# RNGOF on HIV/AIDS & HP:
# RISK MANAGEMENT POLICY

## 2016

**Rwanda NGOs Forum on HIV/AIDS and Health Promotion (RNGOF on HIV/AIDS & HP) Risk Management Policy**

## 1. Purpose of this document

This risk management policy (the policy) forms part of the **Rwanda NGOs Forum on HIV/AIDS and Health Promotion (RNGOF on HIV/AIDS & HP)** internal control and corporate governance arrangements.

The policy explains the Umbrella's underlying approach to risk management, documents the roles and responsibilities of the Board of Trustees, the Audit Committee, the Executive Board, and other key parties. It also outlines key aspects of the risk management process, and identifies the main reporting procedures.

In addition, it describes the process the Board of Trustees will use to evaluate the effectiveness of the Umbrella's internal control procedures.

## 2. Underlying approach to Risk Management

The following key principles outline the Umbrella's approach to risk management and internal control:

- The Board of Trustees has responsibility for overseeing risk management within the institution as a whole
- An open and receptive approach to solving risk problems is adopted by the Board of Trustees
- The Executive Secretary and the members of Executive Board support, advise and implement policies approved by the Board of Trustees or those committees with delegated powers.
- The Umbrella makes conservative and prudent recognition and disclosure of the financial and non-financial implications of risks. Each paper to the Board of Trustees or Executive Board is required to include a section on any key risks in relation to the proposal
- Risk register owners are responsible for encouraging good risk management practice within their areas of responsibility.
- Key risk indicators will be identified and closely monitored on a termly basis by the Executive Board and the Audit Committee

## 3. Role of the Board of Trustees

The Board of Trustees has a fundamental role to play in the management of risk. Its role is to:

a. Set the tone and influence the culture of risk management within the Umbrella. This includes:

   - Determining whether the Umbrella is 'risk taking' or 'risk averse' as a whole or on any relevant individual issue;
   - Determining what types of risk are acceptable and which are not;
   - Setting the standards and expectations of staff with respect to conduct and probity

b. Determine the appropriate risk appetite or level of exposure for the Umbrella;

c. Approve major decisions affecting the Umbrella's risk profile or exposure;

d. Monitor the management of significant risks to reduce the likelihood of unwelcome surprises

e. Satisfy itself that the less significant risks are being actively managed, with the appropriate controls in place and working effectively;

f. Annually review the Umbrella's approach to risk management and approve changes or improvements to key elements of its processes and procedures;

g. Delegate the Audit Committee to review the Umbrella's risk register each term

## 4. Role of the Audit Committee

The key roles of the Audit Committee, acting on behalf of the Board of Trustees, are to:

   - Review and evaluate the key risks identified by the Executive Board.
   - Review the Umbrella's Risk Register on a termly basis.
   - Report annually to the Board of Trustees on the Umbrella's systems of internal control and Risk Register.
   - Monitor the work of internal and external audit in respect of risk.

## 5. Role of the Executive Board

Key roles of the Executive Board are to:

   - Develop and implement policies on risk management and internal control
   - Review the Umbrella's Risk Register on a monthly basis
   - Identify and evaluate the significant risks faced by the Umbrella for consideration by the Audit Committee.
   - Provide adequate information in a timely manner to the Audit Committee on the status of risks and controls.
   - Undertake an annual review of effectiveness of the system of internal control and provide a report to the Audit Committee and from that committee to the Board of Trustees.

## 6. Risk Management as part of the system of internal control.

The system of internal control incorporates risk management. This system encompasses a number of elements that together facilitate an effective and efficient operation, enabling the Umbrella to respond to a variety of operational, financial, and commercial risks. These elements include:

### a) Policies and procedures

Attached to significant risks are a series of policies that underpin the internal control process. The policies are set by the Executive Board and implemented and communicated by senior management to staff. Written procedures support the policies where appropriate.

### b) Termly reporting

Comprehensive termly reporting is designed to monitor key risks and their controls. Decisions to rectify problems are made at regular meetings of the Executive Board and the Audit Committee.

