Q/ZYRZ

企　　业　　标　　准

Q/ZYRZ-JS002-2025

风险管理体系 要求及使用指南

Risk management system requirements and usage guide

2025 年 08 月 05 日发布　　2025 年 08 月 05 日实施

中源认证（江苏）有限公司

目录

前言 II

1 范围 1

2 规范性引用件 1

3 术语和定义 1

4 组织所处的境 2

5 领导作用 3

6 策划 4

7 支持 7

8 运行 9

9 绩效评价 11

10 改进 13

参考文献 15

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件起草单位：中源认证（江苏）有限公司。

本文件主要起草人：黎拥军、陆小辉、刘波、吴娟、王凯等。

1 范围

风险管理体系 要求

本文件规定了建立、实施、保持和持续改进风险管理体系的具体要求，旨在使组织通过系统的方法在制定决策、设定和实现目标以及提升绩效的过程中管理风险，创造和保护价值。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文 件。

GB/T 19001-2016/ISO 9001:2015 《质量管理体系 要求》

GB/T 24001-2016/ISO 14001:2015《环境管理体系 要求及使用指南》

GB/T 45001-2020/ISO 45001:2018《职业健康安全管理体系 要求及使用指南》

GB/T 24353-2022/ISO 31000:2018 《风险管理 指南》

GB/T 23694-2013《风险管理 术语》

3 术语和定义

上述标准内容界定的以及下列术语和定义适用于本文件。

3.1

风险 risk

不确定性对目标的影响。

注 1:影响是指偏离预期,偏离可以是正面的和/或负面的,可能带来机会和威胁。

注 2:目标可有不同维度和类型,可应用在不同层级。

注 3:通常风险可以用风险源、潜在事件及其后果和可能性来描述。

3.2

风险管理 riskmanagement

指导和控制组织与风险(3.1)相关的协调活动。

3.3

风险源 risksource

可能单独或共同引发风险(3.1)的要素。

3.4

事件 event

某些特定情形的产生或变化。

注 1:一个事件可包括一个或多个情形,并且可由多个原因导致。

注 2:事件可能是预期会发生但没发生的事情,也可能是预期不会发生但却发生的事情。

注 3:某事件有可能是风险源。

3.5

后果 consequence

某事件(3.4)对目标影响的结果。

注 1:后果可以是确定的,也可以是不确定的;对目标的影响可以是正面的,也可以是负面的;可以是直接的,也可以是间接的。

注 2:后果可以定性或定量表述。

注 3:任何后果都可能通过连锁反应和累积效应升级。

3.6

可能性 likelihood

某件事发生的概率。

注 1:在风险管理术语中,无论是以客观的或主观的、定性或定量的方式来定义、度量或确定,还是用一般词汇或数学术语来描述(如概率,或一定时间内的频率),“可能性”都用来表示某件事发生的概率。

注 2:“可能性(likelihood)”这一英语词汇在一些语言中没有直接与之对应的词汇,因此经常用“概率(probability)”这个词代替。不过,在英语中,“概率”常常被狭义地理解为一个数学词汇。因此,在风险管理术语中,“可能性”有着与许多语言中使用的“概率”一词相同的解释,而不局限于英语中“概率”一词的意义。

3.7

控制 control

保持和(或)改变风险(3.1)的措施。

注 1:控制包括但不限于保持和/或改变风险的任何流程、策略、措施、操作或其他行动。

注 2:控制并非总能取得预期的改变效果。

4 组织所处的环境

4.1 理解组织及其所处的环境

组织应确定与其发展战略相关，并影响其实现风险管理体系预期结果的能力的各种外部和内部因素。在考虑内外部因素时应明确:

a) 对组织的影响、组织在其内部传达风险管理承诺;

b) 影响相关方或受相关方影响的事项，并适时向相关方传达。

4.2 理解相关方的需求和期望

组织应确定:

a) 与风险管理体系有关的相关方，包括:政府机构、供应商、客户等;

b) 相关方的有关要求，包括相关的法律法规及其他要求并应考虑将这些要求纳入到组织的合规要求中。

c) 需落实的相关方需求和期望。 组织应定期识别相关方需求和期望，并形成文件化信息。

4.3 确定风险管理体系的范围

4.3.1 组织应界定风险管理体系的边界及其适用性，以确定其范围。

4.3.2 在确定风险管理体系范围时，组织应考虑:

a) 所确定的内部和外部因素;

b) 所确定的相关方要求;

c) 职能、运行单元和物理边界;

d) 活动、产品和服务;

e) 实施控制与施加影响的权限和能力。 组织风险管理体系的范围和边界应作为文件化信息予以保持。

4.4 风险管理体系

组织应依据本文件要求，建立、实施、保持并持续改进风险管理体系，包括所需的过程及其相互作用，并持续改进风险管理绩效。

5 领导作用

5.1 领导作用和承诺

5.1.1 在持续改进风险管理体系有效性方面，最高管理者应通过以下方面证实其对风险管理体系的领导作用和承诺:

a) 对风险管理体系的有效性负责;

b) 确保建立风险管理方针和目标，并确保其与组织的战略方向及所处的环境相 一致;

c) 确保将风险管理体系要求融入组织的活动过程;

d) 确保可获得风险管理体系所需的资源;

e) 就有效风险管理的重要性和符合风险管理体系要求的重要性进行沟通;

f) 确保风险管理体系实现其预期结果;

g) 指导并支持员工对风险管理体系的有效性做出贡献;

h) 促进持续改进;

i) 支持其他相关管理人员在其职责范围内证实其领导作用。

5.1.2 以顾客为关注焦点 最高管理者应以顾客满意度为目标，确保顾客的要求得到确定和满足。

5.2 风险管理方针

最高管理者应在确定的风险管理体系范围和边界内制定风险管理方针，风险管理方针应:

a) 适合于组织的活动发展现状和战略规划;

b) 为设定风险管理目标提供框架;

c) 包括满足适用的风险管理等相关政策和法律法规及其他要求的承诺;

d) 包括持续改进风险管理体系，改进风险管理绩效，实现最终风险管理目标的承诺;

e) 支持考虑风险管理绩效改进的设计活动。

最高管理者需确保风险管理方针:

——是可获取的文件化信息;

——在组织内得到了充分沟通;

——定期评审，必要时进行更新。

5.3 组织的角色、职责和权限

最高管理者应在组织内分配并沟通相关角色的职责和权限。

最高管理者应向风险管理团队分配职责和权限，以:

a) 确保建立、实施、保持和持续改进风险管理体系;

b) 确保风险管理体系符合本文件的要求;

c) 明确并实施管理方案以持续满足环保要求，最终实现风险管理目标;

d) 建立所需的准则和方法，以确保风险管理体系的有效运行和控制;

e) 指定有责任和权限管理风险的个人(风险责任人)。

6 策划

6.1 应对风险和机遇的措施

6.1.1 总则

策划风险管理体系时，组织应考虑 4.1 所确定的内部和外部因素以及 4.2 确定的相关方的需求和期望，并对影响组织风险管理绩效的活动和过程进行评审。策划应与风险管理方针保持一致，并应采取能够实现风险管理绩效持续改进的措施。组织应确定需要应对的风险和机遇，以:

a) 确定风险管理目标实现的进度安排;

b) 确保风险管理体系实现其预期结果;

c) 预防或减少不期望的影响;

d) 实现风险管理体系和风险管理绩效的持续改进;

e) 满足合规性义务。

6.1.2 风险源

风险识别的目的是发现、确认和描述可能有助于或妨碍组织实现目标的风险。采用相关、适当、最新的信息对于识别风险非常重要。

组织可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。识别风险宜考虑以下因素及相互之间的关系:

——有形和无形的风险源;

——原因和事件（包括潜在的紧急情况）;

——威胁和机遇;

——脆弱性和应对能力;

——内外部环境变化;

——新兴风险;

——用于确定的风险准则;

——资产和资源的性质和价值;

——后果及其对目标的影响;

——知识的局限性和信息的可靠性;

——与时间有关的因素;

——识别风险所涉及人员的偏见、假设和看法。

不管风险源是否在组织控制范围内，都宜对风险进行识别。需考虑风险带来的多于一种的结果，这些结果可能导致各种有形或无形的后果。

6.1.3 风险分析

风险分析的目的是了解风险性质及其特征，必要时包括风险等级。风险分析包括对不确定性、风险源、后果、可能性、事件、情境、控制措施及其有效性进行详尽考虑。一个事件可能有多种原因和后果，可能影响多个目标。

开展风险分析的细致和复杂程度可有所不同,具体取决于分析目的、信息的可获得性和可靠性以及可

用的资源及合规性。分析技术可以是定性的、定量的或者定量和定性相结合的，具体视情况和预期用途而定。

风险分析可考虑以下因素：

——事件的可能性及后果；

——后果的性质及影响程度；

——复杂性和关联性；

——时间相关因素及波动性；

——现有控制措施的有效性；

——控制措施的合规性。

风险分析可为风险评价提供信息输入，也可为是否需要和如何应对风险，及采取最适宜的策略和方法提供信息支撑。当面对不同类别和不同等级的风险需要做出抉择时，风险分析结果可为决策提供深刻见解。

