

广东中检认证有限公司

风险管理体系 要求

文件编号：Q/GDZJ 006-2025

版本号：A/0

广东中检认证有限公司认证规则编写小组

编制

审核：李传石

批准：熊贵江

发布日期：2025-04-21

实施日期：2025-04-21

声明： 本文件系广东中检认证有限公司（GDZJ）内部文件，涉及 DGZJ 核心秘密，著作权为 DGZJ 专有。未经 GDZJ 书面授权，不得复制、摘编、发布、发表、转载、链接或以其他方式使用本文件，违者将追究相关责任。

[illegible][illegible]

风险管理体系 要求

1 范围

本标准规定了组织建立、实施和保持风险管理体系的要求，并从组织环境、领导作用、策划、支持、运行、绩效评价和改进几个层面规定了企业实施风险管理体系应满足的要求，以确保该体系符合法律法规的要求并满足相关方的需求和期望。

采用风险管理体系是一个组织的战略决策。组织风险管理体系的建立和实施受组织需求和目标、风险要求、所用组织流程以及组织规模和结构的影响。预计所有这些影响因素都会随着时间的推移而改变。

本标准适用于有以下目标的组织：

- a) 通过建立、实施和保持风险管理体系，提升组织风险管理能力；
- b) 通过第三方机构对组织风险管理体系的认证。其他有需求的组织也可参照本标准要求执行。

本文件适用于组织内部和外部建立和实施风险管理体系认证活动。

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，仅所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 19000 质量管理体系基础和术语

GB/T 19001 质量管理体系要求

GB/T 24353 风险管理指南

3 术语和定义

下列术语和定义适用于本文件。

3.1 风险

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

指导和控制组织与风险(3.1)相关的协调活动。

3.3 利益相关者

可以影响、被影响或自认为会被某一决策或活动影响的个人或组织，

3.4 风险源

可能单独或共同引发风险(3.1)的要素。

3.5 事件

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。

3.6 后果

某事件(3.5)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。

3.7 可能性

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。

3.8 控制

保持和(或)改变风险(3.1)的措施。

注 1:控制包括不限于保持和/或改变风险的任何流程、策略、措施、操作或其他行动。注 2:控制并非总能得预期的改变效果。

4 组织环境

4.1 理解组织及其环境

组织应确定与其宗旨和战略方向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,组织应对这些外部和内部因素的相关信息进行了监视和评审。

组织外部环境包括但不限于:

- a) 国际、国内、区域或地方的社会、文化、政治、法律、监管、金融、技术、经济、自然环境;
- b) 对组织目标产生影响的驱动因素和趋势;
- c) 与外部利益相关者的关系,以及他们的认知、价值取向、需求和期望;
- d) 合同关系和承诺;
- e) 组织所处关系网络的复杂性及依赖关系。组织内部环境包括但不限于:
- f) 愿景、使命和价值观;
- g) 治理方式、组织结构、职能、责任和绩效考核;
- h) 战略、目标和方针;
- i) 组织文化;
- j) 组织采用的标准、指南和模型;
- k) 组织在资源和知识方面所具备的能力(即资本、时间、人力、知识产权、程序、系统和技术等):数据、信息系统和信息流;
- l) 与内部利益相关者的关系,充分考虑其认知和价值取向;合同关系和承诺;
- m) 相互依赖性和相互关联性。

4.2 理解相关方的需求和期望

由于相关方对组织稳定提供符合适用法律法规要求的风险管理的能力具有影响或潜在影响,因此,组织应确定:

- a) 与风险管理体系有关的相关方;
- b) 与风险管理体系有关的相关方的要求。

组织应监视和评审这些相关方的信息及其相关要求。

4.3 确定风险管理体系的范围

组织应确定风险管理体系的边界和适用性,以确定其范围。在确定范围时,组织应考虑:

- a) 4.1 中提及的各种外部和内部因素;
- b) 4.2 中提及的相关方的要求;
- c) 组织的风险的承诺及要求。

如果本标准的全部要求适用于组织确定的风险管理体系的范围。组织应实施本标准的全部要求。如果组织确定本标准的某些要求不适用于其风险管理体系范围,应说明理由。只有当所确定的不适用的要求不影响组织的风险管理的能力或责任,方可声称符合本标准的要求。

组织的风险管理体系范围应作为成文信息,可获得并得到保持。

注：本认证规则归广东中检认证有限公司所有，广东中检认证有限公司对其拥有最终解释权。任何组织及个人未经广东中检认证有限公司许可，不得以任何形式全部或部分使用。

如需获取认证规则备案全文请与以下联系人联系：蒋老师，联系电话：

13826281695，或发函至邮箱获取：gdzj_101@163.com。

