UNESCO - Risk Management Policy (final draft)

BSP – August 2016

Table of Contents

I. INTRODUCTION

1. The Director-General has determined Enterprise Risk Management as a priority to strengthen the overall governance and accountability in UNESCO. It is crucial to connect all risk areas and treat them strategically to achieve better results. A proactive and strategic approach, taking into account the broad spectrum of risks, will help to be more present within the UN system, to further focus our efforts and resources on areas where the Organization has a comparative advantage, where it can achieve a real impact and have a lead role, while streamlining our administration to facilitate our work.
2. An enterprise risk management framework is being progressively implemented to embed risk management into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture.
3. This document presents UNESCO's risk management policy and sets forth UNESCO's overall intentions and direction related to risk management and provides a framework to ensure that risk management processes (i) are consistently applied across the Organization and (ii) provide reasonable assurance regarding the achievement of the Organization's objectives.
4. This policy elaborates the rationale for risk management, the responsibilities and accountabilities for managing risks as well as the way in which risk management will be monitored and reported as an integral part of the governance structure.
5. This policy together with the Risk Management Committee (RMC)'s Terms of Reference (Annex I), UNESCO's Risk Management Training Handbook and the risk information provided on the BSP website and Unesteams form UNESCO's Risk Management Framework.
6. UNESCO's Risk Appetite statement is annexed to this policy (see Annex II).

II. DEFINITIONS

7. The following commonly used risk terms are defined below to promote a consistent understanding:

Risk	A potential event that, if it materializes, may have a positive or negative impact on the achievement of UNESCO's objectives. Risk is as much a potential threat as a missed opportunity. A risk can have consequences beyond failure to deliver on results. It may negatively impact on reputation, integrity, credibility and trust from donors and stakeholders. A risk has a cause and effect.
Risk Owner	A risk owner is a person or entity that has been given the authority to manage a particular risk and is accountable for doing so.
Risk Focal Point	The risk focal point in each Sector/Service/Field Office/Division/Category 1 Institute, generally the principal officer of the unit, is the contact point for a risk owner in case the treatment of the risks exceeds his/her mandate. He/she is responsible for raising risks to the RMC in accordance with the risk escalation process.
Risk Register	A risk register is used as a risk management tool and acts as a repository for all risks identified and includes additional information about each risk e.g., nature of the risk, reference and owner, mitigation measures. The register should be revised regularly to assess residual risks and update mitigation measures (see Annex IV for risk register template).

Risk Category	The risks faced by an organization should be categorized according to the organization's needs.
Impact	In risk management terms, the effect of a risk relative to the achievement of the objective.
Likelihood	The possibility that a risk will occur.
Risk Significance	The overall importance of a risk considering both the impact of the event and the likelihood of its occurrence. Risks can be ranked according to their significance. Risk Significance is also referred to as Risk Level. (see Annex III for UNESCO's Risk Assessment Scale).
Risk Tolerance	Risk tolerance is the amount of risk an organization can withstand. The line of tolerability depends on impact and likelihood. It separates the low and medium risks an organization is willing to take from the medium and high risks it is not willing to take. Tolerance levels may be set out in relevant policies and procedures; if not, the head of unit makes the judgment.
Inherent Risk	The risk without considering the application of any mitigating measures or any controls.
Control	An activity or measure that may be part of the risk response. A control may reduce the likelihood of the risk occurring or its impact, or both. Good controls provide assurance over the achievement of objectives.
Residual Risk	The risk after the application of mitigating measures or controls.
Risk Response	Decisions made and actions taken to bring the residual risk within the accepted risk tolerance. The organization can make the decision to accept, control, avoid, or transfer/share the risk.
Risk Appetite	The degree of risk, on a broad-based level, that UNESCO is willing to accept in pursuit of its mission and objectives. For different types of risk, UNESCO may have different levels of tolerance.
Risk Matrix	A graphical representation of key risks or risk categories in relation to each other, reflecting their individual significance in relation to objectives and defined risk tolerance levels. A Risk Matrix can be visualized through a heat map depicting the likelihood and impact of each major risk. It helps determine and prioritize risk responses.
Risk Profile	An organization-wide inventory of risk categories, from internal and external sources, assessed in terms of significance in relation to objectives and defined risk tolerance levels.

III. UNESCO'S OBJECTIVE FOR MANAGING RISKS

8. Risk management is a broad strategic approach to provide better control over the future and ultimately improve UNESCO's chances to reach programme performance within budget and specified timeline. The Organization can be successful only if risks are anticipated, carefully measured and adequately managed against set objectives.

9. The core objective of enterprise risk management is to assess the uncertainty of the future in order to make the best possible decision today. It enables staff at all levels across the Organization to:

   a. Be aware of the need to identify and treat risks
   b. Anticipate and treat potential risk events that may affect the achievement of objectives
   c. Facilitate risk-informed decisions
   d. Maintain forward looking rather than reactive management
   e. Reassure UNESCO's stakeholders and partners about the Organization's capacity to meet its objectives, manage key risks and achieve its objectives.

IV. PRINCIPLES OF RISK MANAGEMENT AT UNESCO

10. The following principles underpin UNESCO's risk management:

    a. The effectiveness of Enterprise Risk Management is dependent on adequate resources. Senior Management is committed to make the necessary resources available to assist those accountable and responsible for managing risk.
    b. Risk management should not only be procedural, but should also initiate change and seek to increase performance. It should enable moving from ex-post crisis management to anticipating risks and opportunities.
    c. Visible ownership by management is a critical factor. It is therefore important to inform and get buy-in from the senior management.
    d. Risk management should be embedded in the programme management cycle. The risk framework should be relevant i.e., linked to objectives and developed in the context of the accountability framework. The overall risk framework should seek to make responsible officers risk aware and more accountable when taking decisions.
    e. The approach should be flexible and simple, focusing on the risks that can be managed.
    f. The corporate risk register lists risk information from all sources (including legal and security) that have been escalated by risk focal points.
    g. Risk responses should be actionable with clear ownership and agreed time-bound mitigation plans. Mitigation plans requiring a substantial investment of resources should be subject to project management principles such as budgets, milestones and performance metrics.
    h. Communication to Member States and donors needs to take place regularly, once a risk management process along with mitigation plans and a monitoring mechanism is in place.

V. RESPONSIBILITIES IN UNESCO'S RISK MANAGEMENT FRAMEWORK

Risk management is everyone's business. The primary responsibility for identifying risks and managing them lies with management at all levels.

i. Each Responsible Officer, at the project design stage and during the course of implementation, should assess potential risks and formalize them. Risks identified in project documents of extrabudgetary projects will serve as a basis for risk discussion with Donors.

ii. Each ADG/Director/Head/Chief of a Sector/Bureau/Field Office/Institute/Division/Unit is responsible for managing risks which pose the greatest challenge to the achievement of the objectives under her/his purview and of its continuing functions.

iii. The Risk Management Committee reports to the Senior Management Team and shall contribute to raising awareness of risk management generally across the Organization and to maintaining the profile of risk management. It is in charge of organization-wide risk management policy, of continuous risk identification and assessment, including of the risks escalated by Sector/Bureau/Field Office, of defining the risk appetite, of addressing risks and incidents and of reporting and communicating on risks. The Risk Management Committee reports to the Senior Management Team.

iv. The Senior Management Team should endorse the risk management policy, identify new emerging corporate risks and address the major risks brought to its attention, including by proposing or supporting the implementation of the mitigation plans proposed by the risk management committee. The Senior Management Team should include risk management in its agenda as and when required.

v. The Director-General approves the outcomes of the work of the Risk Management Committee and takes decision and arbitrates points of attention formalized by the Risk Management Committee and the Senior Management Team. The Director-General is accountable to the Governing Bodies for the development and achievement of UNESCO strategy and objectives, including the overall management of risks to these objectives.

vi. The Governing Bodies, notably the Executive Board in its oversight role, plays a critical role in overseeing an enterprise-wide approach to risk management. Because the Secretariat is accountable to the General Conference through the Executive Board, the Board's focus on effective risk oversight is critical to setting the tone and culture towards effective risk management through strategy setting, formulating high level objectives, and approving broad-based resource allocations.

vii. The Internal Oversight Services (IOS) provide assurance on the risk management framework and provides advisory services to support management's decision making. It specifically provides assurance that controls are well designed and applied to mitigate risks or take opportunities. In addition, IOS has a consulting role at making available to the management tools and techniques to analyze and control risks. Finally, IOS links internal audit work and the achievement of the Organization's objectives.

viii. The Oversight Advisory Committee (OAC), as an external group of audit and evaluation experts, considers the functioning, accomplishments and matters for follow-up of the Risk Management Committee as well as the status of key risks. The Committee also considers the integration of Risk Management principles into the Organization's processes. The role of the OAC is to advise the Director-General on the effectiveness of risk management.

VI. PROCESS

11. Risks should be identified at least at the programming and monitoring phases of the management cycle. They should therefore be an integral part of the preparation of the Draft C/5 and of the

monitoring information provided for the Programme Implementation Report (PIR) in the EX/4. Moreover, Responsible Officers are to factor risks when planning extrabudgetary projects.

12. UNESCO's risk management process is based on the COSO model of enterprise risk management. More details on the methodology to identify, assess, treat and report on risks is available in UNESCO's risk management training handbook.

13. As a general principle, risks should as far as possible be handled and treated by the Risk Owner. In some cases, circumstances pertaining to the treatment itself may exceed the mandate of the Risk Owner or also involve actions by other managers not under the authority of the Risk Owner. Often these risks are common to multiple operational units and are best addressed through a corporate solution. Therefore, major risks that cannot be effectively treated by the Risk Owner must be escalated to a level with sufficient authority to deal with the risk and take appropriate decisions.

14. The escalation of risks from an operational level for consideration and treatment at the corporate level is detailed below:

    a. A risk focal point is designated for each Sector / Service / Field Office /Category 1 Institute. The risk focal point is normally the principal officer of the Sector / Service / Field Office / Institute. [*Programme ADGs may designate a senior-level official as the Sector's risk focal point.*] The focal point is the contact person for a Risk Owner in case the treatment of the risks he/she faces exceeds his/her authority.

    b. The risk focal point for Headquarters Sectors and Services is responsible for recording these risks in the unit's risk register and transmitting the risk register at least annually, or upon request, to the Risk Management Committee highlighting any significant unmitigated risks (see Annex IV - Risk Register template). The risk focal point will also monitor the progress in the implementation of the mitigation plans of the Sector / Service.

    c. The risk focal point for each Field Office [*and Liaison Office*] is responsible for recording these risks in the Office's risk register and transmitting the risk register at least annually, or upon request, to the Division of Field Support and Coordination (ODG/FSC) highlighting any significant unmitigated risks (see Annex IV - Risk Register template). ODG/FSC will consider these and raise significant unmitigated risks common to the field network, and significant unmitigated risks associated with individual Field Offices, to the Risk Management Committee. The risk focal point will also monitor and ensure that mitigation plans of the Office are implemented.

    d. The risk focal point for each Category 1 Institute is responsible for recording these risks in the Institute's risk register and transmitting the risk register at least annually, or upon request, to the cognizant Programme Sector ADG or, in the case of UIS, to the Risk Management Committee, highlighting any significant unmitigated risks (see Annex IV - Risk Register template). The Programme Sector will consider these and raise significant risks that cannot be mitigated at the Sector level to the Risk Management Committee. The Institute's risk focal point will also monitor and ensure that mitigation plans of the Institute are implemented.

    e. UNESCO management committees will identify and escalate unmitigated risks under their purview to the RMC.

    f. The Risk Management Committee shall consider the unmitigated risks escalated to the Committee, advise on Risk Ownership and the formulation of mitigation plans and ensure that these are recorded in the corporate risk register or in the risk register of the Sector / Service / Field Office or Category 1 Institute that is to manage the mitigation plan.

VII. MONITORING OF RISKS

15. The progress made in mitigating the risks listed in the risk register will be monitored regularly in order to determine the residual risk, need further action(s) or acceptance.

    a. The RMC will conduct an annual review of corporate risks and identify new threats/opportunities in light of the current context, latest trends, and findings from oversight bodies such as the Internal Oversight Service, External Auditor and Joint Inspection Unit. The results of this review will be submitted to the Senior Management Team for discussion and approval.

    b. The Risk Management Committee will, twice a year and as necessary, provide a report to the Senior Management Team. The report shall inform the progress: (i) in implementing the risk management framework, (ii) on the corporate risks treated and (iii) seek the decision or the approval of the Senior Management Team when required (e.g., to accept a specific risk, approve a proposed mitigation measure or request funding to implement a mitigating measure).

