|  |  |
| --- | --- |
| **Council 2020** |  |
|  |  |
|  |  |
| **Agenda item: ADM 32** | **Revision 1 to  Document C20/61-E** |
| **5 October 2020** |
| **Original: English** |
| Report by the Secretary-General | |
| REPORT ON the implementation of the risk management action plan | |

|  |
| --- |
| Summary  This document presents an interim report for the implementation of the Action Plan to strengthen the ITU Risk Management Framework, as a follow-up to the progress report presented to Document CWG-FHR-11/12.  The document presents in its Annexes the revised ITU Risk management policy and ITU Risk appetite statement.  Action required  The Council is invited to **consider** this report, to **approve** the recommendations and to **review** and **approve** the revised annexed ITU Risk management policy and Risk appetite statement.  \_\_\_\_\_\_\_\_\_\_\_\_  References  *Document* [*CWG-FHR-11/12*](https://www.itu.int/md/S20-CWGFHR11-C-0012/en) *(Progress report on Strengthening ITU Risk Management Framework: action plan); Council documents* [*C17/74*](https://www.itu.int/md/S17-CL-C-0074/en) *(ITU Risk management policy);* [*C17/73*](https://www.itu.int/md/S17-CL-C-0073/en) *(ITU Risk appetite statement)* |

## 1 Interim report on the implementation of the Action plan to strengthen ITU risk management framework

1.1. Since the endorsement of the Action plan by CWG-FHR in February 2020, HLCM released in March 2020 a Guidance Note on Embedding Risk Management which has been taken into consideration while implementing the plan. In addition, the project has been supported by an external senior consultant to gain quality and assurance that the implementation of the action plan would capitalize on best risk management strategies experienced by other organisations.

|  |  |
| --- | --- |
| Action item / progress achieved | Timeline |
| 1. All organizational and operational entities to be involved in Risk Management  * Kick-off meetings, introducing the objectives of the Action plan and its deliverables both by Council 2020 and by end of 2020, have been conducted with more than 20 key stakeholders incl. Focal points (Bureaux, Regional Offices, Depts. of the General Secretariat, including Finance, HR, IS, Internal Audit). Comments and suggestions from the participants have been taken into consideration. * Proposed revised documents were sent (notably regarding actions #2, #3, #5 and #6 below), requesting feedback from stakeholders. * This participative approach would be continued until the end of the project. | By end of 2020 |
| 1. Risk registers to be developed for the whole organization and have those risks assessed and rated  * Preliminary risk registers and mitigation plans were obtained from organizational entities. * A new risk register template is being developed, which integrates cause and consequences of a risk, as well as the inclusion of controls in place and their effectiveness to estimate a residual risk. * The risk register template and the related operational details of managing risks are part of a new Risk Management Manual which is being finalized. This manual will be essential to support the training activities scheduled in the coming weeks (notably actions #4, #8 and #9 below). * Risks will be identified and assessed using the new risk registers for the next Strategic and Operational plans. | By Council 2020 / Ongoing |
| 1. Set up an internal risk governance structure  * Based on the best practices found in HLCM Risk Management Task Force survey results (March 2019) conducted among 25 UN Organisations, as well as the feedback gathered from the key stakeholders (cf. action #1 above), it is recommended to strengthen the risk governance structure. This enhancement is centered around the integration of a Risk and Internal Control function to oversee the implementation of risk management with a second line of defence accountability. Fully dedicated to Risk management and Internal controls, this function is responsible for coordinating the risk and control management processes, as well as their ongoing improvement including Risk management framework, policies and manual. * Considering the responsibilities assigned to the Risk and Internal Control function and the current structure for dealing with risk management within the organization, the role of the Inter-Sectoral Coordination Task Force (ISC-TF) was aligned accordingly to consult on the recommendations provided by the Risk and Internal Control function. On one hand and based on proposals made by the Risk and Internal Control function, ISC-TF would review risk management framework, policies and manual and prepare recommendations for approval by the Coordination Committee (CoCo) through the Management Coordination Group (MCG). On the other hand, it will review cross-sector moderate level risks on a regular basis, whereas single Sector risks would remain at the Bureau level. * Finally, MCG/CoCo would review high level risks on a regular basis and take decisions related to risk management, ensuring a clear tone at the top to promote a culture of responsible and effective risk management. | By Council 2020 |
| 1. Aim to improve staff accountability at all levels for managing risks  * Trainings and workshops on how to integrate risk management and internal controls in the business processes of the organization will be conducted. This will be done in 2020 4th quarter, using the new Risk register and the new Risk Management manual as guidance. The workshops will be aligned with the on-going process to revise the overall ITU accountability and transparency framework. | By end of 2020 |
| 1. Establish a more systematic risk management process  * The Risk Management Policy and Risk Appetite Statement have been reviewed to ensure a more systematic process to identify, assess and manage risks. They have been focused to their key-principles, and all operational details of managing risks will be part of a new Risk Management Manual. * Unity in the approach and methodology used for risk management across projects (Results-based management, project management, business continuity management, crisis management) and operations (including through a common Risk Register). * Fostering opportunity management, foresight, and innovation, rather than an approach that focuses only on avoiding harm and reacting to issues as they arise. * Greater alignment between risk appetite, categories and impact, ensuring risk management go hand-in-hand with ITU’s perspectives and its willingness to accept risk in key areas. * Systematic integration of risk reporting to the highest level of the organization for decision-making. * Alignment with accountability framework of the organization (current framework presented in Doc. [C20/43](https://www.itu.int/md/S20-CL-C-0043/en)) will be ensured during the process of the revision of the ITU accountability and transparency framework. * The “Three Lines of Defence” model has been introduced in the risk management policy as a solid ground for risk management and governance. | By Council 2020 |
| 1. Review the effectiveness of the internal controls  * A new risk register template is being developed, which integrates controls in place and their effectiveness to assess risk. Further alignment will be undertaken following the trainings and workshops, especially by integrating key controls from SAP automated processes. | By Council 2020 / ongoing |
| 1. Develop a risk management dashboard utilizing the new risk register  * A risk management dashboard will be implemented (using business intelligence tools) to monitor and communicate information related to risk management, providing a visual interface to navigate the risk registers of the organization. | By Q4 2020 |
| 1. Strengthen the capacity of staff to manage risks  * Action item will be implemented in combination with point 4 above, leveraging training and risk management workshops to raise awareness and strengthen the capacity of managers to manage risks. | By end of 2020 |
| 1. Aim to embed risk management in the staff performance management system  * Developing integrated processes, systems and tools that enable the operational teams to feel empowered and in control of their risks will support embedding risk management into the organisation. * Risk accountability and the ability to factor risk management into day-to-day decision-making in operations, should be a core aspect of all individual performance management processes. * This work has already begun by setting precisely in the risk management policy the role and responsibilities of all staff. | By end of 2020 |
| 1. Systematically communicate and report on risk information to membership  * The secretariat will continue reporting on risk management arrangements to CWG-FHR, while reports on the updated risk register and the risk management dashboard will be presented to membership. | Ongoing – Council 2020 |

