|  |  |
| --- | --- |
| **COUNCIL WORKING GROUP ON FINANCIAL AND HUMAN RESOURCES** 7th meeting, Geneva, 30 January – 1 February 2017 |  |
| INTERNATIONAL TELECOMMUNICATION UNION |  |
|  |  |
|  | **Document CWG-FHR 7/8** |
| **15 December 2016** |
| **English only** |

**CONTRIBUTION BY THE SECRETARIAT**

**Draft ITU risk management policy**

|  |
| --- |
| **Background**  Following PP Resolutions 151, 71, and 72, Recommendations from the Independent Management Advisory Committee (IMAC) and the UN Joint Inspection Unit (JIU), ITU is implementing a systematic risk management framework, as a process of continuous improvement of its managerial practices towards increasing efficiency, transparency and accountability.  This document introduces the draft ITU risk management policy.  This policy is complemented by a separate Risk appetite statement ([CWG-FHR/7/9](http://www.itu.int/md/S17-CLCWGFHRM7-C-0009/en)) indicating the amount and type of risk that the organization is willing to take in order to meet its strategic goals and objectives – this includes reference to both the organization’s risk appetite as well as its risk tolerance.  **Action required**  The CWG-FHR is invited to **review** and **endorse** the draft ITU risk management policy.  References  *PP Resolutions* [*71*](https://www.itu.int/en/council/planning/Documents/Strategic%20Plan%20for%20the%20Union%202016-2019__English.pdf) *(rev. Busan, 2014) ,* [*72*](http://web.itu.int/dms_pub/itu-s/opb/conf/S-CONF-ACTF-2014-MSW-E.docx) *(rev. Busan, 2014) and* [*151*](http://web.itu.int/dms_pub/itu-s/opb/conf/S-CONF-ACTF-2014-MSW-E.docx) *(rev. Busan, 2014); JIU review of ITU management and administration (*[*JIU/2016/1*](https://www.unjiu.org/en/reports-notes/JIU%20Products/JIU_REP_2016_1_English.pdf)*).* |

# 1 Introduction

## 1.1 Purpose

The purpose of this policy is to document the common methodology and framework for the implementation of systematic risk management. The driving objective is to facilitate and promote the identification, communication and management of risks through the management reporting lines.

The methodology given in this document follows best practices promoted by professional organizations and is suited to ITU specificities.

## 1.2 Objectives

The main objectives of the risk management policy in ITU are as follows:

* Embed risk management into the business process of the Organization, drawing from the best practices; and
* Allow for the achievement of the organizational goals and objectives, fostering a culture of risk awareness and organizational resilience.

## 1.3 Driving Principles

ITU’s risk management approach is guided by the following principles:

* Integration into business processes: risk management does not stand in isolation, rather it is embedded into pre-existing business processes;
* Discussion centered: regular discussions take place about risk management from the operational entity to executive level;
* Risk response: risks are identified, however there is also a corresponding response to them;
* Different risks at different levels: recognition that different parts of the organization have different objectives, thus may face different risks; and
* Make risk management decisions at the appropriate level: when risks cannot be mitigated at a level, they are reported to and managed at the level above.

# 2 Risk categorization and assessment

## 2.1 Risk perspective

The broad categories of risks are:

* Strategic risks: associated with reducing the capacity of the ITU at achieving its strategic goals; and
* Operational risks: associated with reducing the capacity of the ITU at achieving its operational objectives. Following are indicative broad categories of operational risks identified:
* Organizational
* Infrastructure
* Human resources
* Financial resources
* Stakeholder/ partners
* Environment.

## 2.2 Risk evaluation

Risk is the combination of the likelihood of occurrence (probability) of an event and of its consequence (impact). This assessment of risk aims to prioritize, or rate the risk level (criticality). The Bureaux and the General Secretariat will assess the level of risks by using the following matrix:

**Level of risk matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | **Impact** | | |
|  |  | **Low** | **Medium** | **High** |
| **Likelihood** | **High** | **Medium risk** | **High risk** | **High risk** |
| **Medium** | **Low risk** | **Medium risk** | **High risk** |
| **Low** | **Low risk** | **Low risk** | **Medium risk** |

The likelihood and impact are measured on different levels according to the tables below.

**Likelihood**

|  |  |
| --- | --- |
| Level | Justification |
| Low | An event that is very unlikely to happen |
| Medium | An event that is likely to happen |
| High | An event that is very likely to happen |

**Risk Impact**

|  |  |
| --- | --- |
| Level | Justification |
| Low | Minor impact on activities, reputation, or funding status |
| Medium | Significant impact on activities, reputation, or funding status |
| High | Critical impact on activities, reputation, or funding status and requires immediate attention |

## 2.3 Risk treatment

Defining a risk response involves selecting an action that is appropriate for the risk in question. There are three possible responses to a risk:

* **Acceptance**: the risk is identified, but because of its rather low level and insignificant impact, or because the mitigation efforts outweighs the consequences, the risk is accepted and no particular action is taken to mitigate it;
* **Mitigation**: the risk is identified, but actions have already been carried out or are ongoing to reduce/avoid the risk; and
* **Transfer**: Risk is identified, the responsibility of the risk remains with the risk owner, but the management of the risk mitigation measures is assigned to the appropriate level: another department, division, section, unit, or outsourced.

# 3 Monitoring and reviewing

## Reviewing and updating of risk register

ITU will maintain a list of risks it faces, as well as the corresponding mitigation measures. Risks are regularly reviewed as follows:

* The review of the strategic and operational risks is integrated in the business process operations of ITU, rather than being treated as a periodic exercise;
* As part of the process for the elaboration of the Operational Plans (OPs), the Bureaux and the GS review on a yearly basis the operational risks –identifying, analyzing and evaluating existing or new risks;
* The reviewed risks of the OPs of the Sectors and the GS are consolidated, and the senior management team collectively review all key operational and strategic risks; and
* Operational risks are communicated and consulted with membership through the OPs. The Sector advisory groups have the opportunity to review them and Council makes a final review of the risks and the mitigation measures to be implemented.

# 4 Roles and responsibilities

|  |  |  |
| --- | --- | --- |
| Title | Role | Responsibilities |
| Risk owner | The risk owner is accountable for the management of the risk, having the highest interest in the risk being correctly treated, and has the right level of authority to treat the risk accordingly | * Accountable for the overall management of the risk, including when the risk is transferred * Decides on the risk mitigation measures * Allocates resources/budget for mitigation actions * Manages risk (re)assessment process * Manages risk reporting process |
| Risk management focal point | Coordinates risk management process within respective Bureau or the General Secretariat | * Facilitates risk management within Bureau or the General Secretariat * Maintains and updates risk list * Consolidates and submits information for management review and risk reporting |
| Responsible for implementing mitigation measure | Implements mitigation measure and reports on their implementation to the risk owner | * Implements mitigation measure * Provides input for management review and risk list update |
| Senior management team | Reviews risk on a regular basis and takes decisions related to risk management | * Regularly reviews risks, as part of the organization’s business processes * Takes decisions on the implementation and review of the risk management strategy |

# 5 Communication

Communication with external (Member States) and internal stakeholders takes place during all stages of the risk management process.

Therefore, plans for communication and consultation are developed at an early stage. These address issues relating to the risk itself, its causes, its consequences (if known), and the measures being taken to treat it. Effective external and internal communication and consultation takes place to ensure that those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions are required.

# 6 Review of the Policy

The Policy will be reviewed and updated to draw from emerging best practices and lessons learned every 2 years after its inception.

# ANNEX 1: Risk Register template

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk List** | | **(Insert Sector or GS)**  **(as per the 2017-2020 Operational Plan)** | | | | | | | **Latest review summary** | |
| **Date** | ***Date*** |
| **To be received by** |  |
| **Perspective** | **Description of risk** | **Risk owner** | **Probability** | **Impact level** | **Mitigation measures** | | | **Residual risk** | **Follow up decisions/comments** | |
| **Measure** | **Responsible** | **Status** |
| *Example:* |  |  |  |  |  |  |  |  |  | |
| Financial | Inability of membership to pay assessed contributions | Chief of FRMD | Medium | High | Engagement with membership (incl. CRM system) | FRMD & SPM (PRM) | Ongoing | Risk remains after controls, active management is required | CRM system to help get more information on members' engagement and better manage the relationship | |

# ANNEX 2 - Glossary[[1]](#footnote-1)

**Risk management** refers to a coordinated set of activities and methods that is used to direct an organization and to control the many risks that can affect its ability to achieve objectives.

**Risk** is the “effect of uncertainty on objectives” and an effect is a positive or negative deviation from what is expected.

**Impact** or consequence is the outcome of an event and has an effect on objectives.

**Likelihood** or Probabilityis the chance that something might happen. Likelihood can be defined, determined, or measured objectively or subjectively and can be expressed either qualitatively or quantitatively.

**Risk appetite** is the amount and type of risk that an organization is willing to pursue or retain.

**Risk response** refers to the decisions made to deal with risks that have been identified. The organization can respond to a risk by either accepting it, mitigating it, or transferring it.

**Risk register** is a risk log of identified risks which outlines the description of the risk, the risk owner, the probability and impact of the risk, mitigation measures, and follow up decisions.

**Residual risk** is the level of risk that remains after consideration of all existing mitigating practices and controls. The residual risk provides guidance to the required level of management attention.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. These definitions are based on ISO 31000 2009 Risk Management Dictionary. [↑](#footnote-ref-1)