ZAIN RISK MANAGEMENT POLICY

Version 2.2

Document Control and Revisions Logs

Document Properties

Document Title	Zain Risk Management Policy
Author	Zain Group Risk Management
Creation Date	15/06/2014
Last Updated	17/02/2025
Last Version	2.2

Change Record

Date	Version	Author	Description of change
15/06/2014	1.0	Jacxine Fernandez	Document prepared as per the industry leading practices
16/03/2016	1.1	Jacxine Fernandez; EY	Strategy realigned as per directive from BRC
05/03/2017	1.2	Jacxine Fernandez	Annual review
13/01/2019	1.3	Jacxine Fernandez	Ad-hoc Review
30/01/2020	1.4	Manakkal Kailash	Annual Review
26/01/2021	1.5	Shakeel Aboobakar	Annual Review
25/01/2022	1.6	Manakkal Kailash	Annual Review
31/01/2023	2.0	Manakkal Kailash	Annual Review
25/01/2024	2.1	Manakkal Kailash	Annual Review
17/02/2025	2.2	Manakkal Kailash	Annual Review

Reviewers

Name	Designation	Version	Date
AbdulGhaffar Setareh	Zain Group Risk Director	1.0	15/06/2014
AbdulGhaffar Setareh	Zain Group Chief Risk Officer	1.1	16/03/2016
AbdulGhaffar Setareh	Zain Group Chief Risk Officer	1.2	05/03/2017
AbdulGhaffar Setareh	Zain Group Chief Risk Officer	1.3	13/01/2019
Mohammad Al Tarakma	Zain Group Risk Director	1.4	30/01/2020
AbdulGhaffar Setareh	Zain Group Chief Risk Officer	1.4	30/01/2020
Mohammad Al Tarakma	Zain Group Risk Director	1.5	26/01/2021
AbdulGhaffar Setareh	Zain Group Chief Risk Officer	1.5	31/01/2021
Mohammad Al Tarakma	Zain Group Risk Director	1.6	26/01/2022
AbdulGhaffar Setareh	Zain Group Chief Risk Officer	1.6	31/01/2022
Mohammad Al Tarakma	Zain Group Risk Director	2.0	14/02/2023
AbdulGhaffar Setareh	Zain Group Chief Risk Officer	2.0	14/02/2023
AbdulGhaffar Setareh	Zain Group Chief Risk Officer	2.1	14/02/2024
AbdulGhaffar Setareh	Zain Group Chief Risk Officer	2.2	17/02/2025

Approvals

Name	Designation	Version	Date
AbdulGhaffar Setareh	Zain Group Risk Director	1.0	20/06/2014
Board Risk Committee	Chairperson	1.1	16/03/2016
Board Risk Committee	Chairperson	1.3	07/02/2019
Board Risk Committee	Chairperson	1.4	12/02/2020
Board Risk Committee	Chairperson	1.5	23/02/2021
Board Risk Committee	Chairperson	1.6	10/02/2022
Board Risk Committee	Chairperson	2.0	23/02/2023
Board Risk Committee	Chairperson	2.1	06/03/2024
Board Risk Committee	Chairperson	2.2	24/02/2025

Endorsements

As per	Version	Date
Zain Risk Management Strategy	1. 6	25/01/2022
Zain Risk Management Procedures	1. 6	25/01/2022
Zain Risk Management Strategy	2.0	23/02/2023
Zain Risk Management Strategy	2.1	18/02/2024
Zain Risk Management Strategy	2.2	24/02/2025

Approvals and Revisions

The Strategy & Policy should be reviewed at least annually. Proposed amendments to the procedures should be submitted to the Board Risk Committee (hereinafter referred to as “BRC”) for consideration and approval.

Table of Contents

1. Risk Management Policy

1.1 Overview

To achieve its objectives in dynamic and complex environments, Zain continues to enhance the Enterprise Risk Management process. The Board Risk Committee shall steer initiatives to embed a risk-awareness culture across the enterprise and orient the businesses to risks. This will enable Zain to catalyze and grow to achieve its business objectives.

Key Benefits:

a) Encompasses all types of risks facing an organization

b) Prioritization and management of risks as an interrelated risk portfolio rather than in individual “silos”

c) Scope to align the role of assurance functions and the role of Risk Management

d) Reduction of occurrence of surprises through enhanced monitoring

e) Embeds risk management as a component in all critical decisions throughout the organization

f) Effective reporting to the Board and senior management team on risks and effectiveness of mitigation measures

The Enterprise Risk Management (hereafter referred to as ‘ERM’) framework described in this document has been benchmarked with leading global risk management standards and guidance available such as Committee of Sponsoring Organization (COSO) framework and ISO 31000:2018-02. It has been designed to provide simplicity and practicality required for implementing an enterprise-wide process. Refer Annexure 1 for details on benchmarking.

Enterprise Risk Management process needs to form part of every decision making and monitoring process. In this regard, specific roles and responsibilities, tools, enablers, and guidance have been developed and have been made available for reference. Risks will be systematically assessed, mitigated, and monitored thus embedding the desired risk management culture in undertaking business activities.

1.2 Purpose

- Define the vision for Enterprise Risk Management at Zain
- Develop a well established risk management culture within Zain, that ensures the following:
    - Risks are well defined and captured
    - Quantitative assessments where relevant and feasible
    - Risk measures are accurate
    - Risk remediation plans and Controls are active and monitored
    - Management of risks is proactive and integrated

- Introduce and define the risk management policy associated with the activities of Zain. This policy defines the risk management control framework that allows the Group to identify, monitor, manage, mitigate and control exposure to all the major risks inherent in the activities of the Group.
- Provide the basis for the on-going risk management function in Zain facilitating the optimization of shareholder value, as well as complying with the regulatory requirements and the industry best practices.
- It is envisaged that by implementing this policy , the Group will be able to monitor and control their risk exposures more effectively.
- All personnel carrying out the risk management functions on behalf of the Group should ensure that they comply with the requirements of this Policy.
- This policy shall provide a means to ensure that the Senior Management is in a position to make informed business decisions based on risk assessment;
- This document defines the related roles and responsibilities of Zain' executives, managers, and personnel in the management of risk

1.3 Scope

The scope of this policy includes all people, processes and technologies used for Zain business purposes and is also applicable to all Zain Operating Companies and their subsidiaries.

This policy sets out the Group's risk management guidelines, which are aligned with Zain's overall business strategy as well as assisting the Board and Senior Management in implementing an effective framework for managing the key risks.

This Policy is divided into the following sections:

- Overall principles and guidelines for Risk Management at Zain
- Overall Enterprise Risk Management Framework at Zain
- Sections that provide guidance on the identifying, assessing, monitoring and reporting of the following key risks within the Group
- Strategic Risk Management
- Operational Risk Management
- Financial Credit Risk Management
- Legal & Compliance Risk Management

1.4 References

- Risk Management Procedures
- Risk Management Roles & Responsibilities

1.5 RACI Matrix

Zain Group Risk Management Policy	Responsible (R)	Accountable (A)	Consulted (C)	Informed (I)
Policy development and maintenance	Group Risk Management Function	Board Risk Committee	Executive Management	Risk Owners and Risk Champions
Policy approvals	Board Risk Committee	NA	NA	NA
Policy Enforcement				
- Group Level	Group Risk Management Function	Executive Management	NA	Board Risk Committee
- Operating Companies	OpCo Risk Management Function / OpCo Head of Risk	OpCo Executive Management	Group Risk Management Function	Board Risk Committee
Policy Compliance Monitoring	Risk Management Function; Risk Owners and Risk Champions	Board Risk Committee	NA	NA

1.6 Approvals and Revisions

The Policy should be reviewed at least annually. Proposed amendments to the procedures should be submitted to the Board Risk Committee (hereinafter referred to as “BRC”) for consideration and approval

2. Principles of Risk Management at Zain

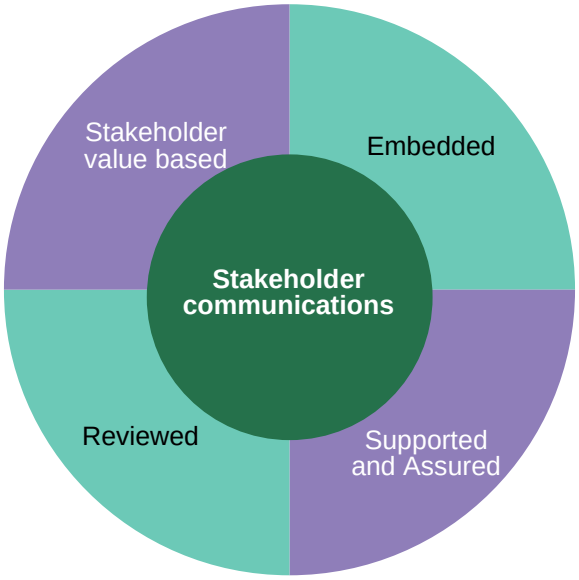
2.1 Vision statement

Enterprise Risk Management's vision is to support the achievement of business and strategic goals through a collaborative risk management environment that proactively identifies and mitigates business risk.

Zain recognizes that profit is the reward for taking and effectively managing risks. Zain will leverage ERM as a part of its strategic decision-making processes. Zain's management understands its capacity to bear risk and accordingly articulates its appetite for risk. Using a systematic and consistent approach Zain will proactively identify current and emerging risks and manage those risks within its appetite.

Zain seeks to be recognized as employing an industry-leading Enterprise Risk Management framework.

Risk Management at Zain is driven by four **key tenets of risk management**:



- **Stakeholder value based:** Risk management will be focused on sustaining the creation of shareholder value and protecting against the erosion of value.
- **Embedded:** The culture of the organization will reflect the risk consciousness of the Board Risk Committee. Risk management will be explicitly embedded in existing processes. This requires suitable business structures, policies and procedures, technology and appropriate staff training in risk management which enables risk to be managed at all levels of the business.
- **Supported and Assured:** Risk management will provide support in establishing appropriate processes and technology to ensure that current risks are being managed appropriately and that early warning indicators are in place to address future risks. Audit Services will provide assurance over the effectiveness of these processes.

