

安全风险管理体系标准 ISO 31000

文 澳大利亚risk@workplaces公司 吉姆·怀廷 译 王光远 宁丙文

在安全风险管理体系领域，一项新的国际标准《ISO 31000:风险管理原则与实施指南》(以下简称ISO 31000)已被国际标准组织(ISO)风险管理技术委员会完成制订工作，并将于2009年正式公布。

ISO 31000 是以澳大利亚和新西兰风险管理标准《AS/NZS 4360: 2004》为基础，实现了安全、健康、环境与财务风险管理的一体化，可以应用于任何企业、组织、协会、团体或个体等(以下以“企业”代表所有对象)，并不特别限定于某些行业或部门，具有广泛的应用范围。

该标准的最大特征是将“创建背景”作为风险管理程序的开始，这样可以使该标准满足多样性的需要。实施这一新的国际标准，企业可以达到如下目的：鼓励采取预防性而非被动性的管理；认识到在整个企业辨识和处置风险的必要性；提高辨识各种隐患的水平；符合相关法律法规和国际标准的要求；提高经济效益；改善企业管理；建立决策和计划的可靠基础；改进事故管理和预防；减少损失等。



风险管理的原则、框架和程序

在ISO 31000中，风险管理的原则、框架和程序之间的关系如图1所示。

1. 原则

1) 风险管理可以创造价值

风险管理有助于企业取得显著成绩，以及提高安全健康、法律法规实施、环境保护、产品质量、经营效率等方面的水平。

2) 风险管理是企业管理的组成部分

风险管理是企业管理层的责任之一，也是企业管理程序的组成部分，而不仅仅是一项单独的活动。

3) 风险管理是决策程序的组成部分

风险管理可以帮助决策者做出更加睿智的选择。风险管理有助于企业实施需要优先采取的措施，也有助于判断风险水平是否可以接受，以及风险处置方法是否适当与有效。

4) 风险管理可以明确地处理不确定性

风险管理可以指出决策过程中具有不确定性的方面，

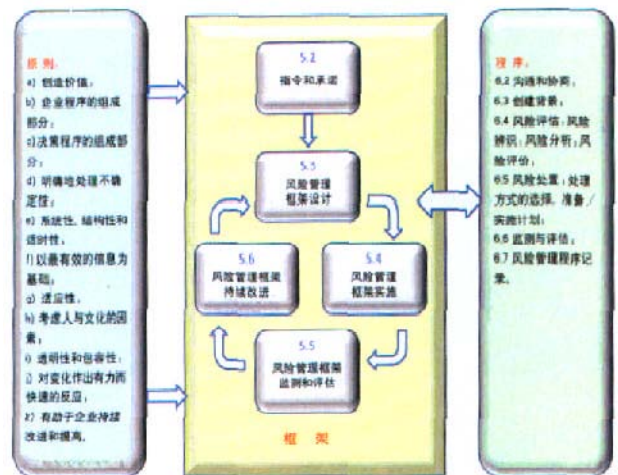


图1 风险管理的原则、框架和程序之间的关系

并能提供相应的处理方法。

5) 风险管理具有系统性、组织性和适时性的特点

系统性、适时性和组织性的风险管理方法有助于企业提高效率和保持可持续性，并能取得具有可比性和可信赖的结果。

6) 风险管理以最有效的信息为基础

风险管理程序以经验、反馈、观察、预测和专家鉴定等信息资源为基础。决策者应掌握这些信息资料,并考虑这些资料的局限性以及专家之间存在分歧的可能性。

7) 风险管理具有适应性

风险管理可以根据企业的外部 and 内部背景及风险概况作出适当的调整。

8) 风险管理应考虑人与文化的因素

企业的风险管理可以辨识出外部与内部相关人员的能力与意图,这些人对企业目标的实现具有促进或阻碍的作用。

9) 风险管理具有透明性和包容性

利益相关者尤其是企业各级决策者的适当和适时参与,可以确保风险管理适合于企业的管理,并能保持更新。

10) 风险管理应对变化作出有力和快速的反应

由于诸如内部与外部事件的发生、背景与知识的改变、新风险的出现等情况的不断变化,企业应当确保风险管理能继续发挥作用,并对变化作出相应反应。

11) 风险管理有助于企业持续改进和提高

企业应当制订和实施提高风险管理成熟度的战略,该战略应当与企业的其他战略一同实施。

2. 框架

风险管理应当在风险管理框架内运行。该框架可以帮助企业在各层面和特定背景下通过应用风险管理程序,以有效管理风险。该框架应当确保来自这些程序的风险信息被适当地报告,并被用作决策的依据。

该框架主要是帮助企业在整个管理系统内将风险管理一体化,因此,企业应改编框架的组成部分以满足其特殊需求。

1) 指令和承诺

风险管理的采用和确保其不断发挥作用,要求企业的管理者给予有力的和持续的承诺。

2) 风险管理框架的设计

了解企业及其背景——在开始设计和实施风险管理框架前,重要的是了解企业的内部与外部背景。企业的外部背景主要包括文化、政治、法律、法规、金融、技术、经济等环境,以及外部利益相关者的价值观等。企业的内部背景主要包括了解资源和理解知识方面的能力、决策程序、价值观和文化等。

风险管理政策——应当阐明企业风险管理的目标和承诺,风险管理政策与企业目标及其他政策之间的联系,风险管理的责任,风险管理政策应当被适当交流等。

与企业程序实现整合——风险管理应当被应用到企业的所有业务和程序中,以确保其相关性、有效性和高效率。

责任——企业应当确保有责任 and 职权管理风险,包括实施和保持风险管理程序,保证任何风险控制适当性和有效性。

资源——企业应当采取实际的手段,为风险管理分配适当的资源,如人力、信息和知识管理系统等。

建立内部沟通和报告机制——这样可以确保风险管理框架的重要组成部分及其后续修订内容得到适当的沟通。

建立外部沟通和报告机制——企业应当制订和实施如何与外部利益相关者进行沟通的计划,如雇佣适当的外部利益相关者,确保信息的有效交流;提供交流和协商的反馈和报告;在危机事件或意外事故发生时与利益相关者进行沟通等。

3) 风险管理的实施

风险管理框架的实施——企业应当明确实施风险管理框架的适当时间和战略;在企业的管理程序中应用风险管理政策和程序等。

风险管理程序的实施——在企业的所有相关部门和职能机构应用风险管理程序,并作为企业管理程序的一部分。

4) 框架的监测和评估

为确保风险管理的有效性,企业应:制订执行的措施;定期估量风险管理计划的进展;定期评估风险管理框架、政策和计划是否仍与企业的内部与外部背景相适应等。

5) 框架的持续改进

以评估结果为基础,作出如何改进风险管理框架、政策和计划的决定。这些决定应当能够改进企业的风险管理和风险管理文化。

3. 程序

风险管理程序包括5个方面的活动:沟通与协商,创建背景,风险评估,风险处置,监测与评估,如图2所示。

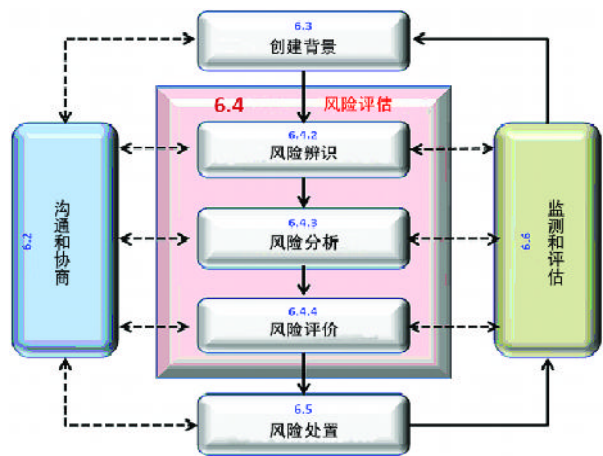


图2 风险管理程序

1) 沟通与协商

在风险管理程序的每一个阶段,与内部和外部利益相关者进行沟通与协商是十分必要的。在早期阶段,应该制订一个与内部和外部利益相关者进行沟通 and 协商的计划,处理与风险本身、风险后果和应当采取的管理措施相关的问题。有效的外部 and 内部沟通与协商可以明确

地解释实施的风险管理程序,使利益相关者了解做出相关决定的依据,采取的特殊措施的原因。

2) 创建背景

通过创建背景,企业在管理风险、制订风险范围和标准时,能够充分考虑内部和外部的影响因素。

创建风险管理程序的背景——风险管理程序的背景将根据企业的需求而发生改变,主要包括:明确风险管理程序的责任;明确被实施风险管理活动的范围、深度、宽度;明确企业的特别计划或活动与其他计划或活动之间的关系;明确风险评估的方法等。

制订风险标准——企业应当制订评估风险重要性的标准。该标准应反映企业的价值观、目标和资源,与企业的风险管理政策相一致。风险标准应当在风险管理程序的开始阶段制订,并不断被修订。

3) 风险评估

风险评估就是指风险辨识、风险分析和风险评价的全过程。

风险辨识——企业应当辨识风险的根源、影响的范围、潜在性的后果等。企业应当根据其目标和能力、面临的危险,去运用风险辨识工具和技术。

风险分析——即对风险的理解,决定风险是否需要被处置,以及最合适的风险处置战略和方法。风险分析包括考虑风险产生的原因和根源,其积极与消极结果,这些结果发生的可能性等。

风险评价——风险评价的目的是帮助在风险分析结果的基础上做出决策,哪些风险需要被优先采取处置措施。

4) 风险处置

风险处置的方法主要包括:通过决定不开始或继续能够产生风险的活动来避免风险;消除风险产生的根源;通过选择保留部分风险等。

风险处置包括一个评估风险处置的循环程序,决定剩余风险的程度是否可以容忍。如果不能容忍,将采取新的风险处置方法。评估风险处置的效果,直到剩余风险达到了公司风险标准的要求。

5) 监测与评估

监测与评估应当成为风险管理程序的计划部分,应当明确地规定监测与评估的责任。监测与评估可以包括日常检查或监督。

ISO 31000可用作认证标准

像ISO 9000质量管理体系、ISO 14000环境管理体系和ISO 18000职业健康安全管理体系那样,这一新标准将取代有关国际标准,为未来所有与风险相关的ISO和IEC(国际电工委员会)标准提供基础。

ISO 31000可能不会被广泛地专门用于风险管理体的认证。然而,它可以提供一种实用、规范的原则、框

架和程序,并涵盖不同的领域——安全、环境、质量和财务等各种风险的管理。

风险可容忍性和风险偏好

ISO 31000标准不能也不应作为规定企业风险管理标准,比如什么级别的风险是可以容忍的,什么级别的风险是不可以容忍的,企业还需根据自身的目标和文化来设定具体的标准。

ISO 31000程序的实施,将使企业明确自身所承受的风险级别的标准,即用一个包括成本—效益分析的正式的、结构化的程序确定风险是否在最低可接受限度(ALARP)。这一风险可容忍性概念如图3所示。

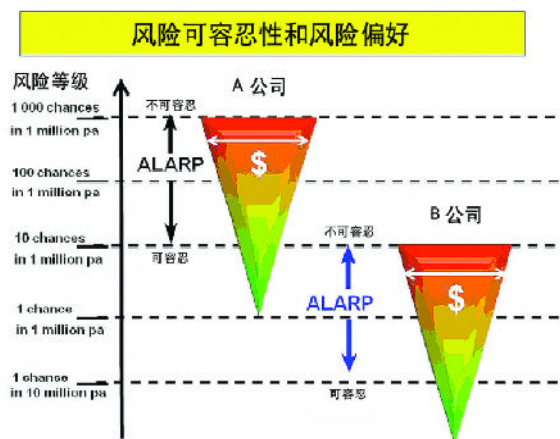


图3 风险可容忍性框架和风险偏好

这个三角形的图示便是风险可容忍性框架,它们的垂直位置表示企业就什么级别的风险是可以容忍的和不可以容忍的而做出的选择。三角形的宽度表示管理者为被容忍的风险级别所花费的时间、费用和精力的量值。在被选择的可容忍的范围内,风险级别越高,管理风险需要花费的费用也就越多。图3可以这样来理解,即B公司比A公司控制风险的标准更高(风险偏好更低)。

即使在同一家公司,对于不同类型的风险(比如安全和财务),风险可容忍性或偏好也可能是不同的;也可能在一个风险领域内因时间和环境的不同而有所不同,比如企业在面临经济压力的情况下比在较好经济形势的情况下可能会容忍更大的风险。风险管理目标以及可容忍性会随着时间的改变而改变。

编辑 宁远