EDCTP

European & Developing Countries
Clinical Trials Partnership

EDCTP-Association Risk Management Manual
October 2017

23/November/2017.

Table of Contents

1 Introduction

1.1 Overview of risk management

Risk as used in this manual is defined 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. It provides the approach for integrating risk into decision making. The aim of risk management 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 monitored/implemented. 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 manual is to describe EDCTP's framework and procedures for risk management, including the control mechanisms and processes for dealing with risks. This manual is geared towards the achievement of objectives in a number of areas. It defines the processes for the management of risks faced by EDCTP. The objectives of preparing this manual include:

- To help EDCTP directors, managers and non-managerial staff to manage risks effectively
- To create a strong culture 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's Executive Director and the Director of Finance and Administration (DFA).

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 EDCTP staff, Board, Audit Committee and other EDCTP stakeholders 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 or 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. Control in place is a mechanism to prevent or reduce the likelihood of a risk occurring, and an activity to reduce the impact of a risk should it occur.
Financial risk	Financial risk is defined as the risk arising from financial operations of EDCTP and includes: • Liquidity risk (funding or cash flow risk) • Cash handling risk (risks relating to security of cash)– per diem payments at EDCTP events • Default risk – non recovery of EDCTP funds from beneficiaries
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.
Operational risk	Operational risk is defined as the risk arising from inadequate or failed internal processes, people, and systems or from external events. Operational risks relate to matters that can go wrong on a day-to-day basis, and are generally not very relevant to the key strategic decisions that affect EDCTP. Operational risks are generally within the control of the organisation through risk assessment and risk management practices, including internal control. Examples of operational risks are: • Non-compliance with the Delegation Agreement and H2020 rules • Non-compliance with internal policies and procedures • Late submission of reports • Inaccurate final reports (errors or omissions by employees) • Failure of IT systems • Loss of key people • Litigation • Fraud • EDCTP incurring ineligible expenses resulting from beneficiaries or other stakeholders not performing according to the terms of the contract.
Reputational risk	Reputational risk is damage to an entity's reputation as a result of failure to manage other risks. Reputational risks include: • Negative public opinion due to non-performance of promised services by EDCTP employees • Unethical and unprofessional behaviour by any member of the EDCTP governance bodies or other stakeholders, including the GA, the Board, Scientific Review Committees (SRC), Scientific Advisory

	Committee (SAC) and staff.
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 response	Risk response is the process of selecting and implementing measures to manage the risk.
Risk status	Risk status is the level of risk at the time of the last risk update.
Strategic risk	Strategic risk is defined as the risk stemming from the entity's strategy and poses the greatest threat to the achievement of the strategy. Examples include poor relationship with funders and poor implementation of the Strategic Business Plan.
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 generally via internal controls. 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 organisation's 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 EDCTP member of staff 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. Risk register review must be included as an agenda item at every management meeting.
- 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 the DFA, comprising 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, is aware of the existence of the risk register 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)/Board

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

4.2 Audit Committee

The Audit Committee is responsible for reviewing the effectiveness of internal control principles, including reviewing financial, operational and compliance controls.

4.3 Management team

The Risk Management Committee is composed of the management team. The management team, at each management meeting, must consider:

- The nature and extent of risks facing the EDCTP
- The extent and categories of risk which it regards as acceptable for EDCTP to bear
- The likelihood of the risk materialising
- EDCTP's ability to reduce the incidence and impact on the organisation should the risks 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 key performances indicators (KPIs)_ that can be tracked and analysed regularly to assess exposure to risk in each area of operation

- Identify the risk owner
- Ensure that risk owners are sufficiently aware of their responsibilities.

5 Risk register

The EDCTP risk register serves as a central repository of 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 risks register list and prioritises 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:

- Date risk was identified and by whom
- A unique number
- Description of risk
- Category
- 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 Legal Officer, with the help of GFA, is responsible for maintaining and updating the EDCTP risk register.

5.1 EDCTP risk types/categories

- Reputational
- Operational
- Financial
- Strategic

5.2 Impact of risk categories

1 Low
2 Medium
3 High

5.3 Likelihood/probability of risk

1 Low (under 15%)
2 Medium (15-50%)
3 High (over 50%)

5.4 Impact/Consequence definitions

Type of risk	Low	Medium	High
Financial damage (amounts in euro)	<500,000	500,000 - 2,000,000	>2,000,000
Reputational damage	little or no impact on relationships with stakeholders	national media criticism	Major reputational damage - international media criticism, Debate at EU and/or AU political level
Strategic	little or no impact on achieving objectives	some adverse impact on one or more objectives (manageable by secretariat)	• Makes the achievement of the overall strategic objectives very difficult (Jeopardises objectives) • Major deviation from target
Operational	Where there are no weaknesses or where the action considered desirable and should result in enhanced control or better value for money.	Action that is considered necessary to avoid exposure to significant risks (failure to take action could result in significant consequences).	Action that is considered vital to ensure that EDCTP is not exposed to high risks. (Failure to take action could result in major consequences for the EDCTP)

5.5 Likelihood/probability scores

Probability	Likelihood	Score
Over 50%	High	3
15 - 50%	Medium	2
Under 15%	Low	1

6 Risk management approach

6.1 Risk identification

The first stage of EDCTP's risk management approach 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 staff.