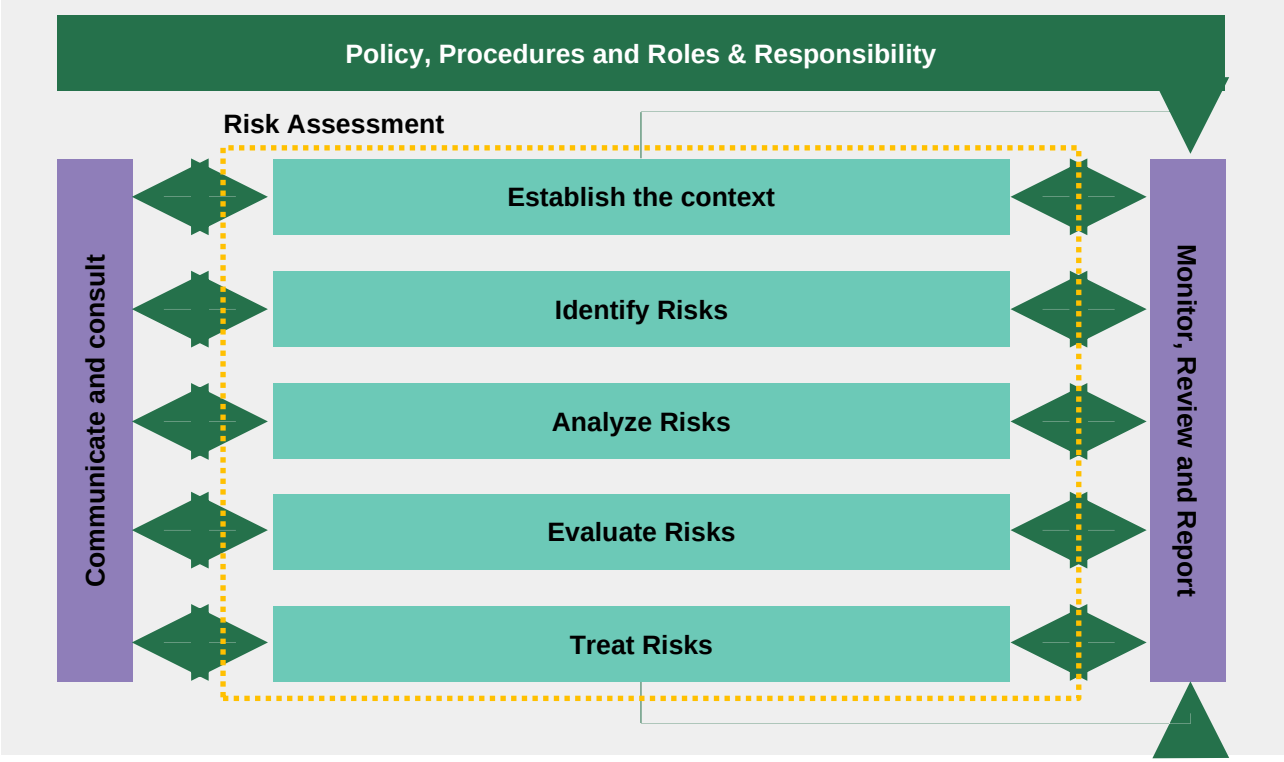
- **Reviewed:** The Board Risk Committee will review the effectiveness of the risk management program on a regular basis to assess its ongoing contribution to the effective and efficient operation of the business in light of changing business conditions.

The primary **guidelines** in effective risk management are as follows:

- **Risk management is everyone's responsibility:** Risk management is everyone's responsibility, from the Board of Directors to individual employees. Each is expected to understand the risks that fall within the limits of their accountabilities and is expected to manage these risks with approved risk tolerances.
- **Significant risks are identified and managed through an integrated approach:** Methods will be established or enhanced to promote a balanced approach to risk that considers risk and return. Each function is expected to undertake risk assessments on no less than an annual basis for the business as a whole, and as determined locally for elements below the functions.
- **Integration into major business processes:** Risk Management will be integrated with major business processes such as strategic planning, business planning, operational management, investment decisions to ensure continuous consideration of risks in all decision- making.
- **A comprehensive, disciplined, consistent approach:** Risk Management is a comprehensive, disciplined, and continuous process in which risks are identified, analyzed, and consciously accepted or mitigated within approved risk tolerances.
- **Continuous evolution:** Risk Management will continue to evolve to reflect industry best practices and Zain's needs. This policy will be reviewed annually by the Board Risk Committee..
- **Consistent with Corporate Policies:** Local risk management policies and processes will be consistent with this corporate policy. Additionally, all local policies and processes will facilitate the upward consolidation and review of all significant business risks.

3. Enterprise Risk Management Framework

The success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the organization at all levels. The framework assists in managing risks effectively through the application of the risk management process at varying levels and within specific contexts of the organization. The framework ensures that information about risk derived from the risk management process is adequately reported and used as a basis for decision making and accountability at all relevant organizational levels.



The objective of the Risk Management Framework is to formalize and communicate Zain's approach to the management of risk. It will have the following attributes:

- Responds to the Executive Management's need for enhanced risk information and improved governance;
- Provides the ability to prioritize, manage and monitor the increasingly complex risks in the business;
- Provides an explicit, comprehensive process to satisfy the regulators, and other stakeholders, that significant risks are being effectively managed.

An effective Risk Management Framework comprises of:

1. **Risk management process;** and
2. **Risk management structure.**

3.1 Risk Management Process

3.1.1 Risk Assessment

Risk assessment consists of four steps:

a) **Risk identification:** Identifying relevant risks that can adversely affect the achievement of Zain's objectives.

b) **Risk analysis:** Understanding the impact and likelihood of risks as well as their root causes and the level of control that Zain can exert over them.

c) **Risk Evaluation**: It involves comparing the risk found during risk analysis and need of risk treatment according to Zain's risk priorities.

d) **Risk Prioritization:** Prioritizing risks based on their level of importance or strategic value to Zain as defined by their ability to adversely impact the achievement of the Zain's strategic objectives. It should also take into account the severity of risk compared to risk appetite

3.1.2 Risk Appetite

To achieve the optimal balance of risk and reward that will enable the achievement of its strategic objectives, Zain's Board Risk Committee has articulated the maximum amount of risk Zain is willing to accept and based on which risk rating criteria have been defined. Any risk that breaches the Zain's stated risk appetite must be mitigated as a matter of priority to within acceptable levels.

Each Unit / Department within Zain may articulate their own risk appetite; however, these should at no time exceed the risk targets set at the Company level. Furthermore, it is necessary that any risk targets set at the Unit / Department level facilitate the consolidation and aggregation of risks at the Company level

The Group Enterprise Risk Management function shall define Company risk appetite and present it to the Board Risk Committee for approval. The Risk appetite shall be reviewed on an annual basis.

These levels are articulated in the Zain Risk Management Procedures v2.2

In addition to the above, Zain has the below 'Zero Tolerance/ Zero Appetite' thresholds:

- Zain has no appetite for fraudulent behaviour.
- Zain has no appetite for illegal or unethical behaviour, internally and externally
- Zain has no appetite for work place discrimination and is committed to providing equal opportunities, respect and dignity to all its stakeholders
- Zain has no appetite for behavior or actions that lead to safety breaches.

3.1.3 Risk Response

Risk response consists of determining the appropriate action to maintain risk within the levels defined by Zain's risk appetite. Appropriately responding to risks involves identifying existing response strategies and the need for any additional response. Accordingly, ownership and responsibilities for the risk response plans are articulated and approved. The following are the possible risk mitigation strategies that can be adopted:

- **Accept** – No action is taken to change the severity of risk and is taken when the risk is already covered in the risk appetite
- **Avoid** – Risk avoidance involves taking the decision not to engage in any activity that may result in the risk event, i.e. usually ceasing the activity that may lead to the risk event
- **Transfer** – Risk transfer involves shifting the impact of a risk event and the ownership of the risk mitigation to a third party
- **Mitigate** – Risk mitigation reduces the probability and / or impact of a potential risk to a more acceptable level. Mitigation could involve allocation of resources, , conducting additional tests on the product, designing redundancy into a system, and designing a quality control or reconciliation. This is primarily about instituting controls to address the impact or likelihood.
- **Adapt** – Adapting may result in significant changes to existing procedures and / or recognizing a potential risk event as an opportunity and then assessing the possibility of different approaches to capitalize on the opportunity.

3.1.4 Risk Monitoring, Review and Reporting

Risk monitoring and review includes an ongoing assessment of the risk management process to ensure the effectiveness of process design, implementation and outcomes and reporting consists of providing the Board Risk Committee and Senior Management with information on Zain's risk profile and the status of risk response plans in accordance with the procedures and roles and responsibilities outlined in this document.

3.1.5 Communicate and Consult

Communication facilitates a holistic approach to identifying, assessing, and managing risk and facilitates the development of a culture where the positive and negative dimensions of risk are openly discussed. By involving stakeholders from all levels of Zain in the risk management process the risk management framework will create an environment where the discussion of risks and the associated response strategies are viewed as an integral part of decision making.

Effective risk management also incorporates the input of different perspectives to balance intrinsic human biases in the understanding of risk.

Stakeholder communication and consultation will be incorporated into the risk management process at Zain primarily using the following three means:

a. **Facilitated workshops –** Risks will be assessed during cross-functional risk assessment workshops. Stakeholders may have a different perspective on the impacts or likelihood of a risk occurring. Assessing risks in a forum that promotes transparent discussion enables Zain to gain a more comprehensive understanding of the risks its faces.

b. **Risk review and aggregation –** Zain's risk governance structure provides a mechanism through which risks are reviewed and aggregated upwards through the organization structure. Review and aggregation enables executives to interrogate and analyze Zain's risk profile from the perspectives of different levels of management.

c. **Risk reporting –** Regular risk reporting provides a mechanism where key stakeholders have the required information for decision making. In addition to upward reporting through the organization structure, business units will have direct reporting lines to the Group Risk Management Function to provide the raw data necessary for objective analysis.