### c) Business planning and budgeting

The project planning and budgeting process is used to set objectives, agree action plans, and allocate resources. Progress towards meeting project plan objectives is monitored regularly.

### d) High level risk framework (significant risks only)

This framework is compiled by the Executive Board and helps to facilitate the identification, assessment and ongoing monitoring of risks significant to the Umbrella. The document is formally appraised annually by the Board of Trustees but emerging risks are added as required, and improvement actions and risk indicators are monitored by the Executive Board on a monthly basis and reported to the Audit Committee each term.

### e) Risk frameworks

Risk register owners develop and use this framework to ensure that significant risks in their area of responsibility are identified, assessed and monitored. The document is formally appraised each term but emerging risks are added as required, and improvement actions and risk indicators are monitored regularly by business units.

### f) Audit Committee

The Audit Committee is required to report to the Board of Trustees on internal controls and alert them to any emerging issues. In addition, the committee oversees internal audit, external audit and management as required in its review of internal controls. The committee is therefore well-placed to provide advice to the Board of Trustees on the effectiveness of the internal control system, including the Umbrella's system for the management of risk. The Committee reviews the Umbrella's Risk Register each term.

### g) Internal audit programme

Internal audit is an important element of the internal control process. Apart from its normal programme of work, internal audit is responsible for aspects of the annual review of the effectiveness of the internal control system within the Umbrella.

### h) External audit

External audit provides feedback to the Audit Committee on the operation of the internal financial controls reviewed as part of the annual audit.

### i) Third party reports

From time to time, the use of external consultants will be necessary in areas such as health and safety, and human resources. The use of specialist third parties for consulting and reporting can increase the reliability of the internal control system. Occasionally the Umbrella will be subject to audit from third parties, such as HEFCE, RCUK or the QAA, and these may provide some review of the Umbrella's risk arrangements.

## 7. Annual Review of effectiveness.

The Board of Trustees is responsible for reviewing the effectiveness of internal control of the Umbrella, based on information provided by the Executive Board. Its approach is outlined below.

For each significant risk identified, the Board of Trustees will:

- Review the previous year and examine the Umbrella's track record on risk management and internal control
- Consider the internal and external risk profile of the coming year and consider if current internal control arrangements are likely to be effective.

In making its decision, the Board of Trustees will consider the following aspects.

a) **Control environment:**

- The Umbrella's objectives and its financial and non-financial targets;

- Organizational structure and caliber of the Executive Board;

- Culture, approach, and resources with respect to the management of risk

- Delegation of authority;

- Public reporting.

b) **On-going identification and evaluation of significant risks:**

- Timely identification and assessment of significant risks;

- Prioritization of risks and the allocation of resources to address areas of high exposure.

c) **Information and communication:**

- Quality and timeliness of information on significant risks;
- Time it takes for control breakdowns to be recognized or new risks to be identified.

d) **Monitoring and corrective action:**

- Ability of the Umbrella to learn from its problems;

- Commitment and speed with which corrective actions are implemented.

The Executive Board will prepare a report of its review of the effectiveness of the internal control system annually for consideration by the Board of Trustees.

# ANNEXES

## Annex 1 : Guidance for completion of Risk Registers

Risk Registers should be completed in line with the guidance provided below. Risk registers are produced in word format, and each risk has its own section in the risk register. Please make sure that the risk register is discussed with the appropriate group before it is submitted for consideration.

Please ensure that the correct month and year appears at the in the top right-hand corner of the register.

### 1. Top row of each section of the register

### Column 1: Risk Reference Number

Number each of the risks, starting with 1. Do not worry about tying this into the Institutional Risk Register, if this risk also appears on that document.

### Column 2: Risk Description

Briefly describe the risk.

### Column 3: Risk Owner

This part of the register is for the job title of the manager responsible for the risk. This needs to be a named individual at senior level within the Directorate or Faculty. While this individual may not be responsible for the whole area covered by the risk, they are responsible for coordinating the 'Action Owners'.

