ISO 31000:2018 风险管理指南
中文版

仅供内部参考学习使用，请勿外传和商用

目 录

前言

ISO（国际标准化组织）是一个全球联合的国际标准组织（ISO 成员机构）。制定国际标准的工作通常通过 ISO 技术委员会进行。对不同主题的技术委员会的感兴趣的每个成员机构，均有权参加该委员会的代表大会。与 ISO 有联系的国际组织、政府和非政府组织也参与了这项工作。ISO 与国际电工委员会（IEC）就电工标准化的所有事宜密切合作。

ISO / IEC 指令第 1 部分描述了用于开发和维护此文件的程序。尤其应注意不同类型 ISO 文件所需的不同批准标准。本文件是根据 ISO/IEC 指令第 2 部分（见 www.iso.org/directives）的编辑规则起草的。

请注意本文件的某些内容可能涉及某些专利权。ISO 不负责识别任何和此有关的专利权。在文件制定过程中确定的任何专利权的细节将在介绍和/或 ISO 收到的专利声明清单中（见 www.iso.org/patents）。

本文档中使用的任何名称都是为了方便用户而提供的信息，并不构成对此进行背书。

关于标准的自愿性质的解释，与合格评定相关的 ISO 特定术语和表达的含义，以及关于 ISO 遵守世界贸易组织（WTO）在技术性贸易壁垒（TBT）原则中的信息参见网址如下：www.iso.org/iso/foreword.html。

本文件由 ISO/TC 262 风险管理技术委员会编写。

本第二版标准用于代替第一版标准（ISO 31000：2009）。

与前一版本相比的主要变化如下：

-审阅了风险管理原则，这是其成功的关键标准；

-从组织治理开始，突出高层管理人员的领导职责和风险管理的整合；

-更加强调风险管理的反复优化性质，指出新的经验、知识和分析可以促使对流程各个阶段的流程要素、行动和控制进行调整；

-精简内容，更加注重保持开放系统模式以适应多种需求和环境。

介绍

此文件供那些通过管理风险来制定决策、设定和实现目标，以及通过提升绩效来创造和保护组织价值的人员使用。

各种类型和规模的组织都面临着外部和内部因素及影响，这些因素和影响使得组织实现其目标面临一定的不确定性。

风险管理是反复优化的，有助于组织制定战略、实现目标和做出明智的决策。
管理风险是治理和领导力的一部分，对于组织在各个层面的管理至关重要。它有助于改进管理体系。

管理风险是组织所有活动的一部分，包括与利益相关方的交流和沟通。

管理风险考虑了组织的外部和内部环境，包括人员行为和文化因素。

如图 1 所示，管理风险基于本文档中描述的原则、框架和流程。这些要素可能已经全部或部分存在于组织内了，但是，为了更高效、有效和一致的管理风险，他们可能需要进行调整和改进。

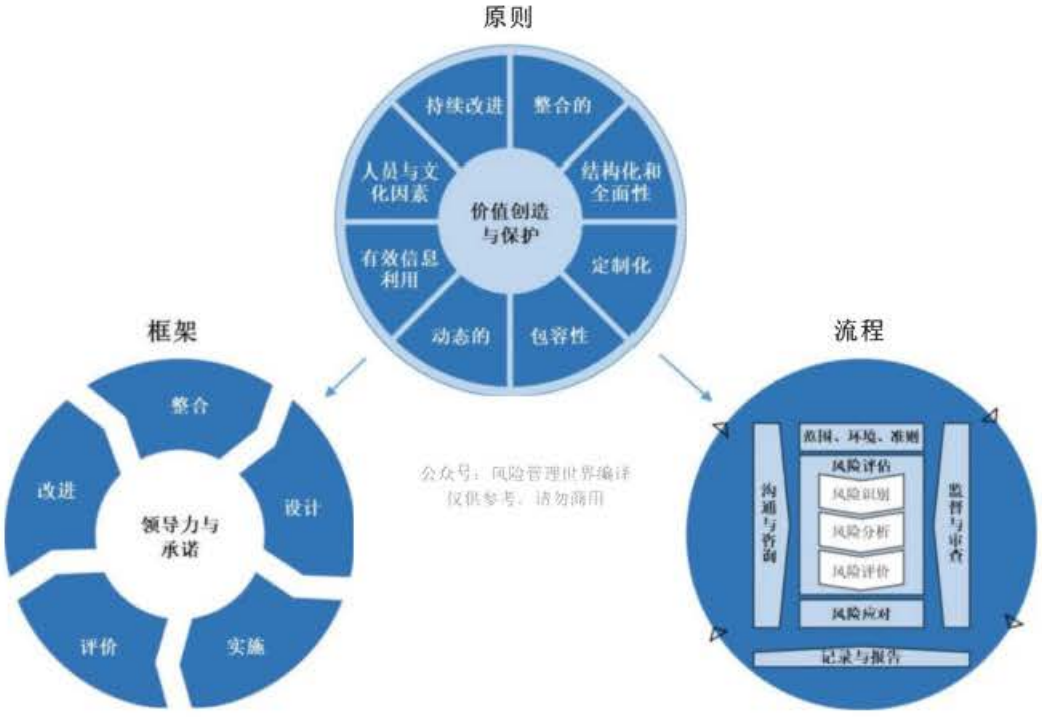

图 1 – 原则、框架和流程

风险管理 - 指南

1 适用范围

本文件提供了组织管理面临的风险的指南。这些指南的应用可以针对任何组织及其背景环境进行定制。

本文件提供了管理任何类型风险的通用方法，并非行业或某一领域特定的。

该文件可用于组织的整个生命周期，可应用于任何活动，包括各层级决策。

2 规范性引用文件

本文档中没有规范性引用文件。

3 术语和定义

就本文件而言，下列术语和定义适用。

ISO 和 IEC 维护了用于标准化术语数据库，地址如下：

- ISO 在线浏览平台：http：//www.iso.org/obp
- IEC Electropedia：可在 http://www.electropedia.org 上找到

3.1

风险

不确定性对目标的影响

注 1：影响是与预期的偏差。它可以是积极的、消极的或两者兼而有之，并且可以锁定、创造机遇或导致威胁。

注 2：目标可以有不同的方面和类别，并且可以在不同的层面应用。

注 3：风险通常以风险源（3.4）、潜在事件（3.5）、后果（3.6）及其可能性（3.7）表示。

3.2

风险管理

指导和控制组织风险（3.1）的协调活动

3.3

利益相关方

对一个决策或活动可以产生影响或受其影响、亦或将会受影响的个人或组织

注 1：“利害关系方”一词可以用作代替“利益相关方”。

3.4

风险源

单独或组合在一起可能会导致风险的要素（3.1）

3.5

事件

一系列特殊状况的发生或变化

注 1：事件可能是一次或多次事件，并可能有多个原因和多个后果（3.6）。

注 2：事件可以是预期不会发生的事情，也可以是没有预期一定会发生的事情。

注 3：事件可能是风险源。

3.6

后果

事件（3.5）影响目标的结果

注 1：后果可能是确定的或不确定的，可能对目标产生正面或负面、直接或间接的影响。

注 2：后果可以定性或定量表示。

注 3：任何后果都可能通过连锁和累积效应升级。

3.7

可能性

事情发生的几率

注 1：在风险管理（3.2）术语中，“可能性”一词用于指发生事件的几率，无论是客观地还是主观地、定性地或定量地进行定义、测度或确定，并且使用一般术语或数学描述（例如给定时间段内的概率或频率）。

注 2：英文术语“可能性”在某些语言中没有直接的同义词；有时会使用术语“概率”来代替。然而，在英语中，“概率”通常被狭义地解释为数学术语。因此，在风险管理术语中，“可能性”应该与“概率”一词在除英语以外的语言中，具有相同的广义解释。

3.8

控制

保持和/或调整风险的措施（3.1）

注 1：控制包括但不限于保持和/或修改风险的任何流程、政策、设备、实践或其他条件和/或行动。

注 2：控制可能并不总是能发挥到预期或假定的调整效果。

4 原则

风险管理的目的是创造和保护价值。它提升了绩效，鼓励创新并支持目标实现。

图 2 中描述的原则为有效和高效的风险管理的特点提供了指导，传达其价值并解释其意图和目的。这些原则是管理风险的基础，应在建立组织的风险管理框架和流程时予以考虑。这些原则可以使组织能够管理不确定性对其目标的影响。

图 2 – 原则

有效的风险管理需要图 2 中的要素，可以进一步解释如下。

a）整合的

风险管理是所有组织活动的组成部分。

b）结构化和全面性

风险管理的结构化和综合性方法有助于获得一致的和可比较的结果。

c）定制化

风险管理框架和流程是根据组织与其目标相关的外部和内部环境来制定的，并与其密切相关。

d）包容的

需要考虑利益相关方的适当和及时的参与，融入他们的知识、观点和看法。这可以提高风险意识并明智的管理风险。

e）动态的

随着组织内部和外部环境的变化，风险可能会出现、变化或消失。风险管理会以适当和及时的方式预测、监督、掌握和响应这些变化和事件。

f）最佳可用信息

风险管理的输入是基于历史和当前的信息以及未来的预期。风险管理应明确考虑到与这些信息和期望相关的任何限制和不确定性。信息应及时、清晰地提供给相关的利益相关方。

g）人员及文化因素

人员行为和文化明显影响着各级和各阶段风险管理的各个方面。

h）持续改进

通过学习和经验积累，不断提高风险管理水平。

5 框架

5.1 概述

风险管理框架的目的是协助组织将风险管理纳入重要的活动和职能。风险管理的有效性取决于是否将其纳入组织治理和决策中。这需要利益相关方，特别是最高管理层的支持。

框架开发包括在整个组织内整合、设计、实施、评价和改进风险管理。图 3 说明了框架的要素。

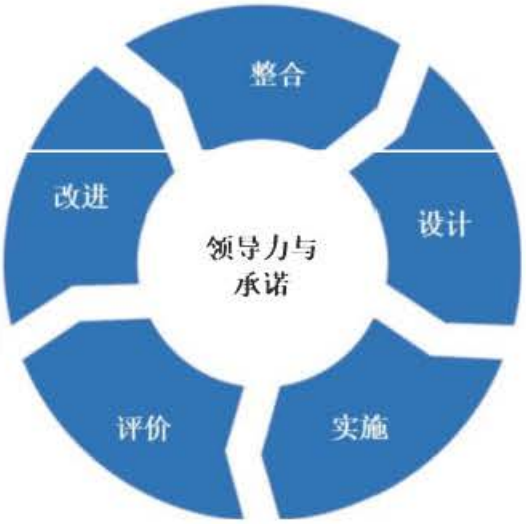

图 3 – 框架

组织应评估其现有的风险管理实践和流程，评估任何差距并依照框架解决这些差距。

框架的组成要素和它们协同作用的方式应该根据组织的具体需求进行定制。

5.2 领导力和承诺

在适当的情况下，高级管理层和监督机构应确保风险管理融入组织所有活动，并应通过以下方式表现出领导力和承诺：

- 针对性的设计和实施框架的所有要素；
- 发布建立风险管理方法、计划或行动方案的声明或政策；
- 确保为管理风险分配必要的资源；
- 在组织内的相应级别分配权限和职责。

这将有助于组织：

- 将风险管理与其目标、战略和文化相结合；
- 承担和界定所有义务及其自愿承诺；
- 确定风险的数量和类型，指导风险准则制定，确保将风险准则传达给组织及利益相关方；
- 将风险管理的价值传达给组织及其利益相关方；
- 促进系统的对风险进行监测；
- 确保风险管理框架适合组织环境。

最高管理层负责管理风险，而监督机构负责监督风险管理。对监督机构的期望或是要求：

- 确保组织在确定组织目标时充分考虑风险；
- 了解组织追求目标所面临的风险；
- 确保管理风险的体系得到有效实施和运行；
- 确保组织在当前的目标下承担了适当的风险；
- 确保有关这些风险及其管理的信息得到适当传达。

5.3 整合

整合风险管理依赖于对组织架构和环境的理解。架构因组织的目的、目标和复杂程度而异。组织架构中的每个部分都需要进行风险管理。组织中的每个人都有责任管理风险。

治理为组织如何处理内外部关系，设置规则、流程和实践以实现其目的提供了指引。管理架构将治理的方向转化为战略和相关目标，来实现组织理想水平的绩效和永续经营。确定组织内部的风险管理责任和监督角色是组织治理的一部分。

将风险管理整合到组织中是一个动态和反复优化的过程，应该根据组织的需求和文化进行定制。风险管理应该成为组织目的、治理、领导力和承诺、战略、目标和运营的一部分，而不是相互分离。

5.4 设计

5.4.1 了解组织及其环境

在设计风险管理框架时，组织应该检视并理解其内部和外部环境。

检查组织的外部环境可能包括但不限于：

- 社会、文化、政治、法律、监管、财务、技术、经济和环境因素，无论是全球的、国家的、区域的、还是本地的；
- 影响组织目标的关键驱动因素和趋势；
- 外部利益相关方的关系、意见、价值观、需求和期望；
- 合同关系和承诺；
- 网络和依赖关系的复杂性。

检查组织的内部环境可能包括但不限于：

- 愿景、使命和价值观；
- 治理、组织架构、角色和责任；
- 战略、目标和政策；
- 组织的文化；
- 组织采用的标准、指南和模式；
- 根据资源和知识（例如资本，时间，人员，知识产权，流程，系统和技术）来理解能力；
- 数据、信息系统和信息的流动；

- 与内部利益相关方的关系，考虑他们的意见和价值观；
- 合同关系和承诺；
- 相互依赖和相互关联。

5.4.2 明确风险管理承诺

在适当情况下，高级管理层和监督机构应通过政策、声明或其他形式清楚地表达组织的目标和对风险管理的承诺，展示并阐明其对风险管理的持续承诺。承诺应包括但不限于：

- 组织管理风险的目的以及与其目标和政策的联系；
- 加强将风险管理理念纳入组织整体文化的需要；
- 带领风险管理整合到核心业务活动和决策中；
- 权限、职责；
- 保证必要资源的充足性；
- 处理相互冲突的目标；
- 组织绩效指标衡量和报告；
- 审查和改进。

组织对风险管理的承诺应在适当时传达给内部和利益相关方。

5.4.3 分配组织角色、权限、职责

在适当情况下，高级管理层和监督机构应确保在组织各级分配和传达有关风险管理的权限和职责，并应：

- 强调风险管理是核心责任；
- 确定具有管理风险职责和权限的个人（风险所有者）。

5.4.4 分配资源

在适当的情况下，高级管理层和监督机构应确保为风险管理分配适当资源，其中可包括但不限于：

- 人员、技能、经验和能力；

- 组织用于风险管理的流程、方法和工具；
- 记录过程和程序；
- 信息和知识管理系统；
- 专业发展和培训需求。

组织应考虑现有资源的能力和局限。

5.4.5 建立沟通和咨询

为支持框架和促进风险管理的有效应用，组织应建立一个经过批准的沟通和咨询方法。沟通涉及与目标受众共享信息。咨询包括参与者期望对决策或其他活动作出贡献，以便更好决策的反馈信息。沟通和咨询方法和内容应反映相关利益方的期望。

沟通和咨询应该及时进行，确保收集、整理、汇总和分享相关信息，提供反馈意见并改进。

5.5 实施

组织应通过以下方式实施风险管理框架：

- 制定适当的计划，包括时间表和资源配置；
- 在整个组织内，确定在什么地点、什么时间、由谁来进行不同类型的决策；
- 在必要时，调整适用的决策程序；
- 确保组织的风险管理安排得到清晰的理解和实施。

框架的成功实施需要利益相关方的参与和了解。这使组织能够明确地应对决策中的不确定性，同时确保在出现任何新的不确定性时可以将其考虑在内。

通过正确的设计和实施风险管理框架，可以确保风险管理流程是整个组织所有活动（包括决策）的一部分，并将充分反映内外部环境的变化。

5.6 评价

为了评估风险管理框架的有效性，组织应该：

- 根据其目的、实施计划、指标和预期行为定期衡量风险管理框架的绩效；
- 确定它是否仍然适合支撑组织目标的实现。

5.7 改进

5.7.1 适应性

组织应持续监控和调整风险管理框架，以解决内外部的变化。这样做，组织可以提升其价值。

5.7.2 不断改进

组织应不断改善风险管理框架的适用性、充分性和有效性，以及风险管理流程的整合方式。

如果已经确定了差距或改进的机会，组织应制定计划和任务，并将其分配给负责实施的人员。这些改进措施一旦实施，将有助于加强风险管理的作用。

6 流程

6.1 概述

风险管理流程涉及系统地将政策、程序和实践应用于沟通和咨询活动，建立环境和评估、应对、监督、审查、记录和报告风险。这个流程如图 4 所示。

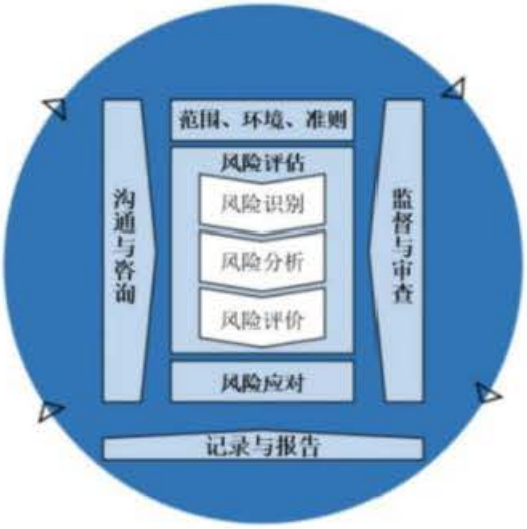

图 4 – 流程

风险管理流程应成为管理和决策的一个组成部分，并融入组织的架构、运营和流程中。它可以应用于战略、运营、计划或项目层面。

组织内部可以有很多风险管理流程的应用方式，这些应用方式是为实现目标而定制的，并适用于其所在的内外部环境。

在整个风险管理流程中，应考虑人员行为和文化因素的动态性和变化性。

虽然风险管理流程通常表现为有一定的顺序，但实际上不同流程步骤之间是可以反复交错使用的。

6.2 沟通和咨询

沟通和咨询的目的是协助利益相关方理解风险、明确作出决策的依据以及需要采取特定行动的原因。沟通旨在促进对风险的认识和理解，而咨询涉及获取反馈和信息以支持决策。两者之间的密切协调应该促进真实、及时、相关、准确和可理解的信息交换，同时需要考虑信息的保密性和完整性，以及个人的隐私权。

与适当的内外部利益相关方进行沟通和咨询，应在风险管理流程的所有步骤内和整个流程中进行。

沟通和咨询的目的是：

- 为风险管理流程的每一步带来不同领域的专业知识；
- 在确定风险准则和评估风险时，确保适当考虑不同的观点；
- 提供足够的信息来促进风险监督和决策；
- 在受风险影响的相关方中建立包容性和责任感。

6.3 范围、环境和准则

6.3.1 概述

确定范围、环境和准则的目的是针对性的设置风险管理流程，实现有效的风险评估和恰当的风险应对。范围、环境和准则涉及界定流程的范围并理解内外部环境。

6.3.2 定义范围

组织应该确定其风险管理活动的范围。

由于风险管理流程可能适用于不同的层面（例如战略、运营、计划、项目或其他活动），因此重要的是明确所考虑的范围、相关目标以及与组织目标的一致性。

在规划时，考虑事项包括：

- 目标和需要作的决策；

- 预期在每一步流程中取得的成果；
- 时间、地点、具体包含和除外的内容；
- 适当的风险评估工具和技术；
- 需要的资源、责任和记录；
- 与其它项目、流程和活动的关系。

6.3.3 外部和内部环境

外部和内部环境是组织制定和实现其目标的土壤。

风险管理流程的环境应根据对组织运行的外部和内部情况的理解来确定，并反映适用风险管理流程的具体活动情况。

了解环境很重要，因为：

- 风险管理是在组织目标和各项活动的环境下进行的；
- 组织本身的因素可能是风险的来源；
- 风险管理流程的目的和范围可能与整个组织的目标相互关联。

组织应考虑 5.4.1 中提到的因素，建立风险管理流程的外部和内部环境。

6.3.4 定义风险准则

相对于目标而言，组织应该明确承担风险的数量和类型。还应该定义评估风险重要性水平和支持决策过程的准则。风险准则应与风险管理框架相一致，并根据具体活动的目的和范围进行针对性设计。风险准则还应反映组织的价值观、目标和资源，并与风险管理的政策和声明保持一致。根据组织的义务和利益相关方的考虑来定义准则。

尽管应在风险评估流程开始时制定风险准则，但它们是动态的，必要时应不断审查和修订。

要设定风险准则，应考虑以下内容：

- 可能影响结果和目标（包括有形和无形）的不确定性的性质和类型；
- 如何定义和衡量结果（包括正面和负面）和可能性；
- 时间相关因素；

- 衡量准则使用的一致性；
- 风险水平如何确定；
- 如何考虑多种风险的组合和序列；
- 组织的风险容量。

6.4 风险评估

6.4.1 概述

风险评估是风险识别、风险分析和风险评价的整个过程。

风险评估应该借助利益相关方的知识和观点，系统的、反复优化并协作的开展。风险评估应该使用最好的可用信息，并在必要时辅以进一步的调查。

6.4.2 风险识别

风险识别的目的是发现、识别和描述可能有助于或妨碍组织实现目标的风险。相关的、适当的和最新的信息对于识别风险很重要。

组织可以使用一系列技术来识别可能影响一个或多个目标的不确定性。应考虑以下因素以及这些因素之间的关系：

- 有形和无形的风险源；
- 原因和事件；
- 威胁和机会；
- 短板和长板；
- 外部和内部环境的变化；
- 新出现的风险征兆；
- 资产和资源的性质和价值；
- 后果及其对目标的影响；
- 知识和信息可靠性的局限；
- 时间相关因素；

- 参与者的偏见、假设和个人价值取向。

组织应识别风险，不管其来源是否在其控制之下。应该考虑到可能有不止一种类型的表现形式，这可能会导致各种有形或无形的后果。

6.4.3 风险分析

风险分析的目的是理解包括风险水平在内的风险性质和特征。风险分析涉及对不确定性、风险源、后果、可能性、事件、情景、控制及其有效性的详细考虑。事件可能有多种原因和后果，并可能影响多个目标。

根据分析目的、信息的可用性和可靠性以及资源的可用性，风险分析可以进行粗细程度、复杂程度不等的分析。分析技术可以是定性或定量的，也可以是定性和定量相结合的方式，这取决于环境和预期用途。

风险分析应考虑以下因素：

- 事件和后果的可能性；
- 后果的特征和强度；
- 复杂性和关联性；
- 时间因素和波动性；
- 现有控制的有效性；
- 敏感性和置信水平。

风险分析可能会受到意见分歧、偏见、风险认知和判断的影响。其他影响因素还包括所用信息的质量、所做的假设和除外条件、对技术的任何限制以及执行情况等。应该考虑、记录这些影响因素并传达给决策者。

高度不确定的事件可能难以量化，这在分析具有严重后果的事件时，可能是一个问题。在这种情况下，使用各种技术的组合通常可以提供更多的参考意见。

风险分析的结果是风险评价的基础，来决定风险是否需要应对，以及如何使用最适合的风险应对策略和方法。这些结果为未来进行决策提供了依据和参考，并且涉及不同类型和水平的风险。