6.1.4 风险评价及措施的策划

风险评价

风险评价将风险分析结果和既定风险准则相比较，以确定是否需要采取进一步行动。风险评价可促成以下决定：

——不采取进一步行动；

——考虑风险应对方案；

——开展进一步分析,以更全面地了解风险；

——维持现有的控制措施；

——重新考虑目标。

决策宜考虑到更广泛的环境,以及对内外部利益相关者的实际和预期影响。

风险评价的结果宜予以记录、沟通,然后在组织适当层级予以确认。

组织应策划：

a) 采取措施管理其：

1) 重要风险源：

2) 合规义务：

3) 6.1.1 所识别的风险和机遇。

b) 如何：

1) 在其风险管理体系过程(见 6.2、第 7 章、第 8 章和 9.1)中或其他业务过程中融入并实施这些措施;

2) 评价这些措施的有效性。

6.2 风险管理目标及其实现的策划

6.2.1 风险管理目标

组织应针对其相关职能和层次建立风险管理目标，此时必须考虑组织的重要风险源及相关的合规义务，并考虑其风险和机遇

风险管理目标应:

a)与风险管理方针一致;

b)可度量(如可行):得到监视;

c)予以沟通;

d)适当时予以更新

组织应保持风险管理目标的文件化信息。

6.2.2 实现风险管理目标和指标措施的策划

组织应考虑如何将实现风险管理目标和指标的措施融入其运营过程。策划如何实现风险管理目标时，组织应确定:

a) 要做什么;

b) 需要什么资源;

c) 由谁负责;

d) 时间进度;

e) 验证结果的方法和时机。

7 支持

7.1 资源

组织应确定并提供建立、实施、保持和持续改进风险管理体系所需的资源，包括:

a) 与风险管理目标相关的人员的能力和意识要求;

b) 提供必要的基础设施，包括与产品生产/服务相关的设施或设备、信息化系统等;

c) 提供必要的监视和测量设备;

d) 确定如何获取必要的知识及知识的更新，包括先进的技术的方法学;

e) 与相关方建立沟通渠道。

7.2 人员能力

组织应:

a) 确定对实现风险管理目标具有影响的人员所需的能力;

b) 实施人员能力评价，确保人员能力满足要求;

c) 采取培训及其他措施，确保在岗人员能够胜任工作。

d) 评价所采取措施的有效性。

组织应保留适当的记录作为能力符合性的证据。

7.3 意识

组织应确保相关人员意识到:

a) 符合风险管理方针的重要性;

b) 符合风险管理目标、风险管理体系要求的重要性;

c) 其职责、权限及活动对于组织风险管理目标实现的影响;

d) 其对风险管理体系有效性的贡献，例如控制重要风险源的方法;

e) 不符合风险管理体系要求所产生的影响，例如未履行合规义务的后果。

7.4 信息交流

组织应确定与风险管理体系有关的内部和外部的信息交流，信息交流应考虑:

a) 在其各职能和层级间就风险管理体系的相关信息进行内部沟通交流;

b) 合规性要求、相关方和组织自身的要求，并按照相关要求进行外部信息交流，适用时包括:风险管理方针、风险管理目标及实现进度情况等信息;

c) 鼓励员工为实现风险管理目标提出合理化的改进建议，并保留改进建议的文件化信息。

组织应对内部和外部的信息交流进行响应，并保留相应的记录。

7.5 文件化信息

7.5.1 总则

组织风险管理体系应包括:

a) 本文件要求的文件化信息;

b) 组织为确保风险管理体系有效性和证实风险管理绩效改进所必需的文件化信息。

注 1：组织正在保持的其他管理体系的文件化信息，可能是风险管理体系文件化信息的一部分。

注 2：不同组织的风险管理体系文件化信息的复杂程度可能不同，其取决于：

——组织的规模及其活动、过程、产品和服务的类型;

——合规性要求;

