

佛山电器照明股份有限公司

全面风险管理工作办法

第一章 总则

第一条 为推动公司深入开展风险管理工作，建立健全风险管理体系，有效防控各类风险，促进企业持续健康稳定发展，根据《中华人民共和国公司法》《企业内部控制基本规范》及其配套指引、《深圳证券交易所上市公司内部控制指引》等相关法律法规和规范性文件，结合公司实际，制定本办法。

第二条 本办法适用于佛山电器照明股份有限公司（以下统称“公司”）及其全资子公司、控股、实际控制企业（以下统称“下属企业”）。

第三条 本办法所称企业风险，指未来的不确定性对企业实现其经营目标和稳定发展的影响。

第四条 本办法所称全面风险管理指公司围绕总体经营目标，通过在企业管理的各个环节和经营过程中执行风险管理的基本流程，培育良好的风险管理文化，建立健全全面风险管理体系，从而为实现风险管理的总体目标提供合理保证的过程和方法。

第五条 风险管理基本流程包括以下主要工作：

- （一）收集风险管理初始信息；
- （二）进行风险评估；

- (三) 制定风险管理策略;
- (四) 提出和实施风险管理解决方案;
- (五) 风险管理的监督与改进。

第六条 公司开展全面风险管理要努力实现以下风险管理总体目标:

- (一) 确保将风险控制在与总体目标相适应并可承受的范围内;
- (二) 确保内外部, 尤其是公司与股东之间实现真实、可靠的信息沟通;
- (三) 确保遵守有关法律法规;
- (四) 确保公司有关规章制度和为实现经营目标而采取重大措施的贯彻执行, 保障经营管理的有效性, 提高经营活动的效率和效果, 降低实现经营目标的不确定性;
- (五) 确保公司建立针对各项重大风险发生后的危机处理计划, 保护公司不因灾害性风险或人为失误而遭受重大损失。

第七条 公司本着从实际出发, 务求实效的原则, 以对重大风险情况、重大风险事件的管理和重要流程的内部控制为重点, 积极开展全面风险管理工作。

第八条 公司开展全面风险管理工作应与其他管理工作紧密结合, 把风险管理的各项要求融入企业管理和业务流程中, 调动各职能部门、业务单位参与风险管理, 建立风险管理三道防线。

各职能部门、业务单位及下属企业是风险管理的第一道防线, 对相关管理活动中的风险管理负有直接责任。各职能部门、业务单位及下属

企业在实现公司及业务战略和任务的过程中，应及时识别、系统分析风险并主动管理风险，及时上报重大风险。

风险管理职能部门作为风险管理的第二道防线，负责风险管理机制和制度建设，为第一道防线提供专业领域的风险管理指引及建议，以协助第一道防线完善其风险控制流程与措施，促进第一道防线对风险管控的实施合理奏效。

审计部门作为风险管理的第三道防线，主要对经营管理过程的重大风险管理及风险管理体系的有效性进行测评或审计，实施独立监督。

第二章 风险管理组织体系

第九条 公司应建立健全风险管理组织体系，规范公司法人治理结构，加强风险管理职能部门和内部审计部门的组织领导，明确各部门、各业务单位风险管理职责。

第十条 公司董事会下设审计与风险管理委员会，审计与风险管理委员会对董事会负责，负责定期审议公司全面风险管理工作报告，指导、监督和评价全面风险管理工作。经董事会授权承担董事会的风险管理职责。

第十一条 公司设立由公司经理层成员组成的合规、内控及风险管理领导小组（以下简称“领导小组”），领导小组的风险管理职责主要包括：

- （一）根据董事会的决定，建立健全风险管理组织架构；
- （二）审议公司风险管理的具体制度；

(三) 审议公司年度合规、内控及风险管理工作计划;

(四) 监督公司风险管理工作开展情况, 对公司各道风险管理工作的开展情况提出指导意见;

(五) 审议重大风险的管理解决方案及实施情况, 协调相关资源支持重大风险应对举措的落实;

(六) 经董事会授权的其他事项。

第十二条 公司应设立专职部门或确定相关职能部门作为风险管理职能部门, 负责统筹公司全面风险管理工作, 主要履行以下职责:

(一) 负责企业风险管理机制和制度建设, 组织协调全面风险管理日常工作;

(二) 汇总各部门的风险管理信息, 建立公司全面风险管理台账;

(三) 实行定期台账动态管理, 有序开展全面风险管理工作;

(四) 负责监督、指导各职能部门、业务单位及下属企业的全面风险管理工作;

(五) 负责组织建立风险管理信息系统;

(六) 提出全面风险管理年度报告;

(七) 办理风险管理其他管理工作

第十三条 公司审计部门在风险管理方面主要履行以下职责:

(一) 研究提出全面风险管理监督评价体系, 制定监督评价相关制度;

(二) 开展监督与评价, 出具监督评价审计报告。

第十四条 公司其他职能部门及业务单位在全面风险管理工作中，应接受风险管理职能部门和公司审计部门的组织、协调、指导和监督，主要履行以下职责：

（一）执行风险管理基本流程；

（二）研究提出本部门或业务单位重大决策、重大风险、重大事件和重要业务流程的判断标准或判断机制；

（三）研究提出本部门或业务单位的重大决策风险评估报告；

（四）做好本部门或业务单位建立风险管理信息系统的工作；

（五）做好培育风险管理文化的有关工作；

（六）建立健全本部门或业务单位的风险管理内部控制子系统；

（七）办理风险管理其他有关工作。

第十五条 公司通过相关程序，指导和监督全资、控股子公司建立与企业相适应或符合企业自身特点、能有效发挥作用的风险管理组织体系。

第三章 风险管理基本流程

第一节 风险管理初始信息

第十六条 公司应广泛、持续不断地收集与本企业风险和风险管理相关的内部、外部信息，包括历史数据和未来预测，把收集信息的职责分工落实到各部门和下属企业。

第十七条 风险管理职能部门应牵头制定信息收集办法和标准，对通过内部讨论、数据收集、外部沟通等方式获取信息做出指引；各职能部

门及下属企业对本部门或单位的信息进行更新和维护，风险管理职能部门对其进行指导和监督。

第十八条 风险信息收集在时间安排上可根据公司风险评估的周期，可以作为年度业务计划或预算的一个重要组成部分，也可以和风险与控制自我评估周期相配合。

第二节 风险评估

第十九条 公司应对收集的风险管理信息和公司各项业务管理及其重要业务流程进行风险评估。风险评估包括风险辨识、风险分析、风险评价三个步骤。

第二十条 风险辨识是指查找公司各业务单元、各项重要经营活动及其重要业务流程中有无风险，有哪些风险。

风险分析是对辨识出的风险及其特征进行明确的定义描述，分析和描述风险发生可能性的高低、风险发生的条件。

风险评价是评估风险对企业实现目标的影响程度等。

第二十一条 公司应列出风险清单，包括风险编号、风险类别、风险名称、风险描述、风险管理者、风险成因，风险成因类别、风险发生的可能性、对公司实现目标的影响程度。

第二十二条 公司应梳理公司层面的战略目标、经营性目标、报告性目标、合规性目标，再将这层层分解形成若干子目标，以目标为源头进行风险分析。

第二十三条 公司应确定风险发生的可能性和风险发生后对目标影响程度的定性、定量评估标准。风险发生的可能性通常指风险发生的概率，风险发生后对目标的影响程度，通常需要考虑财务、声誉、运营、环境、安全等影响因素。

第二十四条 公司在评估多项风险时，应按照风险发生的可能性和风险发生后对目标的影响程度，绘制风险坐标图，对各项风险进行分析和排序，初步确定关注重点和优先控制的风险。

第二十五条 进行风险辨识、分析、评价，应将定性与定量方法相结合。定性方法可采用查阅文件、问卷调查、集体讨论、专家咨询、情景分析、政策分析、行业标杆比较、管理层访谈、由专人主持的工作访谈和调查研究等。在定量方法上，可根据风险管理发展不同阶段，探索在专业机构的协助下，采用更为全面和系统的量化评估方法。

第二十六条 开展风险评估工作时，应依据经营和 Risk 管理的需要确定评估范围，可以是整个集团或某子企业，也可以是某一个部门，或某项特定的业务工作。

第二十七条 公司在 Risk 管理的初级阶段可选用自下而上或自上而下的方法进行风险评估和管理。根据自身规模、Risk 管理工作的基础、高级管理层对业务的熟悉程度、公司具备的项目资源、企业文化建设等实际情况选择具体的开展方式。

第二十八条 自下而上的方法一般包括以下步骤：

(一) 全面开展工作，由各部门对其所涉及的工作流程中各个环节可能存在的风险进行辨识、分析和评价；

(二) 由于风险影响往往会跨越数个部门，因此各部门需要就已经辨识的相关风险进行沟通，修正风险评估结果；

(三) 根据风险的重要性进行排序；

(四) 高级管理层对于重要风险领域进行讨论和分析，并确定需要优先关注的高风险；

(五) 在各部门的协助下，由高级管理层确定风险应对措施。

第二十九条 自上而下的方法一般包括以下步骤：

(一) 以研讨会的形式，由高级管理层根据企业战略目标识别出关键风险；

(二) 根据关键风险点的重要和紧急程度，选取若干作为示范性风险；

(三) 在高级管理层的参与下，由各部门对示范性风险进行深入研究，充分分析风险的成因、特性和发生后的结果，并制定风险应对措施。

(四) 在前一阶段工作的基础上，继续选取其他关键风险点进行深入研究。

第三十条 风险评估由风险管理职能部门组织有关部门和下属企业实施，公司高级管理层、各部门等各方全面参与。根据公司实际情况，可聘请有资质、信誉好、风险管理专业能力强的中介机构协助实施。

第三节 风险管理策略

第三十一条 本办法所称风险管理策略，指公司根据自身条件和外部环境，围绕企业发展战略，确定风险偏好、风险承受度、风险管理有效性标准，选择风险规避、风险降低、风险分担和风险承受等适合的风险管理工具的总体策略，并确定风险管理所需人力和财力资源的配置原则。

第三十二条 风险规避是公司超出风险承受度的风险，通过放弃或者停止与该风险相关的业务活动以避免和减轻损失的策略。

风险降低是公司在权衡成本效益之后，准备采取适当的控制措施降低风险或者减轻损失，将风险控制在风险承受度之内的策略。

风险分担是公司准备借助他人力量，采取业务分包、购买保险等方式和适当的控制措施，将风险控制在风险承受度之内的策略。

风险承受是公司风险承受度之内的风险，在权衡成本效益之后，不准备采取控制措施降低风险或者减轻损失的策略。

第三十三条 公司根据不同业务特点确定风险偏好和风险承受度，明确风险的最低限度和不能超过的最高限度，并据此确定风险的预警线及相应采取的对策。

第三十四条 公司应根据风险发生的可能性及影响程度，结合风险与收益相平衡原则，进一步确定风险管理的优选顺序，明确风险管理成本的资金预算和控制风险的组织体系、人力资源、应对措施等总体安排。

第三十五条 公司应定期总结和分析风险管理策略的有效性和合理性，结合实际不断修订和完善。其中，应重点检查依据风险偏好、风险承受

度和风险控制预警线实施的结果是否有效，并提出定性或定量的有效性标准。

第四节 风险管理解决方案

第三十六条 公司根据风险管理策略，针对各类风险或每一项重大风险制定风险管理解决方案。方案一般应包括风险解决的具体目标，所需的组织领导，所涉及的管理及业务流程，所需的条件、手段等资源，风险事件发生前、中、后所采取的具体应对措施。

第三十七条 风险管理解决外包方案的制定应注重成本与收益的平衡、外包工作的质量、自身商业秘密的保护以及防止自身对风险解决外包产生依赖性风险等，并制定相应的预防和控制措施。

第三十八条 公司制定风险解决的内控方案，应对风险所涉及的管理及业务流程，制定以关键环节为控制重点，涵盖各个环节的流程控制措施。

第三十九条 控制措施一般包括：不相容职务分离控制、授权审批控制、会计系统控制、财产保护控制、预算控制、运营分析控制和绩效考评控制等。

第四十条 不相容职务分离控制要求公司系统地分析、梳理业务流程中所涉及的不相容职务，实施相应的分离措施，形成各司其职、各负其责、相互制约的工作机制。

第四十一条 授权审批控制要求公司根据常规授权和特别授权的规定，明确各岗位办理业务和事项的权限范围、审批程序和相应责任。

第四十二条 会计系统控制要求财务人员严格执行国家统一的会计准则制度，加强会计基础工作，明确会计凭证、会计账簿和财务会计报告的处理程序，保证会计资料真实完整。

第四十三条 财产保护控制要求公司建立财产日常管理制度和定期清查制度，采取财产记录、实物保管、定期盘点、账实核对等措施，确保财产安全。公司应当严格限制未经授权的人员接触和处置财产。

第四十四条 预算控制要求公司实施全面预算管理制度，明确各责任单位在预算管理中的职责权限，规范预算的编制、审定、下达和执行程序，强化预算约束。

第四十五条 运营分析控制要求公司建立运营情况分析制度，经理层应当综合运用生产、购销、投资、筹资、财务等方面的信息，定期开展运营情况分析，发现存在的问题，及时查明原因并加以改进。

第四十六条 绩效考评控制要求公司建立和实施绩效考评制度，科学设置考核指标体系，对公司内部各责任单位和全体员工的业绩进行定期考核和客观评价，将考评结果作为确定员工薪酬以及职务晋升、评优、降级、调岗、辞退等的依据。

第四十七条 公司应当建立重大风险预警机制和突发事件应急处理机制，对可能发生的重大风险或突发事件，制定应急预案、明确责任人员、规范处置程序，确保突发事件得到及时妥善处理。

第四十八条 公司应当按照各部门职责分工和下属企业业务特点，认真组织实施风险管理解决方案，确保各项措施落实到位。

第五节 风险管理的监督与改进

第四十九条 公司应对风险管理信息、风险评估、风险管理策略、风险管理解决方案的实施情况进行监督，对风险管理的有效性进行检验，根据情况变化和存在的缺陷及时加以改进。

第五十条 各部门和下属企业应定期对风险管理和内部控制工作进行自查，及时发现缺陷并改进，自查报告报送公司风险管理和内部控制职能部门。

第五十一条 风险管理职能部门应定期对各部门和子企业风险管理和内部控制工作实施情况进行监督检查，对风险管理策略进行评估，对跨部门和子企业的风险管理解决方案进行评价，提出调整或改进建议。

第五十二条 公司审计部门应至少每年一次对公司各部门及子企业能否按照有关规定开展内部控制工作及其工作效果进行评估，评估报告应直接报送审计与风险管理委员会。

第五十三条 公司可聘请有资质、信誉好、专业能力强的中介机构对企业风险管理和内部控制工作进行评价，出具评估和建议专项报告。

第四章 信息系统

第五十四条 公司应充分发挥信息技术在信息与沟通中的作用，逐步建立涵盖风险管理基本流程和内部控制系统各环节的信息系统，包括信息的采集、存储、加工、分析、测试、传递、报告、披露等。

第五十五条 风险管理和内部控制信息系统应能够实时反映重大风险和重要业务流程的监控状态；能够对超过风险预警上限的重大风险实施

信息报警；能够满足风险管理内部信息报告制度和公司对外信息披露管理制度的要求。

第五十六条 风险管理和内部控制信息系统应实现信息在各部门、下属企业之间的集成与共享，既能满足单项业务风险控制的要求，也能满足公司整体和跨部门、下属企业的风险控制综合要求。

第五十七条 公司应当加强对信息系统开发与维护、访问与变更、数据输入与输出、文件储存与保管、网络安全等方面的控制，保证信息系统安全稳定运行。并根据实际需要不断进行改进、完善或更新。

第五十八条 公司应严格遵守国家有关信息系统和网络安全方面的法律法规，按照“谁运营，谁负责”的原则，补充、调整、更新已有的管理流程和管理程序，建立完善的风险管理和内部控制信息系统。

第五章 风险管理文化

第五十九条 公司应注重建立具有风险意识的企业文化，促进公司风险管理水平、员工风险管理素质的提升，保障公司风险管理目标的实现。

第六十条 风险管理文化建设应融入企业文化建设全过程。大力培育和塑造良好的风险管理文化，树立正确的风险管理理念，增强员工风险管理意识，将风险管理意识转化为员工的共同认识和自觉行动，促进企业建立系统、规范、高效的风险管理机制。

第六十一条 公司全体员工尤其是各级管理人员和业务操作人员应通过多种形式，努力传播企业风险管理文化，牢固树立风险无处不在、风

险无时不在、严格防控纯粹风险、审慎处置机会风险、岗位风险管理责任重大等意识和理念。

第六十二条 风险管理文化建设应与薪酬制度和人事制度相结合，增强各级管理人员特别是高级管理人员风险意识，防止盲目扩张、片面追求业绩、忽视风险等行为的发生。

第六十三条 公司应建立重要管理及业务流程、风险控制点的管理人员和业务操作人员岗前风险管理培训制度。采取多种途径和形式，加强对风险管理理念、知识、流程、管控核心内容的培训，培养风险管理人才，培育风险管理文化。

第六章 风险管理报告

第六十四条 风险管理职能部门应建立风险管理报告制度，形成风险管理报告机制，每年联合编制全面风险管理年度报告，并提交审计与风险管理委员会审议。

第七章 附则

第六十五条 本办法由法律与风控事务部负责修订和解释。

第六十六条 本制度经公司董事会审议通过，自发布之日起生效实施。2021年2月5日印发的《佛山电器照明股份有限公司全面风险管理工作办法》（佛照字〔2021〕3号）自本制度实施之日同步废止。