3.2 Risk Management Structure

The risk management process at Zain is supported by a set of enablers that embed risk management into Zain's business processes. The enablers consist of:

3.2.1 Procedures: The Risk Management Framework defines the Group's risk appetite and underlying principles for managing risks and undertaking transactions. The same has been detailed in the Risk Management Procedures document.

3.2.2 Risk Management Activity Calendar: summarizes the risk management activities to be completed as well as milestones and timeframes. The same has been detailed in the Risk calendar.

Sr. No.	Risk Management Function Activity	Description	Frequency
1	Annual Risk identification and prioritization	Development of top 'Risk That Matter' (RTM) & Risks under the Radar across Zain & all OpCos	Annual
2	Key Risk Indicators trending and movement of RTMs	Refresher of top risks across Zain & OpCos	Quarterly
3	Review risk mitigation	Refresher and assessment of mitigation plans for top risks across Zain & OpCos	Quarterly
4	Board Risk Committee (BRC) meeting to review annual risk assessment and mitigation results	Discussion of top risks & mitigation plans across Group and OpCos and alignment of annual budgeting and planning with the same.	Annual
5	Roll out of self-assessments for existing mitigation plans	Assessment of effectiveness of mitigation plans for identified risks by Risk Owners / Risk Champions / OpCo RM function through residual risk assessment and KRI monitoring	Quarterly
6	Board Risk Committee (BRC) meeting to review quarterly risk updates and mitigation results	Presentation of results of mitigation plans / risks assessment and key risk indicators to the Board Risk Committee by Group Risk Management function	Quarterly

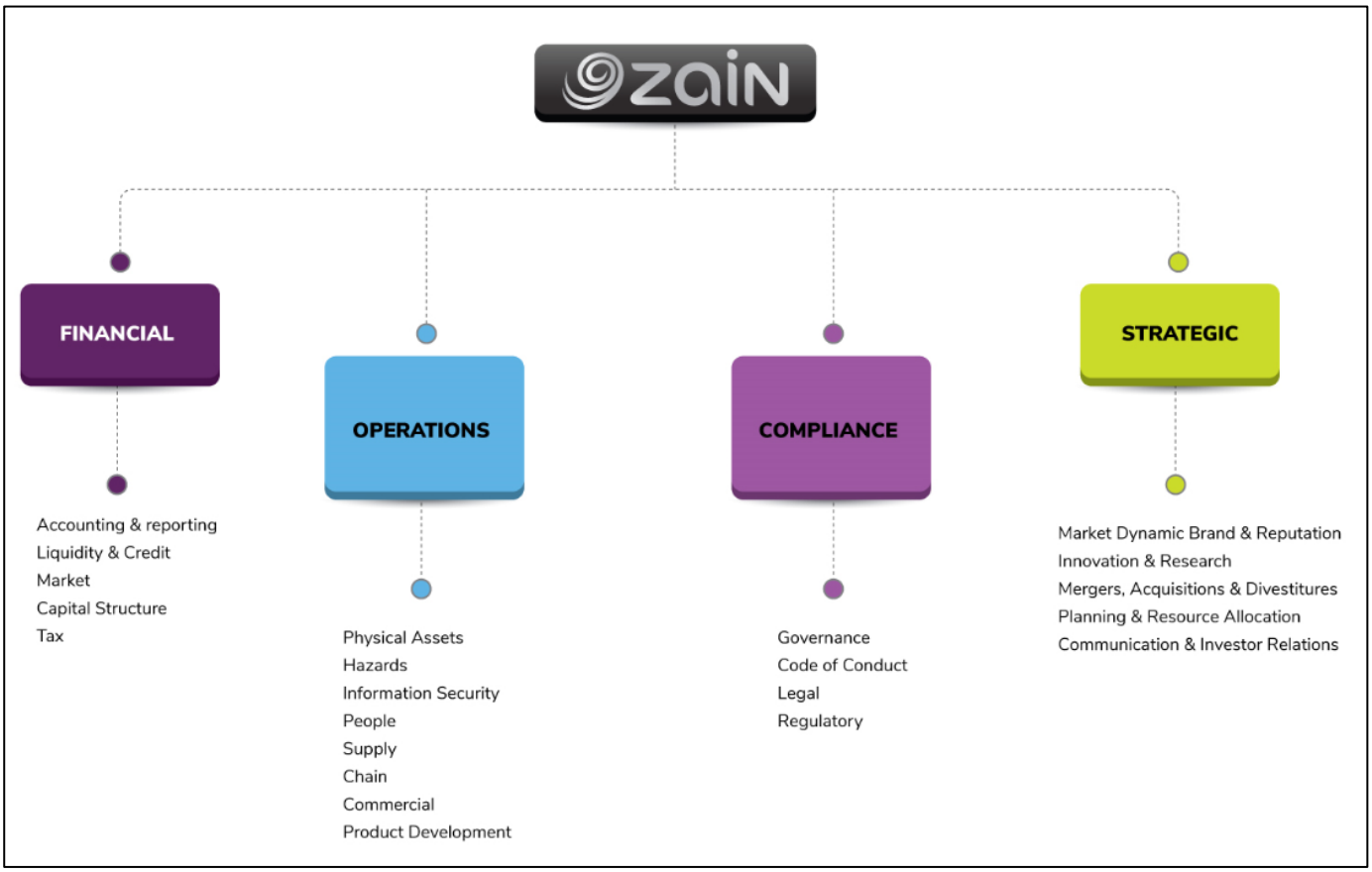
2.3 Risk Management Roles & Responsibilities: Define roles and responsibilities for the risk management activities within Zain as well as the structure for overseeing those activities. The same has been detailed in the Risk Management Roles & Responsibilities document

4. Categories of Risk at Zain

A risk library provides a common language for classifying risk in a consistent manner across Zain. Risks are classified according to the source of their primary root cause. For example, a strategic risk would be a risk that could arise from the failure of Zain to define an appropriate strategy to achieve its objectives. Zain will classify risks using the following criteria:

- By risk type (Strategic, Operational, Financial, Compliance)
- By the Operating Company where the risk event may occur

The illustrative Zain Risk Classification framework is as shown below:



4.1 Strategic Risks

The strategic focus of the organization is driven by the stakeholder expectations, industry outlook, market dynamics as well as the way the organization is governed and guided. This category covers the risks which may impact on the strategic focus and future of the organization. Strategic risk will include risks associated with **stakeholders, market dynamics, mergers and acquisition, planning and resource allocation and governance-related risks.**

An example of a merger and acquisition risk may be inability to grab opportunities for inorganic growth which would constrain the growth of the company and affect its long-term market competitiveness.

4.2 Operational Risks

Operational risk is the risk that operations (resources and processes which come together to create products and provide services) are inefficient and ineffective in executing the company's business model, satisfying customers and achieving the company's quality, cost and time performance objectives. Operations risks will include risks associated with strategy, **sales & marketing, supply chain, procurement, service delivery, HR, Technology (Telecom Networks & IT) and other functions**.

An example of an operational risk is the decline in traditional revenue streams due to increased usage of OTT applications by Zain customers.

4.3 Financial Risks

Financial risk is the risk that cash flows and financial risks are not managed cost-effectively to (a) maximize cash availability, (b) reduce uncertainty of currency, interest rate, credit and other financial risks, or (c) move cash funds quickly and without loss of value to wherever they are needed most. Financial risks will include **liquidity and credit risks, market risk, capital structure risks and tax risks**.

An example of market risk could be significant movements in interest rates that expose the company to higher borrowing costs, lower investment yields or decreased asset values.

In addition, a risk could also have an impact on the financial reporting of the Company. Inaccuracies/ inconsistencies in the financial statements of the company may potentially lead to lower investor confidence, increased threats of litigation, penalties and fines etc. Financial reporting risks include **incorrect revenue accounting, bad debts, tax liability, etc**.

4.4 Legal & Compliance Risks

Non-compliance with industry & government regulations and/or prescribed organizational policies and procedures may result in lower quality, higher production costs, lost revenues, unnecessary delays, penalties, fines, etc. Compliance risks will include **legal and regulatory risks as well as a code of conduct of the organization**.

An example of a regulatory risk could be penalties levied by the Communications and Information Technology regulator for regulatory non-compliance.

5. Sustainability of Risk Management

Risk Management will be sustained at Zain through the following actions:

- Risk Management is explicitly positioned as part of the company's return to sustained health
- Risk Management framework is endorsed by Zain's executives.
- Communication of expectations and behavior is clear
    - Executive Management to cascade their priority of risk management through their chain of command to clearly communicate their expectations regarding responsibility, measurement and behaviors that their direct reports will be held accountable to
- Management across the Company makes better decisions through the coordination and sharing of information
    - Executive Committee membership expanded to include appropriate representation from across the business; and they routinely receive and discuss relevant risk information
- ERM measures are integrated into balanced score card and compensation metrics
    - Measures may be activity driven in the short term (performed risk assessment, implemented action plans) and results driven in the medium term (risk profile improved)

6. Exceptions and Limitations

All exceptions to the Zain Risk Management roles & responsibilities document will be treated as per the Zain Exception Management policy.

