

11

Enterprise Risk Management



Enterprise Risk Management

The company continues to adapt to the advanced and rapid evolution of technology, simultaneously ensuring it adopts a robust, relevant, and agile Risk Management Framework to mitigate actual and potential risks.

At Zain, the Enterprise Risk Management department reports directly to the Board Risk Committee (BRC), showcasing the importance of the long-term sustainability of the business. The BRC oversees compliance with risk management policies and procedures, and reviews the adequacy of the risk management framework in relation to the risks faced by the organization. Framework changes are reviewed and approved by the BRC on an annual basis, and risk trends are reviewed on a quarterly basis. Zain's assurance 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 assesses its social, economic, and environmental impacts from a risk perspective and has continued to align them with the Corporate Sustainability strategy since 2019. These assessments take into account climate change-related risks and opportunities as well as socio-economic risks. Risks that have the most material impact on Zain are identified through proactive research and comprehensive engagement with stakeholders, so mitigation can be planned at an earlier stage.

Climate Related Risks and Opportunities are explained in depth in the Task Force on Climate-Related Financial Disclosures Report on [page 118](#).

Membership Associations from a Risk Perspective

Zain's regulatory functions are the designated single point of contact for Zain's membership with the GSM Association (GSMA) and the International Telecommunication Union (ITU). Through this relationship, the risk department utilizes the resources for its business operations to gain insights on best practices and international standards. These resources ensure that Zain embeds industry leading standards and policies within its security-related operations.

The GSMA is a global organization unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Zain Group is a member of the Association and participates in a Mobile World Congress event regularly. Zain also receives and shares industry information with other peers in areas of roaming, interconnection and security.

Zain is also a member of the ITU, which is the United Nations' specialized agency for information and communication technologies. The ITU facilitates international connectivity in communications networks to allocate global radio spectrum and develop the technical standards that ensure networks and technologies seamlessly interconnect, and improves access to ICTs to underserved communities worldwide.

Risk Management Framework



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

Zain continues to utilize an impact-likelihood matrix to determine the risk rating of the events facing the company across its operations. The impacts are assessed across multiple parameters that 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.

Governance & Culture

Strategy and Objective-Setting

Performance

Review & Revision

Information, Communication & Reporting

Precautionary Principle

As a precautionary principle, Zain complies to applicable environmental requirements in the design of its products and delivery of services. Rapid advancements in technology is one of the company's principal risks, monitored by the BRC, Climate Action Committee, and the Board. Zain's business depends on technology to develop and deliver low carbon products and services customers require. 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.

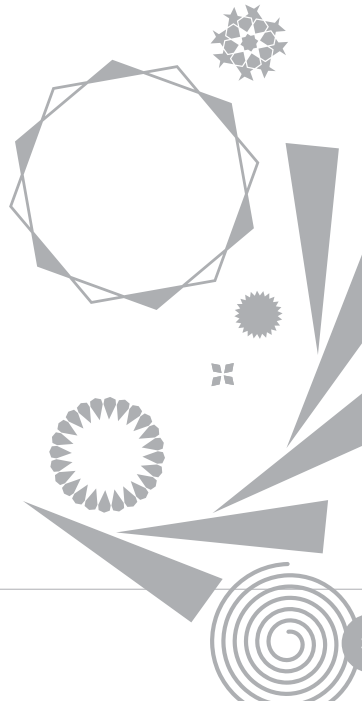


Figure 2: Zain Risk Management Framework (alignment to COSO)

Mission, Vision & Core Values	Strategy Development	Business Objective Formulation	Implementation & Performance	Enhanced Value
-------------------------------	----------------------	--------------------------------	------------------------------	----------------



Data Privacy



The company values personally identifiable information (PII) entrusted by its customers, employees, suppliers and other stakeholders. Zain is committed to the collection, usage, retention, and non-disclosure of PII in a transparent and secure manner, in order to comply with applicable legal and regulatory requirements for processing such information. In 2022, Zain South Sudan received a cybersecurity advisory notice from the National Communications Authority, South Sudan that was shared with all telecom operators in the country. This notice mandated the operators to conduct their own security risk assessments. Zain South Sudan, in consultation with Zain Group's Risk Management, performed a security review and recommended solutions to enhance its security posture.

