国际标准

BS ISO 31000:2018

ISO 31000

Second edition
2018-02-15

风险管理-指引

风险管理-指导方针（法语）

参考序号
ISO31000:2018(E)

版权保护的文件

ISO 版权办公室
Ch.de Blandonnet 8•CP 401
CH-1214 维尼耶，日内瓦，瑞士
电话:+41 22 749 01 11
传真+41 22 749 09 47
copyright@iso.org
www.iso.org

内容

前言

国际标准化组织（ISO）是各国标准化团体(ISO 成员团体)组成的世界性的联合会。制定国际标准的工作通常由 ISO 技术委员会完成。各成员团体若对某技术委员会确定的项目感兴趣，均有权参加该委员会的工作。与 ISO 保持联系的各国际组织（官方或非官方的）也可参加有关工作。ISO 与国际电工委员会(IEC)在所有电工技术标准化方面保持密切合作。

ISO/IEC 指令第 1 部分描述了开发本文档的程序以及进一步维护该文档的程序。特别应注意的是，不同类型的 ISO 文件需要不同的批准标准。本文件是根据 ISO/IEC 指令第 2 部分的编辑规则起草的(参见 www.iso.org/directive)。

需要注意的是，本文件的某些内容可能拥有专利权。ISO 不负责识别任何或所有此类专利权。在文件制定过程中确定的任何专利权利的详细信息将在引言和/或收到的 ISO 专利声明清单中(参见 www.iso.org/patent)。

本文件中使用的任何商业名称都是为了方便用户而提供的信息，并不等同于完全认可。

有关标准的自愿性质的解释，与合格评定有关的 ISO 特定术语和表达的含义，以及 ISO 在技术性贸易壁垒 (TBT) 中遵守世界贸易组织 (WTO) 原则的信息，请参阅以下网址：www.iso.org/iso/foreword.html。

本文件由 ISO/TC 262 技术委员会风险管理工作组编制。

第二版取代替换了经过技术修改的第一版(ISO 31000:2009)。

与上一版相比，主要变化如下:

- ------审查风险管理原则，这是其成功的关键标准;
- ------从组织的治理入手，强调由最高管理者领导力和风险管理的整合;
- ------更加强调风险管理的迭代性质，注意到新的经验、知识和分析结果可以帮助修正流程中每个阶段的要素、操作和控制;
- ------简化内容，更注重维持开放的系统模型以适应多种需求和不同环境。

介绍

本文档适用于通过管理风险、制定决策、设定和实现目标以及提高绩效来为组织创造和保护价值的人员使用。

所有类型和规模的组织都面临着外部和内部的因素和影响，这些因素和影响使其不确定能否实现目标。

风险管理是迭代的，它帮助组织制定战略、实现目标以及做出明智决定。

管理风险是治理和领导力的一部分，是决定所有级别的组织如何管理的基础。它有助于改进管理系统。

管理风险是组织所有活动的一部分，包括与利益相关者的互动。

管理风险需考虑组织的外部和内部环境，包括人类行为和文化因素。

风险管理应基于本文档中概述的原则、框架和流程，如图 1 所示。这些元素可能已经全部或部分存在于组织中，但是，它们可能需要进行调整或改进，以便风险管理是高效、有效且一致的。

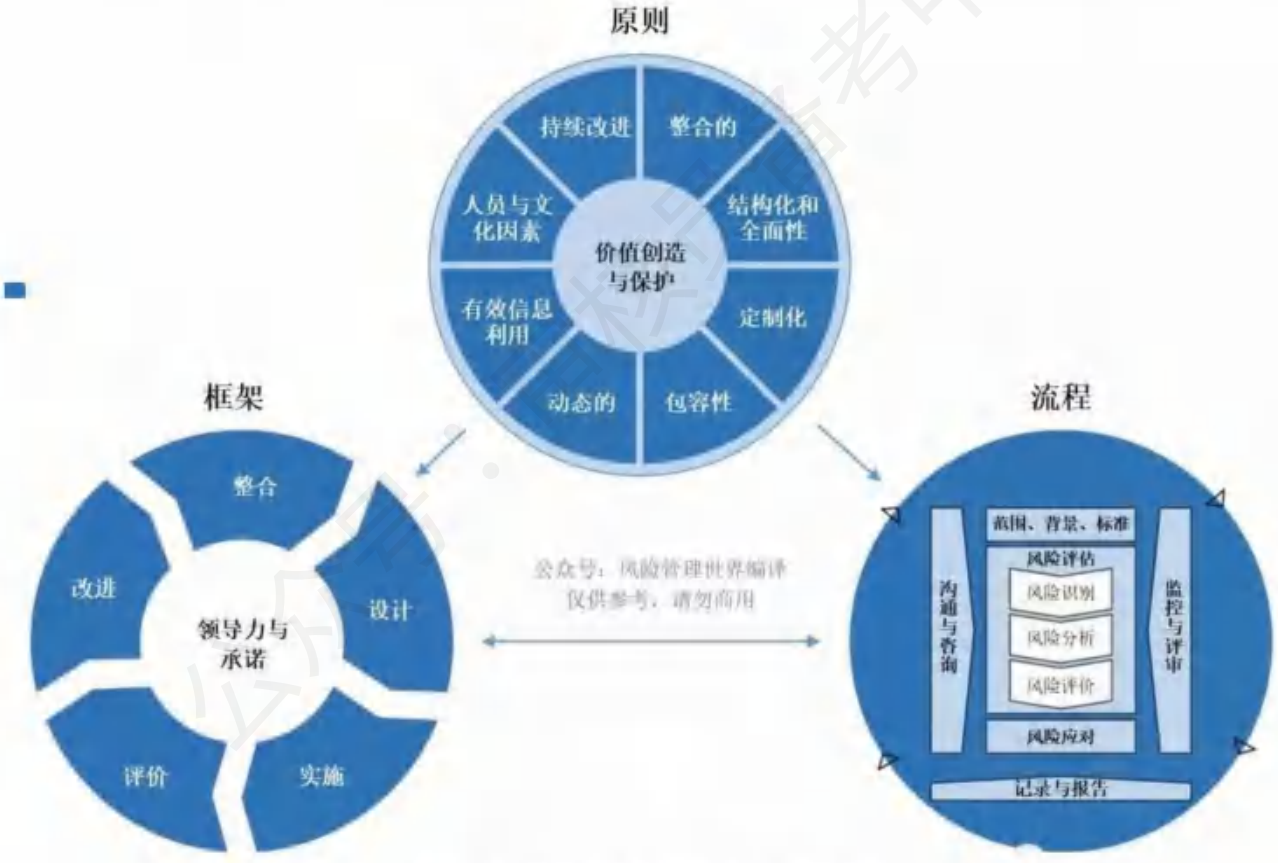

图 1 -原则、框架和流程

本页故意留空

风险管理-指引

1 范围

本文档提供了组织所需面对风险管理的指导方针。 这些指导方针的应用可以根据任何组织及其背景进行定制。
本文档为管理任何类型的风险提供了通用方法，并不是仅限于行业或行业特定的。
本文档可在组织的整个生命周期内使用，并可应用于任何活动，包括各级决策。

2 规范性参考文献

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，以下术语和定义适用。
ISO 和 IEC 标准化术语数据库，在以下地址可找到:

- - - - - - ISO 在线浏览平台:可从 http://www.iso.org/obp 获取

- - - - - - IEC Electropedia:可从 http://www.electropedia.org 获取

3.1 风险

不确定性对目标的影响

注 1：影响是与预期结果的偏差。它可能是积极的、消极的或可能两者兼有，同时将产生或伴随着机遇与威胁。
注 2：目标可以有不同的方面与类别，可以在不同层面上进行应用。
注 3：风险通常被描述为“风险资源”（3.4），“可能性事件”（3.5），“后续影响”（3.6），“可能性”（3.7）。

3.2 风险管理

协调风险管理活动，指导和控制组织的风险(3.1)

3.3 利益相关方

对一个决策或活动可以产生影响、受其影响或认为自己受到影响的组织或个人。

注 1:“利害相关方”一词可用作替代“利益相关方”。

3.4 风险源

有潜在可能引起风险(3.1)的单独或组合的要素。

3.5 事件
特定情况的发生或者变化。
注 1:一个事件可以有一个或多个事件发生，并且可以有多个原因和多个后果(3.6)。

注 2:事件也可以是预期的未发生事件，或未预期的发生事件。

注 3:事件可能是风险来源。

3.6 后果
事件(3.5)影响目标的结果

注 1:后果可以是确定的或不确定的，可以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:任何后果都可以通过级联和累积效应逐步升级。

3.7 可能性
某些事情发生的几率
注 1:在风险管理(3.2)术语中，“可能性”一词指的是事件发生的几率，不论是客观地还是主观地、定性地还是定量的地去定义、测量或确定，并且使用通用的的术语或数学方法描述的(例如在给定的时间段内的概率或频率)。
注 2:英文“可能性”一词在某些语言中没有直接的对应词;相反，通常使用“概率”这个词。然而，在英语中，“概率”通常被狭义地解释为一个数学术语。因此，在风险管理术语中，“可能性”的一词应该与“概率”一词在除了英语之外的其他语言中拥有相同的广泛解释。

3.8 可控制
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/或调整风险的任何过程、策略、设备、实践或其他条件和/或行动。

注 2:控制可能并不总是发挥预期的或假定的调整效果。

4 原则

风险管理的目的是创造和保护价值。它提高了绩效，鼓励创新并支持目标实现。

图 2 中概述的原则指出了有效和高效地风险管理的工作特点，并为其提供指导，同时传达了风险管理的价值并阐明了其目标。这些原则是管理风险的基础，在建立组织的风险管理框架和流程时应该予以考虑。组织可使用这些原则来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包含图 2 中的要素，可以进一步解释如下。

a)集成

风险管理是组织的所有活动的组成部分。

b) 结构化的和全面化

结构化和全面的风险管理方法有助于取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定制的，并且应根据其组织与目标相关的外部和内部环境来定制。

d) 包容性

利益相关方的适当且及时的参与，以使他们的知识、观点和看法得以融入进来。 这可以使其提高意识，且进行明智的风险管理。

利益相关者的适当和及时参与可以使他们的知识，观点和看法得到考虑。 这样可以提高意识并进行明

e) 动态的

随着组织外部和内部环境的变化，风险可能出现、改变或消失。风险管理以适当和及时的方式预测、监控、掌握和响应这些变化和事件。

f) 最佳可得到信息

风险管理的输入基于历史和当前的信息，以及未来的预期。风险管理明确考虑到与此类信息和预期相关的任何限制和不确定性。信息应及时地、清晰地提供给相关的利益相关方。

g) 人文因素

人类行为和文化在每个层次和阶段都对风险管理的各个方面产生重大影响。

h) 持续改进

通过学习和经验，不断提高风险管理水平。

5 框架

5.1 总则

风险管理框架的目的是帮助组织将风险管理整合到重要的活动和职能中。风险管理的有效性将取决于它能否被整合到组织治理和决策中区，这需要利益相关方，尤其是最高管理层的支持。框架开发围绕整个组织中风险管理的整合、设计、实施、评价和改进。图三表明整个框架的构成。

图 3 -框架

组织应评估其现有的风险管理实践和流程，评估任何缺陷，并在框架内解决这些缺陷。

框架的构成部分及其协同工作方式应根据组织的需求进行定制。

5.2 领导力和承诺

在适当情况下，高级管理层和监督机构应确保将风险管理纳入所有组织活动，并通过以下方式显示领导能力和承诺:

- 定制和实现框架的所有构建;
- 发布风险管理的方法、计划或行动方针的声明或政策;
- 确保分配必要的资源以管理风险;
- 以适当的分级方式在组织内分配权力，责任和问责机制。。

这将有助于本组织:

- 使风险管理与其目标、战略和文化保持协同;
- 自愿承诺履行其认知内的义务;
- 确定风险的数量和类型，以指导风险标准的制定，确保将风险标准传达给组织及其利益相关方;
- 将风险管理的价值传达给组织及其利益相关方;
- 促进对风险的系统性监测;
- 确保风险管理框架仍然适合组织的环境。

最高管理层负责管理风险，而监督机构负责监督风险管理。监督机构经常被期望或要求:

- 确保在设定组织目标时充分考虑到风险;
- 了解组织在追求目标时所面临的风险;
- 确保管理此类风险的系统得到有效实施和运行;
- 确保在组织目标的背景下这些风险中是适当的;
- 确保正确传达有关此类风险及其管理的信息。

5.3 整合

风险管理依赖于对组织结构和环境的理解。结构因组织的目的、目标和复杂性而异。组织结构的每个部分都应进行风险管理。组织中的每个人都有管理风险的责任。

治理指导组织的过程，其外部和内部关系，以及实现其目的所需的规则、流程和实践。管理结构将治理方向转换为实现预期的可持续提高绩效和长期生存能力所需的战略和相关目标。确定组织内的风险管理责任和监督角色是组织治理的组成部分。

将风险管理集成到组织中是一个动态的迭代过程，应该根据组织的需求和文化进行定制。风险管理应该是组织目标、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，组织应该审查并理解其外部和内部的环境。

审查组织的外部环境可能包括但不限于:

- 国际、国家、区域或地方的社会、文化、政治、法律、监管、金融、技术、经济和环境因素;
- 影响本组织目标的关键驱动要素和趋势;
- 外部利益相关者的关系、看法、价值观、需求和期望;
- 合同关系和承诺;
- 网络和归属的复杂性。

审查本组织的内部背景可能包括但不限于:

- 理想、使命和价值观;
- 治理、组织结构、角色和责任;
- 战略、目标和政策;
- 组织的文化;
- 本组织采用的标准、准则和模型;
- 在资源和知识方面(如资本、时间、人员、知识产权、流程、系统和技术)的理解能力;
- 数据、信息系统和信息流;
- 与内部利益相关者的关系，考虑他们的看法和价值观;
- 合同关系和承诺;
- 相互依赖和相互联系。

5.4.2 明确风险管理承诺

最高管理层和监督机构应以声明或其他形式，明确地传达组织目标和风险管理承诺，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及其与目标和其他政策的联系;
- 加强将风险管理融入组织整体文化的必要性;
- 将风险管理融入核心业务活动和决策;
- 权力、责任和问责机制;
- 提供必要的资源;
- 处理冲突目标的方式;
- 在组织的绩效指标内进行衡量和报告;

------评估和改进。

风险管理承诺应该在组织内部和利益相关方之间适当沟通的基础上达成。

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：

------强调风险管理是一项核心责任;

------确定有管理风险责任和权力的个人(风险所有者)。

5.4.4 资源分配

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，这些资源可以包括但不限于:

------人员、技能、经验和能力;

------组织用于管理风险的过程、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。

组织应该考虑现有资源的能力和限制。

5.4.5 建立沟通和咨询渠道

为支持风险管理的框架，并促进风险管理的有效应用，该组织应建立沟通和咨询的渠道。沟通包括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。沟通和咨询的方法和内容应反映相关利益相关方的期望。

沟通和咨询应当及时进行，确保相关信息的收集、整理、汇总和共享，并提供反馈以期改进。

5.5 实施

组织应透过以下方式实施风险管理框架:

------制定适当的计划，包括时间计划和资源配置计划;

------确定在整个组织中什么地点、什么时间以及由谁做出、如何做出不同类型的决策;

------必要时修改决策流程以适用;

------确保组织管理风险的安排被清楚地理解和实施。

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，同时确保出现的任何新的或后续的不确定性都被考虑在内。
正确地设计和实施风险管理框架，将确保风险管理过程是整个组织中所有活动(包括决策制定)的一部分，并且将充分考虑到到内外部环境的变化。

5.6 评价

为了评估风险管理框架的有效性，组织应该:
- - - - - - 根据目标、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持本组织目标的实现。