7. Policy compliance

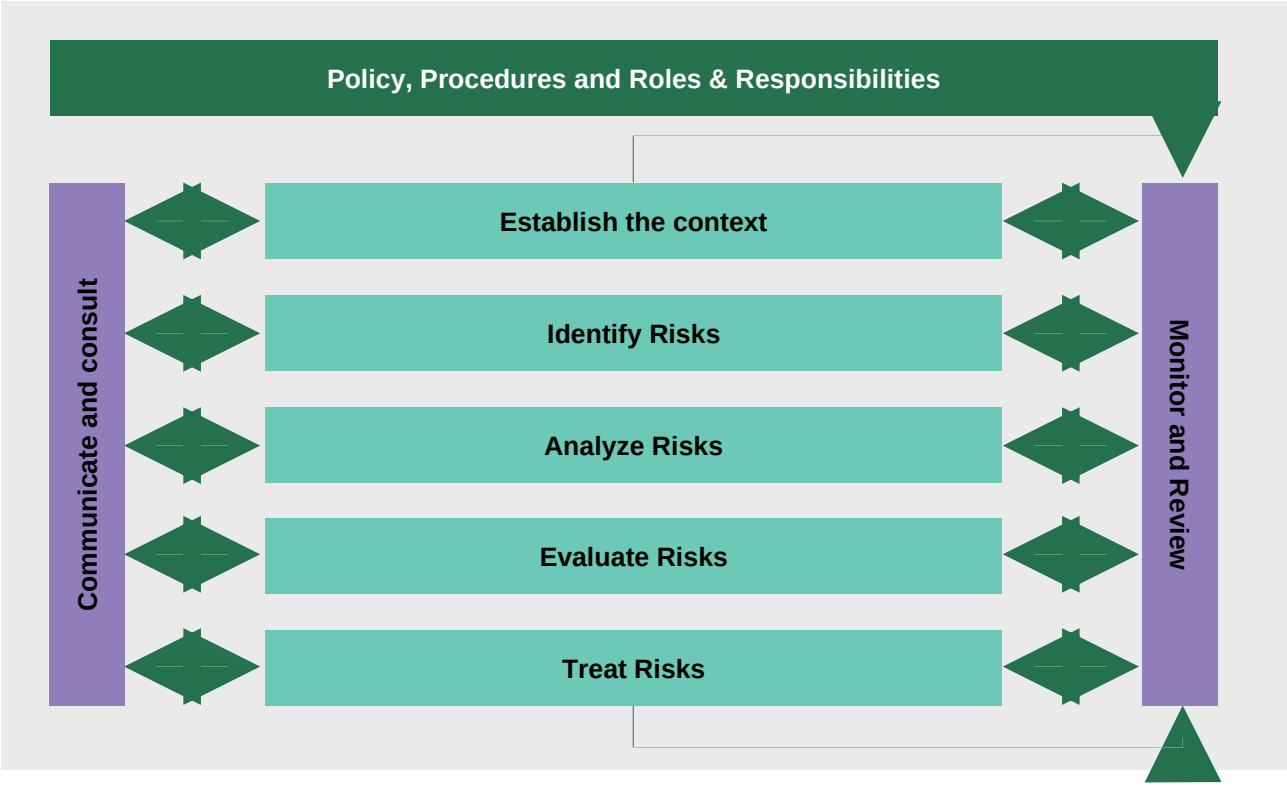
Where non-compliance to approved Zain policies and processes are found the user may be subject to consequence management. Any Third Party found to have violated Zain policies and processes may be subject to penalties.

8. Risk Management Procedures

8.1 Overview

Effective Enterprise Risk Management (hereinafter referred to as "ERM") requires consistent assessment, mitigation, monitoring and reporting of risks across the breadth of Zain. It is essential that the risk management process is aligned to the corporate direction and business objectives through a well-defined methodology for a successful ERM initiative. Hence, the ERM process will be aligned to the business plan and strategic review exercises. Each department will be required to include the results of risk management processes in their respective plans and review presentations. Each Risk Owner will be required to report on the risk management activities undertaken and outcomes thereof in their presentations.

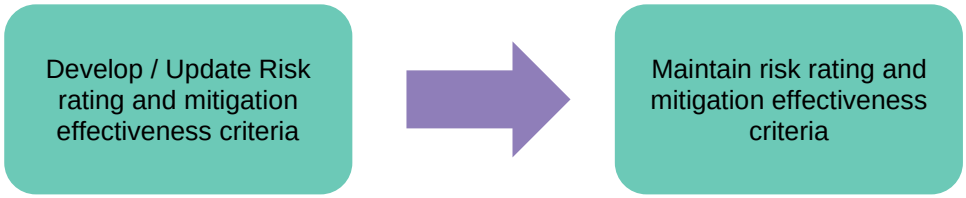
The risk management process consists of the following broad groups of activities as illustrated in diagram below.



Each of the key activities, as presented above, is further detailed out in subsequent sections

8.2 Establish the Context

To establish the boundaries of the processes governing risk management, and to adequately define the basic parameters within which risks must be managed, first the proper context within which risk management can operate should be established. Establishing the context helps in understanding Zain's background and its risks, scoping the risk management activities being undertaken, and defining the set of criteria against which the risks will be measured.



8.2.1 Develop / Update Risk Rating and Mitigation Effectiveness Criteria

Key Participants

- Group Risk Management Team (GRM)
- Executive Management (EM)

Key Activities

- Risk category / classification as defined in Zain's Risk Rating criteria is required to be linked with Zain's Corporate Strategy.
- Based on the following factors, GRM shall assess whether there is a need to update / modify / change risk category / classification
- Changes / update to Zain's corporate strategy.
- Changes / update to Corporate Key Performance Indicators (KPIs).
- GRM team shall request through Executive Management, access to updated Corporate Strategy. Key documents for consideration may also include corporate budget, annual reports, economic analysis, Zain business process models and any other relevant documentation about Zain. External documents such as relevant legislation and market reports should also be considered. Strategic analysis documents, such as SWOT analysis, may be valuable, as they may assist in focusing on relevant aspects of the external and the internal environment.
- GRM team shall coordinate and schedule meetings with Executive Management to discuss and validate the changes being proposed, before it is sent for approval to the Board Risk Committee
- Based on the meetings, GRM team shall update the risk rating and mitigation effectiveness criteria.
- GRM team shall present the updated draft to the Board Risk Committee for approval.

Key Outputs

- Updated risk rating and mitigation effectiveness criteria
- Maintain Risk Rating and Mitigation Effectiveness Criteria

8.2.2 Maintain Risk Rating and Mitigation Effectiveness Criteria

Key Participants

- GRM team

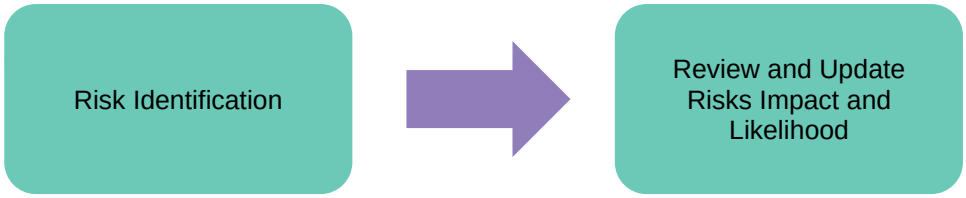
Key Activities

- GRM team shall keep the master copy of Zain's risk rating and mitigation effectiveness criteria and also ensure that only authorized updates are made with appropriate version control.
- GRM shall liaise with Risk Owners and OpCo Head of Risk Management to ensure that the Zain's risk management documents in circulation are up to date.

Key Outputs

- Appropriate version control is ensured for any updates to Risk Rating and Mitigation Effectiveness Criteria and updated version are circulated to relevant personnel.

8.3 Risk Assessment



8.3.1 Risk Identification

Key participants

- Risk Owners
- Risk Champions
- GRM team

Key Activities

- Risk Owners and GRM team shall review the risks specific to the function / department and identify risks that are not valid any longer. The risks identified from the previous assessment and are deemed to be Sunset in the current assessment shall be documented with appropriate justification for 'Sunset'
- Further, Risk Owners and GRM team together shall work toward identifying any emerging risks based on changing market conditions and business dynamics. For this purposes, the nominated Risk Owner shall coordinate within his/her respective function / department.

- The risk register for a function / department or any update thereto shall be reviewed by GRM team along-with the Risk Owner including Risk Champions to validate the applicability of risk to Zain.
- In case, for new risk identified, if there is no Risk Owner nominated, then the new risk shall be discussed with the relevant Director and CxO, before including the new risk into Zain' risk register
- GRM team in coordination with the Risk Champions shall jointly map the risk to defined risk category.

Key Outputs

- Updated risk register – risk identification only

8.3.2 Review & Update Risks Impact and Likelihood (Functional & Enterprise Level)

Key participants

- Risk owners
- Risk Champions
- GRM Team
- Director / CxOs

Key Activities

- GRM team shall facilitate discussion / workshop(s) with Risk Champions to:
    - Confirm / update the assessments of likelihood for each risk based on the probability of occurrence.
    - Align the strategy and business objectives with the entity's stated mission, vision, and core values.
    - Confirm the assessments of impact severity for each risk based on the identified consequences.
    - Obtain Risk Champions, Director / CxO sign off on impact and likelihood assessments for their respective risks.
- Based on the results from these workshops, GRM team and the risk champions shall update the Risk Register to report the Risks that Matter (RTMs) and Risks under the Radar (RuTR).

- The residual rating of the identified risks shall be the basis of classification between Risks that Matter and Risk under the Radar as per below:

Residual Risk Rating	Risk Classification
Critical	**Risk That Matter**
High	**Risk That Matter**
Significant	Risk under the Radar
Moderate	Risk under the Radar
Low	Risk under the Radar

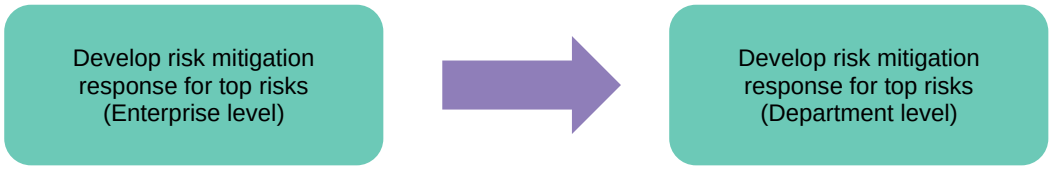
- GRM team and the Risk Champions shall validate the departmental risk register with respective Director / CxO, for final sign off.
- The Risk Assessment exercise will be carried out as an ongoing process. GRM team shall develop an annual plan to include all Zain OpCos for the purpose of scheduling periodic risk identification through risk assessment exercises. The Board Risk Committee shall approve the annual risk assessment plan proposed by the GRM team.

Note: Director / CxOs should be appropriately engaged at each point in the cycle of the risk management process through a process of communication and consultation. Getting stakeholders involved can build acceptance and generate constructive solutions. Failure to identify and include the stakeholders may lead to failure in effective identification and management of key risks.

Key Outputs

- Updated risk registers with impact and likelihood assessments
- Departmental level risk profile heat map
- Proposed new / emerging risks for Executive Management's consideration
- Annual risk assessment plan

8.4 Risk Mitigation / Response



8.4.1 Develop Risk Mitigation / Response for Top Risks (Enterprise level)

Key participants

- Risk Owners
- Risk Champions
- Executive Management (EM)
- GRM team

Key Activities

- The identified Risk owner assisted by Risk Champion shall perform detailed root cause analysis of his/her respective risk, build actionable steps considering the following risk mitigation strategies as detailed out in Risk Management policy:

✦ **Accept** – No action is taken to change the severity of risk and is taken when the risk is already covered in the risk appetite

✦ **Avoid** – Risk avoidance involves taking the decision not to engage in any activity that may result in the risk event, i.e. usually ceasing the activity that may lead to the risk event

✦ **Transfer** – Risk transfer involves shifting the impact of a risk event and the ownership of the risk mitigation to a third party

✦ **Mitigate** – Risk mitigation reduces the probability and / or impact of a potential risk to a more acceptable level. Mitigation could involve adopting a less complicated process, conducting additional tests on the product, designing redundancy into a system, and designing a quality control or reconciliation

✦ **Adapt** – Adapting involves a creative “blue sky” approach to the risk, which may result in significant changes to existing procedures and / or recognizing a potential risk event as an opportunity and then assessing the possibility of different approaches to capitalize on the opportunity, for example a risk that will impact all of the company’s competitors.

- Identify the reasons / causes / drivers which directly contribute towards the existence or possible occurrence of risks / risk events.
- Understand the type of root causes i.e. whether controllable or uncontrollable. Controllable root causes will be subject to mitigation through implementation of action steps and monitoring. Uncontrollable root causes will be monitored on a periodic basis.
- Understand whether root causes arise from factors within the organization (internal) or from the external environment

- Inherent risk is evaluated based on likelihood of occurrence and impact / consequence of the identified risk
- Risk Owner shall further define the key risk indicators, implementation timelines and update the relevant details in the Risk mitigation /response strategy template.
- For top risks, the Risk owners, Risk Champions and GRM team shall identify any existing key performance indicators (KPI) that can serve as Key Risk Indicators.
- The mitigation plans are agreed between the OpCo Risk Manager and the Risk Owners. OpCo Risk Managers present the status of current and proposed plans for the approval of OpCo CEO. Once the mitigation plans are approved by the respective OpCO CEO, OpCo Risk Managers share the risk register with the GRM team.
- Changes as suggested by the OpCo CEO shall be incorporated and communicated to Risk Owners.
- Further, each of the risks is rated for mitigation effectiveness based on the control effectives rating criteria by Risk Owners and GRM team (residual risks).
- The top risks should be presented to the Board on an annual basis by GRM.
- Once top risks are approved, the respective Risk Owner can cascade down the responsibilities to relevant appointed persons within his / her department. Delegation or cascading of implementation strategies shall not relieve the Risk owner from the primary responsibility of implementation of the mitigation plan.

Key Outputs

- Risk mitigation / response strategies (Enterprise level)
- Key risk indicators (Enterprise level)
- Risk Register

8.4.2 Develop Risk Mitigation / Response for Top Risks (Departmental level)

Key participants

- Risk Owners
- Risk Champions
- GRM team
- Director / CxOs

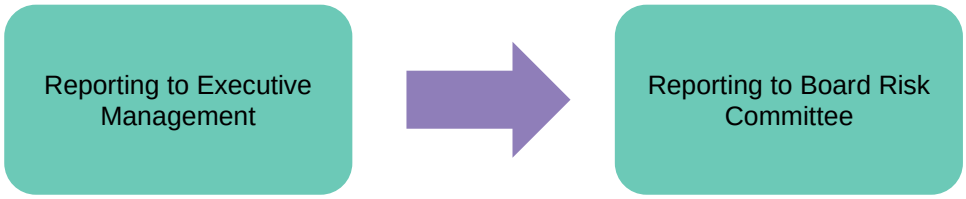
Key Activities

- The identified Risk owner assisted by Risk Champion shall perform detailed root cause analysis of his/her respective risks, build actionable steps considering the following risk mitigation strategies as detailed out in Risk Management Policy.
- Identify the reasons / causes / drivers which directly contribute towards the existence or possible occurrence of risks / risk events.
- Understand the type of root causes i.e. whether controllable or uncontrollable. Controllable root causes will be subject to mitigation through implementation of action steps and monitoring. Uncontrollable root causes will be monitored on a periodic basis.
- Understand whether root causes arise from factors within the organization (internal) or from the external environment
- Risk Owner shall further define the implementation timelines and update the relevant details in the Risk mitigation / response strategy template.
- Once the mitigation strategy is validated with the Risk Owner, the same shall be presented to respective Director / CxO for their review and input. The financial and operational feasibility of the mitigation strategy shall be discussed in the meeting.
- For top down, Risks that Matter, risks shall be identified on inherent level and after consideration of existing and proposed mitigation plan shall be reported on a residual level.
- Each of the risks is rated for mitigation effectiveness criteria by Risk Champion / Risk Owners.
- GRM team consolidates the results and submits the mitigation strategies and updated residual risk profile to respective Director / CxO for final review and approval.
- Once risk strategies are approved, the respective Risk Owner can cascade down the responsibilities to relevant appointed persons within his/her department. Delegation or cascading of implementation strategies shall not relieve the Risk owner from the primary responsibility of implementation of the control strategy.

Key Outputs

- Risk mitigation / response strategies (Departmental level)
- Risk Register with inherent and residual risk rating

8.5 Risk Monitoring and Reporting



8.5.1 Reporting to Executive Management – For Enterprise Level

Key participants

- Risk owners
- Risk Champions
- Group Risk Management (GRM) team
- Executive Management (EM)

Key Activities

- Risk Champions shall coordinate to compile data for top risks with mitigation strategies for reporting purposes. For this purpose, Risk Champions shall update the details of
- Implementation status of mitigation strategies
- Tolerance breaches (of KRIs), and
- Changes to the existing risk profile (if any)
- Risk Champions shall share the results with GRM team within agreed timelines.
- GRM team shall consolidate the results shared by each risk champions in the Reporting Dashboard.
- As part of regular reporting, GRM team shall also update the Reporting Dashboard which could include
    - Update to implementation plan
    - Update to Assessment Cycle
    - RM function's own initiatives and others
    - Updated Enterprise Risk Register
- As part of the Quarterly Executive Management meeting, Reporting Dashboard shall be presented by GRM team.
- In the quarterly meeting, the Executive Management shall discuss the Reporting Dashboard report and shall share their inputs on responding to tolerance breaches, Mitigation response strategies or

changes thereof, rating of emerging risks on impact and likelihood and other areas, if necessary, wherever applicable.

- Executive Management would also discuss and agree on how to address challenges that prevent the implementation risk mitigation strategies (E.g. Budgets, systems, people etc.)
- Based on Executive Management's review, GRM team shall collaborate with risk owners to develop alternative risk mitigation strategies (where required), revise timelines or address any other specific feedback received.

Guidelines for assessment of Quarterly Key Risk Indicators:

- Head of Risk at the respective Zain OpCo shall compile KRI information for the associated Risks that Matter from the relevant divisions in the OPCO.
- Risk Manager shall ensure to document sources of the KRIs, where applicable, in the KRI reporting template
- KRI information shall be reported for 4 quarters of the calendar year to derive the trend of the associated risk
- For deriving the upward or downward trend, thresholds for the KRIs shall be defined, wherever applicable and relevant. The thresholds shall be discussed and agreed with the Risk Owners by the OpCo Risk Manager.
- Thresholds shall be defined with color code in Red, Amber and Green for KRIs, wherever possible.
- Whenver the KRI reaches Amber, the OpCo Risk Manager can revisit the mitigation plans and controls and its effectiveness with the respective Risk Owners. Also, the Risk Owner could provide justification for the threshold being in Amber.
- Whenver the KRI reached Red, the OpCo Risk Manager shall ensure that the Risk Owner in discussion with the CEO shall propose corrective action plans and review existing mitigation plans and controls.

Key Outputs

- RM Reporting Dashboard
- Updated enterprise Risk Register
- Minutes of meeting

8.5.2 Reporting to the Board Risk Committee

Key participants

- Board Risk Committee (BRC)
- Group Risk Management (GRM)
- Any other invitees

Key Activities

- In consultation with Executive Management, GRM team shall prepare the Risk Management Reporting Dashboard for Board.
- Final approved version of the report shall be presented to the Board Risk Committee on a quarterly basis as per Capital Markets Authority requirements

Key Outputs

- Risk Management Reporting Dashboard for the Board Risk CommitteeMinutes of meeting

9. Risk Management Methodology

9.1 Risk Management Parameters

Risk management methodology assists with prioritization of enterprise risks. This is achieved by defining the parameters that distinguish the levels of risk to Zain Group. The parameters include the following:

9.1.1 Impact / Consequence

The impact is defined as the actual impact (e.g. monetary loss, physical damage etc.) that would occur.

Category	Financial			People	Customer	
Sub-category	**Revenue**	**Operational**	**CAPEX**	**Attrition**	**Value Share**	**Market Share**
Measure / Rating	**OpCo Revenue (%)**	**EBITDA Margins (%)**	**Intensity**	**% Of regretted losses**	**Decrease %**	**Decrease %**
Extreme	More than 4%	More than 3%	More than 12%	More than 20%	More than 1.5%	More than 2%
High	More than 2% and up to 4%	More than 2% and up to 3%	More than 10% and up to 12%	More than 17% and up to 20%	More than 1% and up to 1.5%	More than 1.5% and up to 2%
Moderate	More than 1% and up to 2%	More than 1% and up to 2%	More than 8% and up to 10%	More than 13% and up to 17%	More than 0.5% and up to 1%	More than 0.75% and up to 1.5%
Minor	More than 0.5% and up to 1%	More than 0.5% and up to 1%	More than 5% and up to 8%	More than 10% and up to 13%	More than 0.25% and up to 0.5%	More than 0.5% and up to 0.75%
Insignificant	Up to 0.5%	Up to 0.5%	Up to 5%	Up to 10%	Up to 0.25%	Up to 0.5%

Category	Compliance			Reputation	
Sub-category	**Telecom Regulator**	**Other regulatory / compliance (CMA, IFRS, Tax, Manpower laws, HSSE and others)**	**Investor Relations**	**Brand**	**Market Capitalization**
Measure / Rating	**Non-compliances / penalties**		**Trading Volumes**	**Qualitative Assessment**	**Moving in reverse to market index trend**
Extreme	Revocation/ Criminal proceedings/ Fines exceeding 1% of revenue/ Seizure of equipment valued above 1% of fixed assets (equipment only)		More than 0.75% of shares available	Front page negative press/TV coverage; extensive negative social media exposure	More than 5% drop
High	Fines between 0.5% and 1% of revenue/ Seizure of equipment valued between 0.5% and 1% of fixed assets (equipment only)		More than 0.5% and up to 0.75% increase	Negative press/TV coverage (not front page); major negative social media exposure	More than 4% and up to 5% drop
Moderate	Orders to cease non-compliance by regulator/ Fines between 0.1% and 0.5% of revenue/ Seizure of equipment valued between 0.1% and 0.5% of fixed assets (equipment only)		More than 0.3% and up to 0.5% increase	Sustained negative social media exposure; limited negative press coverage/ no TV coverage	More than 3% and up to 4% drop
Minor	Warnings and violation notices by the regulator or appropriate government entity/ Any fines up to 0.1% of revenue/ Seizure of equipment valued up to 0.1% of fixed assets (equipment only)		More than 0.1% and up to 0.3% increase	Limited negative social media exposure; no press exposure	More than 1% and up to 3% drop
Insignificant	Full compliance / No penalties		Up to 0.1% increase	No press or social media exposure	Up to 1% drop

The above Impact Assessment Criteria is a consolidated view of the Group. Each operating country has a different Impact Assessment Criteria across the parameters of **Revenue, EBITDA and CAPEX Intensity** as detailed below

Op Co	Risk Profile	Risk Appetite	Risk Profile	Risk Appetite	Risk Profile	Risk Appetite
Kuwait	Low	3%	Low	3%	Low	10%
Iraq	Medium	5%	Medium	3%	Medium	10%
Sudan	Medium	5%	Medium	5%	Medium	12%
KSA	Low	3%	Low	3%	Low	15%
Jordan	Medium	5%	Medium	3%	Medium	12%
Bahrain	Low	3%	Low	3%	Low	15%
S. Sudan	Medium	5%	Medium	5%	Medium	10%

9.1.2 Likelihood of Occurrence

The likelihood of the risk reflects the frequency with which a risk may occur.

Rating	Likelihood of the risk to occur			Score
	Occurrence in future	% Chance	Occurrence in the past	
Almost Certain	Very high, will be almost a routine feature occurring multiple times within the immediate period.	> 80%	Similar instances have commonly occurred frequently in the past.	21
Likely	High may arise several times within a defined period.	50% to 80%	Similar instances have occurred several times in the past period	13
Possible	Possible, may arise once or twice within a defined period.	10% to 49%	There have been one or two similar instances in the past period.	7
Unlikely	May occur once or twice within next few defined periods.	5% to 9%	Though not routinely but there have been instances in the past few periods.	3
Rare	Not likely, almost impossible to occur within a defined period.	< 5%	Similar instances have never occurred in the past.	1

9.1.3 Risk Mitigation Effectiveness

Risk Mitigation effectiveness signifies the effectiveness and / or existence of risk mitigating controls with respect to the assessed risk in the existing business process.

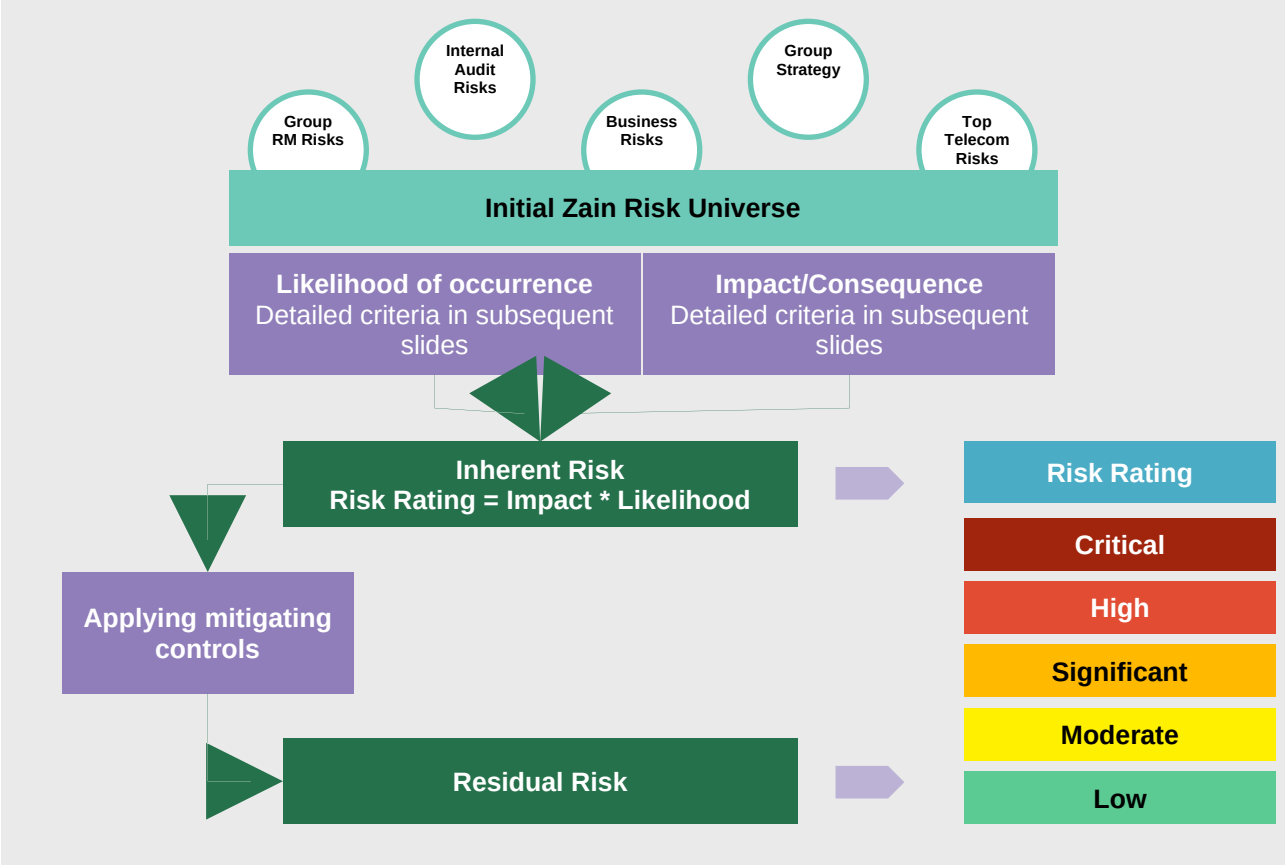
The Risk Mitigation Effectiveness is a function of both Mitigation Plan Status and the trend of the Key Risk Indicators.

Mitigation Plan Status	KRI Trend (Based on Threshold)	Risk Mitigation Effectiveness
All Controls completed / Controls monitored continuously	Green	*Effective*
Controls Partially Completed / Monitored Partially	Green	*Effective needs close monitoring*
All Controls completed / Controls monitored continuously	Amber	*Partially Effective*
Controls Partially Completed / Monitored Partially	Amber	*Partially Effective*
All Controls completed / Controls monitored continuously	Red	*Needs revisit*
Controls Partially Completed / Monitored Partially	Red	*Needs revisit*

Rating	Definition / Description	Score
Needs Revisit	Mitigation plans are either partially implemented or delayed and do not ensure any control over the risk occurrence and impact. AND Key Risk Indicator trend for the trailing four quarters is Red. Mitigation plans must be redesigned and agreed with the Mitigation Plan Owner	1
Partially Effective	Mitigation plans are either partially implemented or delayed and do not ensure any control over the risk occurrence and impact. AND Key Risk Indicator trend for the trailing four quarters is Amber.	1.5
Effective needs close monitoring	Mitigation plans are partially implemented and ensure some measurable control over the risk occurrence and / or impact. AND Key Risk Indicator trend for the trailing four quarters is Green	2
Effective	Mitigation plans are implemented or controls constituting the mitigation plan are continuously monitored. AND Key Risk Indicator trend for the trailing four quarters is Green	4

9.2 Risk Rating

The inherent risk assessment is an aggregate of the perceived consequence of the risk: the level of impact that the potential risk can have on the achievement of business/functional objectives, and the perceived likelihood of occurrence of the potential risk that may lead to the assessed consequence(s).



Impact		Likelihood of Occurrence				
		Rare	Unlikely	Possible	Likely	Almost Certain
	Rating	1	3	7	13	21
Extreme	31	31	93	217	403	651
High	19	19	57	133	247	399
Moderate	10	10	30	70	130	210
Minor	4	4	12	28	52	84
Insignificant	1	1	3	7	13	21

The residual risk approach discounts the gross risk (Impact*Likelihood) by the mitigation plan effectiveness to arrive at the net risk associated with each risk event.