6.2 Risk assessment and measuring

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. Risk is measured by applying the impact and likelihood matrix below, which provides the overall rating

Likelihood/Impact(risk rating)	**Low (1)**	**Medium (2)**	**High (3)**
High (3)	**Medium (Tolerate)**	**High (Treat/Terminate)**	**High (Treat/ Terminate)**
Medium (2)	**Low (Tolerate)**	**Medium (Tolerate)**	**High (Treat/Terminate)**
Low (1)	**Low (Tolerate)**	**Low (Tolerate)**	**Medium (Tolerate)**

Risk score

Risk score is calculated as 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 – 2	Low

3 – 4	Medium
Over 4	High

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

6.3 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/low impact	Tolerate	Monitor/no action
Low likelihood/medium impact	Tolerate	Monitor/no action
Medium likelihood/low impact	Tolerate	Monitor/no action
High likelihood/low impact	Tolerate	Monitor/minimal action
Medium likelihood/medium impact	Tolerate	Monitor/minimal action
Low likelihood/high impact	Tolerate	Monitor/minimal action
High likelihood/medium impact	Treat/Terminate	Immediate action
High likelihood/high impact	Treat/Terminate	Immediate action
Medium likelihood/high impact	Treat/Terminate	Immediate action

6.4 Control procedures

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

6.5 Monitoring risk response processes

The final stage involves continuously monitoring of risk control processes and making modifications when necessary. The monitoring is performed by GFOs, POs, managers, and directors.

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

7 Risk management post-award grant administration

7.1 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:

- Due diligence checklist prior to grant signature
- Joint audits with Participating States
- External auditors
- Site visits
- User-friendly guidelines
- Effective follow-up on management letter points.

7.2 External Audits

As part of the strategy to improve the quality of the financial reports submitted by grantees and to form an informed view of the general effectiveness of the grantees' internal control system, EDCTP has signed an Memorandum of Understanding ((MoU) with one of the Big Four audit firms to conduct internal audits of EDCTP-funded projects. The criteria that will be used in selecting beneficiaries for audit are:

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

7.3 Due diligence checklist prior to grant signature

A due diligence review checklist (Financial Management Assessment Questionnaire for Coordinators) has been developed as a proactive approach to reducing the risk of non-compliance with EDCTP financial guidelines. This checklist is divided into six sections (organisation of the finance department, accounting system, time recording system, fixed asset register and bank accounts) and is now used for conducting a due diligence review of new grantees in order to assess the strength of all new grantees' internal financial control environment. The inherent risk information obtained via due diligence is used to help EDCTP GFOs to take decisions such as which type of bank account – pooled or designated - the new site will be allowed to operate for the project.

7.4 Site visits

Up to four site visits are carried out every year to review the operational and financial management systems and procedures. The financial assessments include 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.

The technical assessments are conducted during site visits to evaluate in-depth that the project is on track and is being conducted in compliance with national and international laws and standards. This will include verifying that all essential documents and approvals are held on file and are up to date.

7.5 Audit Committee

The responsibilities of the Audit Committee include:

- Approving the audit strategy prepared by the Secretariat, including site visits and internal audit plans
- Reviewing the audited financial statements of the Association, including the annual statutory accounts, providing advice on whether the audited financial statements are properly presented and the significant financial reporting judgements contained in them
- Maintaining an appropriate relationship with the Association's auditors
- Reviewing external auditor's management letters and ensuring that corrective actions are taken by the Secretariat to address the weaknesses identified
- Making recommendations to the GA on the appointment, reappointment and removal of external auditors
- Approving the selection of auditees for site visits and reviewing site visit reports
- Reviewing the effectiveness of the external audit process
- Reviewing the association's internal financial controls and risk management systems, including preventing frauds, responding to frauds and whistle blowing procedures
- Approving the Association's statements for internal control and risk management.

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

- The DFA or GFO writes to any site 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 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 and POs not only ensure the implementation of the EDCTP action points, but seek response from grantees to the recommendations made in the site visit report.

7.7 Operational controls

- Operational capacity is assessed by project officers during the evaluation procedures to provide assurance that the beneficiaries have the necessary capacity to conduct the project. This includes the skills and qualifications of the lead persons at the beneficiary organisations.
- During the grant preparation period, the Description of Action is finalised. Attention is paid to the deliverables and milestones that will track the progress of the project, as well as to the risk-mitigation measures in place.
- Review of periodic reports (technical) is used to monitor:
    - Progress against the agreed milestones and deliverables
    - Assess whether any corrective measures are needed
    - Alignment of the project activities with the reported expenditure profile
    - Compliance of the project with national and international standards and laws (ethical and regulatory approvals, ICH-GCP, data protection).

EDCTP

European & Developing Countries
Clinical Trials Partnership

Declaration of Adherence to EDCTP Risk Management Policy

I _____, declare that:

1. I have received a copy of the EDCTP Risk Management Policy (#83254)
2. I have read the Policy and I understand my responsibilities as set out in the Policy.

_____ _____

Signature **Date**

EDCTP

European & Developing Countries Clinical Trials Partnership

Risk Management Policy Deviation Form

This form should be completed in the event of a deviation from the Risk Management Policy.

Name: Job title:
Current procedure in the Risk Management Policy (what should have been done).
What is the deviation (what is done differently)?
Rationale for the change (please explain why there is a deviation).
Date of the deviation
Approved by ED or DFA Signature (ED or DFA): Date:

Risk Reporting Form

This form should be completed in the event a major risk is identified by an EDCTP member of staff.

Risk identified by: Name: Job title:
What is the risk (please explain why you consider it a risk that should be reported)?
What is the potential impact on EDCTP?
Please indicate your recommended course of action.
Date: Signature: