BISAP

BANGLADESH INTEGRATED SOCIAL ADVANCEMENT PROGRAMME

(An Organization for Integrated Social Development)

INTERNAL CONTROL POLICY

Bangladesh Integrated Social Advancement Programme (BISAP)

Address : House # 02, Road # 01, Lake Valley Residential Area, Nuria Madrasha Road, Foy's Lake, Khulshi - 4225, Chattogram, Bangladesh.

Table of Contents

1. Policy Statement:

Bangladesh Integrated Social Advancement Programme (BISAP) realizes that it, in pursuit of its vision- and mission driven interventions, may face risks of different degrees and dimensions. The Organization will incorporate risk assessment and management procedures in its strategic planning, decision-making process and operational planning. The Organization is committed to enhancing the understanding of risk management principles and requisite risk management skills for its staff especially the Senior Management Team (SMT) including the Executive Director (ED). The Organization will develop a system to delegate the responsibilities of risk identification and control to the line management. The Organization's risk appetite is guided by its pursuit of attainment of its objectives through change and innovation in its interventions. The risk appetite will depend on whether the assessment is related to routine work or humanitarian/emergency. The policy explains the Organization's approach to risk assessment and risk management.

2. Purpose:

The risk management policy forms part of the Organization's governance and internal control to make every effort to manage risk appropriately by maximizing potential opportunities whilst minimizing the adverse effects of risks. Mitigating the risks in good time, will enable the achievement of organizational objectives, protect staff, protect business assets and reputation and manage financial sustainability. It also provides a framework to identify, assess, and manage key risks through reporting procedures to evaluate the effectiveness of the Organization's internal controls.

3. Definitions:

In the context of this policy, the definitions of the following terms are articulated.

3.1 Risk: Risk refers to the chance of something bad happening to the Organization's operations and practices. Risk involves uncertainty.

3.2 Risk Assessment: Risk assessment refers to the overall process of identifying and analyzing the risks.

3.3 The Risk Management Process: Risk management process refers to a coordinated response to the risks for their mitigation or elimination.

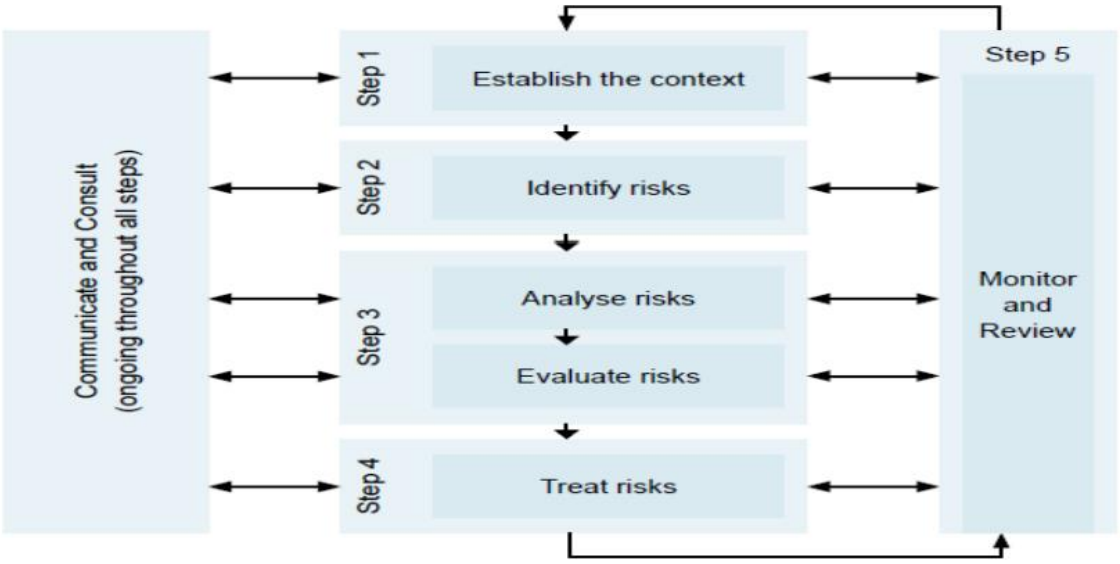
3.4 Risk Appetite: Risk appetite refers to the accepted level of risk the organization is prepared to take in pursuit of the attainment of its objectives. Risk appetite is of two types-high risk appetite and low risk appetite. The Organization will decide whether it will take a high risk or low risk based on its preparation and capacity to cope with the potential risk(s).