VIII. RISK DOCUMENTATION

16. Risk documentation is available to all staff with information on risk management (including policy, templates, training handbook, presentations, RMC minutes, corporate risk register, Executive Board documents). The information is available on unesteams.

IX. POLICY REVIEW

The Risk Management Committee will organize an evaluation of this policy and its implementation within three years of the effective date. Review and update of this policy and the related Risk Management Framework elements will consider the evolving needs of UNESCO and the environment in which it operates as well as the direction of risk management programmes of other UN agencies, leading practice developments, and updates to applicable standards such as COSO *or ISO*.

ANNEX I: TERMS OF REFERENCE OF THE RISK MANAGEMENT COMMITTEE

I. Purpose of the Risk Management Committee

1. The purpose of the Risk Management Committee (RMC) is to:
   a. Support the Senior Management Team (SMT) on the implementation and monitoring of the risk management policy. The scope of risk management covers strategic risks, operational (or programmes/projects) risks, financial and control, compliance risks as well as reputational and external risks.
   b. Contribute to raising awareness of risk management generally across the Organization and to maintaining the profile of risk management.

II. Composition and structure

2. The members of the RMC are:
   a. [Deputy Director-General] (Responsible Officer and Convener)
   b. Director, Bureau of Strategic Planning
   c. Chief Financial Officer
   d. Senior-level staff from each of the Programme Sectors and ODG, FSC, ERI, HRM, KMI, MSS, LA and GE.
   e. Field Offices will be represented by ODG/FSC.
3. Other participants may be invited to meetings of the RMC as required, in particular Field Office Directors and Directors of Category 1 Institutes when deemed necessary by the Chair of the RMC on the basis of the Agenda to be discussed
4. The Internal Oversight Service will participate as an observer.

III. Frequency of meetings

5. The Committee will meet as required to fulfil its remit and will meet no less than once every two months and engage in submitting periodic reporting to the SMT.
6. Minutes, agendas and papers will normally be circulated to members of the Committee at least five days in advance of the meeting. Late papers may be circulated up to two days before the meeting. Only in the case of extreme urgency and with the agreement of the Convener will papers be tabled at meetings of the Committee.
7. Formal minutes will be kept of proceedings and submitted for approval at the next meeting of the Committee. The draft minutes will be agreed with the Convener of the Committee.
8. The Committee may also function between meetings through correspondence and any decision/s taken formally ratified at the next meeting of the Committee.

IV. Standing agenda

9. The Committee meetings will be conducted in accordance to the following agenda:
   a. Review of SMT decisions relevant to risk management
   b. Review of new and emerging risks for potential inclusion in the corporate risk register
   c. Review and update the corporate risk register (including monitoring of risk treatment)
   d. Review the overall effectiveness of ERM at UNESCO.

V. Functioning/Responsibilities

10. The Committee will undertake the following functions/responsibilities in line with the Risk Management Policy:

a. Ensuring that the identification and evaluation of key risks that threaten achievement of the mandate is carried out, and that a register of these risks is maintained;
b. Identifying the strategy in place to manage risks, including identification of appropriate risk owners, and monitoring the satisfactory operation of the management strategy;
c. Being satisfied that other risks are being actively managed, within the appropriate thresholds and kept to an acceptable level;
d. Embedding the risk assessment approach into future planning, management, and reporting;
e. Advising SMT on the UNESCO's overall risk appetite, tolerance and strategy, taking account of the current and prospective internal and external factors;
f. Establishing risk assessment criteria;
g. Reviewing regularly and approving the parameters used in risk assessment measures and the methodology adopted;
h. Receiving and reviewing reports on any material breaches of risk limits and the adequacy of proposed action;
i. Addressing such other matters related to risk management as may arise from time to time.

VI. Authority

11. The Committee is authorized to:

a. Raise to the Director-General matters of risk ownership and mitigation not resolved to the satisfaction of the Chair;
b. Advise on ownership of corporate risks and on the adequacy of mitigation plans for corporate risks;
c. Seek information it requires from staff in order to perform its duties;
d. Obtain professional advice on matter within its terms of reference where required;
e. Request the attendance of staff at a meeting of the Committee as and when required.