Based on the inherent / residual risk score, the risks may be classified as below:

Level of Risk	Description	Risk Score (Impact*Likelihood)	Responsive Action
Critical	Inability to achieve business objectives	≥399	Immediate attention required to develop new mitigation plans and stakeholder engagement (board level) to ensure treatment level is acceptable
High	Constrained ability to meet business objectives	<399	Regular monitoring of risk and/or treatment required along with review of efficiencies and effectiveness by Executive Management
Significant	Significant impact on the achievement of business objectives	<210	Regular monitoring of risk and/or treatment required along with review of efficiency and effectiveness by Senior Management
Moderate	Limited impact on achievement of business objectives	<83	Attention required to ensure appropriate level of mitigation controls are in place and periodic review of effectiveness to be carried out by management team
Low	Managed by routine procedures	<19	Risks are mitigated but efficiencies and effectiveness to be reviewed by management team on periodic basis

9.3 Risk Escalation Criteria

9.3.1 Considerations for Risk Escalation

The following considerations influence the assessment for the escalation of risks:

1. Where residual risk rating of the risks has been rated as **High** and above as reported for the **Risks that Matter** across the enterprise.
2. Where Risk Mitigation plans for the Risks That Matter is delayed or incomplete and the **Key Risk Indicators** for the Risks that Matter have exceeded the thresholds (where applicable) and demonstrate an upward trend.
3. Where Risk Mitigation Effectiveness of the risks has been rated as ‘Needs Revisit’ for both Risks that Matter and in the Unit level risk registers; and
4. Where **Key Risk Indicators** for the risks rated as High and above at unit level have exceeded the thresholds. This shall be tracked at the OpCo by the OpCo Risk Managers.

10. Unit Level Risk Assessment Methodology

10.1 Establishing the Context

Key participants

- Group Risk Management (GRM) team
- Zain OpCo Risk Management team

Key Activities

- OpCo RM team shall identify and understand mission critical processes at the respective Units for the organization;
- OpCo team shall review and leverage department KPIs, past risk assessment & internal audit reports of Zain OpCo to understand the risk environment of the Company;
- Review and align the risk assessment criteria of the Company as per the current risk framework and leading practices of risk management; and
- Zain OpCo Risk team shall agree on the mission critical processes for Risk Management with the Senior Management and design the risk identification roadmap; and
- Group RM shall establish the methodology and provide supervission to the OpCo Risk team

10.2 Risk Identification

Key participants

- Zain OpCo RM team
- Zain OpCo Risk Champions/Risk Owners

Key Activities

- Based on the risk identification roadmap, Zain OpCo Risk Management to schedule risk workshops with the respective process owners;
- Based on the discussions with the process owners, OpCo RM shall identify key risks at process and entity level which pose a material threat to Zain OpCo's achievement of its objectives;
- OpCo RM shall document the key risks and associated preventive, detective and corrective controls identified during the risk workshops in the risk repository;
- OpCo RM shall assess the impact and likelihood of inherent risk based on the approved risk assessment criteria and report the residual risk rating for the identified risks; and
- Determination of the contribution of each risk to the aggregate risk profile and prioritization of the risks for the OpCo.
- GRM team to provide quality assurance and suggest recommendations to enhance the risk reporting process.

10.3 Risk validation & Mitigation

Key Participants

- Zain OpCo RM team
- Zain OpCo Risk Champions/Risk owners

Key Activities

- Based on the risk workshops, development of risk registers at unit level for Zain OpCo with descriptions of inherent risks, existing controls, impact and likelihood, risk score, and owners;
- Development of risk mitigation plan (risk recommendations) for the identified risks, whereever there is a requirement to enhance and strengthen current controls based on residual risk rating;
- Discussion and validation of suggested improvements/changes with process owners and Director of the respective Division; and
- OpCo RM team shall finalize the aggregate risk registers for monitoring on an annual basis.
- Key Risk Indicators, where applicable shall be developed for the residual risks rated High and above.

11. Glossary of Terms and Definition

For the purposes of this document, the following definitions as per ISO 31000 shall apply.

11.1.1 Risk - Effect of uncertainty on objectives

NOTE 1: An effect is a deviation from the expected — positive and/or negative.

NOTE 2: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

NOTE 3: Risk is often characterized by reference to potential **events** (8.1.18) and **consequences** (2.12.19), or a combination of these.

NOTE 4: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated **likelihood** (8.1.20) of occurrence.

NOTE 5: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.

11.1.2 Risk management - Coordinated activities to direct and control an organization regarding risk (8.1.1)

11.1.3 Risk management framework - Set of components that provide the foundations and organizational arrangements for designing, implementing, **monitoring** (8.1.30), reviewing and continually improving **risk management** (8.1.2) throughout the organization.

NOTE 1: The foundations include the policy, objectives, mandate and commitment to manage **risk** (8.1.1).

NOTE 2: The organizational arrangements include plans, relationships, accountabilities, resources, processes, and activities.

NOTE 3: The risk management framework is embedded within the organizations' overall strategic and operational policies and practices.

11.1.4 Risk management policy - Statement of the overall intentions and direction of an organization related to **risk management** (8.1.2)

11.1.5 Risk Appetite - The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value.

11.1.6 Risk attitude - Organization's approach to assess and eventually pursue, retain, take or turn away from **risk** (8.1.1)

11.1.7 Risk management plan - Scheme within the **risk management framework** (8.1.3) specifying the approach, the management components, and resources to be applied to the management of **risk** (8.1.1)

NOTE 1: Management components typically include procedures, practices, assignment of responsibilities, sequence, and timing of activities.

NOTE 2: The risk management plan can be applied to a product, process and project, and part or whole of the organization.

11.1.8 Risk owner - Person or entity with the accountability and authority to manage a **risk** (8.1.1)

11.1.9 Risk management process - Systematic application of management policies, procedures and 9ractices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, **monitoring** (8.1.30) and reviewing **risk** (8.1.1)

11.1.10 Establishing the context - Defining the external and internal parameters to be considered when managing risk and setting the scope and **risk criteria** (8.1.23) for the **risk management policy** (8.1.4)

11.1.11 External context - External environment in which the organization seeks to achieve its objectives.

NOTE External context can include:

- The cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- Key drivers and trends having impact on the objectives of the organization; and
- Relationships with, and perceptions and values of external stakeholders (8.1.14).

11.1.12 Internal context - Internal environment in which the organization seeks to achieve its objectives.

NOTE Internal context can include:

- Governance, organizational structure, roles and accountabilities;
- Policies, objectives, and the strategies that are in place to achieve them;
- The capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- Information systems, information flows and decision-making processes (both formal and informal);
- Relationships with, and perceptions and values of, internal stakeholders;
- The organization's culture;
- Standards, guidelines and models adopted by the organization; and
- Form and extent of contractual relationships.

11.1.13 Communication and consultation - Continual and iterative processes that an organization conducts to provide, share, or obtain information and to engage in dialogue with **stakeholders** (8.1.14) regarding the management of **risk** (8.1.1)

NOTE 1: The information can relate to the existence, nature, form, **likelihood** (8.1.20), significance, evaluation, acceptability, and treatment of the management of risk.

NOTE 2: Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to deciding or determining a direction on that issue. Consultation is:

- A process which impacts on a decision through influence rather than power; and
- An input to decision making, not joint decision making.

11.1.14 Stakeholder - Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

NOTE: A decision maker can be a stakeholder.

11.1.15 Risk assessment - Overall process of **risk identification** (8.1.16), **risk analysis** (8.1.22) and **risk evaluation** (8.1.25)

11.1.16 Risk identification - Process of finding, recognizing, and describing **risks** (8.1.1)

NOTE 1: Risk identification involves the identification of **risk sources** (8.1.17), **events** (8.1.18), their causes and their potential **consequences** (8.1.19).

NOTE 2: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and **stakeholder's** (8.1.14) needs.

11.1.17 Risk source - Element which alone or in combination has the intrinsic potential to give rise to **risk** (8.1.1)

NOTE: A risk source can be tangible or intangible.

11.1.18 Event - Occurrence or change of a set of circumstances.

NOTE 1: An event can be one or more occurrences and can have several causes.

NOTE 2: An event can consist of something not happening.

NOTE 3: An event can sometimes be referred to as an “incident” or “accident”.

NOTE 4: An event without **consequences** (8.1.19) can also be referred to as a “near miss”, “incident”, “near hit” or “close call”.

11.1.19 Consequence - Outcome of an **event** (8.1.18) affecting objectives.

NOTE 1: An event can lead to a range of consequences.

NOTE 2: A consequence can be certain or uncertain and can have positive or negative effects on objectives.

NOTE 3: Consequences can be expressed qualitatively or quantitatively.

NOTE 4: Initial consequences can escalate through knock-on effects.

11.1.20 Likelihood - Chance of something happening.

NOTE 1: In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a period of time).

NOTE 2: The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.

11.1.21 Risk profile - Description of any set of **risks** (8.1.1) A composite view of the risk assumed at a particular level of entity, or aspect of business that positions management to consider the types, severity, and interdependencies of risks, and their impact on company's performance.

NOTE: The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.

11.1.22 Risk analysis - Process to comprehend the nature of **risk** (8.1.1) and to determine the **level of risk** (8.1.24)

NOTE 1: Risk analysis provides the basis for **risk evaluation** (8.1.25) and decisions about **risk treatment** (8.1.26).

NOTE 2: Risk analysis includes risk estimation.

11.1.23 Risk criteria - Terms of reference against which the significance of a **risk** (8.1.1) is evaluated.

NOTE 1: Risk criteria are based on organizational objectives, and **external** (8.1.11) and **internal context** (8.1.12).

NOTE 2: Risk criteria can be derived from standards, laws, policies and other requirements.

11.1.24 Level of risk - Magnitude of a **risk** (8.1.1) or combination of risks, expressed in terms of the combination of **consequences** (8.1.19) and their **likelihood** (8.1.20)

11.1.25 Risk evaluation - Process of comparing the results of **risk analysis** (8.1.25) with **risk criteria** (8.1.23) to determine whether the **risk** (8.1.1) and/or its magnitude is acceptable or tolerable.

NOTE: Risk evaluation assists in the decision about **risk treatment** (8.1.26).