3.5 Risk Register: It is a document (may be MSWord/MS Excel-based or register-based) that pertains to the results of risk analysis and risk treatment/response plans. It helps the Organization to manage the identified risks prudently as well as incorporate suddenly poppedup risks. The Organization can see the performance related to the risk management.

3.6 Potential Risk: Risk is inherent in any intervention in a-ny part of the world. There is no environment free of risk. Risks are broadly divided into two categories- i) external risks: external risks derive from actions of outside actors. External risks include political instability, terrorist activities, etc.) and ii) internal risks: internal risks are related to NGOs' programmatic and organizational actions. Programmatic risks include poor service delivery, lack of capacity etc. and organizational risks include poor human resource management system, poor financial management system, etc.

4. Risk Management Process:

The risk management framework is derived from the Organization's strategic plan, performance management, audit and assurance, business continuity management and project management. The Organization will follow the following risk management process:



Explanation of the 5 Steps, Communication & Consultation, Monitoring & Review:

4.1 Step1: **Establish the Context:** To establish the Context, the Organization will identify the environments in which the risks take place. The environments, both internal and external, includes strategic, operational, financial, competitive, stakeholder, social, cultural, legal. As risks does not occur in vacuum, the Organization must identify the contexts in which it operates. Identifying the contextual environment will help the Organization respond to the next steps.

4.2 Step 2: Identify the Risks: When contexts are known, the Organization will proceed to identify risks (more categorically sources and causes of risks the Organization is exposed to, potential consequences, and existing risk management control).

This step consists of three major sub-steps: i) identifying the category of Risk, ii) risk identifying methods and iii) identifying risk management controls.

i) Identifying Category of Risk: It includes risk categories and examples of related risk. Any organization can face the following potential internal and external risks (but not limited to):

Risk Category	Examples of related Risks
Governance risks	• inappropriate organizational structure, • Senior Management Team lacks relevant skills or commitment, • conflicts of interest, • Negative media story, • Negative public sentiment, • Litigation by staff, ex-staff or partner
Operational risks	• lack of beneficiary welfare or safety, • poor contract pricing, • poor staff recruitment and training, • doubt about the security of assets
Financial risks	• inaccurate and/or insufficient financial information, • inadequate reserves and cash flow, • dependency on limited income sources, • inadequate investment management policies, • insufficient insurance cover, • Diversion of aid materials
External risks	• poor public perception and reputation, • demographic changes such as an increase in the size of the beneficiary group, • turbulent economic or political environment, • changing government policy
Compliance with law and regulation	• acting in breach of Government Law and Policy, • poor knowledge of the legal responsibilities of an employer, • poor knowledge of regulatory requirements of particular activities (e.g., fund-raising, running of care facilities, operating vehicles), • Inappropriate communication by staff on social media.

ii) Risk Identifying Methods: Risk identifying methods includes a one-to-one interview, and workshop. Cause-Effect Analysis helps identify contributing factors (causes) and outcomes (consequences).

iii) Identifying Risk Management Control: Risk management controls include already existing internal controls - policies, reporting, recruitment policy, internal audit, meeting, Human Resource Management System, Procedures, Work Manual, ICT Management, Budgeting, Strategic Planning, etc.

4.3. Step 3: Analyse Risk: When risks are identifies, the Organization will analyse the risks. The step includes i) assessing the likelihood/probability and consequences of each risk, ii) determining the overall level of risk, iii) developing a risk profile, iv) preparing a risk register and v) assigning risk ownership.

i) Assessing the Likelihood and Consequences of a Particular Risk: The likelihood of a particular risk can be assessed using the scales - **Remote Chance, Improbable, Possible, Probable and Almost Certain.** Please see **Annex-1: Detail Description on Likelihood along with Probability** for the highest-level understanding.

