|  |  |
| --- | --- |
| **理事会2020年会议** |  |
|  |  |
|  |  |
| **议项：ADM 32** | **文件 C20/61(Rev.1)-C** |
| **2020年10月5日** |
| **原文：英文** |

|  |
| --- |
| 秘书长的报告 |
| 关于落实风险管理行动计划的报告 |

|  |
| --- |
| 概要  本文件介绍了关于落实旨在加强国际电联风险管理框架的行动计划的中期报告，是第CWG-FHR-11/12号文件中所述进展报告的后续工作。  本文件在其附件介绍了经修订的国际电联风险管理政策和国际电联风险偏好陈述书。  需采取的行动  请理事会**审议**本报告，**批准**建议，并**审议和批准**附件中经修订的国际电联风险管理政策和风险偏好陈述书。  \_\_\_\_\_\_\_\_\_\_\_\_  参考文件  第[CWG-FHR-11/12](https://www.itu.int/md/S20-CWGFHR11-C-0012/en)号文件（“加强国际电联风险管理框架：行动计划”的进展报告）；理事会第[C17/74](https://www.itu.int/md/S17-CL-C-0074/en)号文件（国际电联风险管理政策）；第[C17/73](https://www.itu.int/md/S17-CL-C-0073/en)号文件（国际电联风险偏好陈述书） |

# 1 关于落实旨在加强国际电联风险管理框架的行动计划的中期报告

1.1 自理事会财务和人力资源工作组（CWG-FHR）于2020年2月认可此行动计划以来，管理问题高级别委员会（HLCM）于2020年3月发布了《纳入风险管理的指导说明》，在落实行动计划时已经考虑了此指导说明。此外，该项目得到了外部高级顾问的支持，以提高质量并确保行动计划的落实会利用其他组织所采用的最佳风险管理战略。

|  |  |
| --- | --- |
| **行动项目/取得的进展** | **时间范围** |
| 1) 所有组织和运作实体都参与风险管理  – 与20多个主要利益攸关方，包括联系人（各局，区域代表处，财务、人力资源、信息系统、内部审计等总秘书处各部门）举行了启动会议，介绍了行动计划的目标以及在理事会2020年会议和2020年年底之前的实际成果。已考虑了与会者的意见和建议。  – 已发出拟议文件的修订版（尤其与以下行动2、3、5和6部分相关），要求利益攸关方提供反馈。  – 这种参与性方法将一直持续到项目结束。 | 在2020年年底之前 |
| 2) 为整个组织制定风险登记单并对这些风险进行评估和定级  – 从各组织实体获取初步的风险登记单和缓解计划。  – 正在开发一个新的风险登记单模板，该模板整合了风险的起因和后果，包括已有的控制措施以及这些措施对估计残留风险的有效性。  – 风险登记单模板和相关的风险管理的运作细节属于新的《风险管理手册》的一部分，该手册即将完成。该手册对于支持计划于未来几周开展的培训活动（尤其与以下行动4、8和9相关）至关重要。  – 将使用新的风险登记单为下一份战略规划和运作规划确定和评估风险。 | 在理事会2020年会议之前/仍在进行中 |
| 3) 建立内部风险治理结构  – HLCM风险管理任务组在25个联合国组织中开展了调查（2019年3月），根据调查结果发现的最佳做法以及从主要利益攸关方收集的反馈意见（参见上述行动1），建议加强风险治理结构。加强的重点是整合风险和内控职能，通过第二道防线问责制，监督风险管理的落实。该职能完全专注于风险管理和内控，负责协调风险和管控流程以及这些流程的持续改进，包括风险管理框架、政策和手册。  – 考虑到分配给风险和内控职能的责任以及本组织内部目前处理风险管理的结构，对跨部门协调任务组（ISC-TF）的作用进行了相应调整，对风险和内控职能提供的建议进行咨询。一方面，跨部门协调任务组将根据风险和内控职能的建议，审议风险管理框架政策和手册，并制定建议，由协调委员会（CoCo）通过管理协调组（MCG）批准。另一方面，跨部门协调任务组将定期审议跨部门中等水平的风险，而单个部门的风险仍将由各局负责审议。  – 最后，管理协调组（MCG）/协调委员会（CoCo）将定期审议高风险，并做出与风险管理有关的决策，确保高层有一个明确的立场，促进负责任和有效的风险管理文化。 | 在理事会2020年会议之前 |
| 4) 旨在完善各级职员风险管理问责制  – 举办有关如何把风险管理和内控整合到本组织的业务流程中的培训和讲习班。以新的风险登记单和新的风险管理手册作为指导，在2020年第四季度开展上述工作。这些讲习班将与正在进行的旨在修订国际电联的总体问责制和透明度框架的进程保持一致。 | 在2020年年底之前 |
| 5) 建立更系统化的风险管理流程  – 审议了《风险管理政策》和《风险偏好陈述书》，以确保建立更加系统地确定、评估和管理风险的流程。《风险管理政策》和《风险偏好陈述书》一直专注于关键原则，而管理风险的所有运作细节将成为新的《风险管理手册》的一部分。  – 统一所有项目（基于结果的管理、项目管理、业务连续性管理、危机管理）和运作（包括通过共同的风险登记单）使用的风险管理方式和方法。  – 促进机会管理、远见和创新，而不是只着眼于避害及在出现问题时被动应对的方法。  – 风险偏好、类别和影响之间更趋一致，确保风险管理与国际电联的视角以及在关键领域接受风险的意愿同步发展。  – 在组织的最高级别系统性地整合风险报告，以进行决策。  – 在修订国际电联的问责制和透明度框架的过程中，确保与本组织的问责制框架（第[C20/43](https://www.itu.int/md/S20-CL-C-0043/en)号文件中介绍的现行框架）保持一致。  – 在风险管理政策中引入了“三道防线”模型，作为风险管理和治理的坚实基础。 | 在理事会2020年会议之前 |
| 6) 审议内控措施的有效性  – 正在开发一个新的风险登记单模板，该模板整合了已有的控制措施以及这些措施对评估风险的有效性。在培训和讲习班之后，将进行进一步整合，特别是通过整合来自SAP自动化流程的关键控制措施来实现。 | 在理事会2020年会议之前/仍在进行中 |
| 7) 利用新的风险登记单开发风险管理仪表板  – 将实施一个风险管理仪表板（使用商业智能工具），监测和传达与风险管理有关的信息，并提供可视界面来浏览组织的风险登记单。 | 在2020年第四季度之前 |
| 8) 提高职员风险管理能力  – 本行动项目将结合以上第4点落实，利用培训和风险管理讲习班来提高认识并增强管理者管理风险的能力。 | 在2020年年底之前 |
| 9) 旨在将风险管理纳入职员绩效管理系统  – 开发统一的流程、系统和工具，使运作团队感受更有能力，能够控制他们的风险，从而支持将风险管理融入组织当中。  – 风险问责制以及将风险管理纳入日常运作决策的能力，应是所有单个绩效管理流程的核心方面。  – 通过在风险管理政策中准确设定所有职员的作用和职责，这项工作已经开始。 | 在2020年年底之前 |
| 10) 系统性地把风险信息传达和报告给成员  – 秘书处将继续向理事会财务和人力资源工作组报告风险管理安排，同时向成员介绍关于更新后的风险登记单和风险管理仪表板的报告。 | 仍在进行中 – 理事会2020年会议 |

# 2 建议

2.1 关于落实旨在加强国际电联风险管理框架的行动计划的中期报告提出了以下建议：

1) 通过经修订的国际电联风险管理政策（本报告附件A）；

2) 通过经修订的国际电联风险偏好陈述书（本报告附件B）；

3) 在可用预算范围内，在总秘书处内设置风险和内控的新职能。该职能的主要职责应是：

– 为本组织采用最佳风险管理做法以及不断完善其内控环境提供建议；

– 建议通过风险政策，风险偏好陈述书，手册和向国际电联高级管理团队报告、升级和降级风险敞口的规程；

– 建立用于确定、评估、监测和报告国际电联风险敞口的方法和工具，包括与业务连续性和危机管理（ORMS项目）有关的风险敞口；

– 评估所记录的控制措施的执行有效性（控制措施在一段时间内是否有效执行，从而实际上缓解了相关风险）；

– 发起企业风险管理和控制框架，包括三道防线的运作以及遵守和使用风险偏好措施；

– 牵头将风险管理融入整个组织的工作，升级企业风险管理工具和能力，根据领先的最佳做法不断推进风险管理；

– 在跨机构层面上作为分享企业风险管理最佳做法的联络点，包括安全和业务风险管理分析、判断和决策；

– 管理与企业实施风险管理的第三道防线的接口，并响应外部各方（包括外部审计师、联合检查组和捐助方）有关风险管理的审议；

– 整合风险管理和机构复原力管理方面的最佳做法和经验；

– 在负责国际电联安全风险管理的SSD负责人的监督下，与ORMS协调员和IT业务连续性/灾难恢复管理人员密切合作。

附件A

国际电联2020年风险管理政策

# 1 引言

## 1.1 国际电联的使命和总体战略目标

国际电联的使命是“推动、推进并促进对电信/信息通信技术网络、服务和应用的价格可承受的普遍接入，并将其用于社会、经济和在环境方面具有可持续性的增长和发展。”（第71号决议（2018年，迪拜，修订版）附件1）。

国际电联致力于通过以下五个总体战略目标实现其使命：

– 总体目标1：增长 – 为支持数字经济和社会，促成并推进电信/ICT的获取并加强其使用；

– 总体目标2：包容性 – 弥合数字鸿沟，为所有人提供宽带接入；

– 总体目标3：可持续性 – 管理电信/ICT迅速发展带来的新风险、挑战和机遇；

– 总体目标4：创新 – 为支持社会数字变革促进电信/ICT的创新；

– 总体目标5：伙伴关系 – 加强国际电联成员与所有其他利益攸关方的合作，以便为国际电联的所有总体战略目标提供支持**。**

## 1.2 国际电联风险管理政策的目的和部门目标

一个组织问责制框架的关键要素在于稳健的风险管理和内控系统。本政策以一致且面向业务的方式陈述了国际电联管理风险和控制措施的方法，以支持实现国际电联总体战略目标、预期成果和项目目标。

《风险管理手册》涵盖了国际电联风险和控制管理的日常运作细节，是对本政策文件的补充。这两份文件以及风险偏好政策构成了国际电联的风险管理框架。

国际电联风险管理政策的主要部门目标如下：

– 借鉴最佳做法，将风险管理纳入电联的业务流程；

– 实现本组织的总体目标和部门目标，培养风险意识文化和机构复原力；以及

– 在本组织规定的风险范围内，考虑创新和变化与相关风险之间的平衡。

## 1.3 驱动原则

国际电联的企业风险管理框架与2017年COSO[[1]](#footnote-1)企业风险管理框架保持一致，该框架整合了风险、战略、控制和绩效之间的关系。国际电联的风险管理活动基于COSO的五个组成部分：

i) 治理和文化：治理和文化共同支撑着企业风险管理的所有组成部分。治理确立了监督责任，并加强了“三道防线”的问责制，这种模型[[2]](#footnote-2)是IMAC于2019年建议国际电联采用的。而文化则体现在随后的透明度和风险决策质量当中。

ii) 战略和部门目标的设定：国际电联的风险偏好[[3]](#footnote-3)与国际电联战略和的运作规划保持一致，并支持在日常运作和确定优先事项中实现部门目标。

iii) 绩效：国际电联确定并评估那些影响其实现5个总体战略目标和24个具体战略目标的能力的风险，以及数十种可能会损害国际电联实现其部门目标能力的运作风险。国际电联会根据风险的严重性并考虑国际电联的风险偏好，确定风险的优先级并做出应对。

iV) 审议和修订：国际电联旨在不断改进风险管理并增强风险管理的韧性；随着国际电联寻求使其风险状况与风险偏好保持一致，预计其控制环境将不断发展。

V) 信息、沟通和报告：国际电联调整并不断制定其风险偏好措施，以改善风险信息并推动更具风险敏感性的决策。这有助于在整个组织中纳入更有成效的风险文化。

# 2 风险管理流程和方法

第一步，根据国际电联分配的风险视角将其风险记录在风险登记单中。

## 2.1 风险视角

风险的主要类别，即所谓的视角，包括：

– **战略**风险（例如与经济和竞争环境，技术与创新，国际政治环境，利益攸关方/捐助方，成员会费，声誉有关的风险）；

– **运作**风险（例如与业务流程，服务，合作伙伴，供应商，建筑物，IT基础架构，业务连续性，治理和监督相关的风险）；

– **财务**风险（例如与组织财务稳定性和可持续性有关的风险：资金管理和外汇，离职后健康保险（ASHI）负债，信贷和交易对手，收支管理，财务报告）；

– **信托**风险（例如与员工健康、安全和保障，合规和违约，欺诈和腐败有关的风险）。

## 2.2 风险评估

风险包括事件发生的可能性（概率）及其后果（影响）的组合。此评估由所有职员在风险等级中适当等级执行。

风险评估要考虑现有的控制环境。可能性是通过风险管理手册中详细说明的概率/频率根据具体的矩阵按等级估计的。“影响”是通过风险管理手册中详细说明的视角根据具体矩阵按等级估计的。

为了方便报告，把风险绘制到国际电信联盟的风险等级图上，详情见《风险管理手册》。

## 2.3 风险应对

考虑到风险偏好，风险应对措施包括选择适合于所述风险的行动，可以采取以下形式：

a) **缓解**行动：旨在减轻风险的影响或降低可能性，并且是一次性措施，有具体的目标和期限，可以加强控制和/或降低风险事件的可能性或减轻影响；

b) **转移**行动：已确定风险，风险责任仍由风险责任人承担，但风险缓解措施的管理已分配给适当的级别：另外一个部门、处室、科室、单元或外包；

c) **接受**行动：只要风险在风险偏好范围之内，不加缓解地接受风险也是一种选择。

无论选择哪种行动，都应确定与所述风险相关的**控制措施**。在国际电联的各个级别都设计了控制措施，制定的控制措施旨在确保对报告可靠性做出合理保证；运作的有效性和效率；遵守适用的政策、规章和规则，以及保护资源。控制措施可以采取各种形式，例如规章和规则，办公指令和信息技术系统中和控制等。控制措施与其旨在缓解的风险是相互参照的。通过控制评估所确定的控制措施的有效性将影响一项控制措施能够缓解与之相关联的风险的程度。

## 2.4 风险评估和风险应对的批准

批准风险评估和应对可确保进行适当程度的审议并确保风险应对（缓解和控制）措施在工作计划中得到体现（如适用的话）。风险评估和风险应对的批准流程如下（在《风险管理手册》中有详细的定义）：管理协调组（MCG）/协调委员会（CoCo）对国际电联风险等级图中红色区域内所有风险的评估和应对表示认可；各局主任对各自部门风险的评估和应对表示认可，风险责任人可以对评估在绿色区域的风险和风险应对措施进行管理，放入风险登记单中，而无需额外批准。关于跨部门风险，正在咨询跨部门协调任务组（ISC-TF），需要将其升级到管理协调组（MCG）/协调委员会（CoCo）。

## 2.5 风险应对措施的落实

然后开始落实风险应对（缓解和控制），更新风险记录以体现计算处的风险降低到最终残留风险（在缓解措施之后）。

## 2.6 信息与沟通

有关风险和风险应对的信息和沟通可通过报告和仪表板，通过向到管理协调组（MCG）/协调委员会（CoCo）报告以及通过战略和运作规划向成员国的报告方式提供。这些信息有助于对风险进行定期再评估和持续监测。

## 2.7 监测

监测活动已纳入国际电联的业务流程运作中，贯穿于整个过程中，从评估风险的持续有效性到相关风险应对措施（缓解和控制）。

秘书长每年签署一份内控声明，确认存在内控制度。

每两到三年，将对本政策进行审议和更新，以借鉴新兴的最佳做法和吸取的教训。此次审议由管理协调组（MCG）/协调委员会（CoCo）负责，由秘书长做出最终决策。

# 3 作用和职责

“三道防线”模型通过引入结构化的治理和监督，厘清和区分以下的作用和职责，来支持有效的风险管理：

– 第一道防线：风险责任和管理的职能；

– 第二道防线：监督和/或专门从事风险管理、合规的职能；

– 第三道防线：提供独立保证的职能。

因此，风险管理框架内的作用和职责也作了相应调整，以确保符合模型并与国际电联的组织和报告关系保持一致。

|  |  |
| --- | --- |
| **项目**  **（防线）** | **作用和职责** |
| 风险责任人  （第一道防线） | 风险责任人负责管理风险，对于风险得到正确处理拥有最大利益关系，并且拥有对风险做出相应处理所需要的恰当职权。在各局、区域代表处和总秘书处中确定风险责任人。  风险负责人应与联系人定期合作，确定、评估风险并提出适当的风险应对行动计划，必要时指定风险应对行动负责人。在联系人和风险和内控职能的协调下，风险负责人负责将与部门有关的风险上报至局主任，而对于跨部门风险，在告知风险和内控职能并咨询跨部门协调任务组（ISC-TF）的同时，升级至管理协调组（MCG）/协调委员会（CoCo）进行决策。 |
| 风险管理联系人  （第一道防线） | 通过确保在其指定的局/地区代表处/总秘书部门或职能部门内一致地贯彻本政策，与风险负责人和风险应对行动负责人进行协调，并确保对风险和内控职能的适当跟进，从而促进有效的风险和控制管理流程。 |
| 风险应对行动责任人  （第一道防线） | 负责缓解计划和控制措施的有效落实、监视和绩效评估，相应地更新风险评估的效果，并向风险负责人报告。 |
| 风险和内控职能  （第二道防线） | 负责协调风险和控制管理流程以及该流程持续改进和增强，包括风险管理框架、政策和手册。风险和内控职能负责起草提交跨部门协调任务组（ISC-TF）和管理协调组（MCG）/协调委员会（CoCo）的报告，并确保组织及风险得到了充分识别并将其记录在风险管理系统中。  关于控制措施，风险和内控职能负责审查运作有效性（控制措施在一段时间内是否有效运行，从而实际上缓解了相关风险）。 |
| 各局主任 | 负责定期对与部门相关的风险和应对进行审议和管理。 |
| 跨部门协调任务组（ISC-TF） | 作为审议跨部门风险和风险管理框架的咨询机构。 |
| 管理协调组（MCG）/协调委员会（CoCo） | 定期审议高等级风险，并做出与风险管理相关的决策。审议并批准国际电联风险管理手册，并确保在高层发出明确的声音，以促进负责任和有效的风险管理文化。 |
| 道德规范办公室 （第二道防线） | 道德标准、价值观和原则，包括道德规范办公室将处于第二道防线（2018年3月，UN A/72/773）。 |
| 内部审计 （第三道防线） | 第三道防线为独立保证，传统上涵盖内部审计、调查和评估职能。 |

附件B

国际电联风险陈述书

# 1 引言

本风险偏好陈述书是全面风险管理框架的一个组成部分，因而也是国际电联问责制框架的一个组成部分。本组织的风险管理框架包括本陈述书，《风险管理政策》，《风险管理手册》，由管理协调组（MCG）/协调委员会（CoCo）负责，由秘书长做出最终决策。风险的确定、评估和处理是为强化知情决策而设置的管理可能影响总体目标和部门目标实现的不确定事件的综合程序。

本文件介绍了国际电联在努力实现其总体战略目标和部门目标中愿意承受的风险程度和类型。陈述书承认，本组织从事的活动具有不同风险等级。必须强调，风险较高的活动只能在收益大于成本的情况下进行，而且这些活动不会将风险提升至难以接受的水平，致使对本组织总体战略目标和部门目标的实现造成危害。

本风险偏好陈述书已按照国际电联风险管理政策进行了审议，而此项政策是第71号决议（2018年，迪拜，修订版，附件1）中成员国通过的国际电联战略框架的基础。

# 2 风险偏好

风险偏好广义上是指本组织为实现其战略和运作总体目标愿意接受的风险程度。

所使用的风险偏好等级如下：

– 低风险偏好：本组织规避风险或采取行动将风险事件的可能性或影响降至最低的领域。此风险承受能力的水平与组织的整体风险承受能力一致。

– 中等风险偏好：本组织必须在潜在益处与所作决定的不利成本之间不断取得平衡的领域。

– 高风险偏好：在具体领域，本组织可以选择承担一定量的风险，期望收益的可能性大于无效投资的可能性，而且不会影响本组织的声誉。

国际电联应对主要运作和战略风险的方式如下所述。本清单既未涵盖国际电联工作的方方面面，亦不囊括所有的潜在风险。相反，清单阐明了对关键领域风险的承受意愿，它按“视角”进行分类，与风险管理流程保持一致。

**战略**

– 有关战略目标和部门目标的实现：

• 对损害组织总体战略目标和部门目标有效和高效实现的威胁的低风险偏好；以及

• 创新和技术进步相关风险的高偏好。

– 有关声誉影响：

• 对严重损害国际电联声誉的风险的低偏好。

**运作**

– 有关所提供的服务和基础设施：

• 对组织服务对象提供的服务质量的低风险偏好；以及

• 对严重安全违规、非法进入保密记录或保密记录（如频率登记数据库）丢失的极低风险偏好。

**财务**

– 关于财务报表：

• 对财务信息和记录的准确性和全面性（包括财务记录不完整、不正确、延迟或支撑不足）相关风险的低偏好。

– 关于采购：

• 对导致国际电联的物非所值或财务损失的采购失败的相关风险的低风险偏好。

**信托**

– 有关内部管理和控制：

• 在欺诈、腐败、非法行为和不端行为方面无偏好（即零容忍度）；

• 对人员安全和合规相关风险的低偏好。

# 3 审议

该陈述书在拟定时铭记风险偏好将不断变化。风险偏好陈述书采用的结构可对任何变化做出迅速反应。监督和审议应着眼于培育风险意识文化。

风险偏好陈述书每年审议一次，或在发生重大变化时随时审议。

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

1. 美国反虚假财务报告委员会（Treadway Commission）下属的发起组织委员会（COSO）的文件《企业风险管理 – 与战略和绩效整合》（[www.coso.org](http://www.coso.org)）。COSO于2004年9月首次发布了其企业风险管理整合框架，最新修订版于2017年6月发布。 [↑](#footnote-ref-1)
2. 《有效的风险管理和控制的三道防线》（2013年1月，佛罗里达州阿尔塔蒙特斯普林斯：内部审计师协会）已纳入联合国风险管理、监督和问责制模型中。 [↑](#footnote-ref-2)
3. 见附件B中《国际电联风险偏好陈述书》。 [↑](#footnote-ref-3)