——工艺过程的复杂性及其相互影响；

——人员的能力。

7.5.2 创建与更新

创建和更新文件化信息时，组织应确保适当的：

a) 标识和说明(例如:标题、日期、作者和编号)；

b) 形式(例如:语言文字、软件版本、计算工具、图表)和载体(例如:纸质的、 电子的)；

c) 评审和批准，以确保适宜性和充分性。

7.5.3 文件化信息的控制

组织应对本文件要求的文件化信息应予以控制，以确保在需要的时间和场所可获得适用的文件化信息。适用时，组织应采取以下措施:

a) 分发、访问、检索和使用;

b) 存储和保护，包括保持易读性、防止失密;

c) 变更的控制，包括版本控制;

d) 保留和处置。

组织应识别与风险管理体系策划和运行相关的外部的文件化信息，适当时，应予以控制。

8 运行

8.1 风险应对

8.1.1 概述

风险应对的目的是选择和实施风险处理方案。

风险应对是一个循环提升的过程，包括：

——制定和选择风险应对方案；

——计划和实施风险应对措施；

——评估风险应对措施的成效；

——确定剩余风险是否可接受；

——若不可接受，采取进一步应对措施。

8.1.2 选择风险应对方案

选择最合适的风险应对方案，可在实现目标获得的潜在收益和付出的成本、耗费的精力或由此引发的不利后果之间进行权衡。

风险应对方案之间不一定是相互排斥的，也不一定适用于所有情形。

风险应对方案涉及以下一个或多个方面：

——决定不开始或退出会导致风险的活动,来规避风险；

——承担或增加风险,以寻求机会；

——消除风险源；

——改变可能性；

——改变后果；

——分担风险(如通过签订合同，购买保险)；

——慎重考虑后决定保留风险。

采取风险应对的理由不仅考虑经济因素,还宜考虑所有的组织义务、自愿性承诺和利益相关者的观点,可依据组织目标、风险准则和可用资源选择风险应对方案。

选择风险应对方案时，组织宜考虑利益相关者的价值观、认知和潜在参与程度以及与其沟通和协商的最佳方式。虽然效果相同，但某些风险应对方案相比其他方案更能被某些利益相关者接受。

虽然经过谨慎的设计和实施，但风险应对不一定产生预期结果,甚至可能产生意外的后果。监督和检查宜作为风险应对实施的一部分，以确保不同形式的风险应对持续有效。

风险应对还可能产生需要加以管理的新风险。如果没有可用的应对方案或者应对方案不足以改变风险，组织可将这些风险记录下来，并持续跟踪。

决策者和其他利益相关者宜了解经风险应对后剩余风险的性质和程度。组织可记录剩余风险，对其进行监督和检查，并适时采取进一步应对措施。

8.1.3 编制和实施风险应对计划

风险应对计划的目的是明确如何实施所选定的应对方案，以便相关人员了解应对计划，并监测计划实施进度。应对计划宜明确指明实施风险应对的顺序。

应对计划宜纳入管理计划和组织运营过程中，并征询利益相关者意见。

应对计划中提供的信息应包括：

——选择应对方案的理由，包括可获得的预期收益；

——批准和实施计划的责任人；

——拟采取的措施行动,包括应急预案；

——所需要的资源，包括风险准备；

——绩效考核的标准和方法；

——限制因素；

——必要的报告和监测；

——行动预期开展和完成的时间。

8.2 应急准备和响应

组织应建立、实施并保持对 6.1.2 中识别的潜在紧急情况进行应急准备并做出响应所需的过程。 组织应:

a)通过策划的措施做好响应紧急情况的准备，以预防或减轻它所带来的不利风险因素;

b)对实际发生的紧急情况做出响应;

c)根据紧急情况和潜在风险影响的程度，采取相适应的措施以预防或减轻紧急情况带来的后果;

d)可行时，定期试验所策划的响应措施;

e)定期评审并修订过程和策划的响应措施，特别是发生紧急情况后或进行试验后;

f)适当时，向有关的相关方，包括在组织控制下工作的人员提供与应急准备和响应相关的信息和培训。 组织应保持必要程度的文件化信息，以确信过程能按策划得到实施。

9 绩效评价

9.1 监视、测量、分析和评价

9.1.1 总则

组织应监视、测量、分析和评价其风险管理绩效。

组织应确定:

a)需要监视和测量的内容;

b)适用时的监视、测量、分析与评价的方法，以确保有效的结果;

c)组织评价其风险管理绩效所依据的准则和适当的参数;

d)何时应实施监视和测量;

e)何时应分析和评价监视和测量的结果。 适当时，组织应确保使用和维护经校准或验证的监视和测量设备。 组织应评价其风险管理绩效和风险管理体系的有效性。 组织应按其合规义务的要求及其建立的信息交流过程，就有关风险管理绩效的信息进行内部和外部信息交流。 组织应保留适当的文件化信息，作为监视、测量、分析和评价结果的证据。

9.1.2 合规性评价

组织应建立、实施并保持评价其合规义务履行状况所需的过程。 组织应:

a)确定实施合规性评价的频次;

b)评价合规性，需要时采取措施;

c)保持其合规状况的知识和对其合规状况的理解。 组织应保留文件化信息，作为合规性评价结果的证据。

9.2 内部审核

9.2.1 组织应按计划的时间间隔实施内部审核，通过提供风险管理体系下列信息，以评价风险管理体系的有效性:

a) 是否符合:

组织自身对风险管理体系的要求;

本文件的要求。

b) 是否得到了有效的实施和保持。

9.2.2 组织应建立、实施并保持一个或多个内部审核方案，包括实施审核的频次、方法、职责、策划要求和报告，该审核方案应考虑实现风险管理目标的关键过程和以往审核的结果。

组织应:

a) 规定每次审核的准则和范围;

b) 选择审核员并实施审核，确保审核过程的客观性与公正性;

c) 确保向最高管理者及相关负责人报告审核结果;

d) 针对发现的不符合采取适当的纠正和(或)纠正措施。

组织应保留文件化信息，作为审核方案实施和审核结果的证据。

9.3 管理评审

9.3.1 最高管理者应按策划的时间间隔对组织的风险管理体系进行评审，以确保其持续的适宜性、充分性和有效性，并与组织的战略方向保持一致。

9.3.2 管理评审的输入应包括以下事项:

a) 以往管理评审所采取措施的状况;

b) 以下方面的变化:

与组织相关的内外部因素;

相关方的需求和期望，包括合规性要求;

识别的风险和机遇及其应对措施。

c) 风险管理体系有效性方面的信息，包括:

基于监视和测量的结果的风险管理绩效及其改进;

风险管理目标的实现程度;

不符合和纠正措施;

合规性评价结果;

审核结果。

d) 资源的充分性;

e) 来自相关方的有关信息交流，包括反馈意见;

f) 持续改进的机会。

9.3.3 管理评审的输出应包括:

a) 对风险管理体系的持续适宜性、充分性和有效性的结论;

b) 与持续改进机会相关的决策，包括风险管理体系与业务过程相融合的改进机会;

c) 与风险管理体系变更的任何需求相关的决策，包括资源分配、风险管理方针的调整、 风险管理目标的调整;

d) 风险管理目标未实现时需采取的措施;

e) 任何与组织战略方向相关的结论。 组织应保留文件化信息，作为管理评审结果的证据。

10 改进

10.1 总则

组织应依据风险管理绩效评价的结果确定改进的机会，并实施必要的措施实现风险管理体系的预期结果。

10.2 事件、不符合和纠正措施

组织应建立、实施和保持包括报告、调查和采取措施在内的过程，以确定和管理事件和不符合。

当事件或不符合发生时，组织应:

a) 对事件或不符合做出响应，适用时，采取措施控制及纠正不符合，并处置不符合所产生的后果;

b) 确定不符合的性质和原因，并检查是否存在类似的不符合。评价是否需要采取措 施，以消除事件或不符合的原因，防止事件或不符合再次发生或在其他区域发生。纠正措施 应与所发生的事件或不符合造成影响的重要程度相适应;

c) 实施任何所需的措施;

d) 评审所采取的任何纠正措施的有效性;

e) 必要时，对风险管理体系进行变更。

组织应保留事件或不符合性质内容及采取任何后续措施的记录。

10.3 持续改进

组织应通过下列方式持续改进风险管理体系的适宜性、充分性与有效性：

a） 提升风险管理绩效；

b） 促进支持风险管理体系的文化；

c） 促进工作人员参与风险管理体系持续改进措施的实施；

d） 就有关持续改进的结果与工作人员及其风险责任人进行沟通；

e） 保持和保留文件化信息作为持续改进的证据。

参考文献

[1] GB/T 19001-2016/ISO 9001:2015《质量管理体系 要求》

[2] GB/T 24001-2016/ISO 14001:2015《环境管理体系 要求及使用指南》

[3] GB/T 45001-2020/ISO 45001:2018《职业健康安全管理体系 要求及使用指南》

[4] GB/T 24353-2022/ISO 31000:2018《风险管理 指南》

[5] GB/T 23694-2013《风险管理 术语》

[6] GB/T 27921《风险管理 风险评估技术》

[7] GBTT 19011《管理体系审核指南》