风险管理-原则和指南

引　　言

所有类型和规模的组织都面临内部和外部的、使组织不能确定是否及何时实现其目标的因素和影响。这种不确定性所具有的对组织目标的影响就是“风险”。

组织的所有活动都涉及风险。组织通过识别、分析和评定是否运用风险处理修正风险以满足它们的风险准则，来管理风险。通过这个过程，它们与利益相关方进行沟通和协商，监测和评审风险，以及为确保不再进一步需求风险处理而修正风险的控制措施。本国际标准详细描述了这一系统的和逻辑的过程。

尽管所有的组织在某种程度上都在管理风险，本国际标准建立了一些为使风险管理变得有效而需要满足的原则。本国际标准建议，组织制定、实施和持续改进一个框架，其目的是将风险管理过程整合到组织的整体治理、战略和规划、管理、报告过程、方针、价值观和文化中。风险管理可以在组织多个领域和层次、任何时间，应用到整个组织，以及具体职能、项目和活动。

尽管在过去一段时间在许多行业，为满足不同的需要，已经开展了风险管理实践，但在一个综合框架内采用一致性过程有助于确保在组织内有效、有效率和结合性地管理风险。本国际标准中所描述的通用方法提供了在任何范围和状况下，以系统、清晰、可靠的方式管理风险的原则和指南。

每一个具体行业或风险管理的应用都产生了各自的需求、受众、观念和准则。因此，本国际标准的主要特点是将所包含“确定状况”作为通用风险管理过程开始的活动。确定状况将捕获组织的目标，组织所追求目标的环境，组织的利益相关方和风险准则的多样性，所有这些都将帮助揭示和评价风险的性质和复杂性。

本国际标准描述的风险管理原则、框架和风险管理过程之间的关系，如图 1 所示。

当依据本国际标准实施和保持风险管理时，能够使组织，例如：

—— 提高实现目标的可能性；

—— 鼓励主动性管理；

—— 在整个组织意识到识别和处理风险的需求；

—— 改进机会和威胁的识别能力；

—— 符合相关法律法规要求和国际规范；

—— 改进强制性和自愿性报告；

—— 改善治理；

—— 提高利益相关方的信心和信任；

—— 为决策和规划建立可靠的根基；

—— 加强控制；

—— 有效地分配和利用风险处理的资源；

—— 提高运营的效果和效率；

—— 增强健康安全绩效，以及环境保护；

—— 改善损失预防和事件管理；

—— 减少损失；

—— 提高组织的学习能力

—— 提高组织的应变能力

本国际标准旨在满足众多利益相关方的需求，包括：

a）负责制定组织风险管理方针的人员；

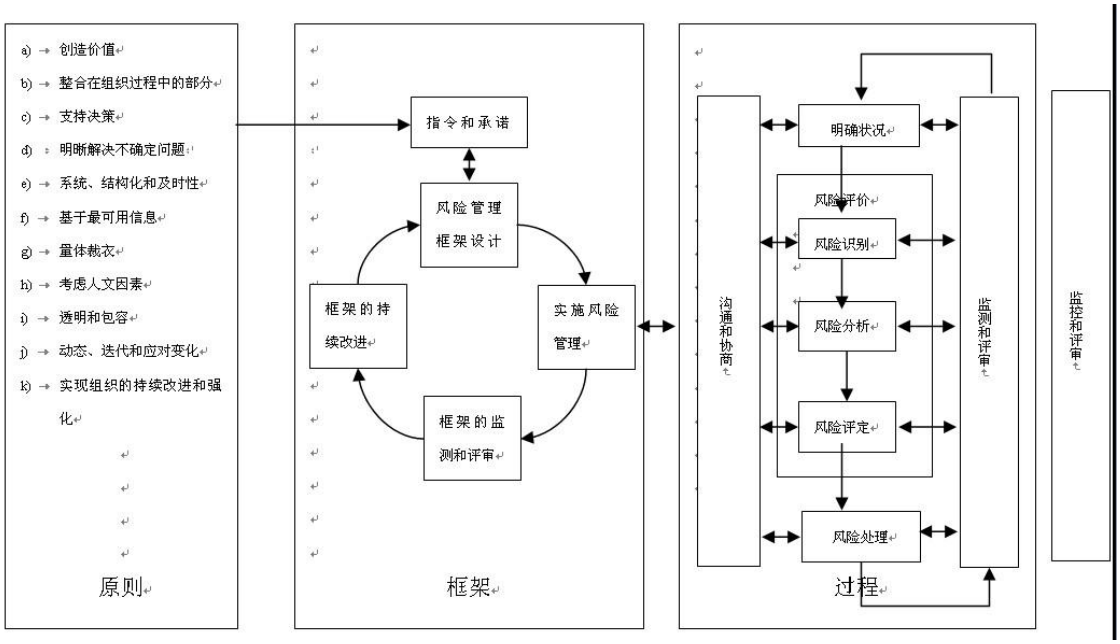
b）负责确保在组织整体、或者某一特定区域、项目或者活动内有效开展风险管理的人员；

c）需要评定组织风险管理有效性的人员；

d）整体或部分地实施风险管理的标准、指南、程序和操作规范的开发者。

目前许多组织的管理实践和过程包含了风险管理的要素，许多组织针对特定类型的风险或环境下已经采用了正式的风险管理过程。在这种情况下，组织可以决定对照本国际标准对其现有的实践和过程开展严格的评审。