VII. Reporting responsibilities

12. The Committee will report to the SMT twice a year (i) on unmitigated critical risks and (ii) on the effectiveness of risk mitigation plans.

13. The Committee will also submit an annual biennial report to the Director-General, for transmittal to the Executive Board, on the key risks facing the Organization.

VIII. Review of performance

14. The Committee will from time to time undertake a review of its own performance and effectiveness and report thereon to the SMT.

IX. Secretariat:

15. The RMC Secretariat will be provided by the [Office of the Director-General] and will perform the following tasks:

a. Preparation of agenda and background material
b. Recording and presentation of escalated risks
c. Ensuring proper documentation of the Committee's decisions
d. Facilitating the work of the Committee with regard to supporting information and communication, tools and training.

ANNEX II: RISK APPETITE STATEMENT

A risk appetite is defined as the amount of risk that is judged to be tolerable and justifiable for an organization. In UNESCO, criteria may differ in different spheres of the organization, e.g. low appetite for risk in security, higher in programme areas where innovation is key.

Risk appetite provides the basis for setting acceptable levels of risk tolerance and thresholds and contributes to the identification and implementation of mitigation actions.

Risks are expressed as residual risk, i.e. the risk after mitigation measures and/or controls have been implemented. In that light, the Organization's risk appetite in broad terms is defined below:

(i) Risks with a small impact are accepted where the likelihood of the risk event is assessed as moderate, low or minimal;

(ii) Risks with a noticeable impact are accepted where the likelihood of the risk event is assessed as low or minimal; and

(iii) Risks with a critical impact are accepted only where the likelihood of the risk event is minimal.

When a risk exceeds the agreed risk appetite – i.e. when the line of tolerability is crossed – for one level of management, the escalation point is reached. The risk can then be transferred to the next higher level of management, for which it constitutes a lower level risk. The higher level of management may act on the risk directly or adjust the risk appetite and let the lower level manage the risk.

The assessment of the risks in excess of this risk appetite is coordinated by the Risk Management Committee. Risks will only be accepted after ensuring that the mitigation measures in place are suitable and appropriate.

Risk appetite is no constant value, it is informed by changing variables such as reported results of control-mechanisms that have succeeded or failed in the past, the changing value of assets potentially to be lost, perception of stakeholders, extent of possible control etc. It has to be readapted by management corresponding to reporting from the operational level and to changes in the external environment.

ANNEX III: RISK ASSESSMENT SCALE

Likelihood:

- F Frequent: likely to occur very often or continuously
- O Occasional: likely to occur several times
- S Seldom: is possible and would probably occur once at the most.

Impact:

- C Critical: infers serious consequences that can jeopardize the achievement of result
- M Marginal: infers minor consequences that can slow the achievement of result
- N Negligible: infers a minimal effect on the achievement of result.

Risk importance:

The risk importance is rated as a combination of likelihood and impact and results into High, Medium or Low risk vis-à-vis the achievements of objectives.

	Likelihood		
	Frequent	Occasional	Seldom
Impact			
Critical	H	H	M
Marginal	H	M	L
Negligible	M	L	L

ANNEX IV: RISK REGISTER TEMPLATE

1. A risk register aims at formalizing the risks faced which can be mitigated to some degree by taking the time to develop a risk management approach to help cope with threats and maximize opportunities. The challenge is to fully identify risks and seek to manage their impact rather than ignoring them. It should include description, ownership (a single Risk Owner) and analysis of cause and consequence of all risks along with their impact and probability. It should further include a pragmatic action plan to mitigate a particular risk or to seize an opportunity. It should lend itself to be easily maintained and updated. By remaining current and up to date, the risk register can be a valuable tool for communications and may serve as a relevant and useful management tool. The Risk register should be reviewed and updated annually.
2. If a risk cannot be effectively treated at operational level managing the respective risk register, this should be indicated and communicated in accordance with the Risk Management Policy. Risk registers should be sent to the Secretariat of the Risk Management Committee.

Risk nb	Risk Category	Risk owner	Risk description	Likelihood	Impact	Importance	Mitigation measure(s)	Risk owner	Residual risk	Likelihood	Impact	To be escalated
1												
2												
3												
4												
5												