11.1.26 Risk treatment - process to modify **risk** (8.1.1)

NOTE 1: Risk treatment can involve:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- Taking or increasing risk in order to pursue an opportunity;
- Removing the risk source (8.1.17);
- Changing the likelihood (8.1.20);
- Changing the consequences (8.1.19);
- Sharing the risk with another party or parties (including contracts and risk financing); and
- Retaining the risk by informed decision.

NOTE 2: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".

NOTE 3: Risk treatment can create new risks or modify existing risks.

11.1.27 Control - Measure that is modifying **risk** (8.1.1)

NOTE 1: Controls include any process, policy, device, practice, or other actions which modify risk.

NOTE 2: Controls may not always exert the intended or assumed modifying effect.

11.1.28 Inherent Risk: Risk to an entity in the absence of any direct or focused actions by management to alter its severity.

11.1.29 Residual risk - risk (8.1.1) Remaining after **risk treatment** (8.1.26)

NOTE 1: Target Residual risk is the amount of risk that an entity prefers to assume in the pursuit of its strategy and business objectives, knowing that management will implement, or has implemented, direct or focused actions to alter the severity of the risk.

NOTE 2: Actual Residual risk is the risk remaining after management has acted to alter its severity. Actual residual risk should be equal to or less than the target residual risk. Where actual residual risk exceeds target risk, additional actions should be identified that allow management to alter risk severity further".

11.1.30 Monitoring - Continual checking, supervising, critically observing or determining the status to identify change from the performance level required or expected.

NOTE: Monitoring can be applied to a **risk management framework** (8.1.3), **risk management process** (8.1.9), **risk** (8.1.1) or **control** (8.1.27).

11.1.31 Review - activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.

NOTE: Review can be applied to a **risk management framework** (8.1.3), **risk management process** (8.1.9), **risk** (8.1.1) or **control** (8.1.27).

12. Policy Communication and Review Frequency

All Zain documents, related process flows, and outcomes shall be reviewed annually and revised as required. All users and management of Zain are responsible for the implementation of this document.

Proposed amendments to the procedures will be submitted to the **Chief Risk Officer** for consideration and subsequently to the **Board Risk Committee** for approval.

13. Document Properties

13.1 Administration

This Policy shall be communicated to all employees through appropriate channels to make them aware of the Organization's commitment to risk management policy.

13.2 Ownership

The owner of this policy is Zain Group Risk Management Department.

13.3 Interpretation

Questions pertaining to the interpretation of this policy may be referred to Zain Group Risk Management Department group.risk@zain.com

Annexure I: Comparison with global standards

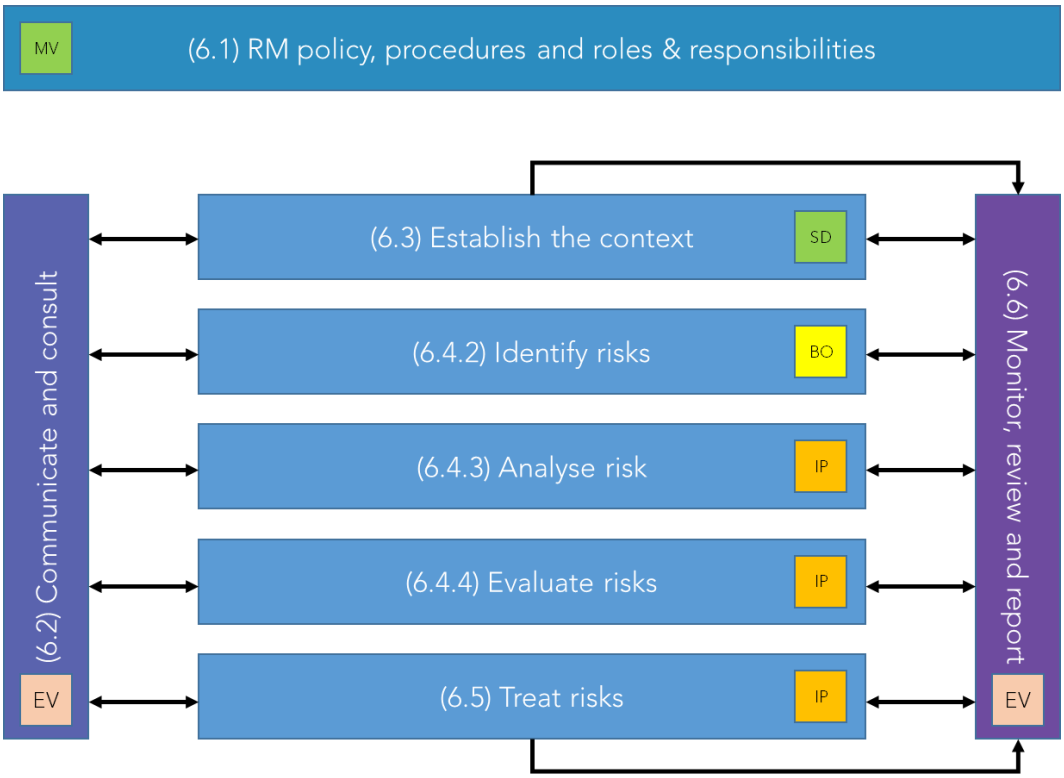


Figure 1: Zain Risk Management Procedures (aligned to ISO 31000:2018) Vs COSO

Figure 2: COSO Risk Management Framework, 2017

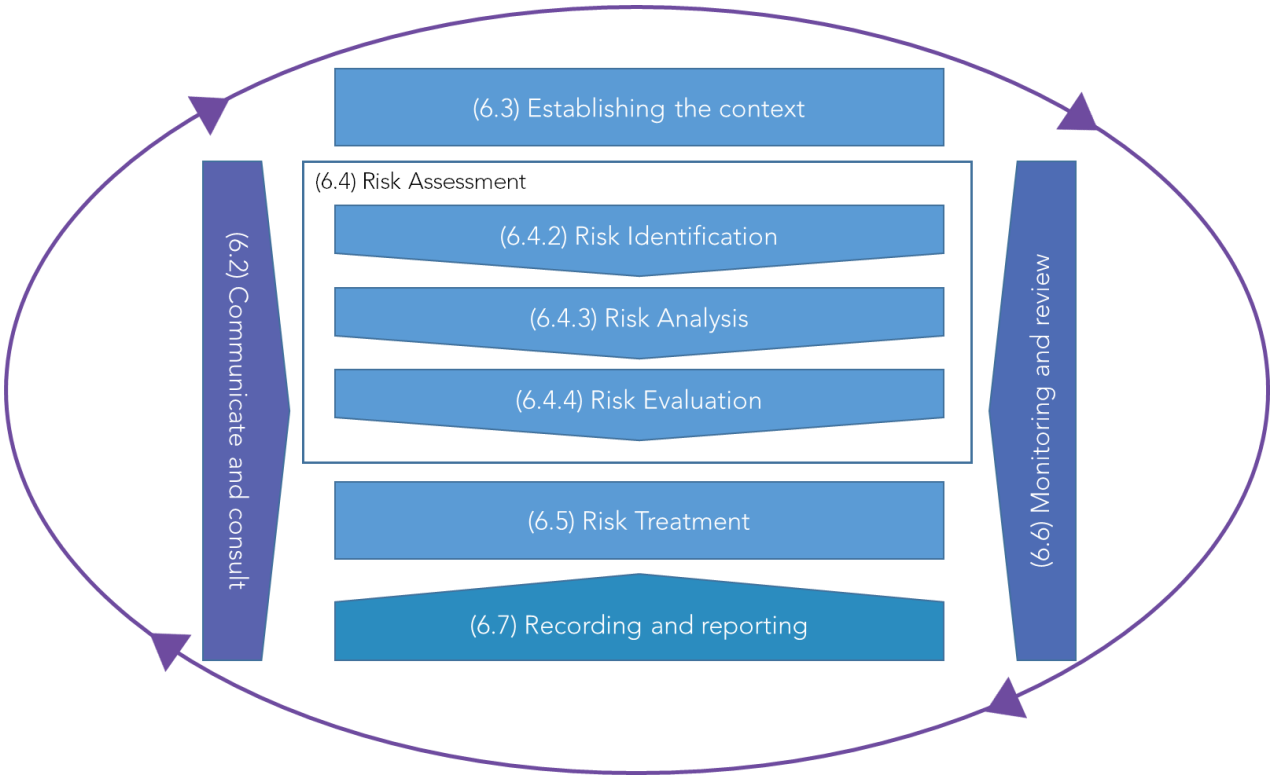


Figure 3: Risk Management Process as per ISO 31000:2018

Zain Risk Management Procedures vs. Global Standards

A comparison of Zain's Risk Management Framework with global standards is provided below. The procedure has built in all elements recommended by commonly adopted global standards.

Comparison with COSO Risk Management Framework and ISO 31000:2009

In 2001, COSO (The Committee of Sponsoring Organizations of the Treadway Commission) launched an initiative to build a commonly agreed and understood framework for Enterprise Risk Management ("ERM"). ERM is a:

- Comprehensive and systematic approach for helping all organizations to manage uncertainty and respond to risk
- Set of common definitions
- Standard against which all organizations can benchmark the effectiveness and completeness of their control processes
- Guide for management in developing an effective risk management architecture

The COSO framework was last updated in 2017 to accommodate the changing risk landscape across organizations.

ISO, the international body charged with achieving standardization, set out to achieve consistency and reliability in risk management by creating a standard that would be applicable to all forms of risk. This would contain:

- One vocabulary;
- A set of performance criteria;
- One, common overarching process for identifying, analyzing, evaluating, and treating risks;
- Guidance on how that process should be integrated into the decision-making processes of any organization.

ISO created a working group comprising experts nominated from 28 countries (up to three from each) and from many other specialist organizations to guide the development of the standard and the associated vocabulary. While the experts possess a very wide range of risk management experience gained in many sectors and applications, their principal role has been to represent the views of their respective national and sector mirror committees and organizations.

Through these mirror committees, a network of hundreds of risk management specialists and their customers from around the world have helped create, review, and shape the eventual ISO 31000:2009 (last updated in 2018)