在本国际标准中，“风险管理（risk management）”和“管理风险（managing risk）”都在使用。在通常的术语意义上，“风险管理（risk management）”涉及的有效管理风险的构架（原则，框架和过程），而“管理风险（managing risk）”指的是运用该架构管理特定风险。



图表 1 风险管理原则、框架、过程之间的关系

1 范围

本国际标准提供了风险管理的原则和通用性指南。

本国际标准可用于任何公共、私有或公有企业、协会，团体或个体。因此，本国际标准不针对任何特定行业或部门。

注：为方便起见，本国际标准涉及的所有不同的用户以通用术语“组织”称谓。

本国际标准可用于整个组织的生命周期及广泛的活动，包括战略和决策、运营、过程、职能、项目、产品、服务和资产。

本国际标准可以应用于任何类型的风险，无论其性质及是否有积极或消极的后果。

尽管本国际标准提供了风险管理的通用性指南，但不意针对组织促进风险管理的统一性。风险管理计划和框架的设计和实施需要考虑到特定组织的不同需求、特定目标，状况、结构、运营、过程、职能、项目、产品、服务、或资产以及展开的具体实践。

意在运用本国际标准来协调现有和将来标准的风险管理过程。本标准提供了一个支持其他标准处理特定风险和行业风险的通用方法，而不是取代这些标准。

本国际标准不意针对认证意图。

2 术语和定义

下列术语和定义适用本标准。

2.1 风险 risk

不确定性对目标的影响

注 1：影响是与期待的偏差——积极和/或消极

注 2：目标可以有不同方面（如财务、健康安全、以及环境目标），可以体现在不同的层次（如战略、组织范围、项目、产品和过程）。

注 3：风险通常以潜在事件（2.19）和后果（2.20），或它们的组合来描述。

注 4：风险通常以事件（包括环境的变化）后果和发生可能性（2.21）的组合来表达。

注 5：不确定性是指，与事件和其后果或可能性的理解或知识相关的信息的缺陷的状态，或不完整。

[ISO 导则 73:2009, 定义 1.1]

2.2 风险管理 risk management

针对风险指挥和控制组织的协调活动。

[ISO 导则 73:2009, 定义 2.1]

2.3 风险管理框架 risk management framework

提供在组织内设计、实施、监测（2.28）、评审和持续改进风险管理（2.2）的基本原则和

组织安排的要素集合。

注 1：基本原则包括管理风险的方针、目标、指令和承诺。

注 2：组织安排包括计划、关系、责任、资源、过程和活动。

注 3：风险管理框架被嵌入到组织的整个战略和运营的方针和实践中

[ISO 导则 73:2009, 定义 2.1.1]

2.4 风险管理方针 risk management policy

一个组织对风险管理的意图和方向的陈述。

[ISO 导则 73:2009, 定义 2.1.2]

2.5 风险态度 risk attitude

组织评价、最终追踪、保留、消除或规避风险的方法。

[ISO 导则 73:2009, 定义 3.7.1.1]

2.6 风险管理计划 risk management plan

在风险管理框架内规定用于风险管理的方法、管理要素、资源的方案。

注 1：管理要素一般包括程序、惯例、职责分配、活动顺序和时间安排。

注 2：风险管理计划可应用于特定的产品、过程和项目、组织的部分或整体。

[ISO 导则 73:2009, 定义 2.1.3]

2.7 风险所有者 risk owner

具有风险管理权限和责任的个人或实体。

[ISO 导则 73:2009, 定义 3.5.1.4]

2.8 风险管理过程 risk management process

管理方针、程序和惯例对沟通、协商、确定状况、以及识别、分析、评价、处理、监测和评审风险活动的系统应用。

[ISO 导则 73:2009, 定义 3.1]

2.9 确定状况 establishing the context

界定外部和内部参数，以便在管理风险和设置风险管理方针的范围及风险准则时，予以考虑。

[ISO 导则 73:2009, 定义 3.3.1]

2.10 外部状况 external context

组织寻求实现其目标的外部环境。

注：外部环境可包括：

—— 文化、社会、政治、法律法规、财政金融、技术、经济、自然和竞争环境，无论国际、国家、区域或地方

—— 对组织目标具有影响的主要驱动和趋势。

—— 与外部利益相关方的关系和其感受和价值观。

[ISO 导则 73:2009,定义 3.3.1.1]

2.11 内部状况 internal context

组织寻求实现其目标的外部环境。

注：内部状况可包括：

—— 治理、组织结构、作用和责任；

—— 方针、目标、以及实现它们的战略；

—— 以资源和知识来理解的能力（如资本、时间、人员、过程、系统和技术）；

—— 信息系统、信息流和决策过程（正式和非正式的）；

—— 与内部利益相关方的关系、以及他们的感受和价值观；

—— 组织的文化；

—— 标准、指南和组织采用的模式；

—— 合同关系的形式和范围

[ISO 导则 73:2009,定义 3.3.1.2]

2.12 沟通和协商 communication and consultation

组织针对风险管理，提供、共享或获取信息，与利益相关方进行对话的持续和反复的过程。

注 1：信息涉及风险管理的存在、性质、形式、可能性、严重程度、评定、可接受性、处理。

注 2：协商是组织与它的利益相关方，在做出决策或确定某一问题的方向前，针对问题双向有事实依据的沟通的过程。协商是：

—— 通过影响力而非权力对决策施加影响；

—— 作为决策的输入，而非加入决策。

[ISO 导则 73:2009, 定义 3.2.1]

