

卓耀认证中心有限公司

Zhuoyao Certification Center Co., Ltd.



风险管理体系要求

文件编号：CTS Q/ZY044-2025

文件版次：A/0版

编 制：文件编制小组

审 核：郭朝岗

批 准：杨超杰

受控状态：**受控**

发布日期：2026 年 6 月 5 日

实施日期：2026 年 6 月 5 日

风险管理体系要求

0. 引言

本技术规范基于 GB/T 46410—2025《风险管理 风险预警》及其他相关风险管理标准（GB/T 23694、GB/T 24353、GB/T 27921）制定，旨在为各类组织建立、实施、保持和改进风险管理体系提供通用要求。

风险管理的核心价值在于帮助组织在不确定的环境中做出明智决策。风险预警作为风险管理的关键活动，能够为组织提供动态、及时、前瞻性的风险信息。本规范遵循动态前瞻、科学可信、紧密衔接、恰当适配的原则，采用过程方法和PDCA 循环（策划-实施-检查-改进），帮助组织系统化地识别、分析、评价、预警和应对风险，保障和促进组织价值创造。

1. 范围

本规范规定了各类组织开展风险管理体系建设的通用要求，包括组织环境、领导作用、策划、支持、运行（含风险预警）、绩效评价及改进等全流程要求。

本规范适用于：

- a) 任何类型、规模、行业或领域的组织，无论其产品、服务、所处行业或风险复杂程度，均可依据本规范建立、实施、保持和改进风险管理体系。
- b) 认证机构对本规范范围内组织进行风险管理体系认证和评价活动的依据。

2. 规范性引用文件

下列文件对于本规范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 23694—2024 风险管理 术语

GB/T 24353—2022 风险管理 指南

GB/T 27921—2023 风险管理 风险评估技术

GB/T 46410—2025 风险管理 风险预警

3. 术语和定义

GB/T 23694—2024 、 GB/T 24353—2022 、 GB/T 27921—2023 及 GB/T 46410—2025 界定的以及下列术语和定义适用于本规范。

3.1 风险管理体系

组织为实现风险管理的方针和目标而建立、实施、保持和持续改进的一组相互关联或相互作用的要素（包括框架、流程、制度、人员、资源等）。

3.2 风险指标

用来度量或反映风险大小的要素。风险指标及其数值需体现出不确定性特征。

3.3 预警区间

组织依据其风险偏好确定的用于区分预警等级的风险指标取值范围。预警等级一般分为不可接受（红色预警）、关注（黄色预警）、正常（绿色预警）三级。

3.4 预警频率

发出预警信息的时间周期，如实时预警、每天 1 次、每周 1 次、每月 1 次等。

4. 组织环境

4.1 理解组织及其环境

组织应确定与其战略、目标相关，并影响其风险管理体系实现预期结果能力的内外部因素，包括但不限于：

a) 外部环境：法律法规、监管要求、行业动态、市场环境、社会经济、自然环境、技术发展等。

b) 内部环境：组织战略、治理结构、文化价值观、资源能力、知识资产、信息数据基础、现有管控措施等。

4.2 理解相关方的需求和期望

组织应确定与风险管理体系相关的相关方（如股东、监管机构、客户、供应商、员工、社会公众）及其风险偏好、风险承受能力和期望要求。

4.3 确定风险管理体系的范围

组织应明确风险管理体系的边界和适用性，形成文件。范围应考虑：

- a) 组织的活动、产品、服务及其影响；
- b) 组织能够实施控制的决策和活动；
- c) 组织的地理位置、职能部门、业务单元。

4.4 风险管理体系与业务流程的融合

风险管理体系应融入组织的治理、战略、策划、管理、报告、流程、方针、文化等各个方面，而非作为孤立的活动存在。

5. 领导作用

5.1 领导作用和承诺

最高管理者应通过以下方式证明其对风险管理体系的领导作用和承诺：

- a) 确保风险管理方针和目标的制定，并与组织战略方向一致；
- b) 确保风险管理融入组织的所有业务流程；
- c) 确保提供体系建立、实施、保持和改进所需的资源；
- d) 确认组织的风险偏好和风险容忍度（预警区间的划分依据）；
- e) 根据风险预警信息，启动和执行由其负责的风险应对措施；
- f) 推动持续改进。

5.2 风险管理方针

最高管理者应制定、实施和保持风险管理方针，该方针应：

- a) 适合于组织的目的、规模、风险概况；
- b) 包含满足适用要求和持续改进风险管理体系的承诺；
- c) 为设定风险管理目标提供框架；
- d) 在组织内得到沟通和理解。

5.3 组织职责与权限

最高管理者应确保风险管理相关职责和权限得到分配和沟通。组织应明确以下三类角色的职责：

5.3.1 管理层及相关制度流程节点负责人

- a) 确认对风险预警的具体需求（预警内容、频率、时间差）；
- b) 确认组织的风险偏好、预警区间、预警频率并适时调整；

- c) 保障风险管理所需的资源投入；
- d) 根据获得的风险预警信息，启动和执行由其负责的风险应对措施。

5.3.2 风险管理部门（或归口管理部门）

- a) 负责风险管理体系的设计和监督工作；
- b) 定期对组织风险管理成效进行评价，按需组织调整改进；
- c) 组织开展风险管理文化与能力建设；
- d) 维护风险指标库和预警运行机制。

5.3.3 业务部门

- a) 按照风险管理设计要求，收集、提供所需的数据；
- b) 在日常业务执行过程中，执行风险控制措施；
- c) 根据获得的风险预警信息，启动和执行由其负责的风险应对措施。

5.3.4 绩效考核部门

- a) 对风险管理体系的设计和执行情况、风险管理成效等内容进行考核；
- b) 将风险管理绩效纳入相关岗位的考核指标。

6. 策划

6.1 应对风险和机遇的措施

策划风险管理体系时，组织应考虑内外部环境及相关方要求，识别需要应对的风险和机遇，并策划相应的控制措施。

6.2 风险管理目标及其实现的策划

- a) 组织应在相关职能和层次上建立风险管理目标，目标应：
 - 与风险管理方针一致；
 - 可测量（如风险预警准确率、风险事件发生率下降、应对响应时间）；

得到监视、沟通和适时更新。

b) 组织应策划实现目标的措施、资源、责任方和时限。

6.3 风险管理流程的设计

组织应按照 GB/T 24353—2022 的要求，设计以下风险管理流程：

- a) 沟通与咨询；
- b) 明确环境（内外部环境、风险准则）；
- c) 风险评估（风险识别、风险分析、风险评价）；
- d) 风险应对；
- e) 监督与检查；
- f) 记录与报告。

7. 支持

7.1 资源

组织应确定并提供建立、实施、保持和改进风险管理体系所需的资源，包括人员、基础设施、信息系统、数据资源等。

7.2 人员与能力

- a) 确定从事影响风险管理绩效工作的人员所必要的能力。
- b) 确保这些人员基于适当的教育、培训或经验能够胜任工作。
- c) 保留培训记录。

7.3 风险预警文化与能力建设

组织应通过培训、经验交流、对标、专题研究等方式，加强风险预警文化和能力建设，确保风险管理在组织内被正确理解和应用。内容包括：

- a) 风险管理意识和价值宣贯；
- b) 风险识别、分析、评价技术方法培训；

- c) 风险预警工具和信息系统操作培训；
- d) 风险应对决策能力培养。

7.4 文件化信息

组织的风险管理体系文件化信息应包括：

- a) 本规范要求的方针、目标、范围。
- b) 风险管理制度文件，包括但不限于：

风险识别、评估与应对制度；

风险预警运行制度（含职责、流程、考核）；

风险信息记录与报告制度；

风险管理监督与改进制度。

- c) 风险指标库（按附录 B 模板建立和维护）。

d) 组织为确保有效策划、运行和控制风险管理过程而确定的必要程序和记录。

8. 运行

8.1 运行策划和控制

组织应策划、实施和控制满足风险管理要求所需的过程，包括风险评估、风险应对及风险预警。运行应遵循 GB/T 46410—2025 第 5 章规定的工作程序。

8.2 风险评估

组织应按策划的时间间隔开展风险评估，包括：

- a) **风险识别**：识别影响目标实现的不确定性因素。
- b) **风险分析**：分析风险的发生可能性、影响程度、风险等级。
- c) **风险评价**：将分析结果与风险准则比较，确定风险等级（可接受、需关注、不可接受），为风险应对和预警提供依据。

8.3 风险预警

8.3.1 梳理风险预警需求与现状

组织应通过对标、内部调研、意见征集等方式，梳理并明确：

- a) 需要使用风险预警信息的业务或管理制度流程节点（如各类审核审批节点、管理或业务执行标准控制节点、周期性的工作计划制定与调整节点、重点工作安排节点等）；
- b) 相关制度流程节点对风险预警信息的内容、频率、时间差等方面的需求；
- c) 已有的各类统计指标及其应用情况，判断其对组织风险预警需求的满足度。

8.3.2 设计风险指标、预警区间、预警频率

风险指标设计步骤：

- a) 明确相关制度流程节点关注的目标指标及其数值；
- b) 识别影响上述目标的主要不确定因素；
- c) 判断已有统计指标是否能度量上述不确定因素：

若是，判断是否满足需求（满足则沿用，不满足则调整优化）；

若否，则新设计风险指标，明确计算公式/模型、时间范围、数据来源、置信度要求、责任主体；

- d) 将目标指标和度量不确定因素的指标设置为风险指标。

预警区间设计：

a) 若将目标指标设置为风险指标：将符合风险偏好的、分段的目标指标值波动范围，作为不同预警等级的预警区间；

b) 若将度量不确定性因素的指标设置为风险指标：根据其与目标指标的逻辑关系及目标指标波动范围，反推出不同预警等级对应的预警区间；

c) 预警等级一般分为：红色预警（不可接受）、黄色预警（关注）、绿色预警（正常）。

预警频率确定：

- a) 考虑因素：决策频率、风险指标数据的可收集分析频率；
- b) 原则：预警频率 $\leq$ 数据可收集分析频率，预警频率 $\geq$ 决策频率。

8.3.3 设计风险预警运行机制

组织应明确：

- a) 职责分工（管理层、风险管理部门、业务部门、绩效考核部门）；
- b) 工作流程（数据收集→指标计算→预警判断→信息发布→应对启动→反馈闭环）；
- c) 各环节的执行时间要求与工作质量保障措施；
- d) 风险预警信息的构成与形式（预警等级、指标值、触发时间、应对建议、责任主体）。

8.3.4 执行风险预警运行机制

- a) 组织应通过信息化、数字化等手段，测试并完善风险预警运行机制；
- b) 在改正设计或执行缺陷后，常态化执行风险预警运行机制；
- c) 保留风险预警记录（预警发布记录、应对措施记录、效果评估记录）。

8.4 风险应对

- a) 根据风险评估结果和风险预警等级，选择适当的应对方式（规避、接受、改变、转移、分担等）；
- b) 制定风险应对计划，明确措施、资源、责任方、时间表；
- c) 剩余风险的评估和管理；
- d) 将风险应对措施纳入组织的业务流程和管理制度。

9. 绩效评价

9.1 监视、测量、分析和评价

组织应确定：

- a) 需要监视和测量的对象（如风险预警准确率、风险事件发生率、预警响应时间、应对措施完成率）；
- b) 适用的方法、时机和评价准则；
- c) 何时对监视和测量结果进行分析和利用。

9.2 内部审核

组织应按照策划的时间间隔进行内部审核，以提供风险管理体系是否符合组织自身要求（本规范）和是否有效实施与保持的信息。内部审核应覆盖所有风险管理相关过程和部门。

9.3 管理评审

最高管理者应按策划的时间间隔评审风险管理体系，以确保其持续的适宜性、充分性和有效性。评审应包括：

- a) 以往管理评审的后续措施；
- b) 内外部环境变化；
- c) 风险管理绩效（含风险预警成效）；
- d) 资源充分性；
- e) 改进机会和变更需求。

9.4 风险预警成效评价

组织应定期评价风险预警工作成效，包括但不限于：

- a) 风险预警的及时性（预警时间差是否满足需求）；
- b) 风险预警的准确性（预警是否有效预示了实际风险）；
- c) 预警响应及应对的有效性；
- d) 风险预警对决策的支持价值。

10. 改进

10.1 不符合与纠正措施

当发生不符合（如风险预警未及时发布、预警数据错误、应对措施未执行）时，组织应：

- a) 对不合作作出反应，采取措施控制和纠正；
- b) 评价消除不符合原因的措施需求，防止再发生；
- c) 实施任何所需的措施；
- d) 保留纠正措施及结果的记录。

10.2 持续改进

组织应持续改进风险管理体系的适宜性、充分性和有效性。改进应基于对绩效评价、内部审核、管理评审、风险预警成效评价、风险事件分析等结果的评价。