# UPR Info - Risk management policy

## Overview

UPR Info recognises that the organisation is exposed to certain risks due to the nature of its activities and the environment in which it operates. The key to UPR Info's success is the effective management of risk to ensure its organisational objectives are achieved.

Risks arise due to the organisation's operation undertakings and from external sources. Risks occur in numerous ways and have the potential to impact performance, reputation, health and safety, partners with which UPR Info operates and the overall performance of the organisation.

The aim of risk management is to provide guidance regarding the management of risk to support the achievement of the organisation's mission and objectives, protect staff and assets and ensure financial sustainability. This will contribute to maximise opportunities in all UPR Info's activities and to minimise adversity.

The policy applies to all activities and processes associated with the normal operation of UPR Info. It forms part of UPR Info governance framework and applies to all employees, contractors, and partners.

## Policy

In order to fully understand such risks, UPR Info has established a Risk Management Policy which provides the framework for how risk will be managed within the organisation. The Risk Management Policy is based on the ISI 3100:2018 Risk management – Principles and

guidelines, and forms part of the governance framework of the organisation. It also integrates with the strategic planning process. The policy addresses both strategic and organisational risks.

We will use our skills and expertise to identify risks across the organisation. UPR Info will also identify operational controls in place which manage risk.

We will assess the size or degree of risk by taking into consideration the potential impact to our operations. Risks will be ranked in common and consistent manner and a Risk register will be maintained containing material risks to the organisation. The Risk register contains information on the type of risks (e.g., Contextual, programmatic, organisational), criteria for adding or removing risks from the register, responsibility to report and review it as well as the frequency of review.

Risk treatment actions and plans will be developed for risks which are unacceptable to the organisation. Risks and the effectiveness of the risk management system will be monitored on a regular basis and we will communicate and consult with relevant stakeholders on our approach to managing risks.

**Risk tolerance**

Our tolerance to adverse risks will be used to determine which risks are treated through the development of risk treatment actions to manage risks to an acceptable level. During this process we will consider additional control measures to manage the risks to acceptable levels.

**Integration with Governance and Strategic Planning**

The Risk Management Policy forms part of the governance framework and integrates with the strategic planning process and programmes implementation work plan. The Policy addresses both strategic and operational risks and the requirement of the organisation to operate in its regulatory environment.

**Accountability**

Ownership of risks and risk treatment actions will be assigned to relevant roles within the organisation. UPR Info has incorporated risk management accountability in executive, management and supervisory roles which are required to report on risks and risk treatment actions.

**Risk Management Oversight**

UPR Info's Board will oversee the Risk Management Policy and the organisation's exposure to risk. Oversight of the effectiveness of our risk management processes and activities will provide assurance to the Board and stakeholders and will support our commitment to continuous organisational improvement.

**Reporting, Monitoring and Review**

The purpose of risk reporting is to create awareness of keys risks, improve accountability for the management if risk and the timely adoption of measures to address and mitigate risks.

Principles (clause 4)

Framework (clause 5)

Process (clause 6)
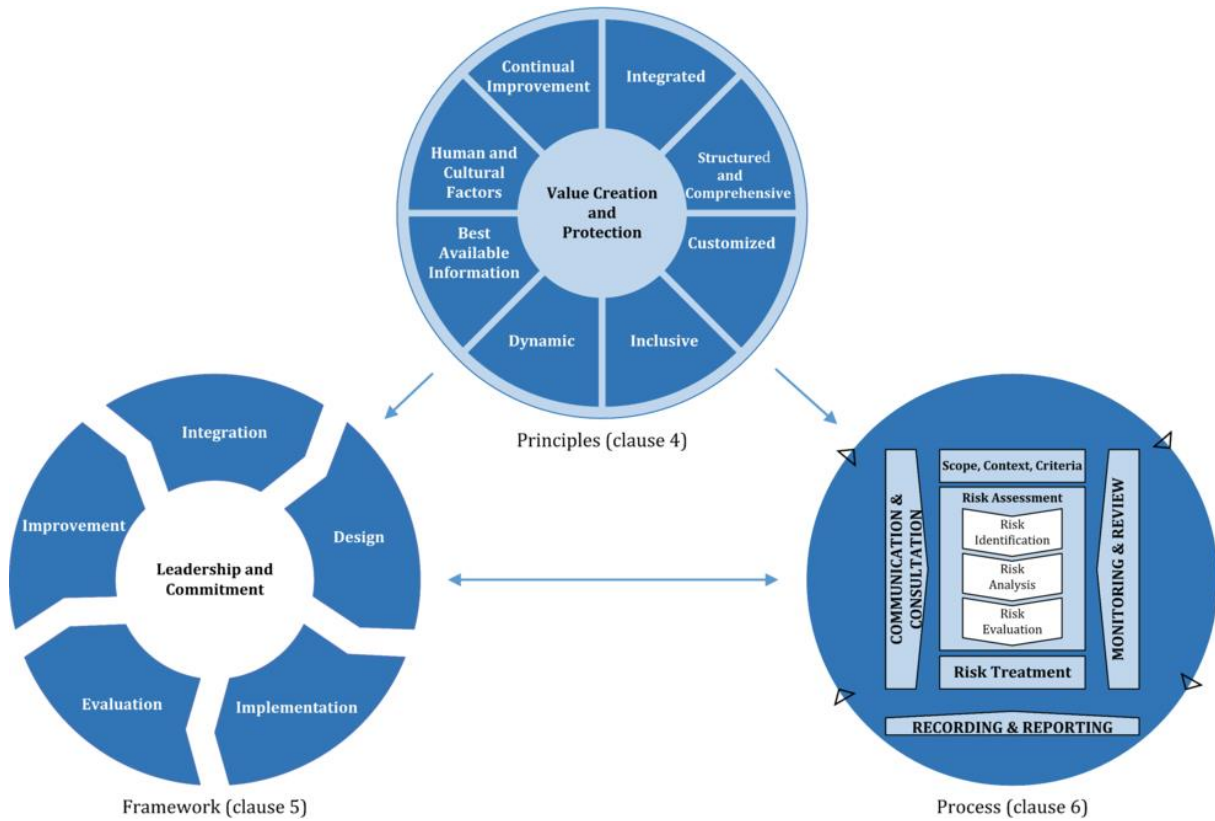
UPR Info will monitor risks and treatment actions on an ongoing basis. Performance of risk management system and outstanding risk treatment actions will be reported to the Executive Board twice per year during Board meetings. Formal reviews of both the risk management system and the Risk Register will take place on an annual basis and the Executive Board will assess the effectiveness of the Risk Management Policy annually.

It is the responsibility of all Executive Board and team members to identify, analyse, evaluate, respond, monitor, and communicate risks associated with any activity, function, or process within their relevant scope of responsibility and authority.

UPR Info has established the following risk governance structure of the organisation to specify who is involved in risk management and what their responsibilities are.

| | |
|---|---|
| Executive Board | Provides policy, oversight, and review risk management |
| Executive Director | Oversee regular review of risk management activities. Drives culture of risk management and signs off on annual risk plans. Continuously support the improvement of risk management policy, strategy and supporting framework. |
| Finance Manager | Ensure that staff complete the risk management plans. Identify, analyse, evaluate, respond, monitor, and communicate risks related to the financial and human resources management of the organisation. |
| Programme managers | Identify, analyse, evaluate, respond, monitor, and communicate risks associated with programmes/projects implementation. Ensure that staff in their programme comply with the risk management policy and foster a culture where risks can be identified and mitigated. |
| Junior staff and partners | Comply with risk management policy and procedures. |

**Communication and Consultation**

UPR Info will communicate and consult with its stakeholders (internal and external) on its approach to risk management.

Mona M'Bikay

Executive Director

January 21st, 2021

# Appendix I - RISK ASSESSMENT/RISK REGISTER FORM

## Risk identification form

| | |
|---|---|
| Programme: | Name of team member and function: |
| Risk category: | Date of Assessment: |
| Location of the risk: | Controls: |
| Causes (contributing factors): | Consequences: |

**Risk Matrix**

| Risk | Potential Impact of the risk | Existing control measures | Status (Monitor/Open/Closed) | Person responsible for action | Review due date |
|---|---|---|---|---|---|
| Risk rating Likelihood (Remote chance, improbable, possible, probable, almost certain) | | | | | |

| Description | | Mitigating measures | | | |
|---|---|---|---|---|---|
| | | | | | |

**Risk treatment plan**

| Risk: | Date logged: |
|---|---|
| Plan Owner: | Priority H/M/L: |
| Reviewer: | Target date: |
| Risk description | ● |
| Treatment plan | ● |
| Objectives | ● |
|    1.  Proposed actions | ● |
|    2.  Resources required | ● |
|    3.  Responsibilities | ● |
|    4.  Timing for implementation | ● |
|    5.  Monitoring requirements (i.e., weekly, monthly, quarterly) | ● |

**Appendix II - Guidance**

**Risks**

| Contextual | Programmatic | Organisational |
|---|---|---|
| Natural disasters | Diversion | High turnover of staff |
| Terrorist activity | Poor service delivery | Financial management |
| Political instability | Non-compliance with program and/or quality control process | Human resources management |
| Lack of public infrastructure | | Lack of capacity |
| Corruption | | Fraud |
| Pandemic | | |
| National strikes | | |
| Unrest | | |
| Restrictions of civic s | | |

| Likelihood level | Description examples | Probability examples |
|---|---|---|
| Remote chance | • May occur only in exceptional circumstances.<br>• Likelihood over 5 years: 1 in 20,000 chances. | < 20% |
| Improbable | • It is not expected to occur.<br>• No recorded incidents or evidence.<br>• Little opportunity, reason or means to occur.<br>• Likelihood over 5 years: 1 in 2,000 chance | >20%-40% |

| Possible | • May occur at some time.<br>• Few or infrequent recorded incidence or evidence.<br>• Some opportunity, reason or means to occur.<br>• Likelihood over 5 years: 1 in 200 chance. | >40%-60% |
|---|---|---|
| Probable | • Likely to occur/recur.<br>• Regular recorded incidents and strong evidence.<br>• Will probably occur in many circumstances.<br>• Likelihood over 5 years: 1 in 20 chance | >60%-80% |
| Almost certain | • Likely to occur/recur.<br>• High level of recorded incidents and strong evidence.<br>• Likelihood over 5 years: 1 in 2 chance. | >80%-100% |

**Risk description**

| Risk category | Risk description |
|---|---|
| Compliance/statutory | Inadequate compliance systems in place which may result in a loss of donor trust. |
| Legal/commercial | Breach of contract resulting in potential fines or litigation. |
| Political/economic | Changes in the political landscape resulting in possible loss of funding. |
| Financial/funding | Failure to effectively manage the financial resources of the organization which may result in financial loss. |
| Management | Poor management systems resulting in duplication and potential loss of productivity. |
| Operational | Disruption to day-to-day activities due to systems or process failure resulting in potential loss of productivity. |
| Service delivery | Reduced quality of service delivery resulting in potential loss of reputation. |
| Work health and safety | Failure of staff to follow procedures resulting in potential injury and health and safety incident. |
| Human resources | Inability to adequately resource programs with possible program delays and loss of reputation. |
| Stakeholders (clients/suppliers) | Financial failure of key supplier resulting in potential impact to delivery of services. |
| IT/information management | Loss of digital records through inadequate IT |

| | systems resulting in potential loss of reputation and/or loss of productivity. |
|---|---|
| Security | Breach of security due to failure to follow procedures resulting in potential theft/or loss of assets. |
| Reputational | Adverse media attention and/or heightened concern of local community. |

**Escalation and retention guidelines**

| Risk level | Treatment guidelines | Escalation and retention guidelines |
|---|---|---|
| Extreme | Immediate action required to actively manage risk and limit exposure. | Escalate to the Board, risks generally not accepted or retained. |
| High | Cost/benefit analysis required to assess extent to which risk should be treated – monitor to ensure risk does not adversely change over time. | Escalate to Director, risks generally not accepted or retained. |
| Medium | Constant/regular monitoring required to ensure risk exposure is managed effectively, disruptions minimized, and outcomes monitored. | Escalate to programme manager and director, specify risk management actions, risks may generally be retained and managed at operational level. |
| Low | Effectively manage through routine procedures and appropriate internal controls. | Monitor and manage at the relevant officer, or operational level, risks generally retained. |

# Contact

Website:                                   http://www.**upr-info**.org

Phone:                                     + 41 (0) 22 321 77 70

*General enquiries*                     info@**upr-info**.org

http://twitter.com/**UPRinfo**

http://www.facebook.com/**UPRInfo**