

ISO31000:2018 版标准与 2009 版的差异分析

雒宏伟 时书毅（上海天祥质量技术服务有限公司）

发表在中国认证认可杂志 2020 年第 3 期

摘要：ISO31000：2009 于 2018 年 2 月进行了换版，2018 版标准在前言中也给出了与 2009 版相比的四个方面的主要变化，但是这些描述过于简单，没有给出具体的解释和说明，使读者不太理解或者并不了解具体的变化。本文将对 2018 版标准和 2009 版标准的差异在上述四个方面进行进一步的分析。

关键词：ISO31000 风险管理

Analysis of Differences Between ISO31000:2018 and

ISO31000:2009

LUO HONGWEI Intertek China

Abstract: ISO31000:2009 has issued a new version in 2018. Although the 2018 version summarizes 4 main different areas in its preface, but they are too simple to be understood very well by audiences. This article further analyzes the differences between 2018 version and 2009 on above 4 areas one by one.

Keywords: ISO31000 Risk Management

ISO31000：2009《风险管理-原则和指南》于 2018 年 2 月进行了换版，发布了 ISO31000:2018《风险管理-指南》。2018 版标准与 2009 版标准虽然没有太大的变化，但是还是有一些不同。2018 版标准在前言中也给出了与 2009 版相比的主要变化，主要有以下四个方面：

1. 评审了风险管理原则，这是其成功的关键准则；
2. 从组织治理开始，突出了最高管理者的领导作用和风险管理的整合；
3. 更加强调风险管理的反复的性质，指出新的经验、知识和分析可以带来对过程各个阶段的过程要素、活动和控制的修订；
4. 理顺内容，更加注重保持开放系统模式以适应多种需求和环境。

但是这些描述过于简单，没有给出具体的解释和说明，使读者不太理解或者

并不了解具体的变化。我们将对 2018 版标准和 2009 版标准的差异在上述四个方面进行进一步的分析。

主要变化 1：评审了风险管理原则，这是其成功的关键准则；

我们将 ISO31000:2018 和 ISO31000:2009 标准的风险管理原则放在一起进行比对，如表 1 所示。

ISO31000:2009 的风险管理原则	ISO31000:2018 的风险管理原则
a) 风险管理创造和保护价值	
b) 风险管理是所有组织过程不可分割的一部分	a) 整合
c) 风险管理是决策的一部分	
d) 风险管理清晰应对不确定性	
e) 风险管理是系统化、结构化和及时的方法	b) 结构化和全面性
f) 风险管理基于最佳可用信息	f) 最佳可用信息
g) 风险管理是定制的	c) 定制
h) 风险管理考虑人文因素	g) 人员及文化因素
i) 风险管理是透明和兼顾的	d) 兼顾
j) 风险管理是动态、反复和应对变化的	e) 动态
k) 风险管理有助于组织的持续改进	h) 持续改进

表 1

从表 1 可以看出 ISO31000:2009 版标准有 11 个风险管理原则，而 ISO31000:2018 则只有 8 个。仔细对比我们发现虽然风险管理原则少了 3 个，但是核心内容并没有明显的变化，只是对 2009 版中风险管理原则进行了评审和修订使其更加准确、简洁。如：

- 2009 版中 “a) 风险管理创造和保护价值” 这一风险管理原则，在 2018 版标准中并非取消，而是被作为 “风险管理的目的” 在 “4 基本原则” 一开始就提了出来。
- 2009 版中 “c) 风险管理是决策的一部分” 这一原则虽然在 2018 版中没有，但是在 5.1 总则中明确 “风险管理的有效性依赖于其整合进入组织的治理包括决策”，2018 版 “a) 整合” 中进一步明确 “风险管理是所有组织活动不可分割的一部分”，决策当然包括其中。
- 2009 版中 “d) 风险管理清晰应对不确定性” 这一原则在 2018 版中也没有。我们可以这样理解：因为风险的定义就是 “不确定性对目标的影

响”，风险管理当然是管理不确定性，应对或管理不确定性是风险管理的核心或者说风险管理本身，不需要作为风险管理原则来要求，因此2018版不再把它作为原则之一。

- 2009版“e) 风险管理是系统化、结构化和及时的方法”这一原则在2018版中改为“b) 结构化和全面性”，新的表述更加准确、简洁。同样的道理“i) 风险管理是透明和兼顾的”改为“d) 兼顾”、“j) 风险管理是动态、反复和应对变化的”改为“e) 动态”。

主要变化 2: 从组织治理开始，突出了最高管理者的领导作用和风险管理的整合；

针对这一变化，下面分三部分进行说明。

1、2018版标准加入了“组织治理”的内容；

- 5.1 总则明确“风险管理的有效性取决于与组织治理包括决策的整合。”
- 5.3 整合“治理为组织的路线、内外部关系、实现其目的所需的规则、过程和实践以提供了指南。管理架构将治理方向转化为实现期望的可持续绩效和永续经营水平所需的战略和相关目标。在组织内部确定的风险管理责任和监督角色是组织治理的不可或缺的部分。”
- 2018版标准不但强调最高管理者的作用和要求，也提出了对监督机构的作用和要求，如：5.2 领导作用和承诺中“最高管理者和监督机构宜确保风险管理整合进入组织所有活动”、“最高管理者负责管理风险，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”。

2、突出了最高管理者的领导作用

虽然2009版标准4.2 指令和承诺明确“管理者宜：”对管理者提出了9项要求，而2018版标准则强调了最高管理者的作用，如：5.1 风险管理的有效性取决于与组织治理包括决策的整合。这需要相关方，特别是最高管理者的支持。5.2 领导作用和承诺“在适当的情况下，最高管理者和监督机构宜确保风险管理整合进入组织所有活动，并宜通过以下方式展现领导作用和承诺：”并对最高管理者提出了4项要求。

3、强调了风险管理的整合

2009版标准中虽然也提出了风险管理整合的要求，并作为风险管理的第二个原则，还在4.1 总则中强调“风险管理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。”在4.3.4 整合到组织的过程明确“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。” 2018 版标准在此基础上，对风险管理的整合提出更高或更加明确的要求，如：在风险管理框架中在 2009 版标准风险管理框架的设计、实施、检测和评审、持续改进的基础上专门增加了“整合”，并在该部分进一步明确“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。” “风险管理宜成为组织目的、治理、领导作用和承诺、战略、目标和运营的一部分，而不是相互分离。”

主要变化 3：更加强调风险管理的反复的性质，指出新的经验、知识和分析可以带来对过程各个阶段的过程要素、活动和控制的修订；

2009 版标准中也提出“风险管理是动态、反复和应对变化的”并作为风险管理的一个原则，并进行解释“风险管理持续发现和响应变化。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。” 2018 版标准则进一步强调了风险管理是反复的，如：6.1 总则明确“虽然风险管理过程通常表现为有一定的顺序，但在实践中这些过程是反复的。” 6.4.1 总则要求“风险评估宜该利用相关方的知识和观点，系统地、反复地、协作地开展风险评估。” 2018 版标准进一步指出学习和经验对风险管理过程的重要性，给出“持续改进”这一风险管理原则的解释是：“通过学习和经验积累，持续改进风险管理。”。

主要变化 4：理顺内容，更加注重保持开放系统模式以适应多种需求和环境。

2009 版标准虽然也明确提出风险管理要适应不同的需求和环境，如：在 4.1 总则中明确“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。” 5.3.4 “风险管理过程的状况根据组织需求而变化。”并要求确定风险管理活动的目标、职责、范围、深度、广度、风险评价方法等。2018 版标准在此基础上在多个条款中进一步明确如何满足在不同层次、不同的需求适应不同的内外部环境的风险管理，如：

- 5.1 “框架的组成要素和它们协同工作的方式宜根据组织的需求进行定制。”
- 6.3.1 “确定范围、环境和准则的目的是为了定制风险管理过程，能进行有效的风险评估和恰当的风险处置。范围、环境和准则涉及界定过程的范围并理解内外部环境。”
- 6.3.2 “由于风险管理过程可应用于不同的层面（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、相关目标以及其与组织目标的一致性。”

- 6.3.3 “风险管理过程的环境宜根据对组织运行的外部和内部的理解来确定，并宜反映风险管理过程应用的具体活动情况。”
- 6.3.4 “风险准则宜与风险管理的框架相一致，并根据具体活动的目的和范围进行定制。”

其实，2018 版标准对比 2009 版标准的变化基本上可以通过 2009 版标准中的原则、框架和流程图（如图 1）和 2018 版标准的原则、框架和流程图（如图 2）清晰的表现出来。当然，ISO31000 的 2018 版标准和 2009 版标准之间还有一些内容上存在差异，但是应该说只是 2018 版标准的表述更加简洁和准确，并没有什么实质性变化，在此不再赘述。