At the Institutional Risk Register level it has been agreed that this will be a member of Executive Board.

### 2. Second, third and fourth rows of each section of the register

The second and third lines provide the appropriate heading for each of the columns below them, and a brief description of the information that is required from you in the fourth row.

### Column 1: Risk Cause

What might cause the risk to occur?

This should be a list of factors which could trigger the risk you have described. Risk owners should consider risk drivers when updating the risk register. This approach involves identifying the risk drivers for a particular risk.

### Column 2: Risk Consequences

What are the possible consequences should the risk occur?

This should be a list of what you think would happen if the risk you have described actually occurred.

**Columns 3, 4 and 5: Gross Risk Assessment**

This set of columns sets out your assessment of the impact of the risk, and the likelihood of it happening, if the Faculty/Directorate/Umbrella did not take any action whatsoever to mitigate against the risk.

**Column 3. Impact:**

- Insignificant
- Minor
- Medium
- Major
- Critical

**1-2 is a minor impact.** This would result in minimal financial or other loss, delay, interruption or inconvenience. There would be little or no damage to the Directorate/Faculty/Umbrella's reputation. The impact could easily and quickly be put right.

**3-4 is a major impact.** This would have a major impact on costs, income and certain key Directorate/Faculty/Umbrella objectives. This would affect a significant part of the Directorate/Faculty/Umbrella.

**5 is a critical impact.** This would result in services been seriously affected and a major loss of income and/or reputation, or high increase in costs.

**Column 4. Likelihood:**

1. Very Low represents 0% to 20% likelihood. Is unlikely/rare.
2. Low represents 20% to 40% likelihood. It is possible.
3. Medium represents 40% to 60% likelihood. It is likely.
4. High represents 60% to 80% likelihood. It is probable or very probable.
5. Very High represents 80% to 100% likelihood. It is almost certain or certain.

**Column 5. Impact x Likelihood**

The figure in this column is obtained by multiplying the impact by the likelihood. Please look at the heat map at the end of this document to determine which colour should appear in this column. You will need to highlight column 5 of row 4 and select the appropriate colour. You can do this by clicking on the area of the register which you wish to colour. Then click on the 'home' tab and find the icon which relates to shading (it is on the bottom row slightly to the right of the center). Clicking

on the icon will reveal a set of colours. Please select one of the standard colours at the bottom of the drop-down menu (selecting the bright red, the darker yellow or the darker green colour).

**Column 6: Existing Controls**

What existing strategies, processes or controls are in place to manage the risk?

What are you currently doing to manage the risk? Please make sure that your description is detailed enough to show how the control operates and how it is monitored. All of the existing controls should be included in this one cell.

**Column 7: Sources of Assurance**

How do we know that these controls are efficient and effective? What are our sources of assurance over the controls for this risk?

There isn't much point in taking action if we have no idea whether that action is working. How do you monitor the effectiveness of the action that is being taken? For example, sources of assurance might include the fact that Performance Indicators or targets have been met. All of the sources of assurance should be included in this one cell.

**Column 8: Early Warning Flags**

What would indicate that the likelihood or impact of the risk is increasing?

Given the sources of assurance that exist, how would you know if the situation was getting worse?

**Columns 9, 10 and 11: Current Risk Assessment**

This set of columns sets out your assessment of the impact of the risk, and the likelihood of it happening, given all of the things that are currently being done, or have been done, to mitigate against the risk. Please see 'Gross Risk Assessment' for an explanation of the meaning of the numbers you're being asked to use. You will need to use the heat map to determine the colour of the 11th column of row 4.

**Columns 12, 13 and 14: Net Risk Assessment**

This set of columns is your assessment of the impact of the risk, and the likelihood of it happening, once the Faculty/Directorate/Umbrella has undertaken all of the actions that are identified in the section of the risk register which looks at 'Actions for Further Control' (see below) to mitigate against the risk. Please see 'Gross Risk Assessment' for an explanation of the meaning of the numbers you're being asked to use. You will need to use the heat map to determine the colour of the 14th column of row 4.