## 2. Recommendations

2.1. The interim report of the Action plan to strengthen the ITU Risk management framework has resulted in the following recommendations:

1. Adoption of the revised ITU Risk Management Policy (Annex A to this report);
2. Adoption of the revised ITU Risk Appetite Statement (Annex B to this report);
3. Creation of a new function within the General Secretariat on Risk and Internal Control, within available budget. The main responsibilities of the function should be:

* providing recommendations for the organization’s adoption of best risk management practices and the continuous improvement of its internal control environment;
* recommending the adoption of risk policies, appetite statements, manuals and protocols for reporting and escalation and de-escalation of risk exposures to ITU’s Senior Management Team;
* establishing the methodologies and tools for identifying, assessing, monitoring and reporting on ITU’s risk exposures, including those related with Business continuity and Crisis Management (ORMS project);
* assessing the operating effectiveness (whether controls operate effectively over a period of time so as to actually result in the mitigation of the relevant risk(s)) of controls as recorded;
* sponsoring the enterprise risk management and control framework, including the operation of the three lines of defence and the adherence to and use of risk appetite measures;
* leading efforts to embed risk management across the organization and making evolve enterprise risk management tools and competencies to continually develop risk management in line with leading best practice;
* acting as the contact point for best practice sharing on enterprise risk management at the inter-agency level embracing both security and business risk management analysis, judgements and decision-making;
* managing the interface with the third line of defence on the corporate implementation of risk management, and responding to scrutiny concerning risk management from external parties, including the External Auditor, the Joint Inspection Unit and donors;
* consolidate best practices and experiences in risk management and organizational resilience management;
* work closely with the ORMS Coordinator and IT BC/DR Manager who are under the supervision of the Head of SSD who has responsibility for Security Risk Management within the Union.

ANNEX A

**2020 ITU RISK MANAGEMENT POLICY**

# 1 Introduction

## 1.1 ITU mission and strategic goals

The mission of the ITU is “*to promote, facilitate and foster affordable and universal access to telecommunication/information and communication technology (ICT) networks, services and applications and their use for social, economic and environmentally sustainable growth and development*” (Annex 1 to Resolution 71 (Rev. Dubai, 2018)).

ITU works to achieve its mission through the following five strategic goals:

* Goal 1 – Growth: Enable and foster access to and increased use of telecommunications/ICT in support of the digital economy and society;
* Goal 2 – Inclusiveness: Bridge the digital divide and provide broadband access for all;
* Goal 3 – Sustainability: Manage emerging risks, challenges and opportunities resulting from the rapid growth of telecommunications/ICT;
* Goal 4 – Innovation: Enable innovation in telecommunications/ICT in support of the digital transformation of society;
* Goal 5 – Partnership: Strengthen cooperation among the ITU membership and all other stakeholders in support of all ITU strategic goals.

## 1.2 Purpose and objectives of the ITU risk management policy

A key element of an organization’s accountability framework is a robust system of risk management and internal control. This policy sets out ITU’s approach to managing risks and controls in a consistent and business-oriented manner, in order to support the achievement of its strategic goals, expected results and project objectives.

A Risk Management Manual, which covers the day-to-day operational details of risk and control management at ITU, complements this policy document. Both documents, together with the Risk Appetite Policy, represent ITU’s Risk Management Framework.

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

* Embed risk management into the business processes of the organization, drawing from the best practices;
* Allow for the achievement of the organizational goals and objectives, fostering a culture of risk awareness and organizational resilience; and
* Allow for a balance of innovations and change with associated risks, within the stated risk boundaries of the organisation.

## 1.3 Driving Principles

ITU’s enterprise risk management framework is aligned with the 2017 COSO[[1]](#footnote-1) Enterprise Risk Management Framework, which integrates the relationship between risks, strategy, controls and performance. ITU’s risk management activities build upon the five components of COSO:

i) Governance and culture: Governance and culture together underpin all the components of enterprise risk management. Governance establishes oversight responsibilities and reinforces accountabilities across the “three lines of defence”, whose model[[2]](#footnote-2) was recommended for ITU’s adoption by IMAC in 2019. Culture is reflected in the subsequent transparency and quality of risk decision making.

ii) Strategy and objective setting: ITU’s risk appetite[[3]](#footnote-3) is aligned to the achievement of ITU’s Strategic and Operational Plans and supports the achievement of objectives in day-to-day operations and in setting priorities.

iii) Performance: ITU identifies and assesses risks that affect its ability to achieve its 5 strategic goals and its 24 strategic targets, as well as with dozens of operational risks that might reduce the capacity of ITU achieving its objectives. ITU prioritizes and responds to them according to their severity and considering ITU’s risk appetite.

iv) Review and revision: ITU aims to deliver continuous improvement and build resilience in managing risk; its control environment is expected to evolve as it seeks to align its risk profile with its risk appetite.

v) Information, communication and reporting: ITU adapts and constantly develops its risk appetite measures to improve risk information and drive more risk-sensitive decisions. This helps to embed a productive risk culture across the organization.

# 2 Risk management process and methodology

As a first step, ITU’s risks are recorded according to their assigned risk perspective in risk registers.

## 2.1 Risk perspective

The broad categories of risks, so called perspectives, are:

* **Strategic** risks (e.g. risks related to economic and competitive environment, technology and innovation, international political environment, stakeholders/donors, membership contributions, reputation);
* **Operational** risks (e.g. risks related to business processes, services, partners, vendors, buildings, IT infrastructure, business continuity, governance and oversight);
* **Financial** risks (e.g. risks related to the financial stability and sustainability of the organization: treasury management and foreign exchange, After Service Health Insurance (ASHI) liabilities, credit and counterparties, income and expenditure management, financial reporting);
* **Fiduciary** risks (e.g. risks related to employee health, safety and security, compliance and breach of obligations, fraud and corruption).

## 2.2 Risk assessment

Risk is the combination of the likelihood of occurrence of an event and of its consequence (impact). This assessment is performed by all staff at appropriate levels of the risk hierarchy.

The assessment of risk takes the existing control environment into account. Likelihood is estimated on a scale according to a specific matrix by probability/frequency detailed in the Risk management manual.Impact is estimated on a scale according to a specific matrix by perspective detailed in the Risk management manual.

To ease the reporting, risks are mapped on the ITU’s risk scale chart, as detailed in the Risk management manual.

## 2.3 Risk responses

Taking into account the risk appetite, risk responses involve selecting an action that is appropriate for the risk in question and may take the form of:

1. **Mitigation** actions**:** are intended to reduce the impact or likelihood of risks, and are one-off measures, which have specific objectives and deadlines, and may strengthen controls and/or reduce the likelihood or impact of the risk event;
2. **Transfer** actions: 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. **Acceptance** actions: accepting the risk without mitigation is also an option, as long as the risk is within the risk appetite.

Whatever the selected action, **controls** relevant to the risk in question should be identified. Controls are designed at various levels of ITU and are established to ensure reasonable assurance regarding the reliability of reporting; the effectiveness and efficiency of operations; compliance with applicable policies, regulations and rules, and the safeguarding of resources. Controls take various forms, such as the regulations and rules; office instructions and controls in information technology systems. Controls are cross-referenced to the risk that they mitigate. The effectiveness of the control, as established through the control assessment, will influence the extent to which a control can mitigate the risk to which is has been linked.

## 2.4 Risk assessment and risk response approval

Approval of risk assessment and response ensures the appropriate level of review and that the risk response (mitigation and control) measure is reflected in workplans, as applicable. The approval process for risk assessment and risk responses is as follows (defined in detail in the Risk Management Manual): MCG/CoCo endorses the assessment of and response to all risks within the red zone of ITU risk scale chart; Directors of the Bureaux endorse assessment of and response to single-Sector risks and risk owners can manage risks and risk responses, which are assessed to be in the green zone, into the risk register without additional approval required. ISC-TF is being consulted for cross-sector risks and escalation to MCG/CoCo is required for decisions.

## 2.5 Risk response implementation

Risk response (mitigation and control) implementation then commences, and the risk record is updated to reflect the reduction in the calculated risk to the resultant residual risk (after mitigation measures).

## 2.6 Information and communication

Information and communication about risks and risk responses is available through reports and dashboards, as well as through reports to the MCG/CoCo, and to Member States through the Strategic and Operational Plans. This information contributes to the regular re-assessment and continued monitoring of risks.

## 2.7 Monitoring

Monitoring activities are integrated in the business process operations of ITU and undertaken throughout, assessing the continued validity of risks and their associated responses (mitigation and control).

A Statement of internal control (SIC) signed by the Secretary-General annually, confirms the existence of a system of internal control.

This Policy will be reviewed and updated to draw from emerging best practices and lessons learned every two to three years. This review is under the responsibility of the MCG/CoCo and ultimate decision-making by the SG.

# 3 Roles and responsibilities

The “Three Lines of Defence” model supports effective risk management by introducing structured governance and oversight that clarifies and segregates roles and responsibilities based on the following:

* First Line of Defence: functions that own and manage risks;
* Second Line of Defence: functions that oversee and or specialize in risk management, compliance;
* Third Line of Defence: functions that provide independent assurance.

Thus the roles and responsibilities within the Risk management framework have been adapted accordingly to ensure compliance with the model and consistency with ITU’s organisation and lines of reporting.

|  |  |
| --- | --- |
| Title  (Line of Defence) | Role and Responsibilities |
| Risk owner  (1st line) | 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. Risk owners are identified across Bureaux, Regional Offices and the General Secretariat.  The risk owner should regularly, in collaboration with the Focal Point, identify, assess and propose suitable risk response action plans and if required designate a risk response action owner. In coordination with the Focal Point and the Risk and Internal Control function, the risk owner is responsible for escalating Sector-related risks to the Director of the Bureau, while for cross-sectoral risks the Risk and Internal Control function is being informed, ISC-TF is being consulted and escalation to MCG/CoCo for decisions takes place. |
| Risk management focal point  (1st line) | Facilitates an effective risk and control management process by ensuring consistent application of this policy within its assigned Bureau/Regional Office/Department or function of the General Secretariat, coordinating with the Risk owners and the Risk response action owner and ensuring due follow-up to the Risk and Internal Control function. |
| Risk response action owner  (1st line) | Is responsible for the effective implementation, monitoring and performance assessment of mitigation plans and controls, and updating effect on the risk assessment accordingly, as well as reporting to the risk owner. |
| Risk and internal control function  (2nd line) | Is responsible for coordinating the risk and control management processes, as well as the ongoing improvement and enhancement of the same, including Risk management framework, policies and manual. The Risk and Internal Control function is responsible for preparing the reporting to ISC-TF and MCG/CoCo and ensuring that organization-level risks are adequately identified and recorded in the risk management system.  Regarding controls, the Risk and Internal Control function is responsible for reviewing the operating effectiveness (whether controls operate effectively over a period of time so as to actually result in the mitigation of the relevant risks. |
| Directors of the Bureaux | Are responsible for the review and management of the Sector-related risks and response on a regular basis. |
| ISC – TF | Acts as a consultative organ for reviewing cross-sectoral risks and the risk management framework. |
| MCG/CoCo | Reviews high level risks on a regular basis and takes decisions related to risk management. Reviews and approves ITU risk management manual and ensures a clear tone at the top to promote a culture of responsible and effective risk management. |
| Ethics Office (2nd line) | The ethical standards, values and principles, including the Ethics Office, will be in the second line of defence (UN A/72/773, March 2018). |
| Internal Audit (3rd line) | The third line of defence is the independent assurance which traditionally covers the internal audit, investigation and evaluation functions. |

ANNEX B

**ITU RISK APPETITE STATEMENT**

# Introduction

This Risk Appetite Statement forms one element of a comprehensive risk management framework and is, in turn, one element of ITU’s Accountability Framework. The Organization’s risk management framework comprises this Statement, the Policy on Risk Management, the Risk Management Manual and is under the responsibility of the MCG/CoCo and ultimate decision-making by the SG. Risk identification, assessment, and treatment is an integrated process to manage uncertain events that may impact on the achievement of the goals and objectives in place, and it aims to enhance informed decision-making.

This document illustrates the amount and type of risk that ITU is willing to take in its drive to attain its strategic and operational goals and objectives. It acknowledges that the activities in which the organization engages in have different risk levels. It is important to underline that higher risk activities will only be undertaken where the benefits outweigh the costs and do not increase risk to an unacceptable level that could jeopardize the achievement of the organization’s strategic goals and objectives or undermine its reputation.

The risk appetite statement has been reviewed in line with the ITU risk management policy, which underpins the ITU strategic framework adopted by Member States in Resolution 71 (Annex 1, Rev. Dubai, 2018).

# Risk Appetite

Risk appetite is defined as the amount of risk, on a broad level, that the Organization is willing to accept in pursuit of its Strategic and Operational Goals.

The risk appetite levels used represent the following:

- LOW risk appetite: areas in which the Organization avoids risk, or acts to minimize the likelihood or impact of the risk event. This level of risk appetite is aligned to the Organizational overall risk appetite.

- MEDIUM risk appetite: areas in which the Organization must constantly strike a balance between the potential benefits, and the downside costs of a decision.

- HIGH risk appetite: in specific areas, the Organization may choose to take a calculated amount of risk, with the expectation that the probability of benefits outweighs the potential for ineffective investment and does not impact the organization’s reputation.

The Union’s approach towards its key operational and strategic risks is described below. This list neither describes all areas of ITU’s work nor an exhaustive list of potential risks, rather it gives an indication of willingness to accept risk in key areas. It is sorted by Perspective to be aligned with the risk management process.

***Strategic***

* With regard to the achievement of the strategic goals and objectives:
  + Low risk appetite for threats to the effective and efficient achievement of the organization’s strategic goals and objectives; and
  + High appetite for risks related to innovation and technological advancement.
* With regard to reputational impact:
  + Low appetite for risks that would significantly harm ITU’s reputation.

***Operational***

* With regard to the services and infrastructure provided:
  + Low risk appetite related to quality of services provided to the constituency of the organization; and
  + Very low risk appetite for significant breaches of security, unauthorized access to, or loss of classified records (e.g. frequency registers databases).

***Financial***

* With regard to the financial statements:
  + Low appetite for risk associated to accuracy and comprehensiveness of financial information and record including incomplete, incorrect, delayed or inadequately supported financial records.
* With regard to procurement:
  + Low appetite for risk associated to procurement failures that lead to poor value for money or financial losses for the Union.

***Fiduciary***

* With regard to internal management and controls:
  + No appetite (i.e. zero tolerance) in the areas of fraud, corruption, illegal acts, and misconduct;
  + Low appetite for risks associated with staff safety and security, and compliance.

# Review

This statement is being drafted bearing in mind that risk appetite will be evolving continuously. It is important that the risk appetite statement is structured to react quickly in response to any change. The monitoring and review process should focus with the view to creating risk awareness culture.

The risk appetite statement is reviewed annually, or whenever significant changes occur.

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

1. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) document Enterprise Risk Management – Integrating with Strategy and Performance (www.coso.org). COSO first published its enterprise risk management integrated framework in September 2004, the last revised version was published in June 2017. [↑](#footnote-ref-1)
2. The Three Lines of Defense in Effective Risk Management and Control, (Altamonte Springs, FL: The Institute of Internal Auditors Inc, January 2013) is embedded in the UN Risk Management, Oversight and Accountability Model. [↑](#footnote-ref-2)
3. See ITU’s risk appetite statement, Annex B [↑](#footnote-ref-3)