CHAPTER 10

Enterprise Risk Management

Zain is consistently adapting to rapid technological advancements while also making certain that it embraces a strong, relevant, and agile Risk Management Framework to address existing and potential risks. The Enterprise Risk Management (ERM) department is responsible for identifying, assessing, prioritizing, and managing potential risks, and takes a proactive approach to risk mitigation and strategic decision-making. An example of this includes assessment of information security controls in place, which address the security threats that are continuously evolving at a rapid pace.

The ERM function reports directly to the Board Risk Committee (BRC), which supervises the adherence to the 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, environment, and human rights impacts from a risk standpoint through proactive research and extensive engagement with its 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 page 105.

MEMBERSHIP ASSOCIATIONS FROM A RISK PERSPECTIVE

Zain Group has various memberships to global associations that ensure the company is in sync with industry standards and global best practices, including:

- The GSMA is a global organization unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change.
- The ITU is the United Nations' specialized agency for information and communication technologies to facilitate international connectivity in communications networks, to allocate radio spectrum globally, and develop the technical standards that ensure networks and technologies seamlessly interconnect, and improve access to ICT to underserved communities worldwide.
- Zain Group also participates in the Mobile World Congress and shares industry information with peers with regards interconnectivity and security.

RISK MANAGEMENT FRAMEWORK

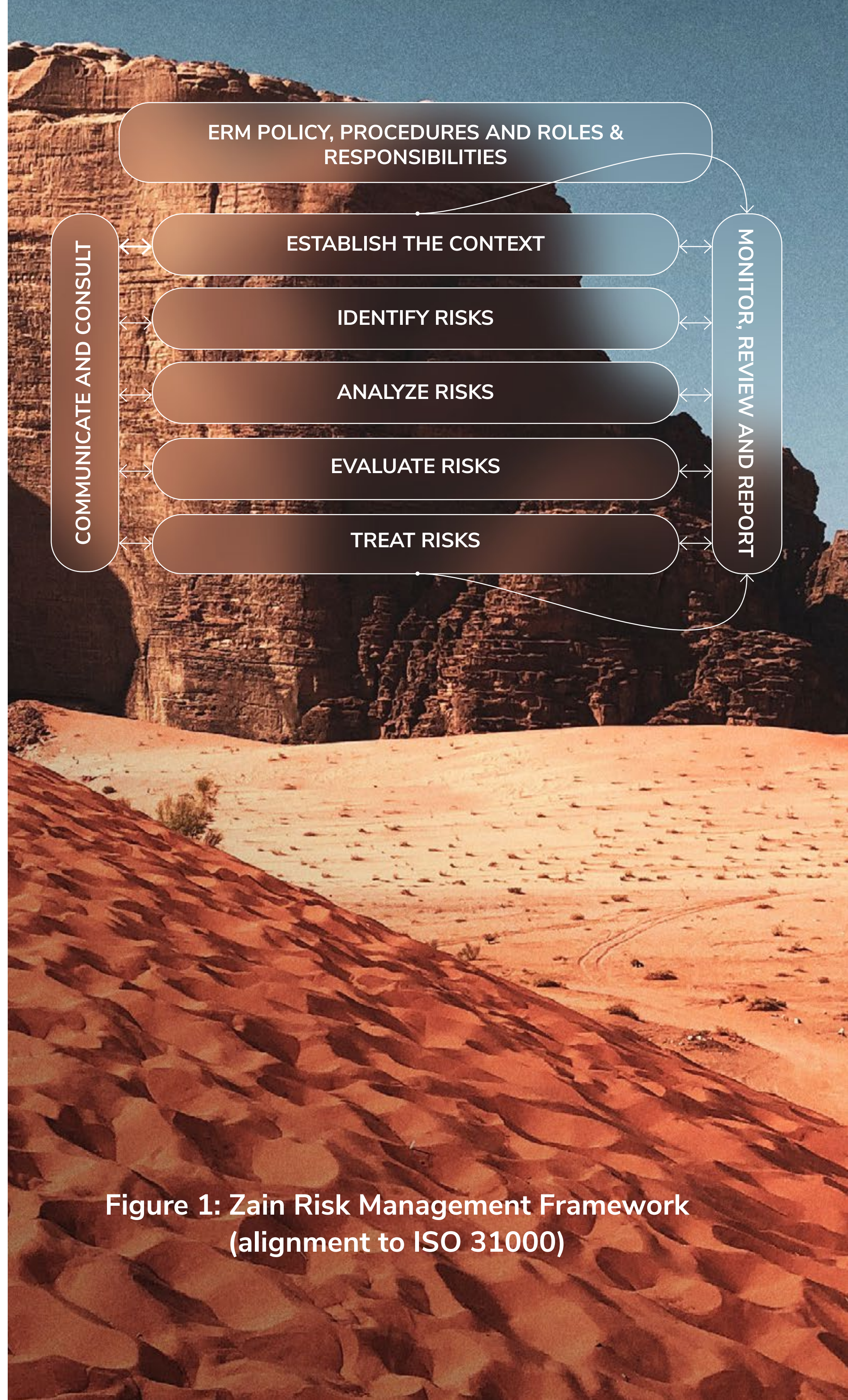


Figure 1: Zain Risk Management Framework (alignment to ISO 31000)

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.

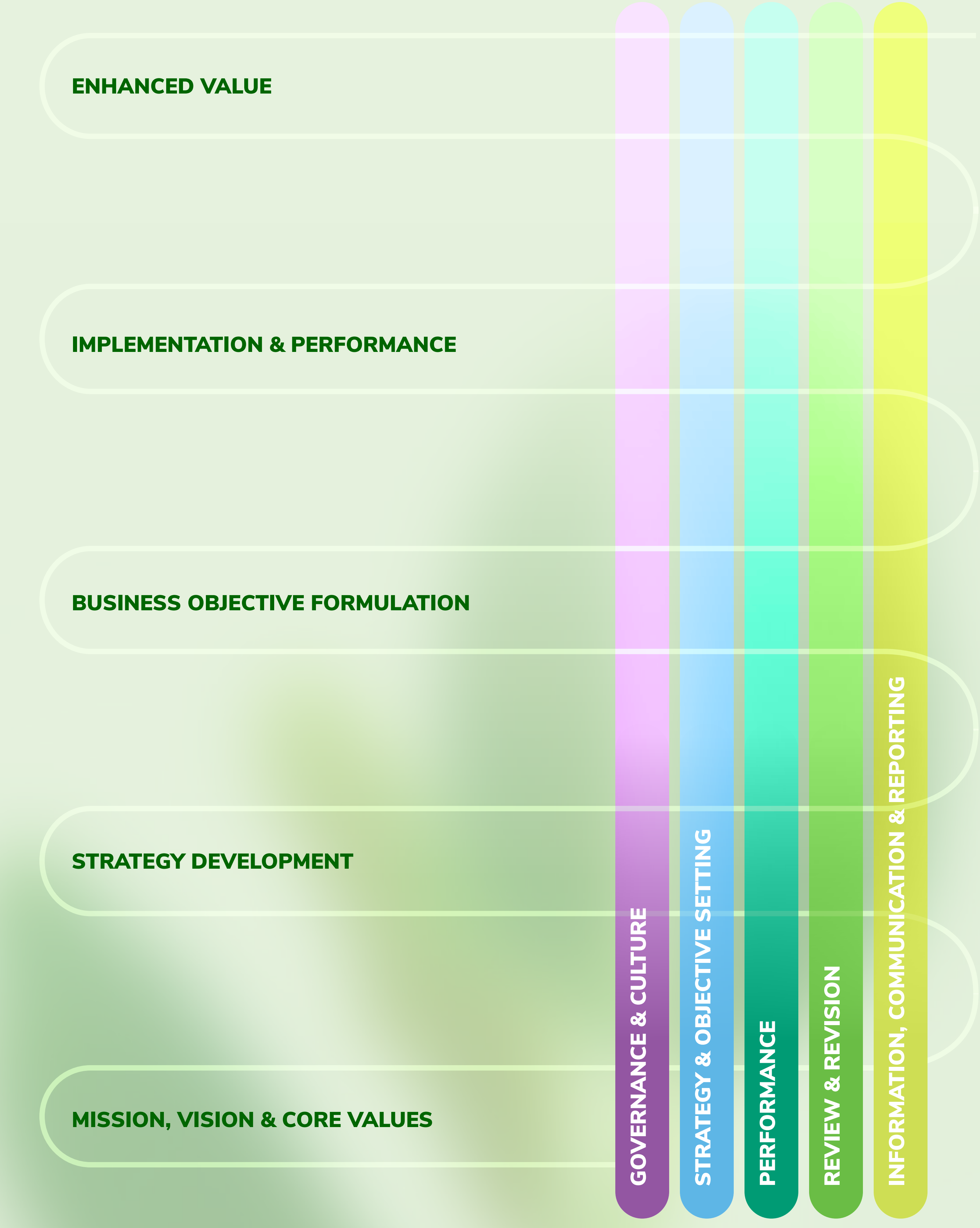

ENHANCED VALUE
IMPLEMENTATION & PERFORMANCE
BUSINESS OBJECTIVE FORMULATION
STRATEGY DEVELOPMENT
MISSION, VISION & CORE VALUES
GOVERNANCE & CULTURE
STRATEGY & OBJECTIVE SETTING
PERFORMANCE
REVIEW & REVISION
INFORMATION, COMMUNICATION & REPORTING

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

PRECAUTIONARY PRINCIPLE

When Zain designs its products and delivery of services, as a precautionary principle, all applicable environmental requirements are taken into consideration. Zain’s business focuses on developing and delivering low carbon products and services as customers require to align to the company’s Net-Zero ambition. Climate-related considerations such as energy use and end-of-life disassembly for repair or reuse are some of the key conisderations included in the checklist when it comes to designing products and services.

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. Through such engagements, the Board Risk Committee, Climate Action Committee (CAC) and the Board monitor key risks such as rapid advancements in technology.

DATA PROTECTION AND PRIVACY

Zain considers data privacy as a crucial part of controls to avoid data leakage. In order to comply with legal and regulatory governing bodies and their requirements, Zain regards the personally identifiable information (PII) entrusted by its customers, employees, suppliers, and other stakeholders highly, and processes involved in the collection, use, retention, and non-disclosure of this information.

In 2023, Zain updated its Data Protection and Privacy Policy to ensure that it continues to meet the highest standards of data protection and privacy for all of its stakeholders. The policy was approved by the Board, and ensures Zain remains compliant to all relevant data protection and privacy laws and regulations. The revised policy covers a range of topics including how the company collects, uses, and stores personal data and the rights of individuals to access and control their personal data.

The policy can be found here

Policies and practices related to collection, usage, and retention of customer information and personally identifiable information 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 implemented several security controls and follows best practices to ensure that all data processed is secure. In 2023, Zain Iraq was ISO 27001 certified, providing further assurance on the implemented controls to safeguard data.

ZAIN JORDAN

A new law for data protection was launched and an analysis was conducted by the Legal and Regualtory team to set workshops with all involved parties to assess the risk for PII data and 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.

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.

ZAIN SOUTH SUDAN

Zain is continuously enhancing its security controls to improve its security maturity and to defend against threats and safeguard data from such threats. Several security control assessments are carried out to identify potential improvements that can be implemented.

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 judicial order.

Further information on Zain's Data Privacy governance and policies can be found in the 'Products and Services' section on page 64.

As of 2023, there have been no reports or complaints from external third-parties and regulatory bodies, or the identification of leaks or losses of customer data.

DATA SECURITY

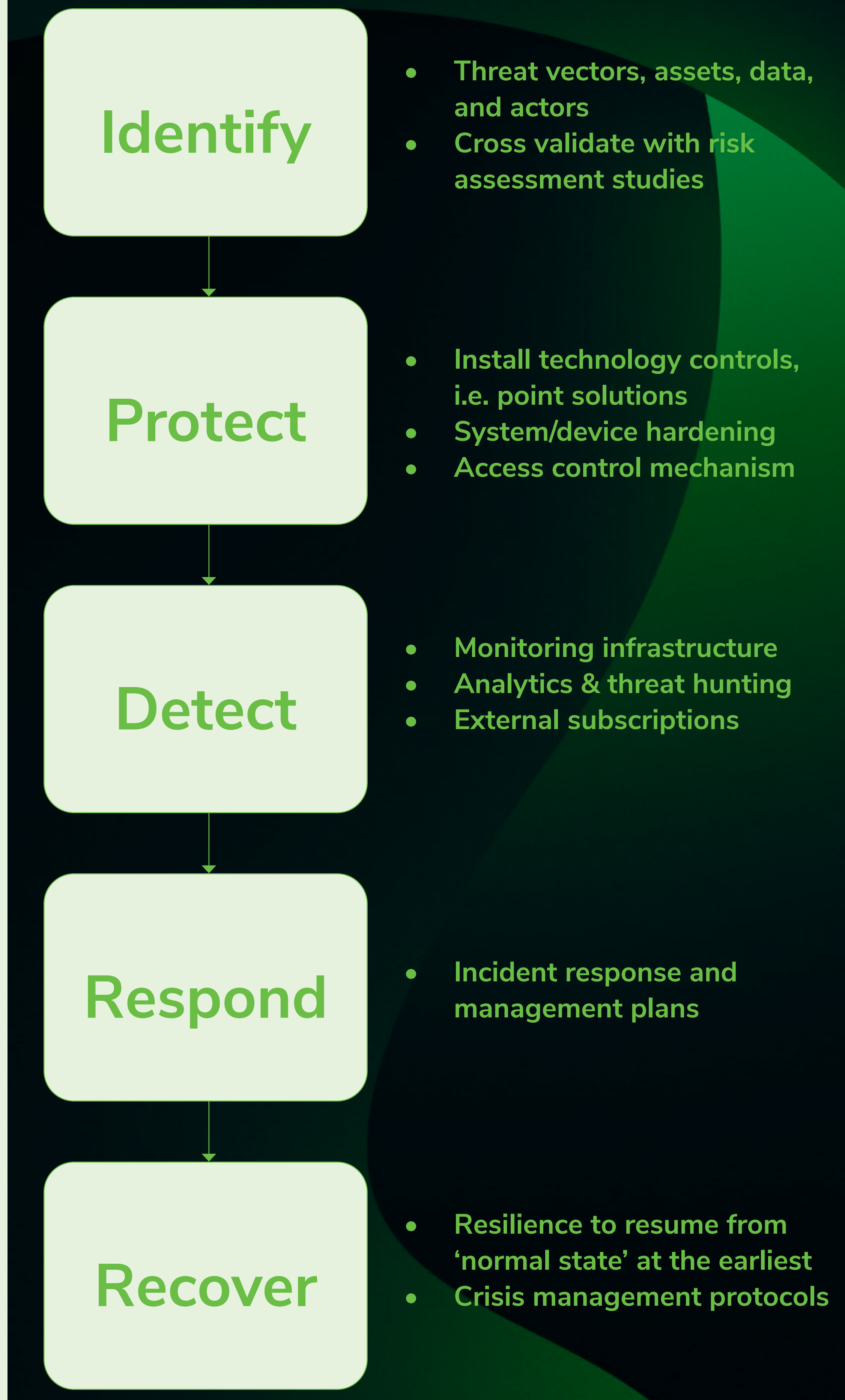
Zain continued its commitment to safeguarding its employees and customers against phishing attacks, where the company facilitated a user-friendly reporting system, allowing individuals to report such attacks and spam emails with a simple click. This initiative streamlines the investigation process, significantly enhancing operational efficiency, and enabling the prompt implementation of corrective actions.

MANAGEMENT APPROACH TO IDENTIFYING AND ADDRESSING DATA SECURITY RISKS

Zain stores and processes information that is highly confidential and can be very valuable in the hands of cyber criminals. This is why the company's infrastructure is considered extremely critical. The threat landscape is ever evolving, which requires a continuous and rigorous enhancement of security controls.

Zain has in-place the necessary security controls and processes aligned with best practices to mitigate and reduce the possibility and impact of cyber attacks. The company has developed cyber resilience, which is the ability to effectively identify, protect, detect, respond and recover from potentially catastrophic cyber security threats. To ensure a safe and secure environment, Zain must protect its infrastructure with the necessary policies, procedures, and continuous monitoring activities to defend against threats.

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



Identify

- Threat vectors, assets, data, and actors
- Cross validate with risk assessment studies

Protect

- Install technology controls, i.e. point solutions
- System/device hardening
- Access control mechanism

Detect

- Monitoring infrastructure
- Analytics & threat hunting
- External subscriptions

Respond

- Incident response and management plans

Recover

- Resilience to resume from 'normal state' at the earliest
- Crisis management protocols

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

- Cyber security/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 monitors for any disruptions that occur throughout its major systems.

Description of systems to provide unimpeded service during service interruptions

Core: Includes PS Core and CS Core (previously mentioned in prior Zain Sustainability Reports).

CS Core: Circuite Switch, handling voice calls and containig functionaities such as mobile switching center (MSC) and gateway MSC (GMSC).

PS Core: Packet Switch, handling data sessions and containig functionalities such as: S+H9erving GPRS support node (SGSN), gateway GPRS support node (GGSN), domain name server (DNS), dynamic host configuration protocol (DHCP) server, packet charging gateway, etc.

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

Zain Group

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

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	99.96%
Charging	100%
Website	99.99%

Zain Kuwait

System	Availability
Core	99.95%
Charging	99.95%
Website	100%

Zain Saudi Arabia

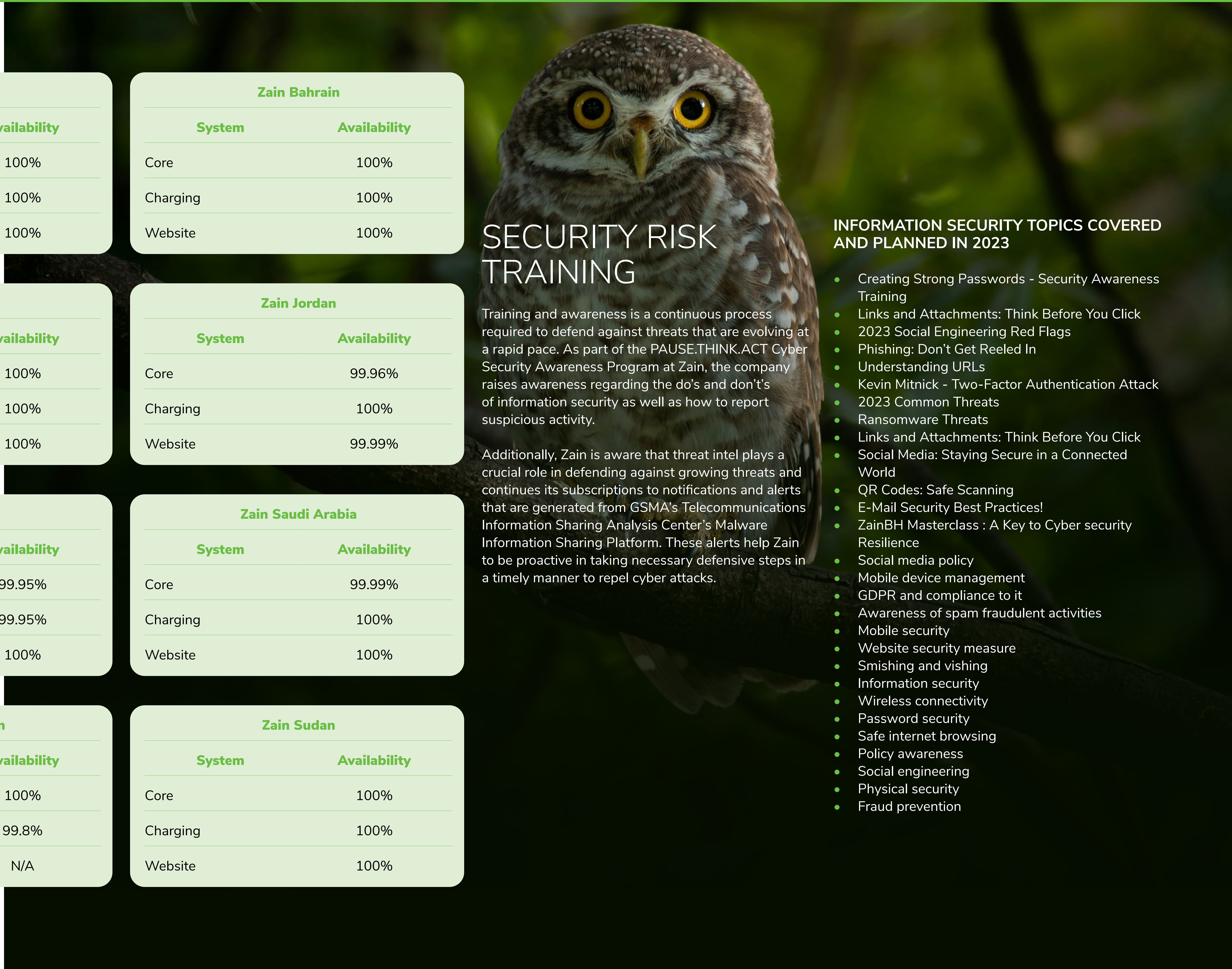
System	Availability
Core	99.99%
Charging	100%
Website	100%

Zain South Sudan

System	Availability
Core	100%
Charging	99.8%
Website	N/A

Zain Sudan

System	Availability
Core	100%
Charging	100%
Website	100%



SECURITY RISK TRAINING

Training and awareness is a continuous process required to defend against threats that are evolving at a rapid pace. As part of the PAUSE.THINK.ACT Cyber Security Awareness Program at Zain, the company raises awareness regarding the do's and don't's of information security as well as how to report suspicious activity.

Additionally, Zain is aware that threat intel plays a crucial role in defending against growing threats and continues its subscriptions to notifications and alerts that are generated from GSMA's Telecommunications Information Sharing Analysis Center's Malware Information Sharing Platform. These alerts help Zain to be proactive in taking necessary defensive steps in a timely manner to repel cyber attacks.

INFORMATION SECURITY TOPICS COVERED AND PLANNED IN 2023

- Creating Strong Passwords - Security Awareness Training
- Links and Attachments: Think Before You Click
- 2023 Social Engineering Red Flags
- Phishing: Don't Get Reeled In
- Understanding URLs
- Kevin Mitnick - Two-Factor Authentication Attack
- 2023 Common Threats
- Ransomware Threats
- Links and Attachments: Think Before You Click
- Social Media: Staying Secure in a Connected World
- QR Codes: Safe Scanning
- E-Mail Security Best Practices!
- ZainBH Masterclass : A Key to Cyber security Resilience
- Social media policy
- Mobile device management
- GDPR and compliance to it
- Awareness of spam fraudulent activities
- Mobile security
- Website security measure
- Smishing and vishing
- Information security
- Wireless connectivity
- Password security
- Safe internet browsing
- Policy awareness
- Social engineering
- Physical security
- Fraud prevention

2023 AWARENESS UPDATES

	Kuwait	Saudi Arabia	Bahrain	Iraq	Jordan	Sudan	South Sudan
Total Staff	1,773	1,798	385	912	1,186	788	145
Total Number of Staff that received awareness content	1,773	1,798	385	912	1,186	788	145
Total number of channels utilized	5	1	4	1	1	2	3
Channels utilized	Posters Banners Corporate Email Newsletter SMS Induction	Phishing Awareness Session	Corporate Email Newsletter PC Lock Screen Live Sessions Awareness Platform	Induction Session	Corporate Email Newsletter	Corporate Email Newsletter Induction Social Media	Corporate Email Newsletter WhatsApp SMS Physical Sessions

The following list consists of the cyber security training courses taken by entreprise risk management employees across Zain's operations.

- Certified Risk and Compliance Professional
- Certified in Risk and Information Systems Control
- ISO22301 Lead Auditor
- COBIT
- Security Operations Management
- Cyber Security 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 27001:2013	10-Jan-21	Zain Bahrain	Binding	Telecommunication Regulatory Authority
	07-Jan-23	Zain Iraq	Voluntary	AQC
	2-Feb-21	Zain Kuwait	Voluntary	DNV-GL
	15-Jan-20 21-Jun-23	Zain Jordan	Voluntary	SGS
	11-Apr-21	Zain Sudan	Voluntary	DNV-GL
Business Continuity Management System ISO 22301:2012	Feb-20 28-Jan-20 29-Jan-23	Zain Kuwait	Voluntary	DNV-GL
Environmental Management System ISO 14001:2015	03-Feb-21	Zain Kuwait	Voluntary	DNV-GL
Quality Management System ISO 9001:2015	03-Feb-21	Zain Kuwait	Voluntary	DNV-GL
	15-Jan-21	Zain Bahrain	Voluntary	DNV-GL
IT Service Management System ISO 20000-1	31-Jan-23	Zain Kuwait	Voluntary	DNV-GL