POLICY FRAMEWORK

Guidelines on matters regarding **Risk Management** of Public Sector Companies and Autonomous Bodies in Khyber Pakhtunkhwa

GOVERNMENT OF KHYBER PAKHTUNKHWA

FINANCE DEPARTMENT

http://www.finance.gkp.pk

CONTROL TABLE			
Version	**Section**	**Remarks**	**Date of issue**
1.0			21.02.2022

Table of Contents

NOTIFICATION

The Provincial Government is pleased to approve the following policy framework to be followed by Public Sector Companies and Autonomous Bodies for matters pertaining to the Risk Management function.

Aspect	Framework
Principles	• The objective of risk management is to effectively manage uncertainty which could have a significant negative impact on the organization's objectives • It is the identification, assessment and prioritization of risks followed by coordinated and economical application of resources to minimize the probability and/or impact of failure and increase the likelihood of success • The authority for risk management and the setting of the risk management policy and risk appetite belongs with the Organization's Board of Directors • The ISO 31000 standard for risk management shall be used as guide for the risk management framework • The Organization shall have a detailed risk management framework that enables common terminology across the organization, uniform processes and structures, consistent roles and responsibilities, and regular and reliable communications
Risk Management Responsibility	The Board of Directors shall: • Proactively manage risks to business assets, including staff, financial and other resources, property, projects and reputation • Take appropriate and timely measures to assess the likelihood and potential impact of risks, and the associated impact on the achievement of objectives, balancing of the cost of managing risks with the anticipated benefits that may derive • Decide on and implement the appropriate risk response to the assessed risk or risks • Monitor and evaluate the outcomes
Roles and responsibilities	• Authority for managing risks flows from the Board of Directors • Information about risks and how they are managed flows to the Board of Directors • Board shall be responsible for development of risk management policy and keep it up to date • The Chief Executive Officer (CEO) shall place before the Board an annual report on risk management along with the advice of the Audit Committee on the adequacy and effectiveness of risk management processes and implementation • Internal audit function shall analyze the effectiveness of the risk management framework and its implementation. Responsibility for implementing and executing risk management framework shall be segregated from internal audit • The CEO shall be responsible for compliance with the risk management policy and shall have authority for managing risks and compliance with the policy. The CEO may delegate authority to another executive, as appropriate. The CEO and his delegate will have specific responsibility for annual reporting of risks to the Board and the Audit Committee

	• All management and staff have a responsibility for identifying, reporting and tackling risks that relate to their function. The management shall support the CEO in implementing the risk management policy and processes • The CEO and management shall build a risk awareness culture within the organization • The CEO shall design a system of risk management which enables identification of risks and effective and proactive communication of these risks • Ensure that overall risks exposure of the entity is within acceptable limits, and that the departments and projects (risk owners) are proactive rather than reactive, resulting in preventive rather than remedial actions • Co-ordinating with the risk owners and members of the senior management in developing and implementing risk management policies and related accounting and internal control procedures
General	• Risk language and terminology shall be consistent with that used across the Organization. Execution of the framework shall be supported by education and training for staff. The framework shall be embedded within existing and planned processes and systems • The CEO or his delegate shall maintain a consolidated risk register of the Organization. Each risk identified in the risk register shall have an owner. The owner of a risk is responsible for taking action to mitigate the risk, where possible. Ownership must sit at the appropriate level, with the person who can take effective action. In updating the risk register, risk owners will describe existing and additional activities to address or mitigate the risk • The CEO or his delegate shall prepare an annual risk report and submit the report to the Audit Committee. The CEO will present the report to the Audit Committee and then to the Board • When responding to a key risk, the business will aim to ensure that the risk does not materialize. To this end, management will determine the most effective risk response, balancing the costs of risk management with the opportunity cost of not taking appropriate action • The CEO shall be responsible for submission of the risk report to the Finance Department, Khyber Pakhtunkhwa

2. The Provincial Cabinet is further pleased to approve the following:

- The activities mentioned above shall be applicable with prospective effect
- Detailed guidelines on matters regarding Risk Management can be downloaded from https://www.finance.gkp.pk/articles/about/wings/corporate-governance-unit-cgu
- In order to operationalize the policy framework, the Finance department may issue guidelines within the broad scope of this policy framework from time to time

- As far as practicable, and prospectively, the administrative departments shall align the provisions of respective legislation of autonomous bodies in-line with principles laid out in these policy frameworks.

3. The Cabinet further directed that all the administrative departments shall take a review of their respective public sector companies / autonomous bodies on these policy framework parameters and shall submit a compliance report to the Chief Secretary office within 60 days from the date of notification of these policy frameworks.

4. It is therefore requested that necessary action may kindly be taken accordingly.

1. Background

1.1. Public Sector Companies (PSCs) and Autonomous Bodies (ABs) have been established to increase efficiency, reduce costs and improve effectiveness of public service delivery across various sectors in Khyber Pakhtunkhwa. There are 168 PSCs and ABs under the ownership and control of the Government of Khyber Pakhtunkhwa (GoKP). These entities have been set-up under different modes such as not for profit companies under section 42 of Companies Ordinance, 1984 (superseded by Companies Act, 2017), as well as statutory bodies under special enactments.

1.2. The performance, effectiveness and operational efficiency of entities is lacking, with significant scope for improvements in the management of entities. PSCs/ABs have low levels of own source revenue and they are significantly reliant on funding from the GoKP. The aggregate costs of funding PSCs and ABs to GoKP is likely to be rising substantially. In the absence of a functioning mechanism to track performance and costs of PSCs/ABs, the Finance Organization has initiated an exercise to determine the cost of PSC/ABs by collecting data from entities across organizations.

1.3. As a first step to improve the performance of PSCs/ABs, the Finance Organization is developing policy guidelines for PSCs/ABs to adopt corporate governance best practices in aspects relating to boards, Chief Executive Officers (CEOs), human resources management, financial management, accounting, Government oversight and performance management. The guidelines are being developed by reviewing relevant legislation, sub-legislation in Pakistan, Corporate Governance Assessments of PSCs in Khyber Pakhtunkhwa conducted by the Finance Organization, and international practice, including from Organization for Economic Co-operation and Development (OECD) countries and non-OECD countries.

2. Rationale

2.1. The purpose of this policy document is to provide guidelines for risk management to all Public Sector Companies (PSCs)/Autonomous Bodies (ABs) of the Government of Khyber Pakhtunkhwa. It defines the broad principles related to the purpose, and requirement of risk management within the PSCs/ABs.

3. Scope and objectives

3.1. The objective of risk management is to effectively manage uncertainty which could have a significant negative impact on the organization's objectives.

3.2. Uncertainty is inherent. Factors that drive risk include:

- the importance of reputation and brand perception;
- intensifying competition;
- challenges for project management;
- and keeping pace with rapid technological change.

3.3. Risk management reduces the probability of objectives being negatively impacted by unforeseen or unmanaged risks. The formal management of risk permits to mitigate risks and achieve a measured level of risk taking.

3.4. Risk Management applies to all activities of the Organization. It forms part of the organization's governance framework and risk management must become part of routine management activity across the organization.

3.5. Risk management is an approach towards setting the best course of action by identifying, assessing, understanding, acting on and communicating risks. The following are the objectives of risk management:

- ensure conformity with applicable rules, regulations, and mandatory obligations.
- assurance to the Board and the Committee that risk management activities are comprehensive and proportionate to the level of risk faced by the Organization.
- ensure that appropriate risk-based information is available to support decision making.
- assist with achieving effective and efficient strategy, tactics, operations and compliance to ensure the best outcome with reduced volatility of results.
- assist in safeguarding the business' assets, including people, finances, property and reputation.

4. Principles of the policy

4.1. Risk management is integral to best management practices and key part of corporate governance. Risk Management is the identification, assessment and prioritization of

risks followed by coordinated and economical application of resources to minimize the probability and/or impact of failure and increase the likelihood of success.

4.2. Authority for risk management and the setting of the risk management policy and risk appetite belongs with the Organization's Board of Directors.

4.3. The responsibility for risk management rests with the Board of Directors, who shall;

- Proactively manage risks to business assets, including staff, financial and other resources, property, projects and reputation;
- Take appropriate and timely measures to assess the likelihood and potential impact of risks, and the associated impact on the achievement of objectives, balancing the cost of managing risks with the anticipated benefits that may derive;
- Decide on and implement the appropriate risk response to the assessed risk or risks; and
- Monitor and evaluate the outcomes.

4.4. The ISO 31000 standard for Risk Management shall be used as a guide for the Risk Management Framework.

4.5. The organization shall have a detailed risk management framework that enables common terminology across the organization, uniform processes and structures, consistent roles and responsibilities, and regular and reliable communications.

5. Roles and responsibilities

5.1. Authority for managing risks flows from the Board of Directors. Information about risks and how they are managed flows to the Board of Directors. The Board of Directors shall be responsible for development of risk management policy and keep it up to date.

5.2. The chief executive officer shall place before the Board of Directors an annual report on risk management along with advice of the Audit Committee on the adequacy and effectiveness of risk management processes and implementation.