The consequences of a particular risk can be assessed using the scales - **Insignificant, Minor, Moderate, Major, and Critical**. Then, in general, the scales will have 3-7 points from the lowest to the highest degree of the likelihood. Points can differ from the below distributions based on the Organization's needs and approach. An example is given below:

Consequence Level	Point Distributed
Insignificant	**1**
Minor	**2**
Moderate	**3**
Major	**4**
Critical	**5**

ii) Determining the Overall Level of Risk: When levels of likelihood and levels of consequence are identified, an overall risk matrix will be prepared.

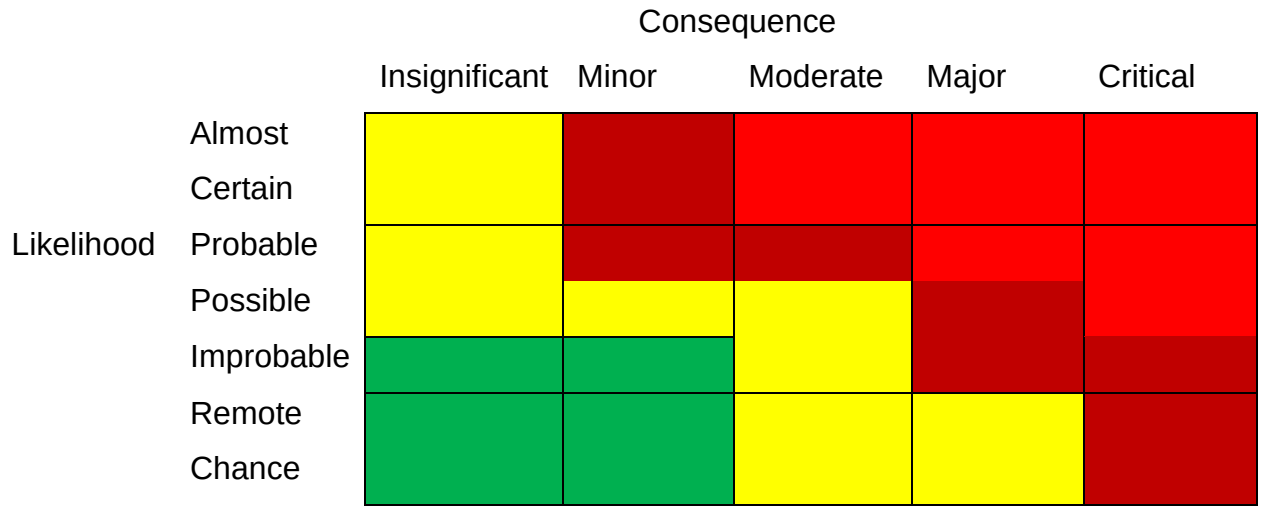
		Consequence				
		Insignificant	Minor	Moderate	Major	Critical
Likelihood	Almost Certain					
	Probable					
	Possible					
	Improbable					
	Remote Chance					

iii) Developing a Risk Profile: Based on the Organization's risk appetite, the above basic matrix (above one) will be coloured. The appetite of risk is aligned with the colours:

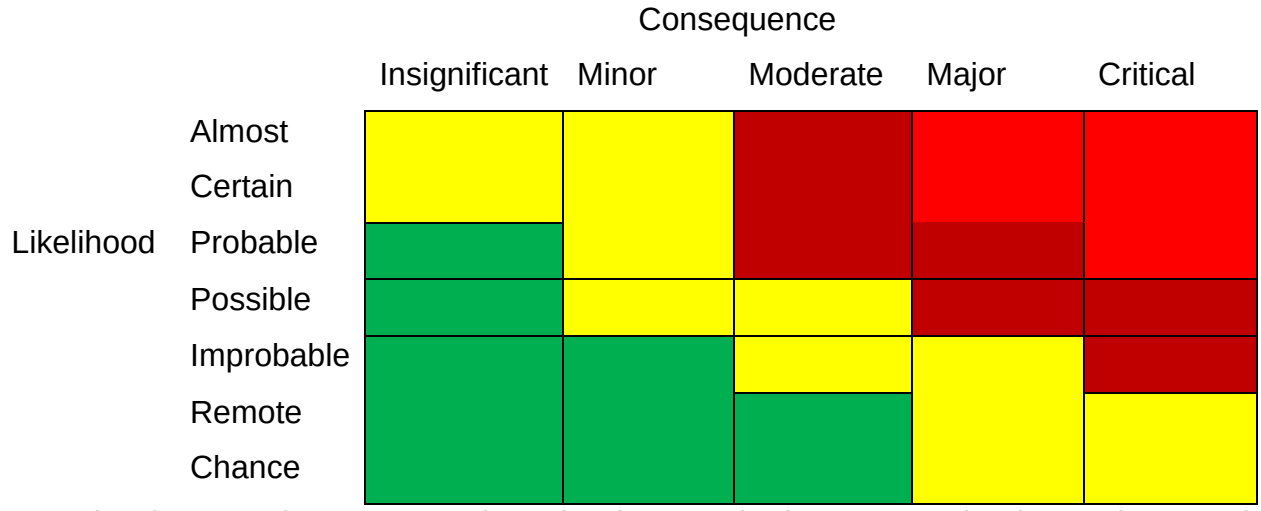
Risk Appetite Level	Aligned Colour
Extreme	
High	
Medium	
Low	

If the Organization has low risk appetite, it might colour the squares more. On the other hand, if it has high risk appetite, it might colour the matrix differently. Two examples are placed below:

Low Risk Appetite-based Matrix:



High Risk Appetite-based Matrix:



Note: The above matrixes are examples only. The Organization can organize the matrixes to suit its plan.

iv). Preparing a Risk Register: After the above steps are completed, the Organization will prepare a Risk Register to record risk information. A sample of the risk register is placed below:

				(5) Risk Rating		
(1) Risk Number	(2) Risk Category	(3) Risk Description	(4) Current Controls	Likelihood	Consequence	Risk Level

(6) Risk Owner	(7) Risk Treatment/Response Plan	(8) Additional Action

v) Assigning Risk Ownership: After risk(s) is/are assessed, the Organization will assign staff to own the responsibilities for managing it/them. Typically, owners are the persons with senior management portfolios having authority and resources urgent for risk treatmentrelated actions.

4.4 Step 4: Evaluate Risk: After risk analysis, the Organization will compare the risk against set criteria. In addition, a decision would be made to treat the risk.

4.5 Step 5: Treat Risk: The purpose of this step is to find out the best means to mitigate the risk. In this step, the most suitable risk treatment options will be selected and applied. If the risk level is 'extreme', then immediate action is needed. If the risk level is 'high', then a cost-benefit analysis is required. If the risk level is 'medium', then regular monitoring is regular. And if the risk level is 'low', then effectively managed through routine procedures and internal controls.

4.6 Communication and Consultation (ongoing throughout all steps): Communication in all steps of the risk management process will be ongoing. Both internal and external stakeholders will be communicated to inform them of what is going on in risk management process. In fact, relevant managers and staff will be consulted to engage them in the risk management process.

4.7 Monitoring and Review: To keep the whole risk management process in progress, monitoring and review of the risk management activities will be responsive to the change management. So, to facilitate the change management, the Organization will delegate monitoring and review authorities and/or responsibilities to the following stakeholders:

5. Risk Governance Structure of the Organization:

The following table provides an overview of the risk governance structure of the Organization along with its responsibilities:

Senior Management Team (SMT)	• To review the performance of the risk management system and outstanding risk treatment actions on a regular basis. • To formally review Risk Register on an annual basis. • To assist the effectiveness of the risk management policy annually.

Audit and Risk Committee	•To oversee a quarterly review of risk management activities and report to the SMT. • To consider how the Executive Committee can obtain assurance that risks are being managed effectively. • To exercise 'risk management performance' for relevant stakeholders including the SMT through multiple actions including a Risk Register check.
Heads of the Departments	•To report to SMT every two months of their respective departments' risk management. • To Identify strategic risks and lead mitigating actions. • To report to SMT how strategic risks are being managed.
Managers	• To provide monthly updates on programs and projects risks management framework to Heads of Departments. • To ensure an appropriate management system of operational and project risk is in place.
Staff	•To comply with risk management policies and procedures through informing the line management of risk factors and undertaking appropriate actions towards those risk factors within his/her jurisdiction. • Ensure partners/ contractors are complying with relevant polices.

6. Risk Management Principles:

Risk management principles underpin the result-oriented risk management process. So, the Organization will apply the following principles in its risk management process:

6.1 Inherence to the Decision Making: Each and every decision under the jurisdiction of the Organization will be taken in compliance with the policy.

6.2 Attachment to the Organization's Vision and Mission: The policy is applied as a vehicle for attaining the organizational vision and mission.

6.3 Systematic, Structured, and Timely Response to Organizational Risk: The Organization will be guided by a well-established mechanism responsive to timely and systematic procedures.

6.4 Human- and Culture-Sensitive Policy: The Organization will scrutinize, without any failure, the local culture in which it operates and human sentiment before applying the policy.

6.5 Transparency and Inclusiveness: The whole risk management process will not show any biasness to any staff based on authorities. All staff will be placed under the prism of scrutiny if any suspicion arises.

6.6 Continuous Improvement: The Organization believes that the improvement of the risk management system and culture is a long process. The improvement can not be met through a shortcut. It deserves dedication, commitment, and time.

7. Partnership-related Risk Management:

The Organization will carry out due diligence of partners/ vendors to mitigate risks. All partners delivering work on behalf of the Organization will have a Memorandum of Understanding (MOU) which will stipulate conditions and policies that must be adhered to.

8. Capacity Building:

The Organization will disseminate the process, principles, etc. of the policy through short-lived training and workshop. They will also be communicated if any change is taken place in the policy.

9. Scope of the Policy:

This Policy applies to the Organization's all activities and risk management framework. It applies to all employees, agents, contractors, subcontractors, consultants, UK and, global partners and any other parties (including individuals, partnerships and corporate bodies) associated with the Organization.

10. Compliance:

The policy will be applied together with other policies and regulations of the Organization. The other policies include Anti-Fraud, Anti-Bribery and Anti-Corruption Policy, Data Protection Policy, Financial Manual, Conflict of Interest Management Policy, Whistle Blowing Policy, Anti Money Laundering Policy, Counter-Terrorism and -Extremism Policy, etc.

11. Annexes:

Annex-1: Detail Description of Likelihood along with Probability:

Likelihood Level	Examples	Probability
Remote Chance	• May occur only in circumstance • Typical frequency once every 500 years or more • Likelihood over 5 years: >0.005% (1 in 20,000 chance)	<20%
Improbable	• It is not expected to occur • No recorded incidents or evidence • Little opportunity, reason, or means to occur • Typical frequency once every 100 years •Likelihood over 5 years: >0.5% (1 in 2,000 chance)	>20% - 40%
Possible	•May occur at some time • Few or infrequently recorded incidents to occur • Some opportunity, reason, or means to occur • Typical frequency once every 20 years • Likelihood over 5 years: > 0.5% (1 in 200 chance)	>40% – 60%
Probable	•Likely to occur/recur • Regularly recorded incidents and strong evidence	>60% - 80%

	• Will occur in many circumstances • Typical frequency once every 5/7 years • Likelihood over 5 years: > 5% (1 in 20 chance)	
Almost Certain	•Likely to occur/recur • High level of recorded incidents and strong evidence • Typical frequency once every 5 years • Likelihood over 5 years: > 50% (1 in 2 chance)	>80% - 100%

Mohammad Dostagir
Chairman

S.M. Tareque Jabed
Chief Executive-BISAP