## 3. The 'Action for Further Control' part of each section

These rows in each part of the risk register are for you to list the additional actions which you are planning to take to mitigate against the risk. A prioritized action list should be developed to manage the risk drivers. This column is for additional actions which are being planned. Actions which are currently being taken, and will continue, should be listed as 'Existing Controls'. Continuing to do what you are currently doing may be a very reasonable thing to do, but this should not be listed in this part of the risk register.

Each of the planned actions should be listed in a separate row. Indicate any new actions for further control as new actions in the status update box.

For each action you will see that to the right of your description, you are asked to give the job title of the action owner. This should be a named individual for each action. If several people are involved in an action, this individual should be the person responsible for coordination of the action overall.

You should then list a 'due date' for each of the actions - the date by which the action will be completed. Please make sure that these dates are genuinely achievable. It is much better to put an achievable date in here than to continue to miss unrealistic targets.

On the risk register following the completion of an action, please make sure that the 'due date' is amended to read 'Completed'. Completed actions from the previous iteration of the risk register should be removed. On the risk register after that, the action should either be removed, or moved to the 'Existing Controls' or 'Sources of Assurance' column (whichever is most appropriate).

The final part of this section of the risk register (status update) allows you to add information that you feel will aid understanding of what has happened. This part of each row only needs to be completed if you think there is something useful to say. For example, if you have amended a 'due date' it would be helpful to explain why this has been done. If you have marked an action as having been completed you might wish to explain in the 'status update' section that this item will be removed in the next version of the risk register.

It may be that the 'Action for Further Control' area is empty for one of the listed risks, because all the action that is deemed necessary in relation to that risk has been completed. Please make sure that, if this area is empty, it is for that reason, and not because you have forgotten to fill in this part of the risk register.

This does not mean that once this part of the risk register is empty, there will never be items which should be listed as 'Actions for Further Control'. It may be that circumstances change, so even if no future actions are listed, these rows should be reviewed every time the risk register is updated.

If you are in a situation where the Faculty/Directorate/Umbrella has already undertaken all 'Actions for Further Control' that were identified in previous iterations of the Risk Register, the figures for the current and net risk assessments will be the same. The area which relates to Actions for Further Control will be also be empty, as all of the planned actions will have been completed and should have either been removed or (if appropriate) moved to the 'Existing Controls' or 'Sources of Assurance' columns.

**Annex 2: HEAT MAP**

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **5** | 🟧 | 🟧 | 🟥 | 🟥 | 🟥 |
| **4** | 🟧 | 🟧 | 🟧 | 🟧 | 🟥 |
| **3** | 🟩 | 🟧 | 🟧 | 🟧 | 🟥 |
| **2** | 🟩 | 🟩 | 🟧 | 🟧 | 🟧 |
| **1** | 🟩 | 🟩 | 🟩 | 🟧 | 🟧 |

## Annex 3: Template for Risk Register.

| Risk 1: | *[Risk descriptor]* | | | | Risk owner: | | | |
|---|---|---|---|---|---|---|---|---|
| **Risk Cause** | **Risk Consequences** | **Gross Risk** | **Existing Controls** | **Sources of Assurance** | **Early Warning Flags** | **Current Risk** | **Net risk** | |
| *What might case the risk to occur* | *What are the possible consenquences should the risk occur?* | *Impact* / *Likelihood* / *IxL* | *What existingstrategies, processes or controls are in place to manage the risk?* | *How do we know that these controls are efficient and effective? What are our sources of assurance over the controls for this risk?* | *What would indicate that the likelihood of the imapct of the risk is increasing?* | *Impact* / *Likelihood* / *IxL* | *Impact* / *Likelihood* / *IxL* | |
| | | | | | | | | |

| Actions for further control to deliver net risk based on existing environment | | | |
|---|---|---|---|
| **Action for Further Control** | **Action Owner** | **Due Date** | Status update |
| **[Detailed action]** | **[Single named owner]** | **[Date]** | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |