ICS 03.100.01
CCS A 02

DB4403

深　　圳　　市　　地　　方　　标　　准

DB4403/T 350—2023

企业合规管理体系

Enterprise compliance management systems

2023-08-10 发布　　2023-09-01 实施

深圳市市场监督管理局　　发 布

目　　次

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。

本文件由深圳市司法局提出并归口。

本文件起草单位：深圳市司法局、深圳市标准技术研究院、北京新世纪跨国公司研究所、深圳市认证认可协会。

本文件主要起草人：周剑君、冯念文、徐玲玲、张敖、姜婷、王志乐、丁继华、刘猛、廖灏璘、黄琳、刘莹莹、林晓君、曹荣、尹雪晨、王欢雪。

引　言

合规是企业可持续发展的基石。企业需要高度重视合规管理，根据自身实际情况搭建行之有效的合规体系，并不断推进完善。合规体系建设需要在保证合规管理独立性的同时，将合规嵌入企业运营和管理的全流程，并不断强化员工的合规意识，建立浓厚的合规氛围。企业有效地进行合规管理，能使企业避免或减少因不合规行为给企业带来的损失，也有利于塑造良好的企业形象。

我国于2017年等同采用ISO 19600:2014《合规管理体系　指南》，制定了GB/T 35770—2017《合规管理体系　指南》。2021年发布的国际标准ISO 37301:2021《合规管理体系　要求及使用指南》及2022年10月12日发布的国家标准GB/T 35770—2022《合规管理体系　要求及使用指南》，规定了合规管理体系的要求，并提供了使用指南和推荐做法。近年来，我国深入推进企业合规建设，国务院国资委等部门出台了一系列企业合规管理制度，企业合规意识逐步增强、企业合规氛围逐渐浓厚。深圳作为以外向型经济为主的城市，企业数量多、业态复杂，为使我市企业得以行稳致远，有充分的必要性和紧迫性加强企业合规建设。制定与国际接轨、立足深圳实际的企业合规管理地方标准，将为打造深圳企业合规示范区建设提供坚实的基础支撑和保障。

本文件为企业建立合规管理体系提供了全面系统的指引和建议，企业可依据自身规模及内外部环境等因素，建立符合自身发展目标的合规管理体系，从而预防、发现和处置合规风险，并证明针对合规已经实施了合理和适当的措施。

企业合规管理体系

1 范围

本文件规定了企业合规管理体系的基本原则、企业环境、领导作用、策划、支持、运行、绩效评价、持续改进、合规管理的重点环节、合规管理的重点人员、合规管理的重点领域。

本文件适用于企业开展合规管理体系建设和评价，包括自评和第三方评价。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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—2016 质量管理体系 基础和术语

GB/T 19001—2016 质量管理体系 要求

GB/T 23694—2013 风险管理 术语

GB/T 35770—2022 合规管理体系 要求及使用指南

SZDB/Z 245—2017 反贿赂管理体系

3 术语和定义

GB/T 19000—2016、GB/T 19001—2016、GB/T 23694—2013、GB/T 35770—2022、SZDB/Z 245—2017界定的以及下列术语和定义适用于本文件。

3.1

最高领导者 top leader

在最高层指挥和控制企业的一个人。

3.2

决策层 decision-maker

对企业的经营管理活动享有最终决策权限的一个人或一组人。

注：决策层包括但不限于董事会。

3.3

管理层 management

对企业的经营管理活动负有管理责任的一个人或一组人。

注：管理层包括但不限于首席执行官、总经理、总监。

3.4

首席合规官 chief compliance officer

领导合规管理部门组织开展相关工作，使企业及企业内部成员行为符合法律规定、监管要求、行业准则和国际条约、规则，以及企业章程、相关规章制度等要求的管理人员。

注：企业根据企业规模及机构设置的不同，明确相关人员履行首席合规官的职责。

3.5

监督层 supervisor

对企业经营管理活动和员工履职行为进行监督的一个人或一组人。

注：监督层包括但不限于企业的监事会、审计部门、监察稽核部门、风控部门和巡察组。

4 基本原则

4.1 有效适宜原则

企业建立的合规管理体系，能与企业性质、经营范围、组织结构和业务规模等实际情况相适应，兼顾成本与效率，能有效运行且能达成企业合规管理目标，并可根据内外部环境的变化持续改进。

4.2 全面覆盖原则

企业合规管理体系覆盖企业经营活动全业务领域、各部门、各层级子企业、分支机构和全体员工，贯穿决策、执行、监督、反馈等各个环节，体现于决策机制、内部控制、业务流程等各个方面。

4.3 客观独立原则

企业从机构设置、制度设计、汇报路径等方面保证合规管理工作的独立性，合规管理部门及人员承担的其他职责不与合规职责产生利益冲突。

4.4 协同联动原则

企业宜推动合规管理与法务、监察、审计、内控、风险管理等工作制度的统筹和衔接，确保合规管理体系有效运行。

4.5 公开易得原则

企业宜将合规管理体系中涉及的政策、程序、制度等及时公开，并及时向企业各层级、员工和利益相关方传达。企业宜使有关信息的获取便利化，确保其易被获取。

5 企业环境

5.1 理解企业及其环境

企业应确定与其合规风险和合规目标相关，且影响企业实现合规管理体系预期结果的能力的内部和外部事项。企业应考虑的事项包括但不限于：

a) 业务模式；
b) 自身的合规文化与第三方业务关系的性质和范围；
c) 法律和监管环境；
d) 经济状况；
e) 社会和文化环境。

5.2 理解利益相关方的需求和期望

企业应确定合规管理体系的利益相关方，并理解利益相关方的需求和期望。

5.3 确定合规管理体系的适用范围

5.3.1 企业应确定合规管理体系的边界和适用性，以确立其范围。企业应根据 5.1 提及的内外部事项以及企业理解利益相关方的需求（见 5.2）、识别合规义务、开展合规风险评估等要求，确定合规管理体系的范围。

注：合规管理体系的范围旨在理清企业面临的主要合规风险，以及合规管理体系适用的国家、地域、行业和/或企业边界，尤其当企业作为集团或其他组织的一部分时。

5.3.2 确定合规管理体系范围的相关信息应作为文件化信息，并可获取。

5.4 建立合规管理体系

企业应结合企业环境，建立、实施、维护和持续改进合规管理体系。合规管理体系应反映企业的价值观、目标、战略和合规风险。

6 领导作用

6.1 最高领导者的作用和承诺

企业最高领导者应以身作则，坚持并积极、明确地支持企业合规与合规管理体系建设。企业最高领导者证实其对合规管理体系的领导作用和承诺的方式包括但不限于：

a) 明确合规管理是企业健康发展的基石，确定合规方针和目标，并与企业价值观、目标和战略一致；
b) 确保合规作为企业的核心价值观之一，合规文化成为企业文化的核心组成部分；
c) 与首席合规官建立直接沟通机制，授予其相关权限并确保其工作的独立性；
d) 确保建立合规工作与员工绩效、考核及职级晋升等挂钩的管理机制；
e) 确保合规管理体系的要求融入企业业务流程，并能促进持续改进；
f) 确保为企业合规管理工作配置充分、适当且可用的资源和技术支持。

6.2 合规职责

6.2.1 通则

企业应基于所在国家、区域、行业以及企业类型、业务规模、商业模式等多方面的差异，根据相关法律法规、标准规范等方面的要求，分析本企业所处的环境，搭建权责清晰的合规管理组织架构，并依据规定履行相应职责，推动合规管理体系有效落地实施。

6.2.2 决策层职责

决策层应对合规管理的有效性负责，履行的合规管理职责包括但不限于：

a) 推行合规经营理念，培育企业合规文化，推动完善合规管理体系；
b) 审议批准合规管理体系建设方案、合规管理工作年度报告以及合规管理基本制度等文件；
c) 审议决定合规管理重大事项；
d) 推动完善企业合规管理体系，并对其有效性进行评价；
e) 决定合规管理部门的设置和职能，以及首席合规官的设置和任免。

6.2.3 管理层职责

管理层向最高领导者和决策层负责，履行的合规职责包括但不限于：

a) 依据合规方针和合规目标，指导各部门企业的合规管理工作；

b） 拟订合规管理体系建设方案；
c） 拟订合规管理基本制度，组织制定合规管理具体制度，批准合规管理工作年度计划；
d） 建立与合规绩效考核挂钩的人员绩效考核制度，确保合规绩效考核制度的实施；
e） 组织应对重大合规风险事件。

6.2.4 业务及职能部门合规职责

业务及职能部门承担本部门合规管理的主体责任，履行的合规职责包括但不限于：
a） 对本部门规章制度、合同等文件及经营管理活动进行合规审查；
b） 建立并完善本部门业务合规管理制度和流程，编制合规风险清单和应对预案；
c） 梳理重点岗位的合规风险，将合规要求纳入岗位职责；
d） 组织开展合规风险识别评估，及时向合规管理部门报告合规风险，组织或配合开展合规风险事件的应对处置；
e） 组织或配合开展违规事件的合规调查和整改。

6.2.5 合规管理部门/首席合规官职责

6.2.5.1 合规管理部门是企业合规工作的牵头部门，应在企业相关管理制度中明确合规管理部门的地位、权限和独立性。合规管理部门向首席合规官负责，履行的合规职责包括但不限于：
a） 组织起草合规管理基本制度和具体制度规定、合规管理工作年度计划、合规管理工作年度报告；
b） 组织开展合规风险识别、评估、预警和应对；
c） 开展规章制度、重大业务活动、重大决策的合规审查；
d） 组织或协助各部门开展合规培训，受理合规咨询和合规沟通事宜，推进合规信息化建设；
e） 依据最高领导者和决策层的授权，规划设计合规管理体系，协助监督层或第三方机构开展合规管理体系有效性的评审；
f） 组织开展合规检查，指导企业开展合规管理工作；
g） 组织或协助开展合规考核评价；
h） 受理职责范围内的违规举报，组织或参与对违规事件的调查，并提出处置建议。

6.2.5.2 首席合规官向企业最高领导者和决策层负责，领导合规管理部门组织开展企业的合规管理工作。

注1：是否设置专职的合规管理部门及首席合规官取决于企业规模、企业面临的合规风险程度等因素。

注2：企业根据实际发展需要，决定是否由合规相关职能部门（如风险管理部门、法律事务部门等）及相应人员（如合规总监、风控总监等）分别兼任合规管理部门和首席合规官。

6.2.6 监督层职责

监督层负责监督合规管理体系的有效运行，履行的合规职责包括但不限于：
a） 监督企业经营管理活动和员工履职行为的合规性；
b） 在职权范围内对违规事件进行调查，按照规定开展责任追究，并提出处置建议。

6.3 合规方针

6.3.1 合规方针应确立企业开展合规管理体系建设的首要原则和行动承诺，由企业最高领导者和决策层审议批准。

6.3.2 合规方针应与企业的价值观、目标和战略保持一致，宜规定：
a） 与企业的规模、性质、复杂性及其环境相关的合规管理体系的应用和环境；

b） 合规与其他职能的结合程度；
c） 对内外部相关方的关系进行管理的原则。

6.3.3 合规方针可包括：

a） 使命宣言；
b） 方针声明；
c） 管理战略；
d） 责任和资源的分配；
e） 违规后果；
f） 影响。

6.3.4 合规方针应用通俗易懂的语言书写以便于所有员工能理解其原则和目的，并以恰当的方式向员工宣贯及向利益相关方传达。

6.4 合规文化

企业应在其内部各个层级建立、维护并推进合规文化，措施包括但不限于：

a） 最高领导者、决策层和管理层以身作则，遵循和落实合规价值观，倡导和推行合规文化；
b） 建立制度化、常态化的合规培训机制，制定年度合规培训计划，将合规作为合规管理重点人员培训的必修内容和任职上岗的必备要求；
c） 通过制定合规手册、签订合规承诺书、开展合规宣誓等方式将合规理念传递至全体员工，确保其了解合规义务；
d） 通过合规建设情况公开披露、宣传等方式，将合规文化传递至利益相关方，确保其了解企业的合规要求；
e） 建立合规绩效考核体系并运行实施，将绩效考核结果与薪酬待遇、职务任免等挂钩；
f） 建立合规奖励机制，鼓励员工提出改进合规管理的意见和建议；
g） 建立健全合规人才的选拔、培养和任用机制。

7 策划

7.1 合规目标及其实现的策划

7.1.1 合规目标确定了企业合规管理实现的结果，企业应在相关职能和层级上确立合规目标。合规目标应可测量、监视和沟通，并作为文件化信息可获取。

7.1.2 策划如何实现合规目标时，企业应确定：

a） 要做什么；
b） 需要什么资源；
c） 由谁负责；
d） 何时完成；
e） 如何评价结果。

7.1.3 企业应适时评审合规目标，并适当更新。

7.2 应对合规风险的措施

7.2.1 风险识别

企业应建立健全合规风险识别机制，准确识别潜在的合规风险。具体做法可包括：

a） 持续收集与合规相关的法律法规、监管规定等合规义务，对照现有业务和流程，识别风险源；
b） 全面系统梳理企业经营管理活动中存在的合规风险，建立合规风险台账；
c） 系统分析风险源、风险类别和风险形成因素。

7.2.2 风险评估

7.2.2.1 企业应定期、及时开展全面合规风险评估，并将结果纳入企业风险评估报告，且应根据法律法规及过往的经验，适时对评估制度和程序予以修订和更新。

7.2.2.2 企业应在合规风险识别（见 7.2.1）的基础上对合规风险发生的可能性、影响程度等进行分析、判断，并确定衡量重要性水平的方法或程序。合规风险评估结果将作为风险应对（见 7.2.3）的主要依据。合规风险评估应考虑：

a） 企业的风险承受度及其对前提和假设的敏感性，并适时与利益相关方有效地沟通；
b） 可能存在的专家观点中的分歧，及风险评估中数据或模型的局限性；
c） 风险评估首先采用定性分析，初步了解风险等级和揭示主要风险，适时进行更具体和定量的分析；
d） 风险后果和可能性通过专家意见、结果建模、实验研究推导等方式确定。

注：风险评估方法见GB/T 24353—2022。

7.2.2.3 当发生下列情形时，企业应对合规风险进行再评估：

a） 新的或变化的活动、产品或服务；
b） 组织结构或战略变化；
c） 重大外部变化，如金融经济环境、市场条件、债务和客户关系；
d） 合规义务变更；
e） 并购；
f） 不合规。

7.2.3 风险应对

企业应细化风险报告机制、细分风险类别、量化报送等级，并根据合规风险类型制定和选择合规风险应对方案，同时应注意针对风险水平合理分配资源。对于可能造成重大资产损失或严重不良影响的重大合规风险事件，应制定合规应急预案，及时预警，明确应急处理职责、路径和要求，由企业最高领导者和决策层统筹领导，明确牵头部门，相关部门协同配合，最大程度化解风险、降低损失。

7.3 合规管理体系变更的策划

7.3.1 当企业确定需要变更合规管理体系时，应对变更实施策划。

7.3.2 企业在策划合规管理体系变更时应考虑：

a） 变更目的及其潜在后果；
b） 合规管理体系的设计和运行的有效性；
c） 资源的可获取性；
d） 职责和权限的分配或再分配。

8 支持

8.1 聘用程序

对所有员工，企业应：

a) 在聘用条件中要求被聘用人员遵守企业的合规义务、方针等，同时有权对任何违反企业合规方针的行为进行处置；
b) 在员工入职后，为员工提供合规相关制度文件的副本或其获取渠道，并提供相关培训；
c) 制定违反合规义务、方针的处理程序；
d) 按照附录 A 的要求，结合合规管理重点人员的合规风险，在员工聘用、调动和晋升前进行尽职调查。

8.2 合规培训

8.2.1 企业应建立制度化、常态化、全员化且与合规风险相适应的合规培训机制，包括但不限于：
a) 将合规培训纳入员工培训计划；
b) 将代表企业开展业务并可能给企业带来合规风险的第三方纳入合规培训范围；
c) 针对不同培训对象开展有针对性的合规培训，与员工的岗位及其面临的合规风险相适应；
d) 依据外部监管环境变化与合规义务变化，不断更新合规培训内容；
e) 进行有效性评估，企业可在员工接受培训后适时安排测评，确保员工理解、遵循合规方针、目标和要求；
f) 开展多种形式的合规培训，必要时可聘请外部专家对员工进行培训。及时评估培训对员工行为或态度的影响程度，以不断优化调整培训形式；
g) 合规培训的内容包括但不限于法律法规、行为准则、合规文化、合规制度、典型案例。

8.2.2 培训记录应作为文件化信息予以保留。

8.3 合规沟通

8.3.1 企业应建立内外部的沟通渠道，沟通内容及方式包括但不限于：
a) 在企业内部各层级公开和传达合规管理方针及合规管理制度、合规文化，确保员工了解并遵循合规相关要求，沟通方式可包括岗前培训、合规培训、合规例会、合规热线等；
b) 与外部监管机构、商业伙伴等利益相关方进行合规事项的沟通协调，促进双方的理解和良好互动，沟通方式可包括网站、电子邮件、定期简报、座谈等；
c) 企业在建立沟通时应将其合规文化、合规目标和义务纳入沟通内容，同时确保所沟通的合规信息来源于合规管理体系且真实可信；
d) 确保并鼓励员工在沟通过程中就合规事项提出疑虑，并明确告知员工合规报告途径；
e) 确保并鼓励员工在沟通过程中提出合规管理体系改进建议；
f) 对与合规管理体系相关的沟通内容进行回应。

8.3.2 企业视情况，保留文件化信息作为其沟通的证据。

8.4 合规考核

8.4.1 企业应建立涵盖所有部门、全体员工及全业务流程的合规考核机制。企业应鼓励员工提供违规线索或提出改进合规管理的意见和建议，对于作出重要贡献的可给予奖励。

8.4.2 企业应将合规管理的有效性和履职行为的合规性等合规管理情况，纳入对部门和员工的综合考核，并将合规管理工作的考核结果，作为绩效考核、员工晋升、评先选优等工作的重要依据。

8.5 合规咨询

企业应建立合规咨询渠道，确保任何员工在企业经营管理行为中对涉及合规的问题感到疑虑时，可向合规管理部门进行咨询并能及时得到回应。

8.6 文件化信息

企业应以适当的形式（例如语言文字、图形）和载体（例如纸质的、电子的）记录和归档合规管理体系运行产生的文件化信息，如合规管理制度文件、合规审查意见、合规检查原始文件、合规培训、沟通、咨询、举报、调查等的相关信息和文件记录。该文件化信息应：

a) 以清晰、易获取和可检索的方式保存；

b) 得到充分保护（例如，防止泄密、不当使用或完整性受损）。

8.7 信息化建设

企业宜建立合规管理信息系统，加强合规管理信息化建设，可运用信息化工具做如下处理：

a) 对文件化信息进行收集、存储、分类和传递；

b) 将合规要求嵌入业务经营流程，强化对企业经营管理活动合规情况的动态监测和过程管控；

c) 为企业开展合规审查、合规检查（见 9.1）、合规绩效评价、合规培训等工作提供保障、支持。

9 运行

9.1 合规审查与检查

9.1.1 企业应将合规审查作为企业经营管理流程的必经程序，建立健全合规审查机制，明确审查范围、流程和标准，并确保进行重大事项决策、重要合同签订、重大项目运营等经营管理活动前，已实施合规审查。

9.1.2 企业应建立健全合规检查制度，制定合规检查计划并实施。

注：合规检查是指合规管理部门不定期对企业部门和所属企业的经营管理和执业行为的合规性开展检查。合规管理部门能调阅所需的任何记录和有关合规文件、档案材料等，并要求相关部门、所属企业及其员工对有关事项作出说明。

9.1.3 企业应对违规事件或行为采取措施，对违规问题进行整改，并通过健全规章制度、优化业务流程等，堵塞管理漏洞，不断提升依法合规经营管理水平。

9.2 合规调查

9.2.1 合规管理部门应就举报线索在合理范围内及时组织开展合规调查，合规调查前应制定适当的调查方案，包括但不限于调查范围、调查程序、调查方法。

9.2.2 合规调查可采用内部调查、外聘第三方调查等调查形式，依据事项的复杂程度与严重程度，邀请法务、审计人员、外部法律专家、律师等参与调查。调查过程应由具有专业能力且不存在利益冲突的人员独立进行。

9.2.3 合规调查过程中保障被调查对象的合法权益。

9.2.4 合规调查结束后，依据违规处理与问责机制对违规行为进行问责处理。

9.2.5 企业应保留有关调查的文件化信息。

9.3 合规报告

9.3.1 企业应建立、实施并维护合规报告渠道，确定适宜的报告准则。业务及职能部门在经营管理活动中发现合规风险，应按有关要求向合规管理部门报告，合规管理部门按要求向最高领导者和决策层报告合规管理情况。合规报告内容包括但不限于：

a) 合规风险识别及分析情况；

b) 合规义务变更时对企业的影响，及企业对此变更采取的新的措施方案；

c） 违规情况分析及采取的纠正措施；
d） 合规管理体系绩效评价的有效性及后续持续改进建议；
e） 与监管机构的沟通情况；
f） 合规审查及合规调查的情况。

9.3.2 当发生性质严重或可能给企业带来重大合规风险的事件，合规管理部门应及时向最高领导者和决策层报告。

9.4 合规举报与违规处理

9.4.1 举报

企业应建立、实施和维护相应的合规举报渠道，确保：
a） 举报渠道畅通，举报渠道可包括：举报信箱、热线电话、邮箱和第三方平台；
b） 指派专人对举报信息进行收集和管理；
c） 对举报内容和举报人进行保密，使其不会受到任何形式的打击报复；
d） 所有员工了解举报程序和保护措施，并能运用相关程序。

9.4.2 违规处理

企业应建立并完善违规处理和整改机制，从对违规事件的应报未报责任、违规行为责任、违规事件的整改三方面，明确责任范围，细化追责问责标准。违规处理和整改机制的内容包括但不限于：
a） 针对违规事件或行为，明确应报未报，或迟报、谎报、瞒报、漏报的处理标准；
b） 依据对违规事件或行为的调查结果，明确违规部门或人员的处置标准；
c） 根据调查结果，及时进行整改并反馈整改情况。

10 绩效评价

10.1 监视、测量、分析和评价

10.1.1 企业应对合规管理体系的有效性进行监视和测量，开发合规管理评价指标体系，对监视和测量的结果进行分析和评价，合理地运用分析和评价结果。

10.1.2 企业应保留对监视、测量、分析和评价的结果的文件化信息。

10.2 内部审核

10.2.1 企业应按合规工作计划，定期开展内部审核，以证实合规管理体系符合企业自身对合规管理体系的要求及本文件的要求，包括合规管理的基本原则、组织环境、管理职责、风险管理、支持、运行、绩效评价、持续改进、合规管理的重点人员、合规管理的重点环节、合规管理的重点领域建设及运行状况等方面。其中，企业合规管理体系中重点环节应符合附录 B 的要求，重点领域应符合附录 C 的要求。

10.2.2 在开展内部审核工作时，企业应：
a） 建立、实施和维护合规管理体系的内部审核管理制度和审核方案，包括频次、方法、责任、策划要求和报告等要素；
b） 规定每次审核的目标、准则和范围；
c） 挑选能胜任的审核员进行审核，确保审核的客观性和独立性；
d） 在实施内部审核后，形成合规内部审核报告，保留审核方案、审核结果及相关材料的文件化信息；

e） 确保审核结果报告提交最高领导者和决策层、相关管理层、合规管理部门。

注1：ISO 19011提供了关于管理体系审核的指南。

注2：企业内部的审核范围和规模依据企业的规模、结构、成熟度和所在区域等决定。

10.3 管理评审

10.3.1 通则

最高领导者和决策层应在策划的时间间隔内对企业的合规管理体系开展管理评审，以确保合规管理体系的适宜性、充分性、有效性。

10.3.2 管理评审的开展

管理评审应包括：

a） 企业内部和外部关于合规管理审核、审计和评价的结果；
b） 合规审核针对违规和潜在违规的分析报告、采取的纠正措施和改进措施的情况及实施的效果；
c） 重大事故、事件、案件、行政处罚的文件；
d） 内部举报及投诉反馈信息，及利益相关方的反馈信息；
e） 合规管理体系的实施和运行情况，实现合规方针、合规目标的情况；
f） 合规管理体系过程监视和测量的结果；
g） 可能影响合规管理体系的内部和外部的环境变化，包括企业环境、相关法律法规和其他要求的变化；
h） 保障合规管理体系正常、有效开展的合规管理资源配置情况；
i） 员工提出的合理的改进建议。

注：邀请外部专家对企业合规管理体系的建立和实施效果进行评审，是企业开展管理评审的一种方式。

10.3.3 管理评审结果

10.3.3.1 企业实施管理评审后，应形成管理评审报告、管理评审决议等管理评审结果，并针对不合规事项提出纠正意见。

10.3.3.2 企业应保留管理评审结果及相关材料的文件化信息。

11 持续改进

11.1 持续改进

企业应结合违规事件或行为与合规管理体系绩效评价结果，在合理的成本和可接受风险的条件下，持续改进和完善合规管理体系，确保其适宜性、充分性和有效性。

11.2 违规与纠正措施

11.2.1 企业出现违规事件或行为时应：

a） 对违规事件或行为作出反应；
b） 采取措施避免事件或行为再次发生；
c） 实施任何必要的措施；
d） 评审所采取纠正措施的有效性；
e） 在必要时，变更合规管理体系。

11.2.2 以下事项的证据应作为文件化信息，并可获取：

a） 违规、不合规事件或行为的性质和所采取的后续措施；
b） 实施纠正措施后的结果。

附 录 A
（规范性）
合规管理的重点人员

A.1 管理人员

企业应促进管理人员切实增强合规意识，带头合规开展经营管理活动，认真履行承担的合规职责，强化对管理人员的合规考核与监督问责。

A.2 重要风险岗位人员

企业应依据合规风险评估情况明确界定重要风险岗位，加强针对性培训，使重要风险岗位人员熟悉并严格遵守业务涉及的各项规定，并加强对其的监督检查和违规行为问责。重要风险岗位人员应遵循回避原则，以有效防控岗位利益冲突风险。

A.3 境外人员

企业应将合规培训作为境外人员任职、上岗的必备条件，确保遵守我国和所在国法律法规及监管等相关规定及合规要求。

A.4 新入职人员

企业应在员工招聘过程中开展尽职调查，开展新入职人员的合规培训，确保其熟悉并能履行与职位和职务相关的合规义务。

A.5 其他需要重点关注的人员

其他需要重点关注的人员应视情况开展强化合规管理意识、合规培训、监督问责等工作，确保其符合相关合规要求。

附 录 B
（规范性）
合规管理的重点环节

B.1 制度制定环节

企业应强化对企业章程、规范等内部管理重要文件的合规审查，把合规要求融合企业制度中，确保符合法律法规和标准的相关规定的要求。

B.2 决策环节

企业应坚持科学决策、依法决策的原则，细化各层级决策事项和权限，将合规审查作为决策前置程序，防范决策风险，保障决策依法合规。对涉及重大事项决策、重要人事任免、重大项目投资、大额资金运作的事项，加强合规论证和审查。

B.3 生产运营环节

企业应严格执行各项合规管理制度，加强对生产运营重点流程的监督检查，确保生产经营过程中按规定的要求操作。

附 录 C
（规范性）
合规管理的重点领域

C.1 廉洁

企业应遵守廉洁相关法律法规、监管规定、行业准则和国际条约、规则、标准，以及企业章程、规章制度等要求，公开声明反对任何形式的不廉洁行为，确保以合规的方式开展业务活动。企业应制定符合相关法律法规的规定和程序、且相关费用控制在规定范围内的赠礼、招待、赞助、捐赠及类似利益流通的相关政策，建立健全企业与商业伙伴、政府工作人员等的交往礼仪与规范。加强员工管理和培训，构建廉洁合规的管理机制和措施，防止腐败行为。

C.2 产品与服务质量

企业应依据适用的相关法律法规、标准规定的产品使用、安全和其他特性的要求，对产品规划、设计、制造、检测、计量、运输、储存、销售、售后服务、回收等环节实施产品全生命周期监督，保障产品符合相关法律法规、标准规定。企业应建立技术研发、生产、应用、服务等方面的管理体系和制度，及时响应监管部门的监管要求。

C.3 安全生产

企业应遵守安全生产相关法律法规、标准等要求，落实全员安全生产责任制，建立健全安全管理体系及安全生产规章制度、应急管理制度、安全教育培训制度，加强安全生产风险管控及监督检查，及时发现并纠正违规问题，保障从业人员安全。

企业应建立健全职业病防治机制，落实职业病预防措施，工作场所应符合职业卫生标准和要求，保障劳动者职业健康权利。

C.4 环境保护

企业应遵守环境保护管理相关法律法规要求，明确各级部门、单位和人员的环境保护职责，实施污染治理设施运行管理和一般工业固体废物和危险废物管理，执行相关环境保护的管理制度，包括环境影响评价、污染源监测、清洁生产审核评估等。企业应规范环境应急管理制度，按法律法规要求实施环境保护信息公开，开展环境保护宣传、教育、培训相关工作。

C.5 知识产权

企业应及时依法申请或登记注册知识产权成果，对已取得的权利及时续展维护。应规范实施知识产权许可和转让，及时制止侵权行为，依法依约规范使用第三方知识产权，防止侵犯第三方合法权益。应规范涉外业务知识产权管理，明确涉外业务中的侵权风险评估、合同责任与义务界定的程序和方法。

C.6 劳动用工

企业应贯彻实施劳动用工相关法律法规，建立和完善劳动规章制度，规范劳动合同签订、履行、变更、竞业禁止约定内容、中止和解除，确保劳动用工各环节合规、规范有序，切实维护企业和员工合法权益。

C.7 财务税收

企业应依照相关税收法律法规规定，规范企业税务管理，完善财务内部管理和监督体系，结合企业情况建立财务决策、财务决策回避、财务风险管理、财务预算管理、资金筹集管理制度。在境外进行纳税活动的企业，应遵守相关法律法规，并依据境外税收政策变化实施变更。

C.8 网络与数据安全

企业应遵守相关的法律法规，采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故。依法保障信息资产的安全，加强信息数据的收集、存储、处理、分发、删除等重点环节的管控，评估数据安全风险，防范信息安全事件的发生，降低突发事件对信息系统的影响，提升信息系统的高可用性。依法建立事件应急处置机制，配备应急响应所需的资源以确保应急响应机制有效实施。

C.9 个人信息保护

企业处理个人信息应遵守相关法律法规，按照权责一致、目的明确、选择同意、最少够用、公开透明、确保安全、主体参与的原则，制定个人信息保护政策，建立和实施技术控制、实施控制、监控控制，保证个人信息的收集、存储、处理、共享、转让和公开披露中的数据安全及合规。企业对个人信息跨境传输时，应遵循相关法律法规的规定。企业应制定并执行个人信息安全应急处理机制，在发生或可能发生个人信息泄露、篡改、丢失时，应依法采取相应补救措施，并通知履行个人信息保护职责的部门和员工。

C.10 商业伙伴管理

企业应对重要商业伙伴开展全面的、基于风险的合规尽职调查，并结合风险特征对其进行合规分级、分类管控。企业应对商业伙伴的履约能力进行定期跟踪和评估，保留在特定业务和交易中对商业伙伴进行检查和审计的权利，如有证据证明商业伙伴存在重大违法行为、违约失信记录，发生质量事故、安全事故或违反廉洁等情形的，可依法依约及时终止与商业伙伴开展业务合作。企业应要求商业伙伴做出合规承诺，宜通过签订合规协议、增加合规条款、开展合规培训与沟通等措施，传播合规理念及良好实践，促进商业伙伴行为合规，防止商业伙伴传导合规风险。

C.11 反垄断

企业应遵守反垄断相关法律法规，避免达成垄断协议，具有市场支配地位的企业不应滥用市场支配地位。达到反垄断法相关规定的经营者集中申报标准的企业，应事先向反垄断执法机构申报，未申报的不应实施集中。

C.12 反洗钱与反恐怖融资

企业应依据相关金融法律法规要求，结合企业自身特点，建立合规的交易、监测体系，有效识别和应对洗钱与恐怖融资风险，建立健全反洗钱的风险管理措施，防范洗钱与恐怖融资风险。

C.13 境外业务

企业应严格遵守国际规则、国内国外投资监管要求和所在国家（地区）法律法规，加强对境外投资及贸易行为的合规管理，将合规培训作为境外人员任职、上岗的必要条件。应结合境外经营实际，在对外贸易、境外投资、对外承包工程、境外日常经营等各领域制定合规操作流程，重点关注、识别、防控投资保护、市场准入、外汇管制、反洗钱、反恐怖融资、进出口管制、环境保护、税收、劳工等领域的风险，确保境外投资经营行为依法合规和境外资产安全。

参 考 文 献

[1] ISO 19011:2018 管理体系审核指南（Guidelines for auditing management systems）
[2] GB/T 20270—2006 信息安全技术 网络基础安全技术要求
[3] GB/T 24353—2022 风险管理 原则与实施指南
[4] GB/T 27921—2011 风险管理 风险评估技术
[5] GB/T 35273—2020 信息安全技术 个人信息安全规范
[6] 国务院国有资产监督管理委员会.中央企业合规管理办法：国资委第42号令.2022年