5.3. Internal audit function shall analyze the effectiveness of the risk management framework and its implementation. Responsibility for implementing and executing risk management framework shall be segregated from internal audit to avoid an possible conflict.

5.4. The chief executive officer shall be responsible for compliance with the risk management policy and shall have authority for managing risks and compliance with

the policy. The chief executive officer may delegate authority to another executive, as appropriate. The chief executive officer and his delegate will have specific responsibility for annual reporting of risks to the Board of Directors and Audit Committee.

5.5. All management and staff have a responsibility for identifying, reporting and tackling risks that relate to their function. The management shall support the chief executive officer in implementing the risk management policy and processes.

5.6. The chief executive officer and management shall build a risk aware culture within the organization.

5.7. The chief executive officer shall design a system of risk management, which enables identification of risks and effective and proactive communication of these risks.

5.8. Ensure that overall risks exposure of the entity is within acceptable limits, and that the departments and projects (risk owners) are proactive rather than reactive, resulting in preventive rather than remedial actions.

5.9. Co-ordinating with the risk owners and members of the senior management in developing and implementing risk management policies and related accounting and internal control procedures.

6. General

6.1. Risk language and terminology shall be consistent with that used across the Organization. Execution of the framework shall be supported by education and training for staff. The framework shall be embedded within existing and planned processes and systems.

6.2. The chief executive officer or his delegate shall maintain a consolidated risk register of the Organization. Each risk identified in the risk register shall have an owner. The owner of a risk is responsible for taking action to mitigate the risk, where possible. Ownership must sit at the appropriate level, with the person who can take effective action. In updating the risk register, risk owners will describe existing and additional activities to address or mitigate the risk.

6.3. The chief executive officer or his delegate shall prepare an annual risk report and submit the report to the Audit Committee. The CEO will present the report to the Audit Committee and then to the Board.

6.4. When responding to a key risk, the business will aim to ensure that this risk does not materialize. To this end, management will determine the most effective risk response,

balancing the costs of risk management with the opportunity cost of not taking appropriate action.

7. Reporting to the Committee

7.1. The chief executive officer shall be responsible for communication with the Board of Directors and Audit Committee. The chief executive officer shall be responsible for submission of risk report to the Finance department as per the timelines given in below table.

7.2. Following is the guidance on the structure of a risk report:

Section	**Purpose**	**Reporting Cycle**
Executive Summary	This section needs to be concise, and the following topics may be included: – Progress update on policy approval, resource allocation – In year achievements in implementing risk management practices – Next year risk management plan to enhance the risk maturity across the organization – Synopsis of top 10 risks.	Yearly
Risk Profile	The "Risk Profile" section of the report provides a graphical presentation of the overall risks on a heat map. This method of presentation provides the reader a quick snapshot of the overall risks faced by the organization. In addition, the comparison between the current and historic "Risk Profile" will allow understanding and documenting the shift in risk ratings (both at inherent and residual levels) that have occurred during a given time period and also to include the reasons behind the trend shift. The most common types of reasoning that can be associated with a change in risk profile may include, e.g.:	Yearly

	– Changes in business strategy, operations etc. – Independent assurance activities indicating that the controls environment is considered less effective than originally assessed – Implementation of risk mitigation strategies – Change in the internal and / or external environment, for example, regulatory, competitor landscape, organizational restructuring etc.,	
Risk Register	This section of the report reflects the narrative part of risks plotted on a heat map. The risk register is the key output from the risk identification and assessment process. It acts as a central repository of all risks identified by the business units. Information to be included: – Risk description – Perceived cause – Risk category – Exposure – Inherent risk probability / likelihood – Inherent risk impact – Inherent risk severity – Existing / current controls – Current risk probability / likelihood – Current risk impact – Current risk severity – Enhancements – Ownership (Name of the responsible person) – Consequences / Exposures	Quarterly Yearly
New and Emerging Risks	The New and Emerging Risks section provides an overview of the new risk added during the quarter. It is important to maintain the risk register current outside of the formal annual risk reporting process.	Quarterly Yearly

	Personnel from within the organization would notify the chief executive officer or his delegate of any new or emerging risks. When new risks are included in the risk report/register, these should be clearly articulated so that the Audit Committee and the Board would have visibility of them.	
Risk Treatment (Mitigation) Plan	This section of the report focuses on providing detail information on the actions put in place to mitigate the risks. It provides a status update on progress against approved risk treatment actions. The stakeholders are likely to deliver on what they will be measured against. The possible information to include under this section is as follows: – Risk description – Risk rating – Description of the risk treatment (mitigation) plan – Due date for completion of risk treatment (mitigation) – Responsible person – Status update i.e. (completed, in progress, delayed etc.) – Enhancements (any additional actions that may be implemented to further mitigate the residual risk severity level)	Quarterly Yearly

8. Definitions

8.1 Board

Board means “Board of Directors of the Organization”.