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，以应对外部和内部的变化。如此，组织可提高自身价值。

5.7.2 持续改进
组织应不断改进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。
如果发现相关的缺陷或改进机会，组织应制定计划和任务，并将其分配给负责实施的人员。一经实施，这些改进措施将有助于加强风险管理的作用。

6 流程

6.1 总则

风险管理流程包括系统地将政策、程序和实践应用于沟通和咨询，建立环境和评估、处理、监测、审查、记录和报告风险的活动。这个过程如图 4 所示。

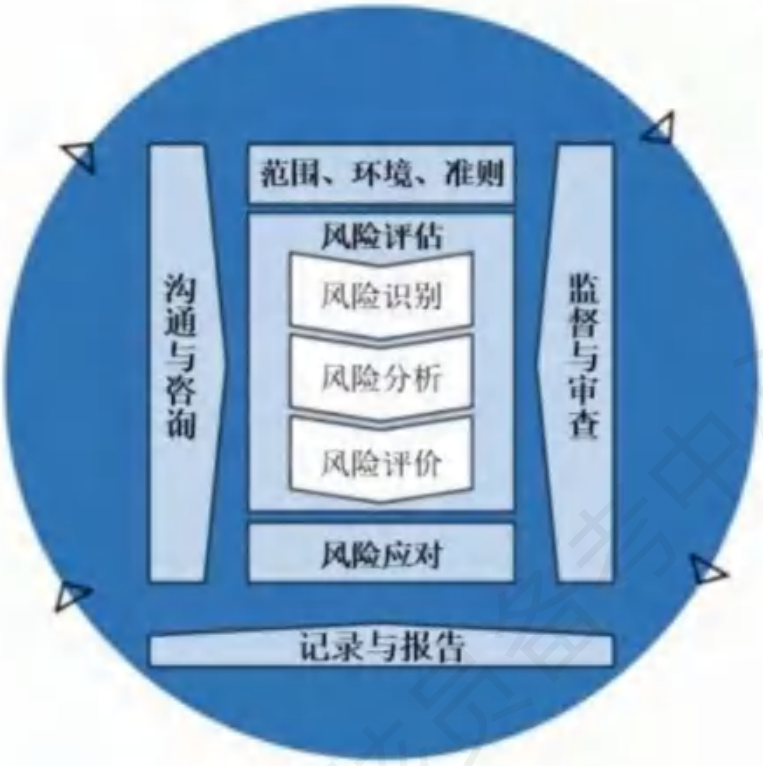

图 4 -流程

风险管理流程应该是管理和决策的组成部分，并融入进组织的结构、运营和流程。它可应用于战略、运营、方案或项目等层面。

组织中可能有许多风险管理流程的应用程式，这些应用程式是为实现目标而定制的，并且适用于其内外部环境。

在整个风险管理流程中，都应考虑到人类行为和文化的动态性和变化性。

尽管风险管理流程通常表现为有一定的顺序性，但在实践中流程步骤可以是循环反复的。

6.2 沟通和咨询

沟通和咨询的目的是为了帮助利益相关方理解风险、明确决策的基础以及需要采取特定行动的原因。沟通旨在提高对风险的认识和理解，而咨询涉及到获得反馈和信息以支持决策。两者之间的密切协调应促成真实、及时、相关、准确和可理解的信息交流，同时考虑到信息的保密性和完整性以及个人的隐私权。在风险管理流程的所有步骤中以及整个过程中，应与适当的外部和内部利益相关方进行沟通和咨询。

沟通和咨询的旨在:

- ---- 为风险管理过程的每个步骤提供不同领域的专业知识;
- ---- 在定义风险标准和评估风险时，确保适当考虑不同的观点;
- ------ 提供足够的信息以促进风险监督和决策;

- - - - - - 在受风险影响的人群中建立一种集体感和主人翁意识。

6.3 范围、环境和标准

6.3.1 总则

确定范围、背景和标准的目的是有针对性的设置风险管理流程，从而实现有效的风险评估和恰当的风险应对。范围、环境和标准涉及到界定流程的范围，且理解外部和内部环境。

6.3.2 定义范围

组织应确定其风险管理活动的范围。

由于风险管理过程可能适用于不同的级别(例如战略、运营、方案、项目或其他活动)，因此必须要清楚考虑的范围、要考虑的相关目标以及它们与组织目标的一致性。

在规划方法时，需考虑因素包括:

- - - - - - 需要制定的目标和决定;
- - - - - - 对流程中各步骤的预期结果;
- - - - - - 时间、地点、具体包含的和应排除的要素;
- - - - - - 适当的风险评估工具和技术;
- - - - - - 需要的资源、责任和记录;
- - - - - - 与其他项目、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目标的基础。

外部和内部环境的

风险管理流程的背景应该建立在对组织运营的外部和内部环境的理解之上，并应反映风险管理流程中适用活动的具体环境。

理解其背景非常重要，因为:

- ---------风险管理在组织的目标和活动范围内进行;
----------组织因素可能是风险来源;
- - - - - - 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。

组织应通过考虑 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 定义风险标准

组织应明确与目标相关的可能发生或不发生的风险的数量和类型。还应该定义评估风险重要性和支持决策过程的标准。风险标准应与风险管理框架保持一致，并根据相应活动的具体目的和范围进行定制。风险标准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。标准的定义应该考虑到组织的义务和利益相关方的观点。

虽然风险标准应在风险评估过程开始时就确定，但它们是动态的，如有必要，应不断加以审查和修订。

制定风险标准时，应考虑以下因素:

- - - - - - 可能影响结果和目标(有形和无形)的不确定性的性质和类型;
- - - - - - 如何定义和度量后果(正面和负面)和可能性;
- - - - - - 有关时间的因素;
- - - - - - 测量方法使用的一致性;
- - - - - - 如何确定风险等级;
- - - - - - 如何考虑多重风险的组合和顺序;
- - - - - - 组织的能力。

6.4 风险评估

6.4.1 总则

风险评估是风险识别、风险分析和风险评估的整个过程。

风险评估应该借鉴利益相关方的知识和观点，以系统地、迭代地且协作地方式进行。它应使用现有的最佳资料，并在必要时辅以进一步调查。

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。对于风险识别而言，准确的最新相关信息是非常重要的。

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;
- ------威胁和机遇;
------- 漏洞和能力;
---------外部和内部环境的变化;
-------- 新出现的风险指标;
-------- 资产和资源的性质和价值;
-------- 后果及其对目标的影响;
---------认知和信息可靠性的限制;
---------与时间有关的因素;
--------- 参与人员的偏见，假设和信仰。

组织应识别风险，无论其来源是否在其控制之下。应考虑到可能存在多种类型的结果，这可能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适当的风险水平在内的风险性质及其特征。风险分析涉及对不确定性、风险来源、后果、可能性、事件、场景、控制及其有效性的详细考虑。一个事件可能有多种原因和后果，并可能影响多个目标。

可以根据分析的目的、信息的可用性和可靠性以及可用的资源，以不同程度的详细度和复杂度进行风险分析。根据具体情况和预期用途，分析技术可以是定性的、定量的，也可以两者兼而有之。

风险分析应考虑以下因素：

- - - - - - 事件和后果的可能性；

- - - - - - 后果的性质和严重程度；

- - - - - - 复杂性和连通性；

- - - - - - 与时间相关的因素和波动性；

- - - - - - 现有控制措施的有效性；

- - - - - - 敏感性和信心水平。

风险分析可能受到任何意见分歧、偏见、对风险的看法和判断的影响。其他影响因素包括所使用信息的质量、所做的假设和排除、技术的任何限制以及执行方式。应该考虑这些影响，并将其记录传达给决策者。

高度不确定的事件很难量化。在分析具有严重后果的事件时，这将会是个难点。在这种情况下，使用技术组合通常会提高分析者的洞察力。

风险分析为风险评估、风险是否需要处理、如何处理以及最适合的风险应对策略和方法的决策提供了参考。对不同类型和不同级别的风险应在何时做出选择的决策制定，分析结果提高了决策者的洞察力。