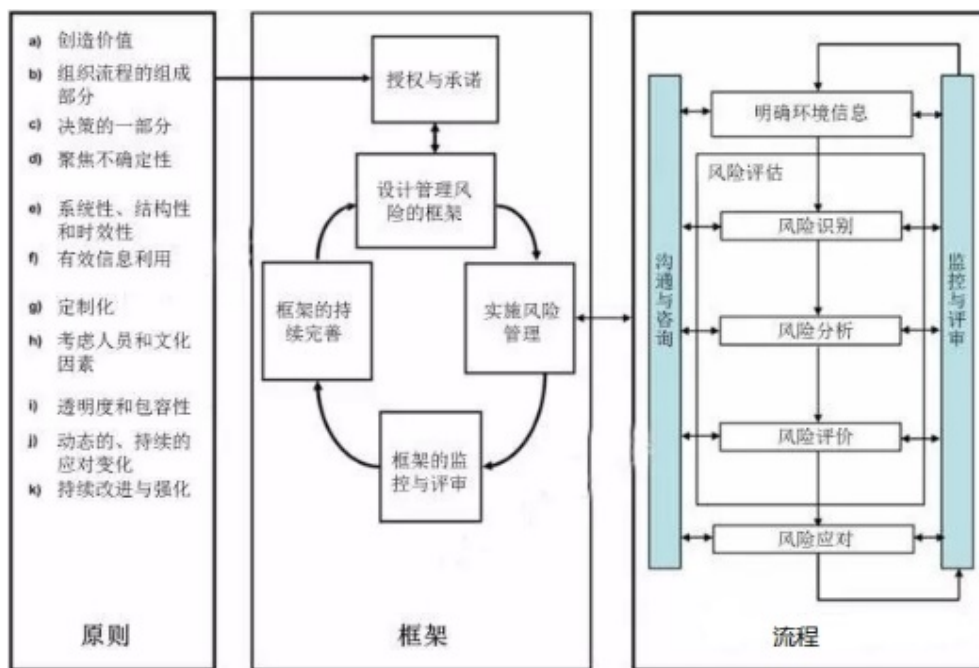


图 1

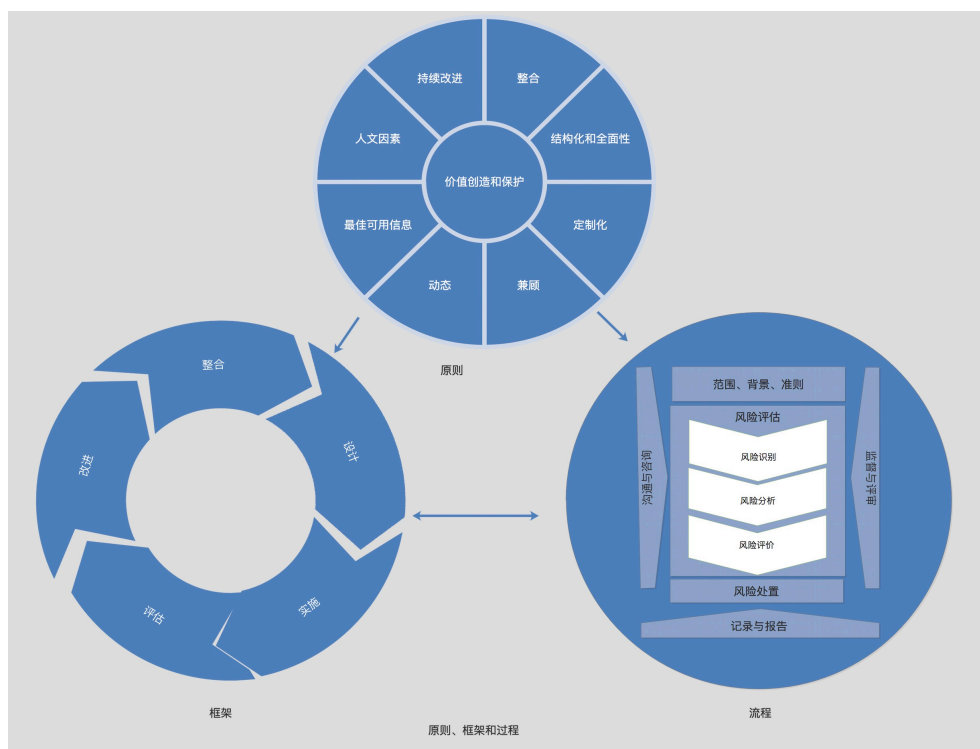


图 2

参考文献

- 【1】 ISO, ISO31001:2018 Risk Management -Guidelines
- 【2】 ISO , ISO31001:2009 Risk Management -Principles and guidelines

作者简介

雒宏伟，研究生导师、博士。研究方向：风险管理、反贿赂管理、合规管理、资产管理、道路交通安全管理。INTERTEK 集团上海天祥质量技术服务有限公司 ISO37001、ISO19600、ISO39001 和 ISO55001 项目经理。

时书毅，INTERTEK 集团上海天祥质量技术服务有限公司新产品项目成员