Risk Management Manual

E D C T P

2015

Version number: 1

Approval date: 5 August 2015

Approved:

Charles S. Mgone
EDCTP Executive Director

1 Introduction

1.1 Overview of risk management

Risk is defined, in the context used in this manual, as any threat that, if it occurs, may prevent the attainment of the objectives of EDCTP, in whole or in part. Risk management provides the framework to identify, assess and manage risks; and the methodology for integrating risk into decision making. The main aim of risk management at EDCTP is to maximise opportunities in all EDCTP activities and to minimise adversity.

Risk exists in all activities and cannot be completely avoided. However, the risks taken and accepted on behalf of the EDCTP must be tolerable; risks must be identified and the management of them consciously accepted. It may not be possible to eliminate all the risks EDCTP may face without undermining the whole basis on which the EDCTP operates or without incurring excessive costs. Therefore in many situations there is likely to be a level of residual risk which is simply not worth eliminating. However, it is necessary to find ways of ensuring that EDCTP directors, managers and staff pay sufficient attention to risk management and do not take excessive risks. Without risk management, there is a real possibility that serious financial and non-financial damages could be caused to EDCTP because avoidable risks were not identified and managed.

1.2 Purpose of this manual

The purpose of this document is to describe EDCTP's framework and procedures for risk management, including the control mechanisms and processes for dealing with risks. It defines the processes for the management of risks faced by EDCTP. The objectives of preparing this document include:

- To help EDCTP directors, managers and staff to effectively manage risks
- To create a strong culture and awareness of risk management
- To act as reference guide for all EDCTP staff
- To ensure consistency in dealing with risks.

1.3 Application of this policy

The policy must be applied to all activities undertaken by, and on behalf of EDCTP. It is therefore the responsibility of every EDCTP employee to know this policy.

1.4 Approval of this manual

This manual has been approved by EDCTP Executive Director.

1.5 Content and structure of the manual

This manual describes EDCTP framework for risk management. This manual will lose its effectiveness if it does not accurately reflect actual procedures for risk management. With this in mind, the continuing suggestions and recommendations of the management and staff are essential to ensure that it accurately reflects actual procedures.

1.6 Deviations from this manual

As a general rule EDCTP's senior management expects this manual to be followed as written. In exceptional cases where a deviation from the manual is required to deal with urgent situations that are not covered in this manual, a deviation can be made and the reasons for the deviation must be documented in writing, and approved by the Executive Director (ED) or Director of Finance and Administration (DFA).

1.7 Distribution and monitoring responsibilities

It is the DFA's responsibility to maintain and distribute appropriate sections of this manual to his/her subordinates and other departments; and to provide training and assistance in its interpretation.

Questions with regard to the application or interpretation of any of these sections should be directed to the DFA.

2 Definition of terms used

Term	Definition
Actions taken	Actions taken to mitigate or deal with the level of risk.
Consequence	Consequence is the outcome of an event, being a loss, disadvantage or gain.
Controls in place	The internal control system and procedures in place at the time of the risk identification.
Likelihood	Likelihood is a qualitative description of probability of the risk happening.
New/Additional actions	Actions planned or taken since the last review to monitor or mitigate further the level of risk.
Reputational risk	Reputational risks include negative public opinion due to non-performance of promised services due to actions done by the EDCTP employees.
Risk	Risk is defined as any threat that, if it occurs, may prevent the attainment of the objectives of EDCTP, in whole or in part. At EDCTP Risk is rated by considering two characteristics: Likelihood (L) of occurrence; and consequence/Impact (I) of occurrence. Risk is calculated: R (Risk) = L (Likelihood) x I (Impact).
Risk Assessment	Risk Assessment is the process of evaluating and comparing the level of risk against predetermined acceptable levels of risk.
Risk Management	Risk Management is a systematic approach to identifying, measuring, monitoring and managing risks. It provides the methodology for integrating risk into decision making.
Risk Owner	Risk owner is the member of staff responsible for managing the risk identified, and is usually the person directly responsible for the activity or function that relates to the risk.
Risk status	Risk status is the level of risk at the time of the last risk update.
Treat	This strategy seeks to reduce the risk probability or its impact by taking early action to reduce the occurrence of the risk to an acceptable limit. Risk mitigation may take the form of implementing new processes, undertaking

