

团 体 标 准

T/UNP 111—2024

企业法律、合规、内控、风险一体化 管理体系 要求

Enterprise legal, compliance, internal control, risk integration
management system—Requirements

2024-05-31 发布

2024-05-31 实施

中国联合国采购促进会 发 布
中 国 标 准 出 版 社 出 版

目 次

前言 III

引言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 企业环境 5

5 领导作用 6

6 策划 7

7 支持 8

8 运行..... 10

9 绩效评价..... 15

10 改进 17

附录 A（资料性） 本文件与相关文件之间的关系 18

参考文献 19

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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由北京首认检测认证服务集团有限公司提出。

本文件由中国联合国采购促进会归口。

本文件起草单位：北京首认检测认证服务集团有限公司、广东粤电靖海发电有限公司、北京德恒律师事务所、北京本始律师事务所、北京首信联合认证有限公司、广东中山三角热电有限公司、郑州大学、北京中电大禹咨询有限公司、广东省能源集团新疆有限公司、广东电力发展股份有限公司青海分公司、贵州粤黔电力有限责任公司、北京德和衡律师事务所、四川君合律师事务所、大唐万宁天然气发电有限责任公司、华能江西清洁能源有限公司、广东云河发电有限公司、国家管网集团广东省管网有限公司、广东省能源集团有限公司沙角 C 电厂、广东粤电湛江生物质发电有限公司、北京智信企业管理咨询有限公司、天地正中(北京)国际信用管理有限公司、中国联合国采购促进会。

本文件主要起草人：张家瑞、吕克芳、吴智鹏、曹桂成、潘华、汤敏志、陈辛鹏、郑永强、肖贵川、周缅、杜洵、霍荟霓、陶光辉、朱美光、薛朝霞、黄聪、梁启明、罗婷婷、李伟芹、赵清梅、高文、汪莹、蔡群、闫哲、张凤羽、王淑勇、王栩男、宋嘉、段炼。

引言

0.1 法律、合规、内控、风险管理现状

企业为防范各种类型的风险,提升“法治促进治理”的效能,持续开展法律管理、合规管理、内部控制、风险管理等工作。但在业务实践中,合规、内控、风险、法务等各个部门基本处于各自为政的状态,多领域并行给部分企业带来管理上的难题。为发挥法治对企业良好发展的促进作用,提高合规在企业的嵌入深度,强化风控对企业的强基固本的作用,需要对四者进一步整合,以实现企业法律、合规、内控与风险管理的集约化管理。

0.2 法律、合规、内控、风险一体化整合框架

本文件旨在为企业提供一个整合管理框架,以期建立法律、合规、内控、风险一体化管理体系。一体化管理体系不仅可帮助企业提高效率、优化资源,形成统一的风险评价和监督;而且各企业通过采用系统的方法,实施法律、合规、内控、风险“四位一体”的管理,为企业实现可持续性发展做贡献。

本文件规定了法律、合规、内控、风险一体化管理体系的要求,使企业能够实现其设定的法律、合规、内控、风险一体化管理的预期结果。

法律、合规、内控、风险一体化管理的系统方法可向最高管理者提供信息,通过下列途径以获得长期成功,并为促进可持续发展创建可选方案:

- 预防或减轻不利影响,以应对风险;
- 减轻风险对企业的潜在不利影响;
- 帮助企业履行法律、合规义务;
- 提升合规管理、内部控制、风险管理的绩效;
- 运用企业生命周期的观点,控制或影响企业产品和服务的设计、制造、交付、消费和处置的方式,防止不合规的影响被无意间转移到生命周期的其他阶段;
- 实施友好的且可巩固企业市场地位的可选方案,以获得财务和运营收益;
- 有助于履行社会责任。

本文件拟不增加或改变对企业的法律法规要求。

0.3 法律、合规、内控、风险一体化整合因素

法律、合规、内控、风险一体化管理的成功实施,取决于最高管理者领导下的企业各层次和职能的承诺与实践。将法律、合规、内控、风险一体化管理及其信息化、数字化管理纳入企业的管理体系中,有助于企业有效应对风险和机遇。

0.4 法律、合规、内控、风险一体化管理 PDCA

构成一体化管理体系的方法是基于策划、实施、检查、改进(PDCA)的概念。PDCA 模式为企业提供了一个循环渐进的过程,用以实现持续改进。该模式可应用于法律、合规、内控、风险的一体化管理体系及其每个单独的要素。该模式简述如下。

- 策划:建立所需的法律、合规、内控、风险一体化管理的目标和过程,以实现与企业的合规与风控方针相一致的结果。
- 实施:实施所策划的过程。

- 检查:依据合规与风控方针(包括其承诺)、合规与风控运行准则,对过程进行监视和测量,并报告结果。
- 改进:采取措施以持续改进。

图 1 展示了本文件采用的结构如何融入 PDCA 模式,它能够帮助新的和现有的使用者理解系统方法的重要性。

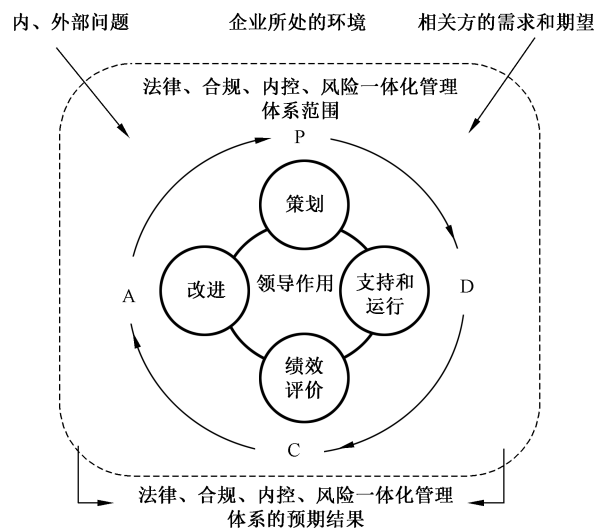


图 1 企业法律、合规、内控、风险一体化管理 PDCA 模式图

0.5 本文件内容

本文件可供寻求以系统的方式管理其四位一体职能的企业使用,从而为企业的可持续性发展作出贡献。

本文件可帮助企业实现其四位一体管理体系的预期结果,结果将为企业自身和相关方带来价值。与企业的合规与风控方针保持一致的四位一体管理体系预期结果包括:

- 提升四位一体的绩效;
- 履行合规与法律义务;
- 实现合规、内控、风险整合管理的协同目标。

本文件重视企业法律、合规、内控、风险一体化管理信息系统与人工智能工具的开发与使用。

本文件符合 ISO 对管理体系标准的要求。要求包括一个高阶结构,相同的核心正文,以及具有核心定义的通用术语,目的是方便使用者实施多个 ISO 管理体系标准。

本文件不包含针对其他管理体系的要求,如:质量、职业健康安全、环境、能源或财务管理。本文件并未提出具体的四位一体管理体系的绩效准则。然而,本文件为使企业能够运用共同的方法和基于风险的思维,将其法律、合规、内控、风险一体化管理体系与其他管理体系的要求进行了整合。

本文件包括了评价符合性所需的要求。任何有意愿的企业均可通过以下方式证实符合本文件:

- 进行自我评价和自我声明;
- 寻求企业的相关方(如:顾客),对其符合性进行确认;
- 寻求企业的外部机构对其自我声明的确认;
- 寻求外部企业对其法律、合规、内控、风险一体化管理体系进行认证或注册。

本文件能够全部或部分地用于系统地改进四位一体管理,然而,只有当本文件的所有要求都被包含在企业的四位一体管理体系中且全部得到满足,企业才能声明符合本文件。

附录 A 显示了本文件与相关文件之间概括的技术对照。

企业法律、合规、内控、风险一体化 管理体系 要求

1 范围

本文件规定了企业用于提升其法律、合规、内控、风险一体化(以下简称“四位一体化”)管理绩效的管理体系要求。

本文件适用于具有一定规模,需要提升风险管理、加强风控效率与效益的各类集团公司、上市公司、头部企业、中大型企业等的法律、合规、内控、风险的一体化建设和管理。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1 与企业 and 领导作用有关的术语

3.1.1

管理体系 management system

企业(3.1.5)用于建立方针、目标(3.2.6)以及实现目标的过程(3.3.5)的相互关联或相互作用的一组要素。

注 1: 一个管理体系关注一个或多个领域,如:质量、环境、职业健康和安全、能源、财务管理等领域。

注 2: 体系要素包括企业的结构、角色和职责、策划和运行、绩效评价和改进。

注 3: 管理体系的范围包括整个企业、其特定的职能、其特定的部门,或跨企业的一个或多个职能。

3.1.2

合规 compliance

履行组织的全部合规义务(3.2.4)。

注: 通过将合规融入组织文化及其工作人员的行为和态度中,使合规具有可持续性。

3.1.3

合规管理体系 compliance management system

管理体系的一部分,用于管理合规因素、履行合规义务(3.2.4),并应对风险和机遇(3.2.3)。

3.1.4

合规方针 compliance policy

由最高管理者(3.1.6)就合规绩效(3.4.11)正式表述的企业(3.1.5)意图和方向。

3.1.5

企业 organization

为实现目标(3.2.6),由职责、权限和相互关系构成自身功能的一个人或一组人的机构。

注: 企业包括但不限于个体经营者、公司、集团公司、商行、企事业单位、政府机构、合股经营的公司、公益机构、社