浅析风险管理的基本原则

雒宏伟（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：ISO31000:2018 提出了风险管理的八大原则，并且指出这些基本原则是风险管理的基础，建议组织在建立风险管理框架和过程时要考虑这些原则。但是标准对于基本原则的解读过于简单，使大家很难理解和贯彻，本文首先讨论了风险管理的目的：创造和保护价值，然后针对这些基本原则逐一进行了解读。

关键词：ISO31000 风险管理

Simple analysis of Risk Management Principles

LUO HONGWEI Intertek China

Abstract: ISO31000:2018 proposes 8 principles for risk management, and points out these principles are the foundation of risk management, suggests that these principles should be considered when organizations establish risk management framework and processes. However, interpretation for these principles in the standard is too simple to be understood and implemented by audiences. Firstly, this article interprets risk management purpose: Value Creation and Protection, then explains these principles one by one.

Keywords: ISO31000 Risk Management

ISO31000:2018 首先明确风险管理的目的是创造和保护价值明确，然后提出了风险管理的八个基本原则：整合、结构化和全面性、定制化、兼顾、动态、最佳可用信息、人文因素和持续改进，并且指出这些基本原则是风险管理的基础，建议组织在建立风险管理框架和过程时要考虑这些原则。但是标准对于基本原则的解读过于简单，使大家很难理解和贯彻。下面我们将对这些基本原则进行解读，希望能够对大家有所帮助。

一、风险管理的目的：创造和保护价值

虽然“创造和保护价值”没有列入风险管理的八大原则，但是它才是最核心的基本原则，而八大原则也需要以此为中心和目的。

风险的定义就是“不确定性对目标的影响”。实现目标始终是组织追求的结果，是判定一个组织、一个体系、一个项目、一个过程有效性的评价标准，因此实现目标是对组织最重要，也是最有价值的事情。因为风险性质的不同，有些风险会带来收益（投资风险、创新风险），管控风险会创造价值；有些风险（如安全风险、合规风险）会造成人身伤害、财产损失、环境破坏或行政处罚，风险管控是可以防止或减少这些伤害、损失、破坏或处罚，达到保护组织价值的目的。如果风险的管控不能给组织创造或保护价值，或者创造或保护的价值与风险管控的成本相比不划算，我们就没有必要投入资源、采取措施来管控这些风险。这也是为什么要进行风险分析和评价的原因。

二、风险管理基本的八大原则

1、整合 Integrated

ISO31000：2108 标准在多个地方反复强调整合，如

- 4a) “风险管理是所有组织活动不可分割的一部分”；
- 5.1 “风险管理框架的目的是支持组织将风险管理整合进入重要的活动和职能。风险管理的有效性取决于和组织治理包括决策的整合。框架制定包含整合”；
- 5.2 “最高管理者和监督机构适用时宜将风险管理整合进入所有组织活动”；
- 5.3 “整合风险管理依赖对组织架构和环境的理解。将风险管理整合进入组织是一个动态和反复的过程”，“风险管理宜成为组织宗旨、治理、领导作用和承诺、战略、目标和运营的一部分，而不是割裂开来”；
- 5.4.2 “承诺宜包括强化将风险管理整合进入组织整体文化的需要；引导将风险管理整合进入核心业务过程和决策”；
- 5.7.2 “组织宜持续改进整合风险管理过程的方式”；
- 6.1 “风险管理过程宜是管理和决策不可分割的一部分，并宜整合进入组织架构、运营和过程。风险管理可应用于战略、运营、计划或项目层面”；
- 6.5.3 “处置计划宜整合进入组织的管理计划和过程”。

从以上内容可以看出，风险管理是可以应用到组织各个方面（组织宗旨、治理、领导作用和承诺、架构、职能、文化、过程）、各个层面（战略、运营、计划或项目、过程、活动等层面）、各个活动（战略、目标、决策、运营等），成为其不可分割的一部分，所以风险管理被很多组织称之为全面风险的管理。

2、 结构化和全面性 Structured and comprehensive

风险管理对组织的重要性决定了组织需要严格管控风险管理过程，以达到期

望和一致的结果，所以对于风险管理过程以及影响风险管理过程的其他因素和过程需要进行策划。ISO31000:2018 给出的风险管理过程包括 :沟通与协商，范围、环境和准则，风险识别、分析和评估，风险处置，监视和评审，记录与报告；标准同时也给出了风险管理的框架：领导作用和承诺、整合、设计、实施、评估和改进。这些都充分展示了标准对风险管理结构化和全面性的要求。虽然标准建议风险管理框架和过程要进行定制，但是并不改变对其结构化和全面性的要求，尤其是目前企业普遍采用的 ISO 的管理体系标准，均是建立在风险管理的基础之上的，不但包含以上风险管理的框架和过程，而且进一步进行了细化，这些标准也被公认为非常全面完善的管理体系标准。

3、 定制化 Customized

标准明确要求风险管理框架和风险管理过程要进行定制，并适合于与目标相关的内外部环境。

组织的目标不同，如影响质量目标实现的是质量风险；影响环境影响目标实现的是环境风险；影响员工健康和安全目标实现的是职业健康安全风险；影响投资回报率目标实现的是资产管理风险；影响合规目标实现的是合规风险，组织为控制这些风险所建立的风险管理框架必然不同。从 ISO 发布的质量管理体系、环境管理体系、职业健康安全管理体系、资产管理体系、合规管理体系标准可以看出满足不同目标的管理框架的差异。

即使目标相同，因为与目标相关的内外部环境不同，具体的风险也不同，如：不同的行业（比如制造工厂和建筑工程公司）的质量风险、合规风险不同。即便是同一个跨国公司，在不同的国家设立的分支机构所面临的风险也会存在一些差异。因此不同组织所建立的风险管理框架，比如：方针、目标、组织架构、职责分配、资源分配等应该不同；风险管理过程，比如风险识别、分析和评价方法（头脑风暴法、事故树、事件树，失效模式影响分析等）不同、评价准则不同，流程也会不同。

另外，风险管理不是越复杂越好，还要考虑风险程度和成本，因此也不存在最佳，只有适宜。为了保证适宜，风险管理的定制化就成为必然。

4、 兼顾 Inclusive

组织管理目的之一就是要平衡和兼顾不同相关方的利益和要求。组织的主要的相关方包括：顾客、员工、股东、供应商、周围社区、监管机构等。当然组织因为所处环境不同、发展的历史阶段不同、价值观和战略不同，相关方对组织的影响程度不同，相同或类似事件给组织带来的风险不同，所以组织对不同的相关方重视程度不同。有些组织如上市公司更关注顾客和股东；有些组织如化工企业

更关注周围社区和监管机构。总之组织要识别对组织有重大影响的相关方和他们对组织的要求，并以此为考虑因素，确定组织风险评价准则，使风险分析和评价更加准确，风险管理更加有效。

5、 动态

组织的内外部环境一直在变，相关方对组织的要求和重要程度也在变，因此组织的风险在变。如果组织不及时的评审风险、就无法做到及时调整风险的应对措施，使得一些新的重大风险得不到管控；同样如果组织不根据变化的风险调整组织的目标、资源配置以及对风险的监视测量，即使制定了管控措施，也不能得到有效实施。因此组织要建立明确职责和流程，使组织能够及时识别内外部环境和相关方要求的变化，重新进行风险评价，根据评价出的风险重新制定或调整风险应对措施、调整目标、资源以及风险的监视测量计划。

6、 最佳可用信息

风险管理需要识别、分析、评估和处置风险。风险的识别、发生可能性、后果以及现有措施的有效性分析需要考虑一些历史信息或外部案例以及对将来的预测。另外，为了确保风险处置措施的合理性和有效性，同样需要使用一些信息。而这些信息会存在缺失、不准确、不匹配、因保密不能访问或将来的信息需要预估的问题。这些都会影响到风险识别的全面性、风险分析的全面性和准确性、风险处置措施的合理性的问题。风险管理应该充分考虑到信息的影响，根据风险的重要程度、信息获取的成本，确定信息创建、收集、加工、储存、检索、使用的要求，使风险管理所需信息从成本效益的角度是最佳的。

7、 人文因素

人的意识和行为（如违章、追求不当利益）本身就是风险源，会直接造成风险并影响风险的重要程度；风险无处不在、并且动态变化，任何组织不可能也不必要识别和管控所有风险，因此我们需要重视员工风险意识和组织风险文化的培养和提高，使大部分员工都能够形成习惯，自觉主动的识别风险、分析风险并采取必要措施控制风险，而不是依赖组织识别风险、提出要求，这样才能从根本上控制组织风险。

8、 持续改进

无论是风险管理框架，还是风险管理过程均需要与组织的目标和内外部环境相适应，而风险管理架构和过程的有效性同样是一个逐步完善和提高的过程。组织需要通过主动创新、学习和借鉴同行、竞争对手和标杆单位的经验和教训，或者通过组织内部的监视、测量、分析和评估、内审和管理评审等其他一些活动及时发现组织风险管理存在的问题，制定措施并进行改进。

参考文献

【1】 ISO，ISO31001:2018 Risk Management -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。