Zain's operations process customers' Personal Identifiable Information to provide tailored products and services based on demographics and customer behavior. The company discloses that the customer usage data could be analyzed to design products based on customers' profiles. The company ensures that when doing so, it is provided in the company's sales contract (terms and conditions) whilst also complying with specific country rules and regulations. Customers are also provided with a privacy notice through various channels, including the website and sales contract, on processing their personal data. Additional information on Data Privacy governance and policies can be found in 'Our Products and Customers' section on [page 77](#).



Policies and practices related to collection, usage, and retention of customer information and personally identifiable information

Zain Bahrain

Zain Bahrain maintained the ISO 27001 Information Security Management certification. This certification validates Zain's implementation of security controls to safeguard customers' information. Examples of security controls include antimalware, end point detection, and access controls. Additional information on this can be found in Zain Bahrain's Data Privacy Policy: <https://www.bh.zain.com/en/copyright/privacy-policy>

Zain Iraq

In 2022, Zain Iraq conducted cybersecurity and vulnerability assessments, penetration testing, telecom signaling security assessment - SS7, and diameter and GTP protocols to safeguard customer information.

Zain Jordan

A new law for data protection is under revision in Jordan, hence discussions were conducted with all involved parties to assess the risk for PII data, with policies and corrective actions set accordingly.

Zain Kuwait

CITRA's data privacy protection regulation is applicable to both public and private sectors that collect, process and store personally identifiable information. In 2022, Zain Kuwait appointed a Data Privacy Officer, responsible for overseeing appropriate technical and regulatory controls to comply with the regulations.

Zain Saudi Arabia

Zain Saudi Arabia is planning to develop and share a privacy policy with data owners in 2023, setting out details of their personal data processing, including the purpose for which the data is collected and how the data may be processed. Currently, Personal Data Protection and Privacy Impact Assessment requirements are being finalized.

Zain Sudan

Zain Sudan has multiple policies in place to ensure secure practices with respect to collection, usage, and retention of customer information and personally identifiable information, which include:

1. Internal Audits
2. Code of conduct
3. Disciplinary Action Policy
4. Legal Compliance Policy

Zain South Sudan

Zain South Sudan is currently developing information security policies to protect customer data. The policies are set to be finalized by H1 2023.

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 a third-party unless requested by law enforcement, in which case it takes place via a judiciary order.

Further information on Zain's Data Privacy governance and policies can be found in the 'Our Products and Customers' section on [page 81](#).

Zain continues to monitor complaints from third-parties and regulatory bodies, identified leaks and losses of customer data as indicated in the table below:

	COMPLAINTS RECEIVED FROM EXTERNAL PARTIES AND SUBSTANTIATED BY THE ORGANIZATION	COMPLAINTS FROM REGULATORY BODIES	TOTAL NUMBER OF IDENTIFIED LEAKS, THEFTS, OR LOSSES OF CUSTOMER DATA
Zain Bahrain	0	0	0
Zain Iraq	0	0	0
Zain Jordan	0	0	2*
Zain Kuwait	0	0	0
Zain Saudi Arabia	0	0	0
Zain Sudan	0	0	0
Zain South Sudan	0	1**	0

* The two incidents in Jordan were due to human behavior and lack of awareness on control measures despite the implemented controls. The summary for those incidents are as follows:

- Customer information leakage by the shop representatives
- Customer information leakage by the dealers
- Only one customer was impacted by the data leak

** National Communication Authority is providing this information to enable the affected entities to undertake their own security risk assessment and incident analysis, subsequently take the appropriate actions to disinfect the infected systems and networks and to secure their systems and networks.

Data Security

Zain continued to place great efforts to protect its employees and customers from multiple phishing attacks by enabling features where users are able to report such attacks and spam emails through the click of a button, making the investigation process more efficient and allowing immediate action to be taken.

Management Approach to identifying and addressing data security risks

Zain's infrastructure is extremely critical as it processes and stores highly confidential and valuable information that is prone to being targeted heavily by cybercriminals. As technology evolves globally, so do cyber threats, resulting in a variety of negative impacts on individuals, enterprises, and societies.