6.4.4 风险评估

风险评估的目的是支持决策。风险评估涉及将风险分析的结果与已确定的风险标准进行比较，以确定需要采取哪些额外行动。这可能导致一个决定：

- - - - - - 什么都不做；

- - - - - - 考虑风险处理方案；

- - - - - - 进行进一步的分析，以更好地了解风险；

- - - - - - 维持现有控制；

- - - - - - 重新考虑目标。

决策应考虑到更广泛的背景，以及外部和内部利益相关方的实际及预期后果。

应在组织的适当级别记录、传达和验证风险评估的结果。

6.5 风险应对

6.5.1 总则

风险应对的目的是选择和实施应对风险的方案。

风险应对涉及以下迭代过程:

- 制定和选择风险应对方案;
- 风险应对方案的规划和实施;
- 评估应对的有效性;
- 决定剩余风险是否可接受;
- 如果不能接受，采取进一步的应对。

6.5.2 风险应对方案的选择

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，风险处理方案不一定相互排斥或适用。

- 通过不开始或不继续引起风险的活动来避免风险;
- 为了寻求机会而承担或增加风险;
- 消除风险来源;
- 改变的可能性;
- 改变的后果;
- 分担风险(例如通过合同、购买保险);
- 以明智的决策来保留风险。

风险应对的原因不仅限于经济方面的考虑，还应考虑到组织的所有义务、自愿承诺和利益相关方的观点。应根据组织的目标、风险标准和现有资源，来选择风险应对的方案。

在选择风险应对方案时，组织应该考虑利益相关方的价值观、观念和潜在参与，以及与之沟通和咨询的最合适的方式。尽管同样有效，与其他人相比，一些利益相关方更容易接受某些风险应对方案。

风险应对即使经过精心设计和实施，也可能不会产生预期的结果，并可能产生意想不到的后果。监测和审查应当成为风险应对方案实施的一个必要部分，以确保不同形式的风险应对保持有效性。

风险应对方案还可能带来需要管理的新风险。

如果没有可用的应对方案或应对方案没有充分降低风险，则应记录该风险并对其进行持续监测。

决策者和其他利益相关者应该意识到风险处理后剩余风险的性质和程度。剩余风险应记录在案，并接受监测、审查，酌情考虑进一步的应对处理。

6.5.3 准备和实施风险应对计划

风险应对计划的目的是具体说明如何实施所选择的处理方案，以便有关人员了解安排，并监测计划的进展情况。应对计划应明确确定实施风险应对方案的顺序。

应与适当的利益相关方协商，将应对计划纳入组织的管理计划和流程中。

应对计划所应包含以下信息:

- 选择应对计划的理由，包括可获得的预期收益;
- 负责批准和实施计划的人员;
- 拟议的行动;
- 所需资源，包括意外情况;
- 结果的计量;
- 限制;
- 所需的报告和监测;
- 何时采取行动并完成。

6.6 监督和审查

监督和审查的目的是保证和提高流程设计、实施和结果的质量和有效性。对风险管理过程及其结果的持续监控和定期审查应是风险管理流程中计划的一部分，其职责应明确界定。

流程的所有阶段均应被监督和审查。监督和审查包括计划、收集和分析信息、记录结果并提供反馈。

监督和审查的结果应纳入整个组织的绩效管理、计量和报告活动。

6.7 记录和报告

应通过适当的机制来记录和报告风险管理的流程和结果。记录和报告旨在:

- 在整个组织内传达风险管理活动和成果;
- 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责的人。

有记录的信息的创建、保留和处理的决定应考虑到，但不限于:它们的使用、信息敏感性以及外部和内部环境。

报告机制是组织治理的一个组成部分，应该提高与利益相关方的对话质量，并支持最高管理层和监督机构履行其职责。报告需要考虑的因素包括但不限于:

- 不同的利益相关方及其特定的信息需求和要求;
- 报告的成本、频率和及时性;
- 报告的方法;
- 信息与组织目标和决策的相关性。

参考书目

[1] IEC 31010，风险管理 - 风险评估技术