2.13 利益相关方 stakeholder

可以影响、被影响、或者觉得自己会被决策或活动影响的个人或组织。

注：决策者可以是利益相关者。

[ISO 导则 73:2009, 定义 3.2.1.1]

2.14 风险评价 risk assessment

风险识别（2.15）、风险分析（2.21）和风险评定（2.24）的整个过程。

[ISO 导则 73:2009, 定义 3.4.1]

2.15 风险识别 risk identification

发现、认识、描述风险的过程。

注 1：风险识别包括风险源（2.16）、事件（2.17）、它们的起因及潜在后果的确定。

注 2：风险识别会涉及历史数据、技术分析、有事实依据的和专家的观点、以及利益相关方的需求。

[ISO 导则 73:2009, 定义 3.5.1]

2.16 风险源 risk source

单独地或以结合的形式具有产生风险的内在可能性的因素。

注：一个风险源可以是有形的或者无形的。

[ISO 导则 73:2009,定义 3.5.1.1]

2.17 事件 event

特殊系列环境的产生或变化。

注 1：.一个事件可以是一个或多个事变，会有多种原因。

注 2：事件可以由一些不发生的事情构成。

注 3：事件有时被称作“事件（incident）”或“事故（accident）”。

注 4：.没有后果的事件可以被称作“near miss”、“incident”、“near hit” 、 “close call”。

[ISO 导则 73:2009, 定义 3.5.1.2]

2.18 后果 consequence

事件对目标的影响结果。

注 1：一个事件可以产生一系列的后果。

注 2：后果可以是确定或不确定的，以及对目标具有积极或消极的影响。

注 3：后果可以被定性或定量地表述。

注 4：初步的后果通过连锁效应可以逐步升级。

[ISO 导则 73:2009, 定义 3.6.1.3]

2.19 可能性 likelihood

某事发生的机会。

注 1：在风险管理术语学中，“可能性”是指事情发生的机会，不论是明确的、测量的，还是客观或主观地、定性或定量地确定的，以及一般性或精确地描述（如在一定时段内的可能性和频率）。

注 2：英文“likelihood”在一些语言中没有直接对应的等同词，而同义词“probability”经常被使用。然而，在英文中，“probability”通常被狭义地理解为数学术语。因此，在风险管理术语学中，“likelihood”以它在许多非英语国家语言中的“probability”所具有的同样的广泛理解来使用。

[ISO 导则 73:2009, 定义 3.6.1.1]

2.20 风险状况 risk profile

任何系列风险（2.1）的描述。

注：该系列风险可包含与整个组织、组织的部分或者其他特定部分相关联的风险。

[ISO Guide 73:2009, definition 3.8.2.5]

2.21 风险分析 risk analysis

理解风险（2.1）的性质和确定风险程度（2.23）的过程。

注 1：风险分析为风险评定和风险处理决策提供了基础。

注 2：风险分析包括风险估测。

[ISO 导则 73:2009, 定义 3.6.1]

2.22 风险准则 risk criteria

评价风险重要性的依据。

注 1：.风险准则基于组织的目标和内外部状况。

注 2：风险准则可出自于标准、法律、方针和其他要求。

[ISO 导则 73:2009, 定义 3.3.1.3]

2.23 风险程度 risk level

以后果和可能性的组合表达的风险的量或组合结果。

[ISO 导则 73:2009, 定义 3.6.1.8]

2.24 风险评定 risk evaluation

将风险分析的结果与风险准则进行比较，以确定风险和（或）其量是否可接受或可容许。

注：风险评定有助于有关风险处理的决策。

[ISO 导则 73:2009, 定义 3.7.1]

2.25 风险处理 risk treatment

修正风险的过程。

注 1：风险处理可包括：

—— 通过决定不启动或停止产生风险的活动而避免风险。

—— 为了追求机会采取或增加风险。

—— 消除风险源。

—— 改变可能性。

—— 改变后果。

—— 与其他方面共同分担风险（包括合同、风险融资）。

—— 通过有事实依据的决策保留风险。

注 2：对消极后果的风险处理有时可以称为“风险减缓（risk mitigation）”、“风险消除（risk eliminate）”、“风险预防（risk prevention）”和“风险减小（risk reduction）”。

注 3：风险处理可以产生新的风险或修正已存在的风险。

[ISO 导则 73:2009, 定义 3.8.1]

2.26 控制措施 control

修正风险的措施。

注 1：控制措施包括任何过程、方针、手段、惯例或其他修正风险的措施。

注 2：控制措施可能不总是产生预期或设想的修正效果。

[ISO 导则 73:2009, 定义 3.8.1.1]

2.27 残留风险 residual risk

风险处理后余留下的风险。

注 1：残留风险可包括未识别的风险。

注 2：残留风险也可被认作“保留的风险（retain risk）。

[ISO 导则 73:2009,定义 3.8.1.6]

2.28 监测 monitoring

不断检查、监督、严格观察或确定状态，以识别所要求或期待的绩效水平的变化。

注：监测可应用于风险管理框架、风险管理过程、风险或控制措施。

[ISO 导则 73:2009, 定义 3.8.2.1]

2.29 评审 review

为达到所建立的目标，确定有关事务的适宜性、充分性和有效性所采取的活动。

注：评审可应用于风险管理框架、风险管理过程、风险或控制措施。

[ISO 导则 73:2009, 定义 3.8.2.2]

3 原则

为了风险管理有效，组织宜在各个层次遵循以下原则。

a）风险管理创造和保护价值

风险管理有助于目标明确的实现和绩效的改进，例如，在人员的健康安全、治安、法律法符合性、公众接受性、环境保护、产品质量、项目管理、运营效率、治理和声誉方面。

b）风险管理是整合在所有组织过程中的部分

风险管理不是与组织的主要活动和过程分开的孤立活动。风险管理是管理职责的部分和整合在所有组织过程中的部分，包括战略规划、所有项目、变更管理过程。

c）风险管理支持决策

风险管理可以帮助决策者做出明智的选择、优先的措施和辨别行动方向。

d）风险管理明晰解决不确定问题

风险管理明确地阐述不确定性、不确定性的性质、以及如何加以解决。

e）风险管理具备系统、结构化和及时性

系统、及时和结构化的风险管理方法有助于提高效率和取得一致、可衡量和可靠的结果。

f）风险管理基于最可用的信息

风险管理过程的输入基于信息源，如历史数据、经验、利益相关方的反馈、观察、预测和专家判断。然而，决策者宜告诫自身和考虑，数据或所使用模型的局限性，或者专家之间分歧的可能性。

g）风险管理是量体裁衣的

风险管理是与组织的外部和内部状况及风险状况相匹配的。

h）风险管理考虑人文因素

风险管理认识到可以促进或阻碍组织目标实现的内部和外部人员的能力、观念和意图。

i）风险管理是透明和包容的

利益相关方、尤其是组织各层面的决策者适当、及时的参与，确保了风险管理保持相关和先进性。参与过程也允许利益相关方适当地发表意见，并将其观点考虑到风险准则的确定中。

j）风险管理是动态、迭代和应对变化的

风险管理持续察觉和响应变化。由于外部和内部事件发生，状况和知识在改变，风险的监测和评审在进行，新的风险出现，一些风险在改变，而另一些风险消失了。

k）风险管理实现组织的持续改进

组织宜制定和实施战略，协同组织的其他方面共同改进风险管理的成熟度。

附件 A 为希望更有效地实施管理风险的组织提供了进一步的建议。

4 框架

4.1 总则

风险管理的成功取决于提供将风险管理嵌入整个组织所有层次的基础和安排的管理框架的有效性。框架有助于通过在组织不同层次和特定状况内应用风险管理过程，有效地管理风险。框架确保从风险管理过程取得的风险信息充分地被报告，以及作为决策和所有相关组织层次责任的基础。

本条款描述了风险管理框架的必要要素和其以迭代的方式相互作用的方法，如图 2。

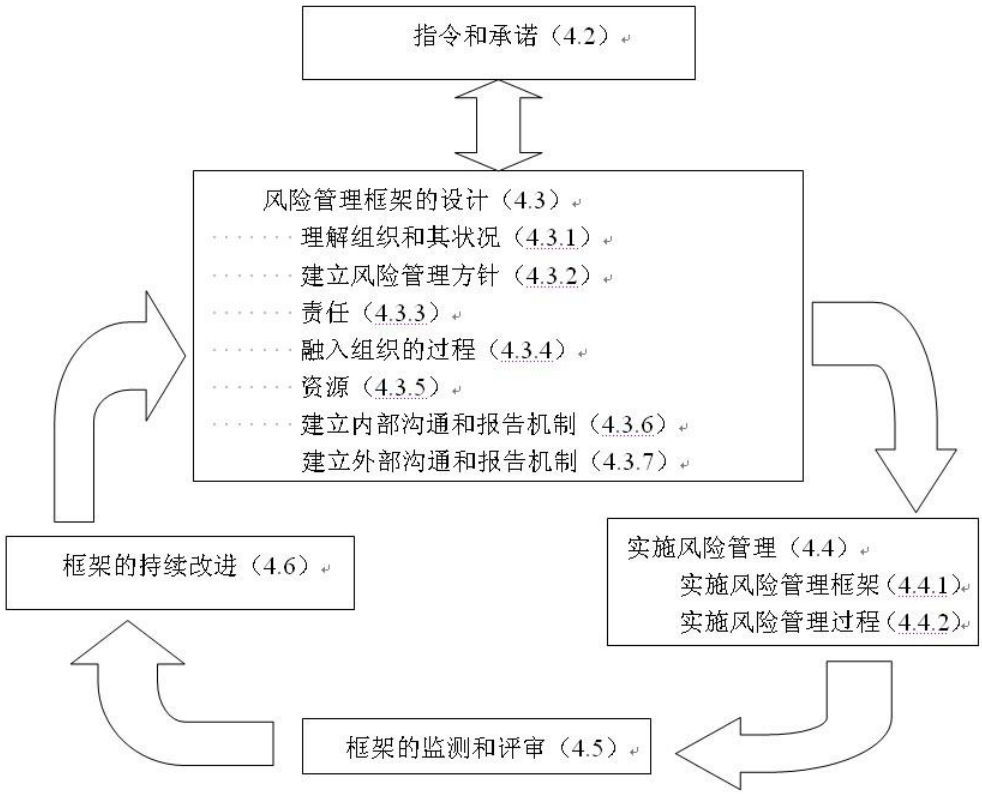


图 2　风险管理框架要素间的相互关系

本框架目的不是规定一个管理体系，而是有助于组织将风险管理整合到它的整个管理体系中。因此，组织宜使框架的要素适用于其特定的需求。

如果组织现存的管理实践和过程包含风险管理要素，或者如果组织已经针对特定的风险或状况采纳了一个正式的风险管理过程，那么对原有的这些实践和过程宜针对本标准进行评审和评价，包括附录 A 中包含的附加内容，以确定它们的充分性和有效性。

4.2 指令和承诺

风险管理的引入和确保它的持续有效需要组织管理着强有力和持续的承诺，以及为实现承诺在所有层次战略的和严密的策划。管理者宜：

确定和签署风险管理方针；

确保组织的文化和风险管理方针一致；

确定与组织绩效参数一致的风险管理绩效参数；

使风险管理目标与组织的目标和战略一致；

确保法律法规的复合性；

在组织内适当的层次分配责任和职责；

确保为风险管理配置必要的资源；

将风险管理的益处通报给所有的利益相关方；

确保风险管理框架持续保持适宜。

4.3 风险管理框架的设计

4.3.1 理解组织和其状况

在开始设计和实施风险管理框架前，评价和理解组织内外部的状况是重要的，因为这会对框架的设计产生显著的影响。

评价组织外部状况可以包括，但不限于：

a)社会和文化、政治、法律法规、财务、技术、经济、自然和竞争环境，无论国际、国内、区

域和当地；

b)影响组织目标的动力和趋势；

c)与外部利益相关方的关系，以及它们的感受和价值观。

评价组织内部状况可以包括，但不限于：

—— 管理方法、组织结构、作用和责任；

—— 方针、目标，以及为实现它们所制定的战略；

—— 以资源和知识来理解的能力（例如，资本、时间、人员、过程、系统和技术）；

—— 信息系统、信息流和决策过程（正式和非正式的）；

—— 与内部利益相关方的关系，以及它们的感受和价值观；

—— 组织的文化；

—— 被组织采用的标准、指南和模型；

—— 合同关系的形式和范围。

4.3.2 建立风险管理方针

风险管理方针宜清楚阐明组织风险管理的目标和承诺，特别要针对：

—— 组织管理风险的基本原理；

—— 组织目标和方针与风险管理方针的联系；

—— 管理风险的责任和职责；

—— 处理利益冲突的方法；

—— 提供有助于管理风险必要资源的承诺；

—— 风险管理绩效测量和报告的方法；

—— 对定期评审和改进风险管理方针和框架，以及对事件和环境变化做出响应的承诺。

风险管理方针宜适当地沟通。

4.3.3 责任

组织宜确保具备管理风险的责任、权限和适当的能力，包括实施和保持风险管理过程和确保任何控制措施的充分性、有效性和效率。这可通过如下途径来实现：

—— 确定有责任和权利管理风险的风险拥有者；

—— 确定负责建立、实施和保持风险管理框架的人员；

—— 确定组织所有层次人员的风险管理过程的其他职责；

—— 建立绩效测量和内部和外部报告和逐级报告过程；

—— 确保确定的合适程度。

4.3.4 整合到组织的过程

风险管理宜益相关、有效和有效率的方式嵌入到所有组织的实践和过程中。风险管理过程宜变成组织过程的部分，而不是分离的。特别是，风险管理宜嵌入方针制定、商业和战略策划和评审和变更管理过程中。

宜具备一个组织的广泛风险管理计划以确保风险管理方针的实施和将风险管理嵌入全部组织的实践和过程中。风险管理计划可以整合到组织其他的计划中，如战略计划。

4.3.5 资源

组织宜为风险管理配置适当的资源。

对如下方面宜予以考虑：

—— 人员、技能、经验和能力；

—— 对于风险管理过程的每步骤所需的资源；

—— 用于管理风险的组织的过程、方法和工具；

—— 形成文件的过程和程序；

—— 管理体系的信息和知识；

—— 培训方案。

4.3.6 建立内部沟通和报告机制

组织宜建立内部沟通和报告机制，用于支持和促进风险的责任和归属。这些机制宜确保：

—— 风险管理框架的关键要素和任何后续的更改被适当地沟通；

—— 对框架和其有效性及结果在内部充分地予以报告；

—— 风险管理的相关信息在适当的层次和时间予以获得；

—— 与内部利益相关方的协商过程被予以提供。

适当时，这些机制宜包括基于多源头强化风险信息的过程，以及可能需要考虑信息的敏感性。

4.3.7 建立外部沟通和报告机制

组织宜制定和实施一个关于如何与外部利益相关方沟通的计划。

这宜包括：

—— 吸引适当的外部利益相关方的关注和确保有效的信息交流；

—— 对外报告法律法规和管理要求的遵守情况；

—— 对沟通和协商进行报告和反馈；

—— 运用沟通来建立组织的信心；

—— 向利益相关方沟通紧急或突发事件。

适当时，这些机制宜包括基于多源头强化风险信息的过程，以及可能需要考虑信息的敏感性。

4.4 实施风险管理

4.4.1 实施管理风险的框架

在实施组织的管理风险的框架时，组织宜：

—— 确定实施框架的适当时间安排和策略；

—— 将风险管理方针和过程应用到组织的过程；

—— 遵守法律法规要求；

—— 确保决策，包括目标的制定和设立，与风险管理过程输出结果一致；

—— 举行信息和培训会议；

—— 与利益相关方进行沟通和协商以确保其风险管理框架保持正确；

4.4.2 实施风险管理过程

风险管理宜通过确保将第五章描述的风险管理过程通过风险管理计划作为组织实践和过程的一部分应用到组织相关职能和层次。

4.5 框架的监测和评审

为了确保风险管理有效和持续改进组织的绩效，组织宜：

—— 针对适当定期评审的参数测量风险管理绩效；

—— 定期测量风险管理计划的进展和偏离；

—— 基于组织的内部和外部状况，定期评审风险管理框架、方针和计划是否仍然适宜；

—— 报告风险、风险管理计划的进展和风险管理方针如何较好地执行；

—— 评审风险管理框架的有效性。

4.6 框架的持续改进

基于监测和评审结果，宜做出如何可以改进风险管理框架、方针和计划的决策。这些决策宜致使组织的风险管理和风险管理文化的改进。

5 过程

5.1 总则

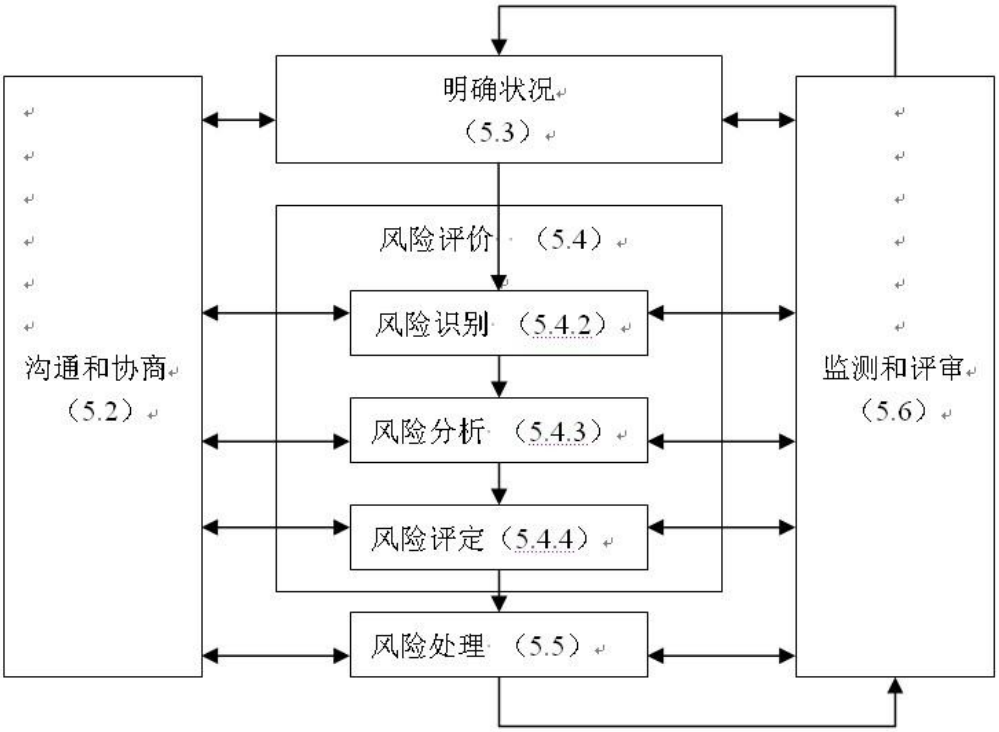
风险管理过程宜是：

—— 整合到管理中的的一部分；

—— 嵌入文化和实践之中；

—— 针对组织的经营过程制作。

它由 5.2 到 5.6 描述的活动组成。风险管理过程如图 3。



图表 3-风险管理过程

5.2 沟通和协商

与内、外部利益相关方沟通和协商宜在风险管理过程所有阶段进行。

因此，沟通和协商计划宜在早期制定。该计划宜针对与风险本身、风险成因、风险后果（如果掌握）以及处理风险措施相关的问题。为确保实施风险管理过程的职责明确，以及利益相关方理解决策的基础和特定措施需求的原因，宜采取有效的外部和内部沟通和协商。

协商团队方法可以：

—— 适当地帮助明确状况；

—— 确保利益相关方的利益被理解和考虑；

—— 帮助确保风险充分地被识别；

—— 将不同领域的专业知识一并用于分析风险；

—— 确保在界定风险准则和评定风险时，不同的观点被恰当地考虑；

—— 确保认同和支持处理计划；

—— 加强在风险管理过程中的变更管理；

—— 制定一个恰当的内部和外部沟通和协商计划。

与利益相关方的沟通协商是重要的，由于他们基于对风险的感知，做出了对风险的判断。这些感知可以由于利益相关方的价值观、需求、臆断、概念和关注点的不同而变化。由于利益

相关方的观点会对决策产生重大影响，因此他们的感知以被识别、记录、以及在决策过程中考虑。

沟通和协商宜提供真实的、相关的、准确的、便于理解的交流信息，同时宜考虑到保密和个人诚实因素。

5.3 明确状况

5.3.1 总则

通过明确状况，组织明确其目标，界定管理风险要考虑的外部和内部参数，确定风险管理过程的范围和风险准则。尽管许多此类参数与风险管理框架设计时所考虑的参数类似（参见 4.3.1），但在明确风险管理过程的状况时，这些参数需要细致地，特别是与特定风险管理过程联系起来考虑。

5.3.2 明确外部状况

外部状况是指组织寻求实现其目标的外部环境。

为了确保在建立风险准则时，目标和外部利益相关方的关注点被予以考虑，理解外部状况是重要的。它基于组织宽泛的状况，但具备法律法规要求的具体细节、利益相关方的观点、风险管理过程范围风险的其他因素。

外部状况可以包括，但不局限于：

—— 社会、文化、政治、法律法规、金融、技术、经济、自然和竞争环境，无论国际、国内、区域，还是本地的；

—— 影响组织目标的主要动力和趋势；

—— 与外部利益相关方的关系，外部利益相关方的观点和价值观。

5.3.3 明确内部状况

内部状况是指组织寻求实现其目标的内部环境。

风险管理过程宜与组织的文化、过程、结构和战略相一致。内部状况是组织内能够影响管理风险方法的方面。内部状况宜明确，因为：

a）风险管理是在组织的目标状况下进行；

b）具体项目、过程或活动的目标和准则，宜依据组织的整体目标予以考虑；

c）一些组织未能意识到实现它们战略、项目或经营目标的机会，这影响了持续的组织承诺、信誉、诚信和价值观。

理解内部状况是必要的，这可包括，但不仅限于：

—— 治理、组织结构、作用和责任；

—— 方针、目标，为实现方针和目标制定的战略；

—— 基于资源和知识理解的能力（如：资金、时间、人员、过程、系统和技术）；

—— 与内部利益相关方的关系，内部利益相关方的观点和价值观；

—— 组织的文化；

—— 信息系统、信息流和决策过程（正式与非正式）；

—— 组织所采用的标准、指南和模式；

—— 合同关系的形式与范围。

5.3.4 明确风险管理过程状况

宜确立组织活动的目标、策略、范围和参数，或风险管理过程应用到的组织的那些部分。风险管理宜充分考虑满足开展风险管理的资源需求。所需的资源、职责、权限和要保存的记录也宜予以规定。

风险管理过程的状况根据组织需求而变化。它可以包括，但不仅限于：

—— 确定风险管理活动的目标；

—— 确定风险管理过程的职责；

—— 确定所要开展的风险管理活动的范围以及深度、广度，包括具体的内涵和外延；

—— 以时间和地点，界定活动、过程、职能、项目、产品、服务或资产；

—— 界定组织特定项目、过程或活动与其他项目、过程或活动之间的关系；

—— 确定风险评价的方法；

—— 确定评价风险管理的绩效和有效性的方法；

—— 识别和规定所必须要做出的决策；

—— 确定所需的范围或框架性研究，它们的程度和目标，以及此种研究所需资源。

对这些和其他相关因素的关注，有助于确保所采用的风险管理方法适合于环境、组织、以及影响目标实现的风险。

5.3.5　确定风险准则

组织宜确定用于评定风险重要性的准则。该准则宜反映组织的价值观、目标和资源。一些准则可以服从或引用法律法规要求或组织签署的其他要求。风险准则宜与组织风险管理方针一致（见 4.3.2），在风险管理过程开始时予以确定，并予以持续评审。

当确定风险准则时，要考虑的因素宜包括如下：

—— 可以出现的致因和后果的性质和类别，以及如何予以测量；

—— 可能性如何确定；

—— 可能性和（或）后果的时间范围；

—— 风险程度如何确定；

—— 利益相关方的观点；

—— 风险可接受或可容许的程度；

—— 多种风险的组合是否予以考虑，如果是，如何考虑及哪种风险组合宜予以考虑。

5.4　风险评价

5.4.1 总则

风险评价是风险识别、风险分析和风险评定的总的过程。

注：ISO/IEC 31010 提供了风险评价技术指南。

5.4.2 风险识别

组织宜识别风险源、影响区域、事件（包括环境变化）以及致因和潜在后果。此步骤的目的是产生一个基于哪些可能产生、增强、阻碍、加快或推迟目标实现的事件的风险的综合表格。识别与不寻求机会相关的风险是重要的。综合识别是非常重要的，因为此阶段没有识别的风险将不会包含在进一步的分析中。

识别宜包括其源是否在组织的控制下的风险，即使风险源或致因可能不明显。风险识别宜包括考查特定后果直接影响，包括联锁和累积影响。也要考虑宽范围的后果，即使风险源或致因可能不明显。也要识别什么可能发生，考虑表明什么后果可以出现的可能致因和场景是必要的。所有重要的致因和后果宜予以考虑。

组织宜应用适合其目标、能力及所面临风险的风险识别工具和技术。在识别风险时，相关和最新的信息是重要的。这宜包括可能的适当背景信息。具有适当知识的人员宜参与到识别风险中。

5.4.3 风险分析

风险分析涉及开展风险的理解。风险分析为风险评定和确定风险是否需要处理以及最适合的风险处理策略和方法，提供了输入。风险分析也可以为必须做出选择及选择涉及不同类型和程度的风险的决策，提供输入。

风险分析包括考虑风险的致因和来源，以及所带来的正面和负面的后果及这些后果发生的可能性。影响后果的因素和可能性宜被识别。通过确定后果和其可能性、以及其他风险特性，来进行风险分析。一个事件可以有多种结果并可以影响多重目标。现存的控制措施和其效果和效率也宜被考虑在内。

后果和可能性的表述方式，以及它们组合确定风险程度的方式，宜反映风险类型、可获得的信息、以及运用风险评价输出的意图。这些全部都宜符合风险准则。考虑不同风险和其源的相互依赖也是重要的。