To mitigate and reduce the possibility and impact of cyber attacks, Zain has developed cyber resilience, which is the ability to effectively identify, protect, detect, respond and recover from potentially catastrophic cybersecurity threats. To achieve cyber resilience, Zain must effectively identify the risks, design robust controls and continuously measure effectiveness to be able to create a sustainable and safe operating environment.

Following is an illustration of a framework referenced in Zain's cyber resilience strategy:



Some examples of cyber security initiatives across Zain's markets include:

- Cybersecurity/vulnerability assessments
- Penetration Testing
- Telecom Signaling Security Assessment
- Reporting all security-related incidents and breaches to the National Telecom Regulatory Authority (NTRA)
- ISO 27001 Information Security Management System certification
- Information Security Training for all employees

Managing Systemic Risks from Technology Disruptions

Mission critical services require continuous availability where breaks in service are intolerable and can result in immediate and significant damage. Zain continues to monitor for any disruptions that occur throughout its major systems:

ZAIN GROUP	
SYSTEM	AVAILABILITY
ERP	100%
Oracle Hyperion	100%
Website zain.com	99.99%

ZAIN BAHRAIN	
SYSTEM	AVAILABILITY
Billing/CRM Service	100%
Charging	100%
Electronic Voucher Distribution	100%
Website bh.zain.com	100%

ZAIN IRAQ	
SYSTEM	AVAILABILITY
Billing	100%
Charging	100%
Electronic Voucher Distribution	100%
Website iq.zain.com	100%

ZAIN JORDAN	
SYSTEM	AVAILABILITY
Billing	100%
Charging	100%
Electronic Voucher Distribution	100%
Website jo.zain.com	100%

ZAIN KUWAIT	
SYSTEM	AVAILABILITY
Billing	99.95%
Charging	99.95%
Electronic Voucher Distribution	99.95%
Website kw.zain.com	99.95%

ZAIN SAUDI ARABIA	
SYSTEM	AVAILABILITY
Billing	99.9996%
Charging	99.9996%
Electronic Voucher Distribution	99.9996%
Website sa.zain.com	99.9996%

ZAIN SUDAN	
SYSTEM	AVAILABILITY
Billing	100%
Charging	100%
Electronic Voucher Distribution	100%
Website sd.zain.com	100%

ZAIN SOUTH SUDAN	
SYSTEM	AVAILABILITY
Billing	100%
Charging	100%
Electronic Voucher Distribution	100%
Website ss.zain.com	100%

Description of systems to provide unimpeded service during service interruptions

1. Electronic Voucher Distribution - System for verification and transfer of credit purchased by customers from shops, website etc to recharge their account for calls, data etc. Used by prepaid customers only.
2. Zain ERP – Enterprise Resource Planning Tool Monitor - uptime in seconds/Month (30*24*60*60 seconds)
3. Oracle Hyperion – Primary financial planning & budgeting tool Monitor - uptime in seconds/Month (30*24*60*60 seconds)
4. Zain website channel – Digital channel to discover services and purchase devices, subscriptions, recharge. Used by both prepaid and postpaid customers Monitor - Website running uptime in seconds/Month (30*24*60*60 seconds)
5. Billing/CRM: The internal billing system used to process and validate billing records, invoices, integration, and reconciliation with other accounting systems.
6. Charging Network allows functionality to be distributed flexibly at a variety of nodes on and off the network, and allows the architecture to be modified to control the services. These networks can separate extra services from the call switching system, making it easier to add new user services such as call screening or call waiting, as well as more complex services such as variable charging, caller ID services, and international messaging.

Security Risk Training

As technology continues to evolve rapidly, it is becoming harder to be aware of new forms of cyber-attacks. As part of the **PAUSE.THINK.ACT** Cybersecurity Awareness Program at Zain, the company continues to raise awareness in regard to the growing popularity of such attacks.

Zain maintains subscriptions to notifications and alerts that are generated from GSMA's Telecommunications Information Sharing Analysis Center's Malware Information Sharing Platform. As cyber attacks are continuously evolving and growing in sophistication and volume, the threat intel that is available to Zain via this platform helps the organization to be proactive in its cyber defenses, and to take the necessary steps to protect Zain and its operating companies from compromise.