6.4.4 风险评价

风险评价的目的是支持决策。风险评价涉及将风险分析的结果与既定的风险准则进行比较，以确定需要采取何种应对措施。这可能会决定：

- 不需要做任何事情；
- 考虑风险应对的不同选项；
- 进一步分析以更好地理解风险；
- 保持现有的控制；
- 重新考虑目标。

决策应考虑到更广泛的环境和背景情况，以及当前和未来对内外部利益相关方的影响。

风险评价的结果应该在组织的适当层面进行记录、传达和验证。

6.5 风险应对

6.5.1 概述

风险应对的目的是选择和实施应对风险的方式。

风险应对涉及以下反复优化过程：

- 制定和选择风险应对方案；
- 计划和实施风险应对方案；
- 评估应对的有效性；
- 确定剩余风险是否可接受；
- 如果不能接受，采取进一步应对。

6.5.2 选择风险应对备选方案

选择最合适的风险应对方案，涉及到为实现目标实施此方案带来的潜在收益，与实施成本或由此带来的不利因素之间的权衡。

在所有情况下，风险应对选项不一定是相互排斥或完全适合的。应对风险的方案可能涉及以下一项或多项：

- 决定不启动或停止实施有风险的活动来避免风险；

- 承担或增加风险以追求机会；
- 消除风险源；
- 改变可能性；
- 改变后果；
- 分担风险（例如通过合同，购买保险）；
- 通过明智的决策保留风险。

选择风险应对的理由，不仅要单纯的考虑成本，应该考虑到组织的所有义务，自愿承诺和利益相关方的观点。风险应对备选方案的选择应根据组织的目标、风险准则和可用资源来进行。

在选择风险应对备选方案时，组织应考虑价值观、认知和潜在涉及的利益相关方，以及与他们沟通和咨询的最佳方式。尽管效果相同的方案，利益相关方也可能有所偏好。

即使经过精心设计和实施，风险应对方案可能达不到预期的效果，而且可能产生预料之外的后果。监督和审查需要成为风险应对方案实施的一个组成部分，以保证不同形式的应对方案持续有效。

风险应对还可能引入需要管理的新风险。

如果没有合适的应对方案或应对方案没有充分改变风险，则应记录风险并持续进行评估。

决策者和其他利益相关方应了解风险应对后剩余风险的特征和水平。剩余风险应形成记录文件并进行监测、审查、并酌情进一步处理。

6.5.3 准备和实施风险应对计划

风险应对计划的目的是明确选择如何实施应对方案，从而让相关人员了解安排情况，并对照计划进行监测。应对计划应明确确定实施风险应对方案的顺序。

应对计划应与适当的利益相关方咨询，并纳入组织的管理计划和流程。

应对计划中提供的信息应包括：

- 选择应对方案的理由，包括获得的预期效益；
- 负责批准和实施计划的人员；

- 建议的行动；
- 所需资源，包括意外事件；
- 绩效评估；
- 约束；
- 所需的报告和监测；
- 何时开始和结束。

6.6 监督和审查

监督和审查的目的是保证和提升流程设计、实施和结果的质量和有效性。在最开始规划风险管理流程时，应该将持续监督和定期审查作为其中的一部分内容，明确界定其职责。

流程的所有阶段都应该进行监督和审查。监督和审查包括计划、收集和分析信息、记录结果和提供反馈。

监督和审查的结果应纳入整个组织绩效的管理、评估和报告等活动中。

6.7 记录和报告

应通过适当的机制记录和报告风险管理流程及其成果。记录和报告的目的是：

- 在整个组织内传达风险管理的活动和成果；
- 为决策提供信息；
- 改进风险管理活动；
- 协助与利益相关方的互动，包括对风险管理活动负有责任的相关方。

应考虑有关创建、保存和处理记录信息的决策包括但不限于：使用信息的敏感性以及内外部环境。

报告是组织治理的一个组成部分，应提高与利益相关方的沟通质量，并支持高级管理层和监督机构履行其职责。报告要考虑的因素包括但不限于：

- 不同利益相关方及其具体的信息需求和要求；
- 报告的成本、频率和时效性；

- 报告的方法；
- 报告信息与组织目标和决策的相关性。