

CERP

**RISK
MANAGEMENT**

Risk Management

‘Risk’ is defined as uncertainty, whether positive or negative, that affects the outcome of an activity or intervention. The term ‘management of risk’ incorporates all the activities required to identify and control exposure to risk that may have an impact on the achievement of CERP’s objectives, activities, programs and projects at the organizational and project levels. Risk management is important: it enables CERP to be innovative and to avoid disasters. At CERP, risk is managed at both the organizational and project levels.

A. Organizational Risks

Organizational risks are risks that relate to CERP as an organization. Risks are monitored by relevant Board Committees and CERP Management. The Finance and Audit Committee analyzes, and monitors risks related to finance, business continuity, internal financial controls, planning and political risks, procurement and fiduciary and risks. CERP’s HR management analyzes and monitors all human resources processes. The Administration and Policy Committee deals with risks related to IT security, administrative processes, risks related to security, health and safety, and legal and regulatory compliance. Each Committee is required to develop its framework of risk analysis and assess risks under their purview in accordance with the framework in their quarterly meetings and suggest appropriate actions to manage risks.

The day to day managers of organizational risks are the Finance, Operations and Human Resource Departments.

CERP Management and Board Committees will undertake to produce comprehensive risk registers for their respective functional area. These registers will be updated on quarterly basis. The below risk register template is provided for guidance:

Risk ID	Risk Description	Risk Assessment			Impact (Cost/Time)	Mitigation Measures	Contingent Measures	Residual Risk	Risk Owner
		L	M	H					

B. Project Risks

Project risks are risks that relate to each of the CERP projects. These risks are monitored by project PIs and by the Project Managers in the monthly oversight meetings. CERP encourages all projects to develop a robust risk framework in accordance with the requirements of their funding bodies and in consultation with CERP Management. Project risks that result in low impact at the organizational level will be dealt at the level of the project PIs. However, all project risks that have the potential to create medium or high impact at the organizational level will be brought to the attention of the relevant Board Committee on a quarterly basis for analysis and decisions.

Managers escalate identified project risks to their PIs and CERP Management, who will discuss these issues with project PIs and escalate the matter to the CEO if necessary. PIs will assess the project level impact and propose mitigation strategies at this level, share these with CERP Management before they are finalized. For risks that impact CERP Core, decisions will be taken by CEO who will make recommendations to the CERP Board.

As a standard practice, all Program and Project Managers will produce comprehensive risk registers for their respective programs or projects. These registers will be updated on quarterly basis. The below risk register template is provided for guidance:

Risk ID	Risk Description	Risk Assessment			Impact (Cost/Time)	Mitigation Measures	Contingent Measures	Residual Risk	Risk Owner
		L	M	H					

C. Downstream Partner Level Risk

Downstream partners are required to maintain Risk Registers at their level, with respect to all CERP projects and activities. CERP management and project teams are required to ensure the downstream partners maintain the risk register and demand immediate escalation of the issues.

The downstream partners must include all risks, including but not limited to the following:

1. Operational risks
2. Travelling & Safety risks
3. Environmental risks
4. Safeguarding risks

The risk framework at the organizational and project levels should use the following principles:

