

DB4403

深 圳 市 地 方 标 准

DB4403/T XXXXX—XXXX

企业合规管理体系

Enterprise compliance management systems

(征求意见稿)

XXXX-XX-XX 发布

XXXX-XX-XX 实施

深圳市市场监督管理局

发布

目 次

前言	II
引言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 基本原则	1
5 组织体系与管理	2
6 专项领域与管理	6

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。

本文件参考了ISO 37301《合规管理体系 要求及使用指南》（英文版）。

本文件由深圳市司法局提出并归口。

引 言

为有效开展合规，目前国际标准化组织已发布了ISO 37301《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。2017年我国等同采用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》，同时也深入推进合规改革，发布相关合规管理措施，为企业长远发展和持续成功提供助益。

合规是企业实现成功和可持续发展的基石，是一个持续的过程。合规的可持续性体现在将合规融入企业的治理、管理、所有业务过程以及人员的行为和意识，建立并维护合规文化。推行企业合规管理，能够使企业有效维护自身诚信，避免或尽量减少因不合规行为给企业带来的损失。

本文件为企业制定合规管理体系提供了细致全面的指引和建议，帮助企业预防、发现和处理合规风险，并证明企业为实现上述目标已经实施了合理和适当的措施，企业可根据自身规模及内外部环境等因素制定符合自身发展目标的合规管理体系。

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、组织体系与管理、专业领域与管理等。
本文件适用于深圳企业（经营者）开展合规管理体系建设和评价，包括自评、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 23694—2013 风险管理 术语

GB/T 24353—2009 风险管理 原则与实施指南

GB/T 27921—2011 风险管理 风险评估技术

GB/T 35770 合规管理体系 指南

SZDB/Z 245-2017 反贿赂管理体系

ISO 37001 反贿赂管理体系要求及使用指南（Anti-bribery management systems — Requirements with guidance for use）

ISO 37301 合规管理体系要求及使用指南（Compliance management systems — Requirements with guidance for use）。

3 术语和定义

GB/T 23694、GB/T 35770界定的以及下列术语和定义适用于本文件。

3.1

经营者 undertakings

从事商品生产、经营或者提供服务的自然人、法人和非法人组织。

4 基本原则

4.1 有效适应原则

经营者合规管理应从经营范围、组织结构和业务规模等实际情况出发，兼顾成本与效率，强化合规管理制度的可操作性，提高合规管理的有效性。同时，经营者应随着自身业务改变与外部环境的变化持续调整和改进合规管理体系。

4.2 全面覆盖原则

经营者合规管理应覆盖经营者经营活动全业务领域、各部门、各层级子经营者、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

经营者合规管理应充分发挥内部监督与外部制约机制，从组织机构设置、制度设计、汇报路径等方面保证合规管理工作的独立性，合规管理机构及人员承担的其他职责不应与合规职责产生利益冲突。

4.4 协同联动原则

经营者应推动合规管理与法律风险防范、监察、审计、内控、风险管理等工作的统筹和衔接，确保合规管理体系有效运行。

5 组织体系与管理

5.1 组织环境

5.1.1 理解经营者自身情况及外部环境

经营者应确定内部和外部问题，如与合规风险相关、与合规目标相关和影响组织实现合规管理体系预期成果能力问题。同时，经营者应考虑更大范围的内部和外部因素，如监管、社会和文化环境、经济形势、内部方针、程序、过程和资源。

5.1.2 理解利益相关方的需求和期望

经营者应确定合规管理体系的利益相关方及利益相关方的要求。

5.1.3 建立经营者合规机制

经营者应根据本文件，建立合规机制，充分认识到设置合规管理组织体系的重要性，设立独立的合规部门，高度重视合规部门的建设。

5.2 领导职责

5.2.1 经营者决策层职责

经营者决策层职责应包括：

- a) 批准合规管理规划、制度和年度报告；
- b) 推动完善合规管理体系；
- c) 决定合规管理负责人或负责部门；
- d) 听取合规管理部门就重大合规事项的汇报；
- e) 决定合规管理负责部门的设置和职能；
- f) 研究决定合规管理重大事项；
- g) 按照权限决定违规人员的处理事项。

5.2.2 经营者管理层职责

经营者管理层职责应包括：

- a) 根据决策层的决定，建立健全合规管理组织架构；
- b) 批准合规管理具体制度规定；
- c) 根据合规管理规划，采取有效措施确保合规制度的实施；
- d) 明确合规管理流程，确保合规融入业务领域；
- e) 及时制止并纠正一切不合规行为，按照权限对违规人员进行责任追究并提出处理建议。

5.2.3 经营者监督层职责

经营者监督层职责应包括：

- a) 监督经营者决策层的决策与流程是否合规；

- b) 监督经营者决策层和管理层合规管理职责履行情况；
- c) 向决策层建议合规管理负责人的任免。

5.2.4 经营者合规管理部门/负责人职责

5.2.4.1 经营者合规管理部门职责

经营者合规管理部门职责应包括：

- a) 研究起草合规管理体系，制订经营者合规管理建设规划和实施方案；
- b) 制订年度合规管理工作计划，推动合规管理工作贯彻落实；组织编报合规管理年度报告；
- c) 持续关注重大法律法规等变化，组织开展合规风险识别和预警，参与公司重大事项合规审查和风险应对，有效进行风险评估工作；
- d) 组织协调开展专项合规工作，参与公司重大事项决策、重要规章制度、重大合同的法律合规审查；
- e) 设定合规培训计划指标，组织、协助业务部门、人力资源部门、培训部门开展合规培训；
- f) 组织开展合规检查工作，督促违规整改和持续改进，参与违规事件处置；
- g) 参与经营者合规管理考核、评价工作；
- h) 指导所属经营者开展合规管理工作；
- i) 参与合规管理工作经费预算审核与统筹。

5.2.4.2 经营者合规管理部门负责人职责

经营者合规管理部门负责人职责应包括：

- a) 组织制订合规管理规划、制度及规定；
- b) 组织起草合规管理年度报告；
- c) 参与重大决策并提出合规建议；
- d) 领导合规管理部门开展工作；
- e) 向领导层汇报合规管理重大事项。

5.2.5 经营者业务部门合规职责

经营者业务部门职责应包括：

- a) 按照合规要求完善业务管理制度和流程；
- b) 主动开展合规风险识别和隐患排查；
- c) 配合进行合规问题调查并及时整改。

5.3 评价与改进

5.3.1 模式

5.3.1.1 评价考虑因素

5.3.1.1.1 评价考虑因素应包括：

- a) 以往评价所采取措施的状况；
- b) 与合规管理体系有关的外部 and 内部事项的变化；
- c) 合规绩效应考虑以下事项：不符合、不合规与纠正措施；监视和测量的结果；审核的结果。
- d) 持续改进的机会。

5.3.1.1.2 评价应体现：

- a) 合规方针的充分性;
- b) 合规团队的独立性;
- c) 合规目标的达成度;
- d) 资源的充分性;
- e) 合规风险评估的充分性;
- f) 现有控制和绩效指标的有效性;
- g) 与提出疑虑的人员、相关方的沟通, 包括投诉和反馈;
- h) 调查情况;
- i) 报告机制的有效性。

5.3.1.2 评价结果

5.3.1.2.1 评价结果应包括持续改进的机会、变更合规管理体系的任何需要的决定。

5.3.1.2.2 评价结果应文件化并可获取。

5.3.2 持续改进

5.3.2.1 经营者应对合规风险进行监测。

5.3.2.2 经营者出现不符合或不合规事件时, 应:

- a) 对不符合或不合规事件做出反应;
- b) 采取措施避免事件再次发生;
- c) 实施任何所需的措施;
- d) 评价所采取纠正措施的有效性;
- e) 如必要, 变更合规管理体系。

5.3.2.3 经营者应结合违规事件与合规管理体系评价结果, 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制度。

5.3.2.4 文件化信息应作为以下事项的证据可获取:

- a) 违规事件的性质和采取的后续措施;
- b) 纠正措施的结果。

5.4 保障机制

5.4.1 合规培训

5.4.1.1 经营者应建立制度化、常态化合规培训机制, 包括:

- a) 将合规培训纳入员工培训计划;
- b) 针对不同培训对象开展有针对性的合规培训;
- c) 根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;
- d) 确保员工能通过培训, 理解、遵循合规目标和要求;
- e) 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。

5.4.1.2 合规培训的内容可为行为准则、法律法规、行业典型案例、合规事件等。

5.4.2 合规沟通

经营者应制定合规沟通方案, 制定时应考虑以下方面:

- a) 结合自身合规管理要求;
- b) 确定沟通的过程, 确保结合了相关方的意见;

- c) 与监管机构、合作伙伴等利益相关方进行合规沟通，促进经营者与利益相关方的理解和良好互动；
- d) 确保人员能在沟通过程中提出合规疑虑；
- e) 对与合规管理体系相关的沟通内容进行回应。

5.4.3 合规审查

5.4.3.1 经营者应在合规管理制度中建立健全的合规审查机制，并在以下方面进行重点审查：

- a) 合规制度应符合国家法律法规及相关政策、不应与内部管理制度相冲突、应符合公司规章制度管理规范要求；
- b) 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行为前，应进行合规审查。

5.4.3.2 经营者应落实合规审查中提出的建议，审查资料以文件化形式留存。

5.5 咨询、举报与查处

5.5.1 合规咨询

经营者应建立合规咨询渠道，确保任何员工在商业行为中对涉及合规的问题感到疑虑时，可及时向合规管理部门进行咨询。

5.5.2 举报渠道

经营者应建立和维护合规举报渠道，包括：

- a) 确保举报渠道畅通，举报渠道包括举报信箱、热线电话、邮箱等；
- 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，不应采取任何形式打击报复。

5.5.3 合规调查

合规管理部门应就举报线索展开调查，建立调查管理机制：

- a) 调查过程中保障被调查对象的合法权益；
- b) 调查可采用内部调查、外聘第三方调查等形式；
- c) 合规管理部门根据事项的复杂程度与严重程度，可邀请法务、审计、巡视、纪检监察、外部法律专家、律师等参与调查；
- d) 政府执法开展调查时，经营者有关部门和人员应配合执法机关展开调查活动，并向执法机关如实提供相关情况。

5.5.4 违规处罚

经营者应建立违规处罚机制：

- a) 强化违规问责，完善违规行为处罚机制，明晰违规责任范围，细化惩处标准；
- b) 发现违规事件或行为，应报未报，或迟报、谎报、瞒报、漏报的，根据情节和不良影响程度等，按照管理权限，对相关责任人予以问责处理；
- c) 出现违规行为，根据调查结果及时整改并反馈整改情况；
- d) 高级管理人员出现违规行为，根据章程、制度文件、领导干部管理制度等相关要求追究责任；
- e) 员工出现违规行为，按照公司员工管理及责任追究相关制度追责。

5.6 合规考核评价

经营者应建立合规考核评价机制，评价合规绩效和合规管理体系的有效性：

- a) 将合规管理情况，特别是合规管理的有效性和履职行为的合规性，纳入对部门和员工的综合考核，细化评价指标；
- b) 将合规管理工作的评价结果，作为绩效考核、干部任用、评先选优等工作的重要依据；
- c) 在合规考核中，对各部门、各所属单位及员工存在以下情况的，给予负面评价：
 - 1) 违法违规行为或重大合规风险；
 - 2) 未按要求履行合规管理职责；
 - 3) 因不合规行为或事项被监管处罚等情形。
- d) 当员工在工作中主动合规，及时发现和处置合规风险，或为经营者合规管理工作作出贡献的，应在考核中予以正面评价。

5.7 合规信息化建设

经营者宜加强合规管理信息化建设。

- a) 可通过信息化手段优化合规管理流程，记录和保存相关信息。
- b) 可运用信息化工具，加强对经营管理行为依法合规情况进行实时在线监控和风险分析。

6 专项领域与管理

6.1 风险评估

经营者应定期开展全面合规风险评估并将结果纳入经营者的全面风险评估报告。

6.1.1 风险识别与预警

经营者应建立合规风险识别预警机制：

- a) 全面系统梳理经营管理活动中存在的合规风险，建立合规风险台账；
- b) 持续地收集与合规相关的法律法规、监管规定，对照现有业务和流程，识别风险源；
- c) 系统分析风险源、风险类别、风险形成因素、可能发生的后果及发生的概率；
- d) 对有典型意义、普遍存在的以及可能造成严重后果的风险及时发布预警。

6.1.2 风险评估分析

经营者应在合规风险识别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，并确定风险重要性水平的过程，作为风险应对的主要依据。合规风险评估分析应考虑：

- a) 经营者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数据和模型的局限性；
- c) 风险分析可首先采用定性分析，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风险分析；
- d) 风险后果和可能性可通过专家意见、结果建模、实验研究推导等方式确定。

6.1.3 风险应对

6.1.3.1 经营者应根据不同的合规风险类型制定和选择合规风险应对方案，细化风险报告机制，细分风险类别区分和量化报送等级。对于重大合规风险事件，经营者决策层统筹领导，经营者合规管理部门负责人牵头，相关部门协同配合，最大限度化解风险、降低损失。

6.1.3.2 涉及海外经营风险的，应制定合规应急预案，明确应急处理职责、路径和要求，并报送经营者决策层备案。

6.2 重点环节

6.2.1 制度制订环节

经营者应强化对规章制度等重要文件的合规审查，确保符合法律法规、监管的相关规定要求。

6.2.2 决策环节

经营者应坚持科学决策、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。对涉及重大问题决策、重要干部任免、重大项目投资、大额资金运作的事项，加强合规论证和审查。

6.2.3 生产运营环节

经营者应严格执行合规等各项管理制度，加强对重点流程的监督检查，确保生产经营过程中按章、按规操作。

6.3 专项领域

6.3.1 廉洁

经营者应加强廉洁领域的合规管理，包括但不限于：

- a) 遵守国（境）内外反腐败法律法规及党纪要求，公开声明反对任何形式的贿赂和舞弊行为，确保以合规的方式开展业务活动；
- b) 建立反贪污贿赂管理体系并形成文件化信息，并在实施过程中逐步完善，以保证行之有效；
- c) 制定并实施礼品、招待、赞助、捐赠及类似利益流通的标准和规范性文件，以保证：
 - 1) 符合相关法律法规的规定和程序；
 - 2) 相关费用控制在规定范围。
- d) 指定的管理人员定期/不定期进行审核，应对以下内容开展详尽调查并保持定期更新：
 - 1) 特定的交易、项目或活动；
 - 2) 计划或持续于特定类别的商业伙伴建立或者维持业务关系的行为；
 - 3) 特定岗位的某些员工。
- e) 对采购、运营、销售、人力资源、法律和监管等流程实施财务控制和非财务控制措施：
 - 1) 财务控制措施包括但不限于：履行单一职责，付款的提出和审批不应为同一人；付款审批宜实行梯度授权制度；严格规范授权制度；付款应至少有两人审批；付款同意书需附带支持文件；务必对重大财务实施定期管理评审等；
 - 2) 非财务控制措施包括但不限于：使用通过资格预审的供应商、分包商和顾问；对商业伙伴提供服务内容及服务费用的必要性、合法性、合理性进行评估；制定公平、公正、公开的招投标制度；对潜在高贿赂风险的交易实施严格监督管理；保护投标和其他价格敏感信息的完整性和机密性；向员工提供有效工具和模板（如实操指南、行为准则、检查清单等）。
- f) 严格实施反贿赂控制措施，包括但不限于：
 - 1) 实施反贿赂控制措施并评估该措施管控风险是否有效；
 - 2) 要求商业伙伴进行反贿赂承诺并确保其了解经营者反贿赂方针及处置贿赂事件的程序。
- g) 制定相关制度，以杜绝损害经营者正当利益的舞弊行为发生，防范经营者内、外部人员为谋取自身利益，采用欺骗等手段造成经营者利益受损。包括但不限于以下行为：
 - 1) 收受回扣；

- 2) 将正常情况下可以使经营者获利的事项转移给他人;
 - 3) 因虚假交易事项使经营者支付款项;
 - 4) 故意隐瞒、错报交易事项;
 - 5) 伪造、变造支付记录或凭证。
- h) 明令禁止团体或个人为谋取不当的经营者经济利益而产生舞弊行为, 包括但不限于:
- 1) 为不适当的目的而支出, 如支付贿赂或回扣金;
 - 2) 出售经营者不真实或不存在的资产;
 - 3) 故意错报交易事项、记录虚假交易事项, 虚增经营者收入或低估经营者负债, 出具错误的财务报告, 从而误导投资者做出不适当的投资决策;
 - 4) 隐瞒或删除应对外披露的重要信息。

6.3.2 产品与服务质量

经营者应加强产品与服务领域的合规管理, 包括但不限于:

- a) 生产经营应取得生产许可、强制性认证等资质;
- b) 产品质量安全要求, 符合保障人体健康和人身、财产安全的国家标准、行业标准, 不应存在掺杂、掺假, 以假充真, 以次充好, 或者以不合格产品冒充合格产品的行为;
- c) 产品质量安全过程控制应符合法律法规规定, 禁止使用列入淘汰名录的技术、工艺、设备和材料;
- d) 产品发生产品质量问题的, 应按照规定履行退货、换货、修理义务, 需要召回的, 应按要求履行召回义务;
- e) 产品经营者、经营协助者、市场开办者应履行相关义务;
- f) 及时响应监管部门监督检查工作。

6.3.3 安全生产

6.3.3.1 安全生产组织和管理

经营者应建立全员安全生产责任制明确各岗位的责任人员、责任范围和考核标准等内容, 确保相关人员履行各自的职责。

6.3.3.2 安全生产风险管理

经营者应建立安全生产风险管理制度, 包括但不限于:

- a) 建立安全风险分级管控制度, 按照安全风险分级采取相应的管控措施;
- b) 对重大危险源应:
 - 1) 登记建档, 进行定期检测、评估、监控;
 - 2) 制定应急预案;
 - 3) 告知从业人员和相关人员在紧急情况下应采取的应急措施;
 - 4) 按照有关规定将重大危险源及有关安全措施、应急措施备案。
- c) 教育和督促从业人员严格执行本单位的安全生产规章制度和安全操作规程; 向从业人员如实告知作业场所和工作岗位存在的危险因素、防范措施以及事故应急措施;
- d) 为从业人员提供符合相关标准的劳动防护用品, 并监督、教育从业人员按照使用规则佩戴、使用;
- e) 根据生产经营特点, 对安全生产状况进行经常性检查, 对检查中发现的安全问题, 应:
 - 1) 立即处理;
 - 2) 若不能处理的, 及时报告有关负责人;

3) 将检查及处理情况如实记录在案。

6.3.3.3 安全生产保障

经营者应保障安全生产所需的资金、人力和物资，应确保规定提取和使用安全生产费用，专门用于改善安全生产条件。

6.3.3.4 安全生产教育和培训

经营者应定期针对从业人员、被派遣劳动者、实习人员、特种作业人员等组织分级分类的安全生产教育和培训。

6.3.4 环境保护

6.3.4.1 环境保护合规管理

经营者应明确：

- a) 业务经营所在地的环境资源；
- b) 环境保护的各项法律法规要求；
- c) 环境保护的对象、目标和方针，并与合规体系相适应；
- d) 环境保护合规工作负责人，统筹环保合规工作的制度拟定、执行评估、应急管理、纠正措施等。

6.3.4.2 环境保护合规监督

经营者应建立环境保护合规监督机制，包括但不限于：

- a) 行政负责人和安全负责人等签订安全环保目标责任书；
- b) 强化联动，开展环境保护合规的总部检查、联合检查和专项检查；
- c) 构建分级环保隐患排查防控体系，各层次的隐患排查中发现的问题及时填入环保隐患排查清单；
- d) 对环境舆情、环境保护违法违规行为、突发环境事件进行统计、调查、处理。

6.3.4.3 环境保护合规风险应急

经营者应建立环境保护合规应急机制，包括但不限于：

- a) 向环境排放污染物的企业，生产、贮存、经营、使用、运输危险物品的企业，产生、收集、贮存、运输、利用、处置危险废物的企业，以及其他可能发生突发环境事件的企业，应编制环境应急预案；
- b) 完善环境应急体系，适时修订突发环境事件、辐射事故等领域应急预案，动态更新突发环境事件应急预案备案单位名录；
- c) 建设环境应急物资库，配备充实环境应急物资和装备；
- d) 组建环境保护应急管理队伍，提升应急队伍现场处置能力；
- e) 做好应急值守，组织开展应急演练，快速响应和妥善应对突发环境事件。

6.3.4.4 环境保护合规培训教育

经营者应定期对企业员工进行环境保护合规培训教育，包括但不限于：

- a) 对所有环保管理负责人进行培训；
- b) 对车间一线人员进行环保培训；
- c) 环境保护主题宣传活动。

6.3.5 知识产权

6.3.5.1 知识产权的获取

经营者应及时申请注册登记各类知识产权，明确有关专利申请、集成电路布图设计登记、商标注册、著作权登记、商业秘密保护等知识产权获取及其后续维护或主动放弃的管理措施和工作程序。

6.3.5.2 知识产权的维护

经营者采取措施开展知识产权维护，包括但不限于：

- a) 明晰处置和运营知识产权管理规定；
- b) 明确职务发明成果的界定条件以及委托或合作开发成果知识产权归属的处置原则；
- c) 明确有关专利权、商标权、著作权等知识产权转让、许可、投资、质押的管理措施和工作程序。

6.3.5.3 知识产权的运用

经营者应注重生产经营环节知识产权管理，明确在原材料及设备采购（包括软件等）、技术和产品开发、技术转让（许可）与合作、委托加工、产品销售、广告宣传或展销、招投标、进出口贸易、企业合资及并购和上市等环节中所可能涉及的各项知识产权事务的管理措施和工作程序。

6.3.5.4 上市审查的知识产权

经营者上市前，应对知识产权进行审查，包括但不限于：

- a) 已有的无形资产的法律状态、存续年限、法律风险等进行整体的评估与规划；
- b) 对上市公司准备使用的无形资产的权属和法律状态以及招股说明书中的相关内容的审查；
- c) 知识产权获取、丧失、转让等信息的完整地披露。

6.3.5.5 涉外业务的知识产权

经营者应积极开展涉外业务中的知识产权管理，包括但不限于：

- a) 对拟引进的技术或者产品的相关知识产权状况进行调查分析，并对侵权风险进行综合评估；
- b) 签订技术或产品引进合同、输出合同（包括代理合同）应明确技术或产品引进的许可方式和范围、后续改进成果的归属和分享、权利维护、双方的保密责任和义务、引进技术或产品发生知识产权侵权时供方应承担的法律责任等内容。

6.3.6 劳动用工

6.3.6.1 劳动者的使用

经营者应确保劳动者使用各环节合法合规，规范有序，切实维护企业和员工合法权益，包括但不限于：

- a) 经营者自用工之日起即与劳动者建立劳动关系，并应订立书面劳动合同，且不应违法违规解除劳动合同；
- b) 经营者应按国家法律法规要求，合理安排员工工作时间和休息休假；
- c) 经营者工资分配应遵循按劳分配原则，实行同工同酬；
- d) 经营者应建立、健全劳动安全卫生制度，严格执行国家劳动安全卫生规程和标准，对劳动者进行劳动安全卫生教育，防止劳动过程中的事故，减少职业危害；
- e) 经营者应对女职工和未成年工（年满十六周岁未满十八周岁的劳动者）实行特殊劳动保护；
- f) 经营者应采取保护措施保护劳动者个人信息；

- g) 劳动者离职签署的竞业限制协议应符合法律法规的规定，竞业限制期限由双方约定产生，但最长不应超过两年。

6.3.6.2 职业健康

企业应采取措施保障劳动者职业健康权利，包括但不限于：

- a) 经营者应建立健全职业病防治机制：
- 1) 依照相关职业卫生标准的要求，制定、落实职业健康检查年度计划；
 - 2) 确保职业病防治所需要的专项经费；
 - 3) 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；
 - 4) 建立劳动者职业健康监护制度，包括劳动者上岗前、在岗期间、离岗时、应急的职业健康检查和职业健康监护档案管理。
- b) 经营者应加强劳动者职业健康检查管理，组织劳动者定期进行职业健康检查。加强劳动者职业健康报告和档案管理，及时将职业健康检查结果及职业健康检查机构的建议以书面形式如实告知劳动者。

6.3.7 财务税收

6.3.7.1 财务税收管理体制

6.3.7.1.1 经营者应实行资本权属清晰、财务关系明确、符合法人治理结构要求的财务税收管理体制，应：

- a) 建立财务决策制度，明确决策规则、程序、权限和责任等；
- b) 建立财务决策回避制度。对投资者、经营者个人与企业利益有冲突的财务决策事项，相关投资者、经营者回避；
- c) 建立财务风险管理制度，明确经营者、投资者及其他相关人员的管理权限和责任，按照风险与收益均衡、不相容职务分离等原则，控制财务风险；
- d) 建立财务预算管理制度，以现金流为核心，按照实现企业价值最大化等财务目标的要求，对资金筹集、资产营运、成本控制、收益分配、重组清算等财务活动，实施全面预算管理。

6.3.7.1.2 经营者应在章程等规范性文件中明确投资者和经营者的财务管理职责。

6.3.7.2 资金筹集

经营者筹集资金，应按规定核算和使用，诚信履行合同，依法接受监督，执行相关有关资本管理制度。

6.3.7.3 资产营运

经营者应根据风险与收益均衡等原则和经营需要，确定合理的资产结构，并实施资产结构动态管理。

6.3.7.4 成本控制

经营者应建立成本控制系统，强化成本预算约束，推行质量成本控制办法，实行成本定额管理、全员管理和全过程控制。

6.3.7.5 收益分配

经营者应完善收益分配制度。

6.3.7.6 税收管理

经营者应依照相关税收法律法规规定，规范企业税务管理。

6.3.7.7 信息管理

经营者可以结合经营特点，优化业务流程，建立财务和业务一体化的信息处理系统。

6.3.7.8 财务税收监督

经营者应建立、健全内部财务监督制度。

6.3.8 网络与数据安全

6.3.8.1.1 经营者应遵守适用的法律法规。应采取必要措施，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，使网络处于稳定可靠运行的状态，保障网络数据的完整性、保密性、可用性：

- a) 在运营过程中宜开展数据识别，建立数据保护目录并及时更新；
- b) 依据相关标准，对识别数据开展分级分类管理；
- c) 开展风险防控，建立数据安全责任和评价考核制度，制定数据安全保护计划并开展定期安全风险评估；
- d) 开展审计追溯，对数据处理全周期进行文件化记录。

6.3.8.1.2 保障信息资产的安全，加强信息数据的收集、使用、存储、共享、传输等重点环节的管控，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：

- a) 信息数据的收集：
 - 1) 制定和公开个人信息保护政策并严格遵守；
 - 2) 搜集个人信息，应向个人信息主体明示个人信息保护政策并获得同意；
 - 3) 搜集不满十四岁未成年人个人信息前，应取得未成年人父母或其他监护人的单独同意；
 - 4) 自个人信息主体以外的其他途径搜集个人信息，应知晓个人信息来源及个人信息提供者已获得个人信息处理授权同意范围，并依据相关法律法规要求履行安全保护义务。
- b) 信息数据的存储：
 - 1) 应依据重要数据和个人信息主体约定的存储期限或者个人信息主体授权同意的有效期存储重要数据和个人信息；
 - 2) 应根据相关法律法规规定存储个人生物特征识别信息；
 - 3) 应按要求采取安全措施并以合同等形式进行约定。
- c) 信息数据的使用：
 - 1) 经营者提供定向推送或信息合成服务时，应显著区分定向推送和非定向推送内容，应去标识化；
 - 2) 经营者在开展数据加工活动时，当得知可能危害国家安全、公共安全、经济安全和社会稳定的，应立即要求停止加工活动。
- d) 信息数据的传输：
 - 1) 向接收方传输数据时，应按法律要求采取安全技术措施并进行合同约定；
 - 2) 向境外传输重要数据和个人信息等敏感数据，应遵守相关法律法规规定。
- e) 信息数据的共享：共享、转让重要数据，应明确双方的数据安全保护责任和义务，并采取加密、去标识化和匿名化等安全技术措施。
- f) 投诉、举报受理处置：应建立投诉、举报受理处置制度，并对查实的投诉举报依法采取停止传输等处理措施。
- g) 事件应急处置：应建立事件应急处置机制，宜对数据安全事件分级，配备应急响应所需的资源以确保应急响应机制有效实施。

6.3.9 个人信息保护

6.3.9.1 经营者应严格遵守有关法律法规和规章，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，制定个人信息保护合规方案，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、报告中的数据安全及合规。

6.3.9.2 经营者应针对个人信息最小化管理，应遵循数据搜集最小化、权限控制最小化、存储时间最小化原则。

6.3.9.3 经营者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，应立即采取补救措施，并通知履行个人信息保护职责的部门和个人。

6.3.9.4 经营者应采取数据加密、去标识化和匿名化等安全技术措施保障个人信息安全。

6.3.10 商业伙伴管理

6.3.10.1 经营者应对重要商业伙伴组织开展有记录的、基于风险的合规尽职调查，并结合风险特征对商业伙伴进行合规分级、分类管控，重点关注与商业伙伴合作义务及责任相关的合规义务履行能力和履行情况，重点关注中高合规风险的商业伙伴的合规风险管控，并对不同风险级别的商业伙伴采取不同的合规管理措施。当发生以下情形时，再通过尽职调查评估商业伙伴合规风险：

- a) 商业伙伴出现新的或变更的活动、产品或服务；
- b) 商业伙伴组织结构或战略改变；
- c) 商业伙伴出现重大的外部变化，如金融经济环境、市场条件、债务和客户关系等；
- d) 商业伙伴合规义务发生改变；
- e) 商业伙伴发生并购、重组；
- f) 商业伙伴出现不合规事件。

6.3.10.2 经营者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，应及时终止与商业伙伴开展业务合作。

6.3.10.3 经营者应要求商业伙伴作出合规承诺，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。

6.3.11 反垄断

6.3.11.1 防止垄断协议行为

经营者应有效识别垄断协议的潜在风险并避免从事垄断协议的行为，包括但不限于：

- a) 具有竞争关系的经营者不应利用技术手段、规则、数据和算法等方式达成固定价格、分割市场、限制产（销）量、限制新技术（产品）、联合抵制交易等横向垄断协议和轴辐协议；
- b) 经营者与其交易相对人不应利用技术手段、规则、数据和算法等方式达成固定转售价格、限定最低转售价格等纵向垄断协议；
- c) 与竞争者直接沟通或参与行业会议时，当竞争者有意讨论价格、成本、数量、库存量、交易条件、交易对象、销售市场、限制新技术新产品等与竞争有关的竞争性敏感信息时，应明确拒绝并做好避席的相关证据记录；
- d) 避免以折让、回馈、固定利润率或者成本分摊等方式要求，或者以胁迫、利诱、延迟或取消供货等方式迫使经销商从事转售价格维持的行为。

6.3.11.2 防止滥用市场支配地位

具有市场支配地位的经营者要有效识别并防范滥用市场支配地位的行为，包括但不限于：

- a) 以不公平的高价销售商品或者以不公平的低价购买商品；
- b) 无正当理由以低于成本的价格销售商品，排除、限制市场竞争；
- c) 无正当理由拒绝与交易相对人进行交易，排除、限制市场竞争；
- d) 无正当理由对交易相对人进行限定交易，排除、限制市场竞争；
- e) 无正当理由实施搭售或者附加不合理交易条件，排除、限制市场竞争；
- f) 无正当理由对交易条件相同的交易相对人实施差别待遇，排除、限制市场竞争。

6.3.11.3 防止违规实施经营者集中的行为

经营者应避免实施具有或者可能具有排除、限制竞争效果的集中。实施集中行为宜开展以下工作：经营者集中达到反垄断法相关规定的申报标准的，经营者应事先向反垄断执法机构申报，未申报的不应实施集中。

6.3.11.4 防止滥用行政权力排除、限制竞争行为

行政机关和法律、法规授权的具有管理公共事务职能的组织不应滥用行政权力排除、限制竞争，经营者对于此类滥用行政权力排除、限制竞争行为应予以明确拒绝，并向反垄断执法机构投诉和举报。

6.3.11.5 反不正当竞争

经营者在经营活动中，不应违反相关法律法规，扰乱市场竞争秩序，损害其他经营者或者消费者的合法权益，包括但不限于：

- a) 实施混淆行为，引人误认为是他人商品或者与他人存在特定联系。混淆行为包括但不限于：
 - 1) 擅自使用与他人有一定影响的商品名称、包装、装潢等相同或者近似的标识；
 - 2) 擅自使用他人有一定影响的经营者名称（包括简称、字号等）、社会组织名称（包括简称等）、姓名（包括笔名、艺名、译名等）；
 - 3) 擅自使用他人有一定影响的域名主体部分、网站名称、网页。
- b) 对其商品的性能、功能、质量、销售状况、用户评价、曾获荣誉等作虚假或者引人误解的商业宣传，欺骗、误导消费者。
- c) 侵犯商业秘密的行为，包括但不限于：
 - 1) 以不正当手段获取权利人的商业秘密并披露、使用或者允许他人使用此商业秘密；
 - 2) 违反保密义务或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密。
- d) 编造、传播虚假信息或者误导性信息，损害竞争对手的商业信誉、商品声誉。
- e) 利用网络从事生产经营活动的经营者，不应利用技术手段，通过影响用户选择或者其他方式，实施破坏其他经营者合法提供的网络产品或者服务正常运行的行为，包括但不限于：
 - 1) 未经其他经营者同意，在其合法提供的网络产品或者服务中，插入链接、强制进行目标跳转；
 - 2) 误导、欺骗、强迫用户修改、关闭、卸载其他经营者合法提供的网络产品或者服务；
 - 3) 恶意对其他经营者合法提供的网络产品或者服务实施不兼容。

6.3.12 反洗钱与反恐怖融资

经营者应依法采取预防、监控措施，建立健全反洗钱内部控制制度，包括：

- a) 建立反洗钱工作部门，负责大额现金支付的审批报备、反洗钱工作文字数据的收集分析上报、对反洗钱工作的指导与培训等。经营者应对反洗钱工作部门的人员进行定期审查；
- b) 开展有效的客户尽职调查措施，合理划分和调整客户风险等级；

- c) 针对高风险客户或者高风险账户持有人采取加强型识别或控制措施,如查看高风险客户控制措施的相关文件等;
- d) 依据国(境)内外金融法律法规的监管要求,结合企业自身特点,建立可疑交易的跟踪、监测体系;
- e) 定期开展洗钱、恐怖融资风险评估,并根据评估内容进行内部检查,评估及检查内容应文件化以备检查。
- f) 组织开展反洗钱、反恐怖融资宣传、培训工作,提高员工安全意识;
- g) 配合反洗钱调查,依法履行巨额现金收付申报、反洗钱特别预防措施等义务,不应为洗钱等违法犯罪活动提供便利;
- h) 发现未履行反洗钱义务的情况,应向反洗钱行政主管部门、有关主管部门举报;发现洗钱活动,应向反洗钱行政主管部门、有关主管部门以及公安机关举报。

6.3.13 投资并购

6.3.13.1 经营者应建立健全投资管理制度,包括但不限于:

- a) 投资管理流程、管理部门及相关职责;
- b) 投资决策程序、决策机构及其职责;
- c) 投资项目负面清单制度;
- d) 投资信息化管理制度;
- e) 投资风险管控制度;
- f) 投资项目完成、中止、终止或退出制度;
- g) 投资项目后评价制度;
- h) 违规投资责任追究制度;
- i) 对所属经营者投资活动的授权、监督与管理制度。

6.3.13.2 经营者应制定并购方案,包括但不限于:

- a) 并购主体情况,包括并购方、出让方和并购对象的基本情况以及其他重要股东;
- b) 并购目的及理由分析;
- c) 并购方式和程序;
- d) 并购价格和定价原则、方法;
- e) 涉及的债权、债务和担保抵押等情况及处理办法;
- f) 涉及的职工安置、劳动关系处置等情况及处理办法;
- g) 涉及的重要法律纠纷、诉讼等情况及处理办法;
- h) 并购资金来源,如需筹集资金应说明并购资金筹集及偿还等安排;
- i) 对于并购行为的合法性分析;
- j) 对于并购行为的投资收益预测及财务分析;
- k) 并购过程中包括并购完成后存在的风险分析及防范措施;
- l) 并购完成后对于并购对象的战略规划或资产重组计划;
- m) 并购行为需保留文件化信息。

6.3.14 捐赠

经营者捐赠应充分考虑自身经营规模、盈利能力等财务承受能力,遵循依法合规、自愿无偿、量力而行、诚实守信原则,合理确定捐赠支出的方式、规模和标准,制定捐赠审批制度,诚实进行对外捐赠,合规履行社会责任,包括但不限于:

- a) 按照捐赠制度,做好相关财务处理;

- b) 按照规定程序捐赠，捐赠数额不应影响正常经营活动和职工切身利益；
- c) 在捐赠过程中，应进行严格审查，严肃杜绝以权谋私、假公济私、转移单位资产、向受赠人或受益人索要或收受回扣、佣金、信息费等财物；
- d) 对外捐赠应进行备案管理，以备后续审查。

6.3.15 境外业务

经营者应加强对海外投资及贸易行为的合规管理，严格遵守国际规则、国内国外投资监管要求和所在国（地区）法律法规等。应结合境外经营实际，就合规行为准则和管理办法制定合规操作流程，进一步细化标准和要求。也可将具体的标准和要求融入到现有的业务流程中，便于员工理解和落实，确保各项经营行为合规，包括但不限于：

- a) 境外业务遵守所在国家或地区的法律和我国对境外企业的各项管理规定，依法进行经营活动；
- b) 境外相关业务部门主动进行日常合规管理工作，识别业务范围内的合规要求，制定并落实业务管理制度和风险防范措施，组织或配合合规管理部门进行合规审查和风险评估，组织或监督违规调查及整改工作；
- c) 对境外经营相关部门和境外分支机构的所有员工开展合规培训；
- d) 境外经营相关部门和境外分支机构可制定单独的合规绩效考核机制，考核内容包括但不限于按时参加合规培训，严格执行合规管理制度，积极支持和配合合规管理机构工作，及时汇报合规风险等。

6.3.16 反欺诈

经营者应有效防范和化解欺诈风险：

- a) 制定欺诈风险管理的基本制度，并保证管理制度执行的有效性；
- b) 建立欺诈风险管理组织架构，明确职能部门、业务部门及其他部门的职责分工和权限确定欺诈风险报告路径；
- c) 培养员工反欺诈意识，积极了解反诈方法，高度重视防诈骗工作，将反诈工作纳入日常工作部署，严格落实主体责任。

参 考 文 献

- [1] GB/T 24353—2009 风险管理 原则与实施指南
 - [2] GB/T 35770 合规管理体系 要求及使用指南
 - [3] SZDB/Z 245—2017 反贿赂管理体系
 - [4] ISO 37001 Anti-bribery management systems — Requirements with guidance for use
 - [5] 《中华人民共和国环境保护法(2014修订)》(主席令第九号)
 - [6] 《中华人民共和国公益事业捐赠法》(主席令第十九号)
 - [7] 《中华人民共和国产品质量法(2018修正)》(主席令第二十二号)
 - [8] 《中华人民共和国劳动法(2018修正)》(主席令第二十四号)
 - [9] 《中华人民共和国反洗钱法》(主席令第五十六号)
 - [10] 《中华人民共和国反垄断法》(主席令第六十八号)
 - [11] 《中华人民共和国劳动合同法(2012修正)》(主席令第七十三号)
 - [12] 《中华人民共和国安全生产法(2021修订)》(主席令第八十八号)
 - [13] 《中华人民共和国个人信息保护法》(主席令第九十一号)
 - [14] 《企业财务会计报告条例》(国务院令第287号)
 - [15] 《中华人民共和国反不正当竞争法》
 - [16] 《国务院反垄断委员会关于平台经济领域的反垄断指南》(国反垄发〔2021〕1号)
 - [17] 《中央企业投资监督管理暂行办法》(国资委令第16号)
 - [18] 《职业健康检查管理办法(2019修订)》(国家卫生健康委员会令第2号)
 - [19] 《企业财务通则(2006修订)》(财政部令第41号)
 - [20] 《企业知识产权合规标准指引(试行)》(上海市浦东新区检察院发布)
 - [21] 《合肥市劳动用工条例(2018修正)》
-