ATPS RISK ASSESSMENT
FRAMEWORK
2023

ATPS RISK ASSESSMENT FRAMEWORK 2023

AFRICAN TECHNOLOGY POLICY
STUDIES NETWORK (ATPS)

8th Floor, Chancery Building, Valley Road
P. O. Box 10081-00100, Nairobi, Kenya
Email: executivedirector@atpsnet.org   Phone No: +254-202714092

Date:
3rd March 2023

RISK MANAGEMENT FRAMEWORK 2023
For the African Technology Policy Studies Network (ATPS)

1. Introduction

The purpose of this Risk Management Framework is to establish a structured and consistent approach for identifying, assessing, managing, monitoring, and reporting risks across the operations of the African Technology Policy Studies Network (ATPS). Effective risk management supports the ATPS's mission, enhances accountability, protects assets, strengthens internal controls, and ensures compliance with donor and regulatory requirements.
The framework is aligned with ISO 31000:2018 Risk Management Guidelines.

2. Definition

2.1 Risk

Risk is defined as the impact of uncertainty on objectives. Risk may be positive or negative and may arise from events that create opportunities or pose threats to achieving objectives. Risk is normally expressed in terms of risk drivers, potential events, their consequences and their likelihood.

2.2 Risk Management

Risk Management is the systematic process of identifying, assessing, and mitigating threats or uncertainties that can affect an organisation. It involves making informed decisions about which risks to avoid, reduce, transfer, or accept, while ensuring that residual risk remains within acceptable limits.

2.3 Monitoring

Monitoring means continuous checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected. It applies to the framework, processes, and controls.

2.4 Level of risk

The level of risk means the magnitude of a risk or combination of risks expressed in terms of the combination of consequences and their likelihood.

2.5 Risk acceptance

Risk acceptance means an informed decision to take a particular risk. Accepted risks are subject to monitoring and review.

2.6 Risk appetite

Risk appetite means the amount of risk, on a broad level, the organisation is willing to accept in pursuit of value.
The ATPS shall define its risk appetite annually and review it during strategic planning.

2.7 Risk matrix

The risk matrix is a tool for ranking and displaying risks by defining ranges for consequence and likelihood.

3. Objectives of the Framework

The framework aims to:

- Promote awareness of organisational and business risk and embed a risk-conscious culture across the organisation.
- Identify, assess, control and report on any business risk that may undermine the delivery of ATPS's strategic and operational priorities.
  Strengthen compliance with donor, regulatory, and governance requirements

4. Scope

This framework applies to all programs, departments, staff, volunteers, and project locations. It covers the following main categories of risk:

1. Financial Risks
   - Unpredictable funding due to overreliance on a single or few donors
   - Fraud and poor financial management
2. Operational Risks
   - Inability to achieve objectives due to human error, capacity deficits, or unexpected fiscal outcomes
3. Compliance Risks
   - Non-compliance with donor regulations
   - Non-compliance with the set regulations, laws and procedures.

5. Governance Structure

5.1 Board of Directors / Governing Body

- Approves the Risk Management Framework.
- Reviews high-level organisational risks and mitigation plans.
- Oversees effectiveness of risk governance.

5.2 Executive Director / Senior Management

- Ensures each department identifies, reports, and manages risks.
- Allocates resources for managing key risks.
- Establishes a risk management function within the organisation
- Approves of risk catalogue and assessment methods
- Inculcates a risk awareness culture

5.3 Internal Audit/ Risk Management Function

- Provides independent assurance on the effectiveness of risk management processes.
- Evaluates whether risks are properly identified, managed, and monitored.
- Reports to the Board and Executive Director on the control environment.

5.4 Departmental Heads

- Own risks within their departments.
- Implement mitigation actions.
- Submit periodic risk updates.

5.5 Staff and Volunteers

- Identify risks in daily activities.
- Follow mitigation measures and report incidents promptly.
- Comply with policies and procedures

6. Risk Management Process

The organisation shall put in place preventive controls and other measures that ensure the risks do not adversely affect the achievement of its strategic objectives and reduce the impact if they do occur. These events may be political, economic, social, technological, environmental and legal.

The cycle of risk management procedures shall provide a framework for managing ad hoc risks as they arise. Sufficient documentation shall be done at all levels of the Risk Management Process, including explanations and evaluations that allow competent third parties to understand the nature of the risk.

Risk Management is embedded within the organisation as a key part of strategic planning, operational planning, and operations. It is a systematic process for evaluating and addressing risks to make informed decisions. The process of assessing and mitigating risk is the responsibility of all staff. This process contains five (5) key stages as follows:
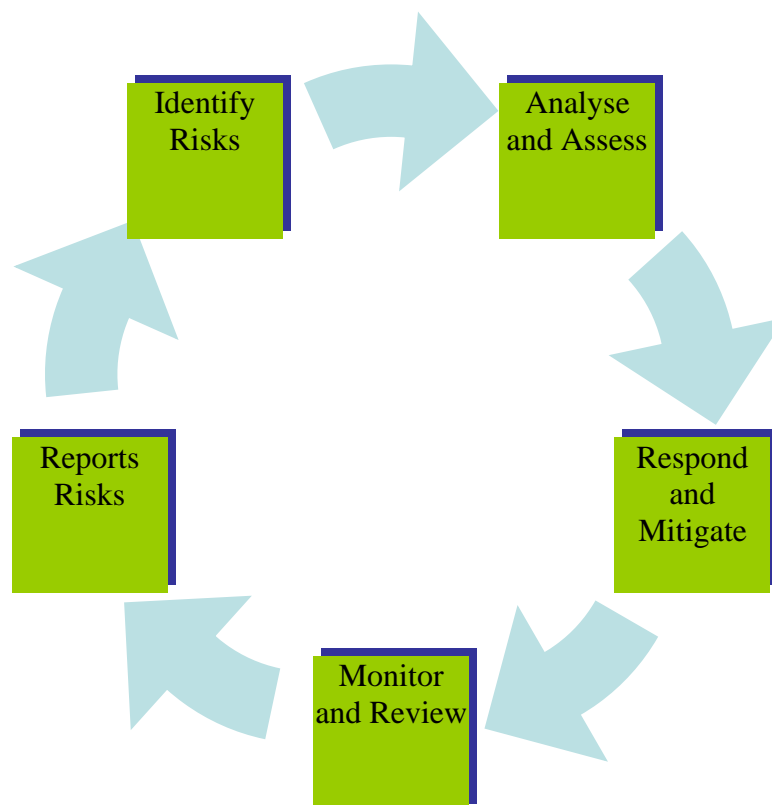
Figure 1: The Risk Management Process

6.1 Step 1: Risk Identification

Risk identification is a continuous and ongoing activity, with individual risks and the impact and/or likelihood of risks materialising changing regularly. Risk identification is the process of determining what risks might prevent the organisation from delivering its objectives, whether these are strategic or operational.

Risks can be triggered/identified from a number of sources, including:

- Changes to the operating environment. This can be through a change in donor rules and preferences.
- Planning, whether strategic, business or operational level.
- Through the audit committee or internal audit function.
- Executive team/management/group strategic sessions
- Monitoring of audit risks.
- Performance monitoring.
- Risks identified through external audit.
- Executive team risk workshops.

As part of the organisational culture, risk features as a standing agenda/point of discussion on the executive team meetings and working groups.

Many risk prompts and tools exist, and risks are most likely to be identified where different tools are adopted based on the circumstances. Such tools include:

- Environmental scanning approaches such as:
  - **PESTLE** – Political, Economic, Social, Technological, Legal and Environmental
  - **SWOT** – Strengths, Weaknesses, Opportunities and Threats
- Process-based approach that incorporates:
  - Input risks, including assets and employees
  - Process risks, including management processes
  - Output risks, including timeliness and quality
  - Outcome risks, including impact and reputation

Furthermore, risks are classified into specific categories, including financial, operational, compliance, strategic, reputational, and program delivery risks.

6.2 Step 2: Risk Assessment

Risk assessment allows the organisation to consider risk sources through root cause analysis and the extent to which potential events will have an impact on the achievement of objectives. The organisation shall assess risks both quantitatively and qualitatively, then measure the risk in terms of impact and likelihood.

Each identified risk is assessed based on:

      a. Likelihood (Low / Medium / High)

      b. Impact (Low / Medium / High)

This produces a **risk rating** (e.g., High, Medium, Low) using a risk matrix as shown below:

Table 1: The Risk Matrix

Impact ↓ / Likelihood →	Low	Medium	High	Very High	Critical
Low Impact	Low	Low	Medium	Medium	High
Medium Impact	Low	Medium	Medium	High	High
High Impact	Medium	Medium	High	High	Critical

For every risk identified, the organisation shall assign a probability score on its likelihood of occurrence. The likelihood shall range from 1 to 5 and shall be based on the table below:

Table 2: Risk Likelihood

Score	Description	Scoring Criteria
1	Rare	History of no occurrence of the event. • The event may never occur
2	Unlikely	History of no or seldom occurrence of the event. • The event may occur only in exceptional circumstances.
3	Possible	History of occasional occurrence of the event. • The event could occur at some time.
4	Likely	History of regular occurrence of the event. • The event is expected to occur in most circumstances.
5	Most Certain	History of normal occurrence of the event. • The event shall occur.

6.3 Step 3: Risk Response / Mitigation

If the risk assessment indicates that the residual risk is outside the organisation's risk appetite, the organisation shall undertake additional controls or 5T mitigation measures as follows:

Table 3: Risk Response/Mitigation

Terminate	Terminate the risk by doing things differently and thus removing the risk where it is feasible to do so. Countermeasures are put in place that either stop the threat or problem from occurring or prevent it from having any

	impact on the ATPS
Treat	Treat the risk - take action to control the risk by reducing the likelihood of the risk developing or limiting the impact on the objective to acceptable levels.
Transfer	Pass the management of the risk to a third party via, for instance, an insurance policy or a penalty clause, such that the impact of the risk would no longer be an issue.
Tolerate	Tolerate the risk – either because nothing can be done at a reasonable cost to mitigate it, or the likelihood and impact of the risk occurring are at an acceptable level.
Take More	If the identified event constitutes an opportunity for the organisation, it may be desirable to take more risk, with the appropriate controls in place.

6.4 Step 4: Monitoring and Review

Because the environment in which the ATPS operates in, which changes regularly, and as such its risks, it is critical to monitor and review risks regularly. This is done through:

- A risk register that is monitored and reviewed regularly to ensure it remain relevant.
- Risk agenda during strategic meetings
- Follow up of External audit recommendations
- Monitoring through the internal audit function

6.5 Step 5: Reporting

It is important to ensure that knowledge about risks is communicated and shared across the organisation. Risk reporting shall comprise of the following:

a) Risk Register

   The Internal Audit department shall maintain an up-to-date register of all the risks identified and details of how they have been disposed of. This register shall be available for inspection at all times by the Executive Director and the Board of Directors.

b) Risk Action Plans

   The management shall put in place an effective action plan when either the existing controls are ineffective or require improvement, or in the unlikely event that no controls exit at all. Risk action plans shall comprise one or more actions that remedy identified risks or control weakness when recording the risk treatment in the risk registers, the descriptions shall detail who is doing what and what is it they are doing.

c) Risk Escalation Reports

   Risks deemed to be critical, high and significantly out of appetite and described as being out of risk tolerance report should be presented to the Executive Director/Board on a quarterly basis.

7. Risk Management Strategic Approach

The risk management strategic approaches of the organisation shall be designed to effectively address the risks associated with its mandate. These strategic approaches encompass a set of principles, objectives and actions that guide the organisation to identify, assess, and manage risks in its vision. They include:

> ➤ Data-Driven Risk Assessment - generate evidence-based and data-driven risk assessments to influence decision-making and policy direction
> ➤ Collaboration and Partnerships - form partnerships with local and international organisations, governments, NGOs, and community leaders to pool resources, share expertise, and coordinate efforts to effectively address financial constraints.
> ➤ Technology & innovation - leverage on the power of data analytics, artificial intelligence and automation to improve the quality, speed and efficiency of risk identification, assessment and response
> ➤ Climate change - develop an effective climate governance structure to ensure that the organisation properly assesses climate-related risks and opportunities arising from various lines of operations and takes appropriate strategic decisions on how to manage those risks and opportunities

8. Contravention of the Policy

Failure to comply with the obligations under this policy shall lead to disciplinary action taken by the organisation in accordance with the Human Resource Policy and Procedure Manual.

9. Review of the Framework

This Risk Management Framework shall be reviewed annually by senior management and approved by the Board. Updates shall be made to reflect changing risks, new donor requirements, or organisational growth.

Approval

Table 4: Version Control

Version	Date	Prepared By	Reviewed By	Approved By
1.0	Date Prepared	ATPS Secretariat	Executive Director	Board of Directors

African Technology Policy Studies Network (ATPS)

Contact Executive Director:
executivedirector@atpsnet.org
8th Floor Chancery Building, Valley Road

P. O. Box 10081-00100, Nairobi
Tel: +254 (020) 2714092
www.atpsnet.org

The African Technology Policy Studies Network (ATPS) is a transdisciplinary network of researchers, policymakers, private sector actors and the civil society promoting the generation, dissemination, use and mastery of Science, Technology and Innovations (STI) for African development, environmental sustainability and global inclusion. In collaboration with like-minded institutions, ATPS provides platforms for regionaland international researchand knowledge sharingin order to build Africa's capabilities in STI policy research, policymaking and implementation for sustainable development.