Security Risk Training

- QR Codes Attacks
- Bluetooth Attacks
- Insider Threats
- Passwords and two-factor authentication
- Application Updates
- Physical Security
- Malicious Downloads
- Impersonation Attack
- Shoulder Surfing
- Internet Scams

The following list consists of the cybersecurity training courses taken by the Enterprise Risk Management employees across all operations:

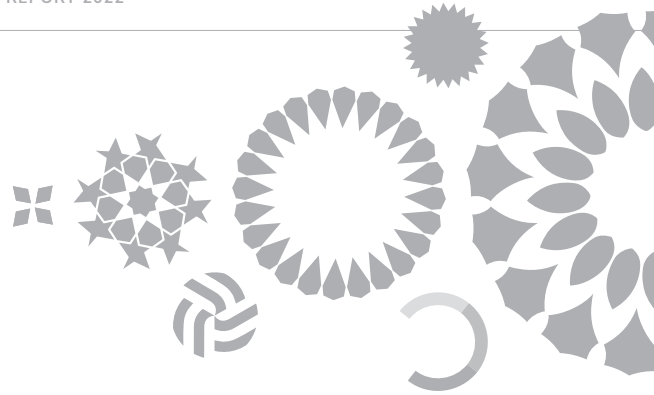
- Certified Information Security Manager – CISM
- Amazon Web Services Solution Architect - Associate
- Amazon Web Services Security Specialty
- ISO 27001 Lead Implementer
- Certified Information Security Manager preparation course
- Cybersecurity Leadership and Management
- Enterprise risk management
- BCM ISO 22301
- Web Application Firewall training (Barracuda)
- 2022 Social Engineering Red Flags
- Telecom Security Workshop
- The External Attack Surface Is Bigger Than You Think
- Fortinet Fast & Secure 2022
- Certified Ethical Hacker (CEH)
- Certified Application Security Engineer (CASE.net)
- Zain Talk - Data Privacy Protection Awareness
- Implementing the NIST Risk Management Framework

2022 AWARENESS UPDATES *

	GROUP	KUWAIT	KSA	BAHRAIN	IRAQ	JORDAN	SUDAN	SOUTH SUDAN
Total Staff	200	1,478	1,752	195	1,069	1,211	783	116
Total Number of Staff that received awareness content	200	1,478	1,752	195	1,069	1,211	783	116
Total number of channels utilized	3	1	3	4	1	4	3	3
Channels utilized	Corporate Email	Corporate Email	Corporate Email	Corporate Email	Induction Session	Corporate Email	Corporate Email	Corporate Email
	Newsletter	Newsletter	Newsletter	Newsletter		Newsletter	Newsletter	Newsletter
	SMS		Wall Display	Digital Banners		Games	Induction	Posters
	Induction		Phishing Exercise	Physical Workshop		Videos	Infosec Week	SMS
				Online Sessions		Awareness Sessions		

* All group-wide employees received security awareness content on mitigating security risks.

Initiatives with External Stakeholders



INITIATIVE	DATE OF ADOPTION	OPCOS IN SCOPE	NATURE OF INITIATIVE (BINDING/VOLUNTARY)	RANGE OF STAKEHOLDERS INVOLVED
Stamp of Approval for Maintenance & Operations	20-May-2019	Zain Kuwait	Voluntary	Uptime Institute Professional Services
	10-Jan-2021	Zain Bahrain	Binding	Telecommunication Regulatory Authority
Information Security Management System ISO 27001:2013	02-Feb-2021	Zain Kuwait	Voluntary	DNV-GL
	15-Jan-2020	Zain Jordan	Voluntary	SGS
	05-Apr-2018	Zain Sudan	Voluntary	DNV-GL
Business Continuity Management System ISO 22301:2012	Feb-2020	Zain Kuwait	Voluntary	DNV-GL
	28-Jan-2020			
Environmental Management System ISO 14001:2015	03-Feb-2021	Zain Kuwait	Voluntary	DNV-GL
Quality Management System ISO 9001:2015	16-April-2018	Zain Sudan	Voluntary	DNV-GL
	03-Feb-2021	Zain Kuwait	Voluntary	DNV-GL
	15-Jan-2021	Zain Bahrain	Voluntary	DNV-GL