	more preliminary work, or changing conditions so that the probability of the risk is reduced, by adding resources or time to the programme.
Terminate	This strategy seeks to eliminate the risk or to protect the project objectives from its impact. Although not all risks can be eliminated, some may be avoided by terminating the action (for example, to close a grant).
Tolerate	This strategy indicates that decision has been taken to accept the risk, or no suitable strategy has been identified to deal with the risk. Risk acceptance may also occur when the cost of dealing with it would not be cost effective.

3 EDCTP risk management policy and responsibilities

- Risk management is an integral part of the responsibility of each member of staff, implying that it is everyone's responsibility; employees at all levels can provide insight into the nature, likelihood and impact of risk. However, it is the responsibility of managers to identify, evaluate, respond, monitor and communicate risks associated with any activity, function or process within their relevant scope of responsibility and authority. Each member staff, particularly Project Officers (POs), Grant Finance Officers (GFOs) and Grant Finance Assistants (GFAs), has a responsibility for maintaining good internal controls and managing risk. Everyone should be aware of the risks that are present in their activities. As new risks are identified they must be reported to the appropriate level of authority. The line manager, if necessary, should report it to senior management with any recommended risk response strategies
- A risk register is maintained to record and prioritise the main risks EDCTP faces (see content of EDCTP risk register in section 5 of this manual)
- Risk management is considered in all grant approvals in a manner appropriate to the nature and scope of the project
- The management committee, chaired by DFA and comprises representatives from all EDCTP departments, is responsible for ensuring that all risks are identified and managed appropriately
- Directors and managers shall ensure that everyone in their department(s) understands their risk management responsibilities and must make clear the extent to which the staff are empowered to accept risks
- The DFA will provide support to staff in identifying, assessing and managing risks
- The management committee is responsible for setting up policies on risk management and internal controls and to ensure the risk management process is incorporated into planning and decision making.

4 Risk management structure

4.1 Responsibilities of the General Assembly (GA) and Board

It is the responsibility of the GA and Board to set the tone of risk management of the EDCTP-Association right from the approval of the workplans, procurement policy and procedures, and other relevant policies and documents.

4.2 Management team

The Risk Management Committee is composed of the management team. The management team must consider:

- The nature and extent of risks facing EDCTP
- The extent and categories of risks which it regards as acceptable for EDCTP to bear
- The likelihood of the risk materialising

- The EDCTP's ability to reduce the incidence and impact on the business of the risks that do materialise
- The costs of operating particular controls relative to the benefits obtained in managing the related risks.

The responsibilities of the management team include to:

- Build sound systems of internal controls into the daily operations of EDCTP
- Approve policies for measuring, categorising and monitoring risks
- Create a culture of low risk tolerance
- Assess and prioritise internal and external risks faced by EDCTP
- Develop KPIs that can be tracked and analysed regularly to assess exposure to risk in each area of operation
- Ensure that risk owners are sufficiently aware of their responsibilities.

5 Risk register

The EDCTP risk register serves as the central repository for risk information. Its main purpose is to provide EDCTP management, staff and auditors information on the main risks faced by the organisation and is used as the main tool for managing and reducing the risks identified. The EDCTP risk register provides information on the following:

- Who is responsible for managing each risk identified (risk owner)
- Risks identified in terms of likelihood of occurring and impact if it does occur
- A grading of each risk according to a risk assessment table
- An outline of proposed mitigation actions (preventative and contingency).

The register is not a static document; it will change when existing risks are regraded or when new risks are identified.

The EDCTP risk register lists and prioritise the main risks EDCTP faces, and is used as the basis for decision-making on how to deal with risks. When risks are identified, they are graded according to likelihood and impact, and then recorded in the risk register.