风险程度的确定和其前提和假设的敏感性的信心，宜在风险分析中予以考虑，并有效沟通给决策者以及适当的利益相关方。诸如专家间观点的分歧、不确定性、可用性、质量、数量、信息的持续相关性、或模型的局限性等因素，宜予以阐述和可以重点强调。

风险分析可以在不同程度的细节上进行，这取决于风险本身、分析目的、可用的信息、数据和来源。依据环境条件，分析可以定性的、半定量或定量的，也可以是组合的方式。

后果和其可能性可以通过模拟一个或一系列事件的结果，或由实验研究或可用数据推断确定。后果可基于有形和无形的影响表述。在某些情况下，一个以上的数值或描述，需要界定对于不同时间、地点、团体或状况的后果和其可能性。

5.4.4 风险评定

风险评价的目的是，基于风险分析的结果，帮助做出有关风险需要处理和处理实施优先的决策。

风险评定包括将分析过程中确定的风险程度与在明确状况时建立的风险准则进行比

较。基于这种比较，处理需求可予以考虑。

决策宜考虑更为宽泛风险含义，包括考虑风险获益组织外的团体对风险的容忍性。决策宜依据法律法规和其他要求做出。

在某些情况下，风险评定可导致对决策的进一步分析。风险评定也可导致，除了保持现存措施，不以任何方式处理风险的决策。通过组织的风险态度和已建立的风险准则，对此决策施加影响。

5.5 风险处理

5.5.1 总则

风险处理包括选择一种或几种修正风险的方案，以及实施那些方案。一旦实施了方案，处理提供或改进了控制措施。

风险处理包括了一个循环过程：

—— 评价风险处理；

—— 确定残留风险程度是否可容许；

—— 如果不可容许，产生新的风险处理；

—— 评价该处理的有效性。

风险处理方案不必互相排斥或适宜所有情况。方案可以包括以下内容：

a）通过决定不开展或停止产生风险的活动，来规避风险；

b）为寻求机会，接受或提高风险；

c）消除风险源；

d）改变可能性；

e）改变后果；

f）与另一方或多方共担风险（包括合约和风险融资）；

g）通过有事实依据的决策，保留风险。

5.5.2 选择风险处理方案

选择最合适的风险处理方案包括，针对以法律法规和诸如社会责任和自然环境保护的其他要求所获得的利益，平衡成本和实施的工作量。决策也宜考虑可以批准在经济层面上不合理的风险处理的风险，例如，严重的（高负面后果）但稀少（低可能性）的风险。

一些方案是可以单独或综合考虑或应用。组织一般可以从综合方案的采用获益。

当选择风险处理方案时，组织宜考虑利益相关方的价值观和观点，以及与他们沟通最适合的方法。如果风险处理方案可以影响组织别处的风险或与利益相关方关联的风险，这宜包含在决策中。尽管同样有效，有些风险处理可以比其他一些更让一些利益相关方接受。

风险处理计划宜清晰确定每个风险处理宜实施的优先顺序。

风险处理自身会引入风险。重要风险会是风险处理措施的故障或失效。监测需要成为风险处理计划的整合部分和给出措施持续有效的保证。

风险处理也可引入需要评价、处理、监测和评审的次级风险。宜将这些次级风险结合到与原

始风险同样的处理计划中，而不是作为新的风险处理。两种风险的联系宜确定和保持。

5.5.3 准备和实施风险处理计划

风险处理计划的目的是将如何实施已选择的处理措施形成文件。将要实施的风险处理方案。处理计划中提供的信息宜包括：

—— 选择风险处理措施的原因，包括所期待获得的效益；

—— 负责改进和实施计划的人员；

—— 建议的措施；

—— 资源需求，包括紧急情况时；

—— 绩效测量和控制；

—— 汇报及监测要求；

—— 时间和日程安排。

处理计划宜组织管理过程整合并与适当的利益相关方讨论。

决策者和其他利益相关方宜意识到风险处理后残留风险的性质和程度。残留风险宜形成文件并进行监测、评审，适当时，进一步处理。

5.6 监测和评审

监测和评审都宜是风险管理过程的已计划的部分，包含常规检查或监督。可以定期或不定期。监测和评审的职责宜明确界定。

组织的监测和评审过程宜包含风险管理过程的所有方面，目的是：

—— 确保控制措施在设计和运行上有效和有效率；

—— 获得进一步改进风险评价的信息；

—— 从事件（包括“near-miss）、变化、趋势、成功和失败中分析和吸取教训；

—— 探测内外部状况的变化，包括风险准则的变化和会需要修正风险处理和优先的风险自身；

—— 识别出现的风险。

在实施风险处理计划的进程中需要绩效测量。可将结果融入组织整体绩效管理、测量和外部和内部报告活动中。

监测和评审的结果宜予以记录和在内外部适当地报告，也可用作风险管理框架评审的输入（见 4.5）。

5.7 记录风险管理过程

风险管理活动宜可追溯。在风险管理过程及整体过程中，记录提供了方法和工具改进的基础。关于记录的建立的决定宜考虑：

—— 组织持续学习的需求；

—— 出于管理意图，重新使用信息益处；

—— 涉及建立和保持记录的成本和工作量；

—— 对记录的法律法规和运行需求；

—— 获取的方法、检索的难易和储存媒介；

—— 保存期限；

—— 信息的敏感性。