86, 1.54), South Sudan (0.65, 1.26).

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.

Our biggest operating costs are energy-related to cater to cooling requirements for our telecom and IT systems that require temperatures of approximately 23°C for optimum performance, which is much lower than ambient temperatures in our operations. Our total energy consumption in 2024 was 129.77 MWh and 1066.42 million liters of diesel across seven operations. The 2024 overall energy cost based on actual nine-month operations ending September 2024 and estimated for the calendar year is estimated at USD 155.26 million.

### 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.

To address the power challenge, Zain South Sudan deployed green power solutions including battery-hybrid innovations, solar systems, outdoor equipment, and connection of base station sites to the grid, and performed site-sharing deployments with other MNOs. The strategy followed by Zain is to transform the identified physical and transition risks into opportunities by responding in a way that helps reduce our operating costs with payback periods that do not exceed six years. The implementation of energy efficient solutions led to a reduction in our opex by USD 1.8m in 2023. The benefits of such initiatives will continue for at least five more years (during the life-time of the equipment that was deployed). The initiatives also helped Zain reduce its $CO_2$ emission by 11,106.85 metric tons in 2023.

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

The potential financial impact comes from the implementation of energy efficient solutions on our telecom sites. This financial impact figure has two components: A saving in opex of USD 1.8m in 2023, and an estimated saving in capex of USD 3.6m, totaling USD 5.4m in savings in a single year. It is estimated that opex savings could reach USD 2.25m per year from 2025 due to some initiatives that were implemented late during the reporting year. This provides a maximum annual saving on capex and opex of USD 5.8m.

## Risk Management 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 takes 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 life-time 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.