The EDCTP risk register is used to record the following risk information:

- Risk number
- Description
- Classification
- Likelihood/probability
- Consequence/impact
- Risk response strategy
- Root cause
- Controls in place
- Planned action
- Risk owner
- Status
- New/additional actions since the last review
- Actions taken.

The Management Accountant (MA), under the supervision of the DFA, is responsible for maintaining and updating the EDCTP risk register. The management team should at the end of every year discuss the content of risk register with the objective of ensuring that all risks have been captured and relevant risk status updates have been appropriately made.

6 EDCTP Risk Management Overview

1. EDCTP risk types

- Financial damage
- Reputational damage
- Achieving objectives.

2. EDCTP risk classification

- Reputational
- Operational
- Financial
- Political
- Grants/Finance
- Strategic
- Governance/policy.

3. Impact of risk categories

1 Negligible
2 Moderate
3 Serious
4 Critical

4. Likelihood/probability of risk

1 Low (under 15%)
2 Medium (15-50%)
3 High (51-80%)
4 Very high (over 80%)

5. Impact/Consequence definitions

	Impact/Consequence				
		Negligible	**Moderate**	**Serious**	**Critical**
Type of risk	**Financial damage**	<500,000	500,000 - 2,000,000	2,000,000 - 20,000,000	>20M loss
	Reputational damage	little or no impact on relationships with stakeholders	national media criticism	International media criticism, Debate at EU and/or AU political level	Damage severe enough to suspend operations or undermine ability to operate
	Achieving objectives	little or no impact on achieving objectives	some adverse impact on one or more objectives (manageable by secretariat)	Jeopardises objectives	Threatens future continuity

6. Likelihood/probability scores

Probability	Likelihood	Score
Over 80%	Very High	4
51 - 80%	High	3
15 - 50 %	Medium	2
Under 15%	Low	1

7 Risk management methodology

1. Risk identification

The first stage of EDCTP's risk management methodology is risk identification. This is so because no one can manage a risk without first being aware that it exists. Actively identifying the risks before they materialise makes it easier to think of methods that can be used to manage the risks. Both external and internal events which affect the achievement of EDCTP objectives must be identified. Risk identification involves looking at specific events and conditions that could result in risk materialising. At EDCTP risks are identified: at management level, mainly key risks affecting strategy; and at day-to-day operational level by Grant Finance Officers, Project Officers and Grant Finance Assistants.

2. Risk assessment

The second stage is risk assessment. At this stage risks are analysed, considering likelihood and impact, as a basis for determining how they will be managed.

Likelihood/Consequences matrix

Impact/Likelihood	Negligible	Moderate	Serious	Critical
Very High	Tolerate	Treat	Treat/minimal action	Terminate
High	Tolerate	Treat	Treat/minimal action	Treat/minimal action
Medium	Tolerate	Tolerate	Treat	Treat
Low	Tolerate	Tolerate	Tolerate	Tolerate

Risk score

Risk score is calculated R (Risk) = L (Likelihood) x I (Impact).

The focus will be on reducing most of the significant risks rather than eliminating them. Judgement will be involved in deciding what level of risk is as low as reasonably practicable. However good the organisation's risk identification and assessment processes are, there will always be some unexpected risk.

Risk score table

1 – 4	Low
6 – 8	Medium
9 – 12	High
Over 12	Very high

This stage involves using the results of a risk analysis to group risks into risk families.

3. Risk response selection

The third stage involves management selecting the appropriate risk response strategies (Tolerate, Treat, Treat immediately or Terminate)