8.2 Committee

Committee means “Audit Committee of the Board”.

8.3 Current Risk/Residual Risk

Existing level of risk taking into account the controls in place.

8.3 Enterprise Risk Management

A process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

8.4 Event

An occurrence or incident, from external or internal sources, that affects the achievement of objectives.

8.5 Function

Function means “Internal Audit and Risk Management Function”.

8.6 Internal Audit

Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

8.7 Inherent Risk/Gross Risk

Level of a risk before any control activities are applied.

8.8 Impact

The impact of an event is the magnitude of its effect on achieving objectives. Events can have negative impact, positive impact, or both. For a given kind of event, the possible impacts may range from less severe to most severe.

8.9 Organization

Organization means an Autonomous Body or Public Sector Company, owned or controlled, directly or indirectly, by the Government of Khyber Pakhtunkhwa.

8.10 Probability

The probability of an event is its likelihood. This will typically be an estimate and may be subjective because of the absence of useful empirical data.

8.11 Project Risk

Risk that could cause doubt about the ability to deliver a project on time, within budget and to quality.

8.12 Risk

Risk is the combination of the probability of an event and its consequence. Consequences can range from positive to negative.

8.13 Risk Appetite

The amount of risk that an entity is prepared to accept, tolerate or be exposed to at any point in time.

8.14 Risk Assessment

The overall process of analysis and evaluation of a risk with regard to its impact and the likelihood of its being realized, and the selection of an appropriate risk response.

8.15 Risk Culture

The set of shared attitudes, values and practices that characterize how an entity considers risks in its day-today activities.

8.16 Risk Management

Risk management is a comprehensive process which integrates recognition of risks, risk assessment, developing strategies to manage, and mitigation of risk using resources.

8.17 Risk Profile/register

A documented and prioritized assessment of the range of specific risks faced by an entity.

8.18 Risk Response

The set of actions that may be taken in response to a risk, as follows:

Transfer the risk: This may be done by asking a third party to take on the risk.

Accept/tolerate the risk: The ability to take effective action against some risks may be limited, or the cost of taking action may be disproportionate to the potential benefit gained. In this instance, the only management action required is to monitor the risk to ensure that its likelihood or impact does not increase. If new management options arise, it may become appropriate to treat this risk in the future.

Mitigate risk probability: Take action to reduce and manage the probability of a risk, with the goal of reducing the risk to an acceptable level.

Mitigate risk impact: Take action to reduce and manage the impact of a risk, with the goal of reducing the risk to an acceptable level.

Terminate the underlying activity: This involves quick and decisive action to eliminate or avoid a risk altogether by ending the business activity that gives rise to the risk.

Exploit the risk: Opportunities can be exploited in a positive manner.

8.19 Risk Treatment

The selection and execution of an appropriate method for dealing with risk. This will involve one or a combination of the strategies defined above: transfer, accept/tolerate, mitigate probability, mitigate impact, terminate and/or exploit.

9. Effective date and scope of policy

9.1. This Policy Note is effective from 01.02.2022 and PSCs/ABs shall comply with this policy note on or after effective date of this policy note.

9.2. This policy is applicable to Public Sector Companies / Autonomous Bodies owned by the Government of Khyber Pakhtunkhwa and notified by the Finance Department from time to time.

9.3. The Finance department, Government of Khyber Pakhtunkhwa may issue guidelines for the purposes of risk documentation and reporting from time to time and the ABs/PSCs shall comply with such guidelines.

Template – 1

Risk Register

S. No.	Risk Identification			Inherent Risk Assessment				Current Risk Assessment						Consequences / Exposure		
	Risk description	Perceived Cause	Risk Category	Exposure (PKR 'Million)	Likelihood	Magnitude	Inherent Risk Severity	Existing/ Current Controls	Likelihood	Impact	Current Risk Severity	Enhancements	Owner	Inherent	Current	Target

Template – 2

Risk Treatment Plan

Rank	Risk Description	Rating	Treatment /Actions	Date Due	Owner	Status	Comments % Completion

Template – 3

Risk Trend Analysis

Rank	Risk Description	Residual Risk Severity	Trend	Reason for Change	Improvement Required?	Improvement Status
		High				
		Medium High				
		Medium				
		Medium Low				
		Low				

Legends:

Completed | Work in progress | Possible Delay / Delayed | Not applicable