Risk response strategy		
Likelihood/Impact combination	**Risk response strategy**	**Monitoring strategy**
Low likelihood/negligible impact	Tolerate	Monitor/no action
Low likelihood/moderate impact	Tolerate	Monitor/no action
Low likelihood/serious impact	Tolerate	Monitor/minimal action
Low likelihood/Critical impact	Tolerate	Action
Medium likelihood/negligible impact	Tolerate	Monitor/no action
Medium likelihood/moderate impact	Tolerate	Monitor/minimal action
Medium likelihood/serious impact	Treat	Action
Medium likelihood/critical impact	Treat	Immediate action
High likelihood/negligible impact	Tolerate	Monitor/no action
High likelihood/moderate impact	Treat	Action
High likelihood/serious impact	Treat immediately	Immediate action
High likelihood/critical impact	Treat immediately	Immediate action
Very high likelihood/negligible impact	Tolerate	Monitor/minimal action
Very high likelihood/moderate impact	Treat	Action
Very high likelihood/serious impact	Treat immediately	Immediate action
Very high likelihood/critical impact	Terminate	Immediate action

4. Control procedures
The fourth stage involves the implementation of policies to help ensure the risk responses are effectively carried out.

5. Monitoring risk response processes
The final stage involves continuously monitoring of risk control processes and making modifications when necessary. The monitoring is performed by staff (POs, GFOs and GFAs) and managers and directors.

Risk Monitoring			
Frequency of monitoring	**Review process**	**Risk code**	**Strategy**
Routine	Interdepartmental		Monitor/no action
	Management/Senior management meeting		Monitor/minimal action
			Action
Real time	Through management lines		Immediate action

8 Risk management post-award grant administration

8.1 Introduction

To achieve the objective of ensuring that EDCTP funds are used in line with EDCTP financial guidelines without incurring excessive costs - in a cost effective manner - different approaches are used:

- Internal audits by an external audit firm
- Due diligence checklist prior to grant signature

- Site visits
- Effective follow-up on management letter points.

8.2 Internal audit by an external audit firm

As part of the strategy to improve the quality of the financial reports submitted by beneficiaries and to form an informed view of the general effectiveness of the beneficiaries' internal control system, EDCTP has signed a memorandum of understanding with PWC Netherlands to conduct audits of EDCTP-funded projects. In selecting sites for PWC internal audit, more weighting is given to sites with any one of the following criteria:

- Actual expenditure is more than €325,000
- End date of the project is not within the next 12 months
- Projects with many Grant Finance Officer observations in previous financial reports
- Sites with more than one EDCTP funded project
- Previous unfavourable site visit reports
- Sites with high staff turnover in the finance department.

8.3 Due diligence checklist prior to grant signature

A due diligence review checklist has been developed as a proactive approach to reducing the risk of non-compliance with EDCTP financial guidelines. This checklist is divided into four sections (organisation of the finance department, accounting system, bank accounts and experience of managing donor projects) and is used for conducting a due diligence review of new beneficiaries to assess the strength of all new beneficiaries' internal financial control environment. The inherent risk information obtained via due diligence is used to help EDCTP Grant Finance Officers and Grant Finance assistants to take decisions such as which type of bank account – pooled or designated- the new site will be allowed to operate for the project.

8.4 Site visits

Site visits are carried out every year to review the financial management systems and procedures of EDCTP beneficiaries. These included a review of the following:

- Bank reconciliation statements to ensure that bank reconciliations are performed and reviewed on a regular basis
- Financial transaction documents
- Fixed asset registers
- Payroll reports
- Extent of compliance with EDCTP financial guidelines
- Overall financial and internal control systems.

8.5 Effective follow-up on audit reports and management letter points

- GFO or GFA writes to all the sites with a qualified report requesting them to report on the actions taken or planned in respect of the observations and recommendation raised in the external auditors' management reports. Net financial impacts resulting from unresolved observations are treated as ineligible expenditure and are accordingly deducted from actual expenditure in the final financial report
- GFOs or GFAs regularly follow up on the action plans relating to all significant external audit findings detailed in the management letter and any issues that gave rise to the qualification of audit reports
- Following each site visit letters are sent to the Project Coordinators (PC) of the sites visited informing them of the findings of the EDCTP team during their visit with recommendations and suggested action points. Similarly, in each site visit report, EDCTP action points are listed. EDCTP GFOs, GFAs and POs not only ensure the implementation of the EDCTP action points, but seek response from beneficiaries to the recommendations made in the site visit report.