ICS 03.080
CCS A 12

T/CCPS

团　　体　　标　　准

T/CCPS 0005—2024

法务、合规、内控、风险一体化管理原则与实施指南

Principles and Implementation Guidelines for Integrated Management of Legal Affairs, Compliance, Internal Control, and Risk

2024-3-20发布　　2024-3-20 实施

中华文化促进会　发布

全国团体标准信息平台

目次

全国团体标准信息平台

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。

本文件中的某些内容可能涉及专利，文件的发布机构不承担识别专利的责任。

本文件由北京一法企业管理有限公司提出。

本文件由中华文化促进会归口。

本文件起草单位：北京一法企业管理有限公司、河北建设集团股份有限公司、贵州习酒股份有限公司、北京德和衡律师事务所、华博云（北京）技术有限公司、中油测井技术服务有限责任公司、法猎（北京）科技有限公司、成都产业投资集团有限公司、深圳市合同管理咨询有限公司、北京首信联合认证有限公司、上海训大教育科技有限公司、上海英格尔认证有限公司

本文件主要起草人：陶光辉、岳建明、张孝昆、李洁、陈秀玲、刘克江、冯玉晗、姜慧、刘为民、雒宏伟、刘磊、吴让伟、杨刚、郑崴、张元、张彤晖、孙伟搏、李庆、邹雨庭、郑爱玲、代晓冲、陈建、方伟、李晓烜、王绍华、董锐、周政兴、于翔、黄涛、陈建明、陶庆辉、张家瑞、申源泉、张钺、高恩、郑水强、温旭伟、李伟、马晓黎、黎阳、张龙、张晓婵

引　言

0.1 驱动背景

中大型企业等组织为有效防控各项各类风险，持续开展法务、合规、内控、风控等工作，但在实践中，法务管理、合规管理、内部控制、全面风险管理等各职能经常处于分散管理的状态，对组织风险管控机制整合与价值促进带来了诸多困惑。

为统筹发挥风险管控对组织长远发展的推动和保障作用，提高管理效能、减少交叉重复，有必要推动构建法务、合规、内控、风险一体化管理体系。

0.2 体系目的

本一体化管理旨在为组织提供一个整合管理框架，帮助组织提高风险管控效率、优化管理资源，形成统一的风险评估、应对、评价和监督机制，采用系统的方法，实现法务、合规、内控、风险“四位一体”管理。

本文件规定了法务、合规、内控、风险一体化管理基本原则，建立了法务、合规、内控、风险一体化管理的基本模型，提供了一套有序的法务、合规、内控、风险一体化管理操作指南。

系统的方法，包括：

——协同的管理目标；

——全面的风险评估；

——整合的风险管控机制；

——汇编的风险管理制度；

——管理控制手段的有效嵌入；

——PDCA 循环管理。

0.3 关键因素

法务、合规、内控、风险一体化管理体系取得成效，关键在于组织最高领导者的承诺与实践。组织间各职能的分工与配合，有效的风险管控意识和文化，对各类风险的充分识别，对管控措施的整合运用等，构成一体化管理体系成功的必要因素。

本文件不拟增加或改变对组织的法律法规要求。

0.4 文件使用

本文件符合 ISO 对管理体系标准的要求。这些要求包括一个高阶结构，相同的核心正文以及通用的术语，方便使用者同步实施多个 ISO 管理体系标准。

本文件包括了评价符合性所需的内容，任何有愿望的组织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；

——寻求组织的相关方（例如：顾客、咨询机构），对其符合性进行确认；

——寻求外部对其法务、合规、内控、风险一体化（协同）管理进行体系认证。

全国团体标准信息平台

法务、合规、内控、风险一体化管理 原则与实施指南

1 范围

本文件规定组织能够用于提升其法务、合规、内控、风险一体化管理绩效的管理原则与实施指南。

本文件可帮助组织实现对其法务管理、合规管理、内部控制、风险管理等进行整合，达到 1+1+1+1>4 的效果。这些整合将为组织自身和利益相关方带来价值。

本文件适用于具有一定规模，需要提高风险管控效率，集中行使同类职能，加强风险管控赋能的各类集团公司、上市公司、中大型企业等组织。

本文件能够全部或部分地用于改进法务、合规、内控、风险一体化整合管理，然而，只有当本文件的所有要求都被包含在组织的整合管理体系中且全部得到满足，组织才能声明自身管理体系符合本文件。

2 规范性引用文件

下列文件（包括其更新版）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。

GB/T 27914-2023 风险管理 法律风险管理指南

GB/T 35770-2022 合规管理体系 要求及使用指南

GB/T 24353-2022 风险管理 指南

GB/T 26317-2010 公司治理风险管理指南

BSI PAS 99:2012 整合管理体系的框架——通用管理体系要求的规范

COSO 2013 内部控制整合框架

3 术语和定义

下列术语和定义适用于本文件。

3.1 与领导作用有关的术语

3.1.1 管理体系 management system

组织(见 3.1.2)用于建立方针、目标(见 3.2.6)以及实现这些目标的过程(见 3.3.4)的相互关联或相互作用的一组要素。

注1：一个管理体系可关注一个或多个领域（例如：质量、环境、职业健康和安全、能源）。

注2：管理体系的范围可能包括整个企业等组织、其特定的职能、其特定的部门或跨组织的一个或多个职能。

3.1.2 组织 organization

为实现目标(见 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。

注：组织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、社团，或上述单位中的一部分或结合体，无论其是否具有法人资格、公营或私营。

3.1.3 最高管理者 top management

在最高层指挥并控制组织(见 3.1.2)的一个人或一组人。

注1：最高管理者有权在组织内部授权并提供资源。

注2：若管理体系(见3.1.1)的范围仅覆盖组织的一部分，则最高管理者是指那些指挥并控制组织该部分的人员。

3.1.4 相关方 interested party

能够影响决策或活动、受决策或活动影响，或感觉自身受到决策或活动影响的个人或组织(见3.1.2)。

注：相关方可包括顾客、社区、供方、监管部门、非政府企业、投资方和员工等。

3.1.5 治理机构 governing body

对组织（见 3.1.2）的活动、治理、方针负有最终责任和权力的一个人或一组人，最高管理者（见3.1.3）向其报告并对其负责。

注1：并不是所有的组织，尤其是小型组织，都会有一个独立于最高管理者的治理机构。

注2：治理机构可能包括但不限于董事会、董事会委员会、监事会或受托人。

3.1.6 一体化 integration

将两个或两个以上的不相同或不协调的事项，采取适当的方式，将其融合为一个整体，形成协同效应，以实现组织目标的一项措施。

3.2 与策划有关的术语

3.2.1 内控 internal control

组织内实现控制目标的过程。

3.2.2 风险 risk

不确定性对目标的影响。

注1：影响指对预期的偏离——正面的或负面的。

注2：不确定性是一种状态，是指对某一事件、其后果或其发生的可能性缺乏（包括部分缺乏）信息、理解或知识。

3.2.3 合规 compliance

履行组织的全部合规义务(见 3.2.4)

3.2.4 合规义务 compliance obligations

法律法规和其他要求 legal requirements and other requirements（许用术语）组织(见 3.1.2)应遵守的法律法规要求(见 3.2.5)，以及组织应遵守或选择遵守的其他要求。

注1：合规义务是与合规管理体系(见3.1.1)相关的。

注2：合规义务可能来自于强制性要求，例如：适用的法律和法规，或来自于自愿性承诺，例如：企业的和行业的标准、合同规定、操作规程、与社团或非政府企业间的协议。

3.2.5 要求 requirement

明示的、通常隐含的或应满足的需求或期望。

注1：“通常隐含的”是指对组织(见3.1.2)和相关方(见3.1.4)而言是惯例或一般做法，所考虑的需求或期望是不言而喻的。

注2：法律法规要求以外的要求一经组织决定遵守即成为义务。

3.2.6 目标 objective

要实现的结果。

注1：目标可能是战略性的、战术性的或运行层面的。

注2：目标可能涉及不同的领域（例如：财务、健康与安全以及环境的目标），并能够应用于不同层面[例如：战略性的、组织层面的、项目、产品、服务和过程(见3.3.4)]。

3.3 与支持和运行有关的术语

3.3.1 能力 competence

运用知识和技能实现预期结果的本领。

3.3.2 文件化信息 documented information

组织(见 3.1.2)需要控制并保持的信息，以及承载信息的载体。

——为组织管理体系运行而创建的信息（可能被称为文件）；

——实现结果的证据（可能被称为记录）。

注1：文件化信息可能以任何形式和承载载体存在，并可能来自任何来源。

注2：文件化信息可能涉及：

3.3.3 外包 outsource

安排外部组织(见 3.1.2)承担组织的部分职能或过程(见 3.3.4)。

注：虽然外包的职能或过程是在组织的管理体系(见3.1.1)覆盖范围内，但是外部组织是处在覆盖范围之外。

3.3.4 过程 process

将输入转化为输出的一系列相互关联或相互作用的活动。

注：过程可形成也可不形成文件。

3.4 与绩效评价和改进有关的术语

3.4.1 审核 audit

获取审核证据并予以客观评价．以判定审核准则满足程度的系统的、独立的、形成文件的过程(见3.3.4)。

注1：内部审核由组织(见3.1.2)自行实施执行或由外部其他方代表其实施。

注2：审核可以是结合审核（结合两个或多个领域）。

注3：审核应由与被审核活动无责任关系、无偏见和无利益冲突的人员进行，以证实其独立性。

3.4.2 符合 conformity

满足要求(见 3.2.5)。

3.4.3 不符合 nonconformity

未满足要求(见 3.2.5)。

注：不符合与本文件要求及组织(见3.1.2)自身规定的附加的合规管理体系(见3.1.1)要求有关。

3.4.4 纠正措施 corrective action

为消除不符合(见 3.4.3)的原因并预防再次发生所采取的措施。

注：一项不符合可能由不止一个原因导致。

3.4.5 持续改进 continual improvement

不断提升绩效(见 3.4.9)的活动。

注：该活动不必同时发生于所有领域，也并非不能间断。

3.4.6 有效性 effectiveness

实现策划的活动和取得策划的结果的程度。

3.4.7 监视 monitoring

确定体系、过程(见 3.3.4)或活动的状态。

注：为了确定状态，可能需要实施检查、监督或认真地观察。

3.4.8 测量 measurement

确定数值的过程(见 3.3.4)。

3.4.9 绩效 performance

可度量的结果。

注1：绩效可能与定量或定性的发现有关。

注2：绩效可能与活动、过程(见3.3.4)、产品（包括服务）、体系或组织(见3.1.2)的管理有关。

4 组织环境

4.1 理解组织及其环境

组织应确定与其宗旨、业务和管理相关并影响其实现法律合规管理、内控风险管理效果等外部和内部因素。这些因素应包括受组织影响的或能够影响组织的内外环境状况。

组织对这些外部和内部因素的相关信息，持续进行监视和评审。

注1：这些因素可能包括需要考虑的正面和负面条件。

注1：考虑来自与国际、国内、各地区的各种法律法规、技术、市场、文化、社会和经济环境的因素，有助于理解外部环境;考虑与组织的价值观、文化、知识和绩效等有关的因素，有助于理解内部环境。

4.2 理解相关方的需求和期望

组织应明确：

a) 与法务管理、合规管理、内部控制、风险管理等及一体化管理有关的相关方；

b) 相关方的有关需求和期望；

c) 相关方的职责分工、关系界定及管理要求。

4.3 确定一体化管理范围

组织应确定法务、合规、内控、风险一体化管理的目标、主线、内容与边界，以确定其建设范围。

确定范围时组织应考虑：

a） 4.1 所提及的内、外部因素；

b） 4.2 所提及的相关方的需求；

c） 4.2 所提及的法务、合规、内控、风险一体化管理要求。

注1：范围一经界定，该范围内组织的所有活动、产品和服务均纳入法务、合规、内控、风险一体化管理。

注2：范围应作为文件化信息予以保持，并可为相关方所获取。

4.4 一体化管理体系及其过程

为实现预期结果，提升法务、合规、内控、风险一体化管理绩效，组织应根据本文件的要求建立、实施、保持并持续改进法务、合规、内控、风险一体化管理体系，包括所需的过程及其相互作用。

4.4.1 组织建立并保持法务、合规、内控、风险一体化管理体系时，宜考虑在 4.1 和 4.2 中所获得的知识，嵌入在 4.1 和 4.2 过程中所提出的要求。

4.4.2 组织应确定法务、合规、内控、风险一体化管理体系所需的过程及其在整个组织的应用，且应：

a） 确定这些过程所需的输入和期望的输出；

b） 确定这些过程的顺序和相互作用；

c） 确定和应用所需的准则和方法（包括监视、测量和相关绩效指标），以确保这些过程的有效运行和控制；

d） 确定这些过程所需的资源并确保其可获得；

e） 分配这些过程的职责和权限；

f） 按照 6.1 的要求应对风险和机遇；

g） 评价这些过程，实施所需的变更，以确保实现这些过程的预期结果；

h） 改进这些过程。

5 领导作用

5.1 领导作用与承诺

5.1.1 治理机构和最高管理者

治理机构和最高管理者应通过下述方面证实其在法务、合规、内控、风险一体化管理方面的领导作用和承诺：

a） 对法务、合规、内控、风险一体化管理的有效性负责；

b） 确保建立法务、合规、内控、风险一体化管理方针，明确一体化管理目标，并确保其与组织的战略方向相一致；

c） 确保将法务、合规、内控、风险一体化管理要求融入组织的业务过程；

d） 确保可获得法务、合规、内控、风险一体化管理所需的资源；

e） 确保法务、合规、内控、风险一体化管理沟通有效并得到充分重视；；

f） 确保法务、合规、内控、风险一体化管理实现其预期结果；

g） 指导并支持员工对法务、合规、内控、风险一体化管理的有效性做出贡献；

h） 促进适用过程方法和基于风险导向的思维；

i） 促进持续改进；

j） 支持其他相关管理人员在其职责范围内证实其领导作用。

注：本文件所提及的“业务”一词可广义地理解为涉及组织存在目的的经营与管理活动。

5.1.2 组织机构一体化

治理机构和最高管理者应通过确保以下方面得到实施：

a） 治理机构协同化。董事会是法务、合规、内控、风险一体化管理的领导机构，总经理和经营层是执行机构。董事长、党组织负责人、总经理按照各自职责承担一体化管理的第一责任；

b） 管理机构一体化。组织设立法务合规内控风险职责统一的职能部门，或者承担不同职责的部门由同一个组织层面的领导分管，或者建立部门层面的联席会议机制；

c） 岗位职责一体化。组织在同一个部门下设一体化的法务、合规、内控、风险岗位，或者对分处不同部门的法务合规内控风险岗位在职责分工、知识结构、教育背景等方面提出一体化的要求；

d） 组织应在其内部各个层级建立、维护并推广法务、合规、内控、风险一体化管理文化。

5.2 一体化管理方针

5.2.1 治理机构和最高管理者应在界定的一体化管理范围内建立、实施并保持法务、合规、内控、风险一体化管理方针，该方针应：

a） 适合于组织的宗旨和所处的环境，包括其活动、产品和服务的性质、规模和环境影响；

b） 为制定法务、合规、内控、风险一体化管理方针目标提供指引；

c） 包括法务、合规、内控、风险一体化管理的承诺；

d） 包括持续改进整合管理体系以提升法务、合规、内控、风险一体化绩效的承诺。

5.2.2 沟通一体化管理方针

组织法务、合规、内控、风险一体化管理方针应：

a） 以文件化信息的形式予以保持；

b） 在组织内得到沟通；

c） 可为相关方获取。

5.3 角色、职责和权限

治理机构和最高管理者应确保在组织内部分配并沟通一体化管理相关角色的职责和权限。

治理机构和最高管理者应对下列事项分配职责和权限：

a） 确保法务、合规、内控、风险一体化管理符合本文件的要求；

b） 可获得组织法务、合规、内控、风险一体化管理的绩效报告；

c） 治理机构应对最高管理者运行法务、合规、内控、风险一体化管理体系进行监督；

d） 最高管理者为建立、制定、实施、评价、维护和改进法务、合规、内控、风险一体化管理体系提供资源，并将其与员工绩效考核挂钩。

6 策划

6.1 应对风险和机遇的策划

6.1.1 总则

组织应建立、实施并保持满足 6.1.1～6.1.3 的要求所需的过程。

策划法务、合规、内控、风险一体化管理时，组织应考虑：

a） 4.1 所提及的因素；

b） 4.2 所提及的要求；

c） 法务、合规、内控、风险一体化管理范围；

d） 6.1.2 中包括的义务、规范、准则以及与 4.1 和 4.2 中识别的其他因素和要求等所需要应对的风险和机遇，以：

——确保法务、合规、内控、风险一体化管理能够实现其预期结果；

——预防或减少不期望的影响，增强有利影响；

——实现持续改进。

组织应确定其法务、合规、内控、风险一体化管理范围内的潜在紧急情况，包括那些可能具有影响的潜在紧急情况。

组织应保持以下内容的文件化信息：

——需要应对的风险和机遇；

——6.1.1～6.1.3 中所需的过程，其详尽程度应使人确信这些过程能按策划得到实施。

——组织应通过强化信息化建设和数字化转型，为法务、合规、内控、风险一体化管理提供保障。

6.1.2 合规义务、内控规范与风险准则

组织应：

a) 确定并获取与其业务有关的合规义务、内控规范与风险准则；

b) 确定如何将这些合规义务、内控规范与风险准则应用于组织；

组织应保持其合规义务、内控规范与风险准则的文件化信息。

6.1.3 措施的策划

组织应策划：

a) 采取相应措施管理并定期更新维护其重要合规义务、内控规范与风险准则，以及 6.1.1 所识别的风险和机遇。

b) 如何在其法务、合规、内控、风险一体化管理过程中或其业务过程中，融入并实施这些措施；

c) 评价这些措施的有效性（见 9.1）。

当策划这些措施时，组织应考虑其可选技术、财务和经营要求。

6.2 一体化管理目标及其实现的策划

6.2.1 组织应针对其相关职能，建立法务、合规、内控、风险一体化管理目标。

组织法务、合规、内控、风险一体化管理目标应：

a) 与法务、合规、内控、风险一体化管理方针一致；

b) 可测量；

c) 得到监视；

d) 予以沟通；

e) 适当时予以更新。

组织应保持法务、合规、内控、风险一体化管理目标的文件化信息。

6.2.2 组织应在一体化管理目标的引导下，明确法务、合规、内控、风险一体化管理原则。

组织法务、合规、内控、风险一体化管理原则包括：

a) 以风险为导向；

b） 遵循业务规律；

c） 效率、合规与风控并进。

6.2.3 策划如何实现法务、合规、内控、风险一体化管理目标时，组织应确定：

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，包括用于监视实现其可测量的法务、合规、内控、风险一体化管理目标的进程所需的参数（见 9.1.1）。

组织宜考虑如何能将实现法务、合规、内控、风险一体化管理目标的措施融入其业务过程。

6.3 变更的策划

当组织确定需要对法务、合规、内控、风险一体化管理进行变更时，变更应按所策划的方式实施（见 4.4）

组织宜考虑：

a） 变更目的及其潜在后果；

b） 法务、合规、内控、风险一体化管理体系的完整性；

c） 资源的可获得性；

d） 职责和权限的分配或再分配。

7 支持

7.1 资源

组织应确定并提供建立、实施、保持和持续改进法务、合规、内控、风险一体化管理所需的资源。

7.2 能力

组织应：

a） 确定对法务、合规、内控、风险一体化管理绩效的具有影响的人员所需的能力；

b） 基于适当的教育、培训或经历，确保这些人员是能胜任的；

c） 确定与其重要业务事项和法务、合规、内控、风险一体化管理相关的培训需求；

d） 适用时，采取措施以获得所必需的能力，并评价所采取措施的有效性。

注：适用的措施可能包括：向现有员工提供培训、指导，或重新分配工作；或聘用、雇佣能胜任的人员。

组织应保留适当的文件化信息作为能力的证据。

7.3 意识

组织应确保在其控制下工作的人员意识到：

a） 法务、合规、内控、风险一体化管理方针；

b） 与他们的工作相关的重要业务事项和相关的实际或潜在的影响；

c） 对组织法务、合规、内控、风险一体化管理有效性的贡献；

d） 不符合法务、合规、内控、风险一体化管理要求的后果。

7.4 沟通

7.4.1 总则

组织应建立、实施并保持与法务、合规、内控、风险一体化管理有关的内部与外部信息沟通所需的过程，包括：

a） 信息沟通的内容；

b） 信息沟通的时机；

c） 信息沟通的对象；

d） 信息沟通的方式。

策划信息沟通过程时，组织应：

——应遵守其法务、合规、内控、风险一体化管理要求；

——确保所交流的法务、合规、内控、风险一体化管理形成的信息一致且真实可信；

组织应对其法务、合规、内控、风险一体化管理相关的信息沟通做出响应。适当时，组织应保留文件化信息，作为其信息交流的证据。

7.4.2 信息沟通

组织应：

a） 针对沟通需求，综合考虑沟通的多样性和障碍；

b） 确保沟通中考虑利益相关方的意见；

c） 确保人员能在沟通过程中提出疑虑；

d） 确保其信息交流沟通过程使在其控制下工作的人员能够为持续改进做出贡献；

e） 在组织各职能就法务、合规、内控、风险一体化管理相关信息的信息沟通，适当时，包括交流法务、合规、内控、风险一体化管理的变更；

f） 通过其建立的沟通过程，对外沟通包括法务、合规、内控、风险一体化管理文化、目标和要求在内的与法务、合规、内控、风险一体化管理相关的信息。

7.5 文件化信息

7.5.1 总则

组织法务、合规、内控、风险一体化管理应包括：

a） 本文件要求的文件化信息；

b） 组织确定的实现法务、合规、内控、风险一体化管理有效性所必需的文件化信息。

注：不同组织的法务、合规、内控、风险一体化管理文件化信息的复杂程度可能不同，取决于：

—— 组织的规模及其活动、过程、产品和服务的类型；

—— 证明履行其合规义务、内控规范及风险准则的需要；

—— 过程的复杂性及其相互作用；

—— 在组织控制下工作的人员的能力。

7.5.2 创建和更新

创建和更新文件化信息时，组织应确保适当的：

a） 标识和说明（例如：标题、日期、作者或参考文件编号）；

b） 形式（例如：语言文字、软件版本、图表）和载体（例如：纸质的、电子的）；

c） 评审和批准，以确保适宜性和充分性。

7.5.3 文件化信息的控制

组织法务、合规、内控、风险一体化管理及本文件要求的文件化信息应予以控制，以确保其：

a） 在需要的时间和场所均可获得并适用；

b） 得到充分的保护（例如：防止失密、不当使用或完整性受损）。

为了控制文件化信息，组织应进行以下适用的活动：

——分发、访问、检索和使用；

——存储和保护，包括保持易读性；

——变更的控制（例如：版本控制）；

——保留和处置。

组织应识别其确定的法务、合规、内控、风险一体化管理策划和运行所需的来自外部的文件化信息，适当时，应对其予以控制。

8 运行

8.1 运行策划和控制

法务、合规、内控、风险一体化管理是在界定四者关系的基础上，以业务事项为对象，以对各类风险的预防、控制与应对为主线，进行多层级多方面的协同管理，包括：组织职责、管理制度、管控措施及评价机制等多方面的一体化。

8.1.1 组织应明确法务管理、合规管理、内部控制、风险管理之间的关系，发挥四者各自的独特价值。

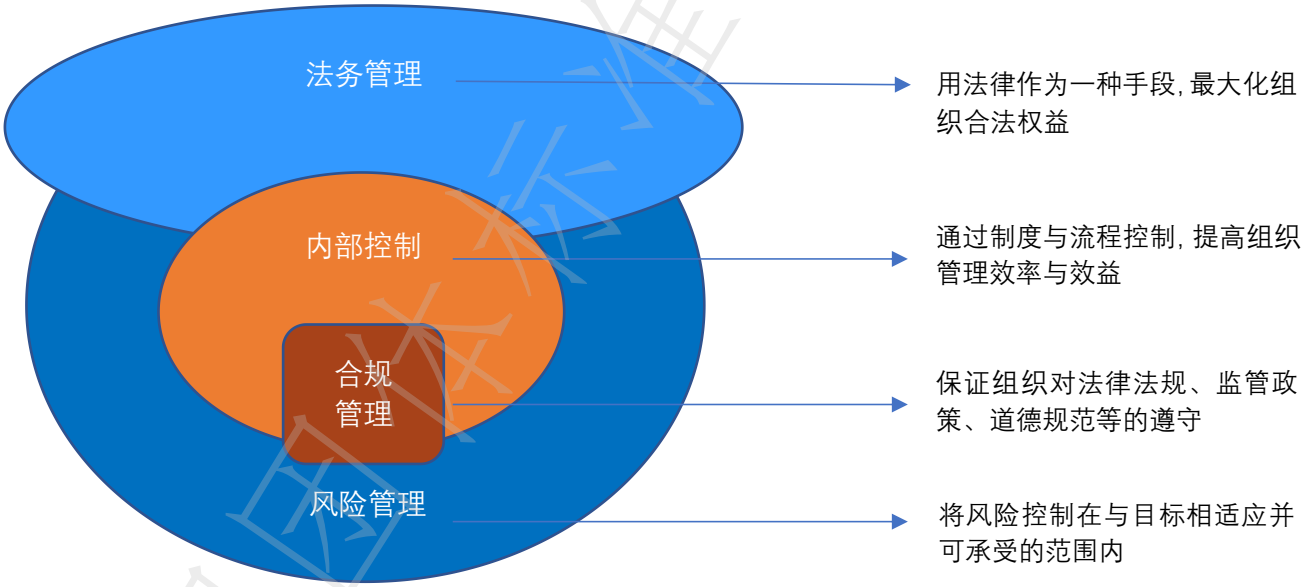

图 1 法务管理、合规管理、内部控制、风险管理的关系图

8.1.2 一体化组织职责

组织对其法务管理、合规管理、内部控制、风险管理等组织或部门进行梳理，在顶层结构上形成合规内控风险委员会，对分散的职责进行统筹，有效整合相关职责工作，并配备相应能力的人员。这些整合的职责包括但不限于：

a) 法律合规咨询；

b) 法律合规审查；

c) 项目法律合规支持；

d） 合规管理制度；

e） 合规管控机制；

f） 部门权责清单；

g） 内部控制流程；

h） 风险管理策略；

i） 诉讼仲裁案件；

j） 风险管控措施。

8.1.3 一体化管理制度

组织应对其法务管理、合规管理、内部控制、风险管理的规章制度进行整合。制度可以汇编成册，也可单独成册，但应统一梳理、避免冲突和重复。

8.1.3.1 规章制度自身应是合法合规合理的。

8.1.3.2 对于已有法务、合规、内控、风险相关的规章制度，宜制定关于这四类制度如何一体化的制度，或者用制度的使用说明来统筹各项分散的制度。

8.1.4 一体化管控措施

组织在整合法务管理、合规管理、内部控制、风险管理等管控机制时，可用的机制包括但不限于一体化的风险评估、组织层和业务层及项目层的风险应对，以及岗位层的风险应对。

8.1.4.1 风险评估宜对多项风险同时进行评估，包括法务风险、合规风险、内控风险以及外部风险等，且应以组织的经营管理行为或过程为对象。风险评估之后，宜形成全面风险数据库

具体的经营管理行为过程，包括但不限于：

a） 投资过程；

b） 销售过程；

c） 采购过程；

d） 研发过程；

e） 运营过程；

f） 战略管理过程；

g） 资产管理过程；

h） 工程建设过程；

i） 合同管理过程；

j） 人力资源管理过程；

k） 行政管理过程；

l） 财务管理过程；

m） 信息管理过程。

8.1.4.2 组织级风险应对主要体现在对风险管控的意识、理念与文化宣传之上。

a） 理念应是全面风险管控的理念，对各类风险均应建立起相关的意识，并持续宣传。

b） 文化应是强调风险对组织的生存和发展的持续影响，主要是消极层面的。文化控制应作为组织文化的一部分。

c） 宣传应是加强对全体员工的培训和宣贯，应全面且针对具体问题而制定，宜与风险评估的结果关联起来。

8.1.4.3 业务级和项目级风险应对主要体现为业务部门或组织项目策划针对性风险管控措施，包括具体的制度、流程和机制。通常是通过在经营管理的某个环节置入控制节点，以达到对业务层和项目层风险的统一控制。

风险管控手段包括但不限于：

a） 事前审查；

b） 强制咨询；

c） 联席会议；

d） 检查或抽查；

e） 风险主题例会；

f） 绩效考评；

g） 标准化指引文件。

8.1.4.4 岗位级风险应对主要体现为对岗位的风险管控职责予以明确并与岗位绩效关联的管控措施。

包括但不限于：

a） 岗位合规内控职责信息卡；

b） 岗位权责表；

c） 岗位风险跟踪；

d） 基于岗位的风险培训。

8.1.5 一体化评价机制

组织应对法务、合规、内控、风险一体化管理的设计与执行有效性进行统一评价。评价结果宜与组织绩效考核挂钩。评价的指标，可以是合一的，也可以是分别设计的，但应在同一标准上进行设置。

8.1.5.1 评价指标的设计，可采用累计制，也可采取扣分制。

8.1.5.2 对于法务、合规、内控、风险进行一体化管理的实施成熟度，宜纳入评价指标。

8.2 现状评估

组织在建立法务、合规、内控、风险一体化管理体系之前，宜对其法务管理、合规管理、内部控制、风险管理以及一体化管理的现状等进行评估。

8.2.1 评估内容

8.2.1.1 组织应对外部环境进行扫描。组织宜通过对所在政治经济环境、所在行业、商业模式、合作伙伴、所在社区等情况进行扫描，完成对外部环境的归纳。

8.2.1.2 组织内部管理环境的剖析。组织宜对公司的组织结构、授权体系、治理模式、管控模式、业务流程、组织文化等情况进行剖析，完成对内部环境的剖析。

8.2.2 评估方法

a) 访谈法；

b) 问卷法；

c) 研讨会法；

d) 资料阅读法；

e) 网络调研法；

8.2.3 评估报告

组织应保留对法务、合规、内控、风险一体化管理的现状评估报告，作为下一步工作的基础。

8.2.3.1 对于一体化管理现状的评估报告中提及的问题，应制定程序，以保证其在后续一体化管理中得到适宜的解决。

8.2.3.2　一体化管理现状评估报告宜定期、持续更新。

8.3　建立管理模型

8.3.1　考虑因素

一体化管理体系的实施方案应分析相关因素包括：

a)　一体化的管理职能；

b)　一体化的管理制度；

c)　一体化的管理工作机制；

d)　一体化的管控文化。

8.3.2　管理模型

组织可根据 8.1 和 8.2 所述，进一步搭建适宜的法务、合规、内控、风险一体化管理模型。

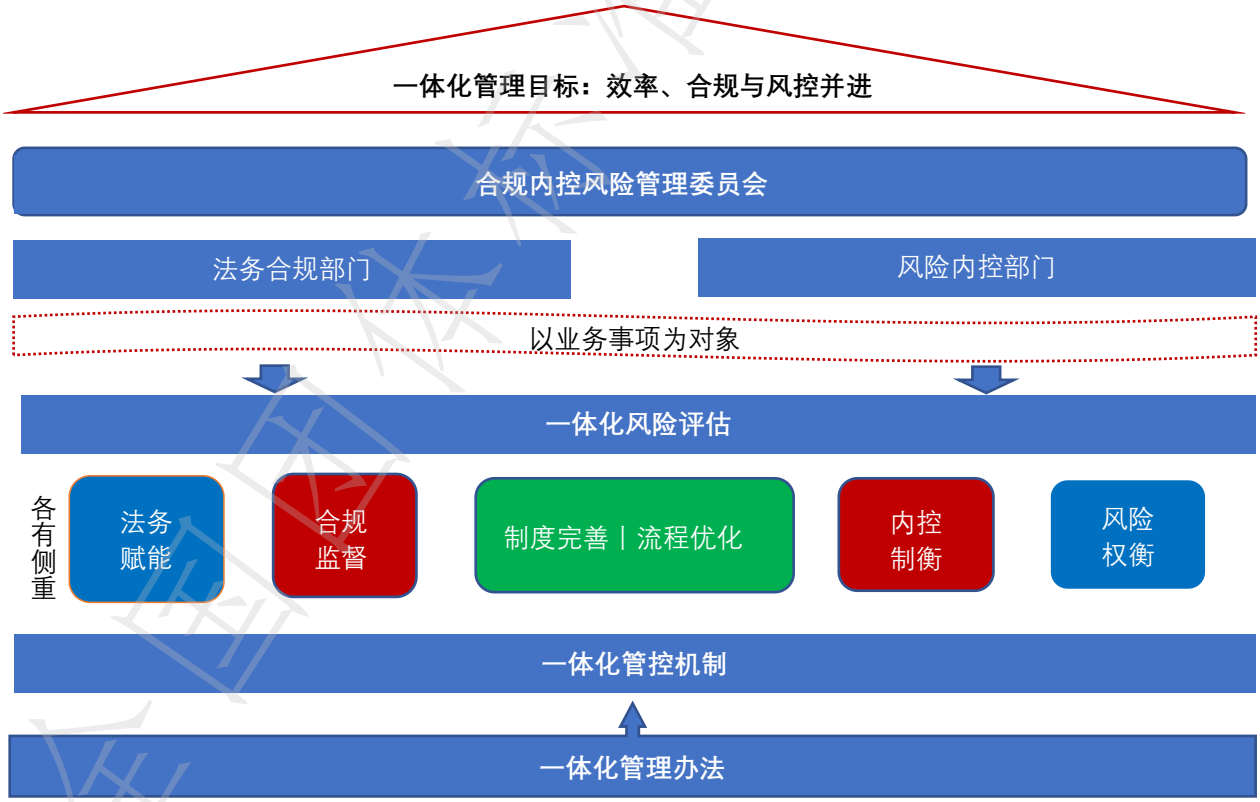

图 2 法务、合规、内控、风险一体化管理模型图

a)　管理模型可以是有形的，也可以是无形的。

b） 管理模型体现组织对法务、合规、内控、风险一体化管理的实施指导。

c） 管理模型应包括法务管理、合规管理、内部控制和风险管理的共通内核，并区分其各自侧重点。

8.4 一体化管理运行

组织对法务管理、合规管理、内部控制、风险管理进行统筹及整合（一体化管理），应根据组织的业务、管理与风险三方面特点，突出法务、合规、内控、风险四个子项各自价值，完成职责、制度、机制、评价的协同运行，发挥 1+1+1+1>4 的价值。

8.4.1 职能协同

a） 组织应在既有职能上，统筹安排法务管理、合规管理、内部控制、风险管理的岗位职责；

b） 组织应将四者的职能安排到一个管理部门之内或者在四者专项职能之上，考虑安排一个统一的管理高层，并在董事会层面有所体现。

8.4.2 制度协同

a） 组织应梳理法务、合规、内控、风险相关制度，将有关制度进行整合，或考虑制定专门的法务、合规、内控、风险一体化管理制度。

b） 组织应建立制度协同的定期检查过程，包括对制度的监督实施。

8.4.3 机制协同

a） 组织既有法人治理和集团管控模式应支持一体化管理机制；

b） 组织应根据法务管理、合规管理、内部控制、风险管理的不同侧重点，建立四者同时统筹运行机制；

c） 统筹运行机制应同时考虑法务支持效率最大化、合规底线监督、内控有效制衡和风险适当权衡；具体机制包括但不限于：

1） 一体化的审查；

2） 一体化的检查；

3） 一体化的调查；

4） 全面风险监测与预警；

5） 统一清单管理。

8.4.4 评价协同

a） 组织宜根据法务、合规、内控、风险各自侧重点，评价一体化管理体系运行的有效性：

1） 法务评价，侧重于支持效率；

2） 合规评价，侧重于底线坚守；

3） 内控评价，侧重于流程控制；

4） 风险评价，侧重于权衡判断。

b） 评价协同，宜同时考虑四者价值观的平衡，且纳入统一评价过程。

8.5 控制程序

组织宜建立统一的控制程序运行法务、合规、内控、风险的一体化管理体系，包括：

a） 职责协同效果；

b） 风险清单更新；

c） 风险应对措施；

d） 体系成熟度评价等子过程。

8.6 一体化管理体系文件

8.6.1 组织可建立一体化的管理体系文件，将法务管理手册、合规管理手册、内部控制手册、风险管理手册作为其组成部分，并对统一的管理体系文件进行宣传和推广。

8.6.2 一体化管理体系文件内容包括：

a） 一体化管理基本原则；

b） 一体化管理组织架构；

c） 风险评估形成的全面风险数据库；

d） 法务管理策略；

e） 合规管理制度；

f） 内控管理流程与权限；

g） 风险管理策略；

h） 一体化管理成熟度评价；

i） 一体化管理培训；

j） 一体化管理文化。

8.7 一体化管理保障

8.7.1 信息化手段的运用

组织应通过信息化建设，为一体化管理提供技术保障。

8.7.2 必要保障

组织应在机构、人员、经费、技术等方面为一体化管理工作提供必要条件，保障相关工作有序开展。

8.7.3 文化保障

组织应通过高层带头落实、风险综合管控承诺、宣传培训、绩效考核、违规处置等，建立和运行一体化的风险管控理念，培植一体化价值观，形成一体化运行的良好氛围。

8.8 一体化与独立性保持

8.8.1 发挥法务、合规、内控、风险的各自独立价值

组织在一体化管理框架下，鼓励发挥法务、合规、内控、风险各自的独立价值。

8.8.2 一体化与独立性的统筹

组织法务、合规、内控、风险一体化运行，是对原有体系的统筹和提升，不宜为追求形式上一致而忽视其原有价值。

9 绩效评价

9.1 监视、测量、分析和评价

9.1.1 总则

组织应确定：

a） 需要监视和测量的内容；

b） 适用时的监视、测量、分析与评价的方法，以确保有效的结果；

c） 何时实施监视和测量；

d） 何时分析和评价监视和测量的结果。

组织应评价其法务、合规、内控、风险一体化管理绩效。

组织应就有关法务、合规、内控、风险一体化管理绩效的信息进行内部和外部信息交流。

组织应保留适当的文件化信息，作为监视、测量、分析和评价结果的证据。

9.1.2 有效性评价

组织应建立、实施并保持评价其一体化管理状况所需的过程。

组织应：

a) 确定实施一体化管理有效性评价的频次；

b) 评价合法合规合理性，需要时采取措施；

组织应保留文件化信息，作为有效性评价结果的证据。

9.2 内部审核

9.2.1 总则

组织应按计划的时间间隔实施内部审核，以提供关于法务、合规、内控、风险一体化管理体系的信息：

a) 是否符合：

1）组织自身的管理体系要求；

2）本文件的要求。

b) 是否得到了有效的实施和保持。

9.2.2 内部审核方案

组织应建立、实施内部审核方案，包括实施审核的频次、方法、职责、策划要求和内部审核报告。

建立内部审核方案时，组织应考虑相关过程的重要性、影响组织的变化以及以往审核的结果。

组织应：

a) 规定每次审核的准则和范围；

b) 选择审核员并实施审核，确保审核过程的客观性与公正性；

c) 确保向相关管理者报告审核结果；

d) 及时采取适当的纠正和纠正措施；

e) 保留文件化信息，作为审核方案实施和审核结果的证据。

9.3 管理评审

9.3.1 总则

最高管理者应按计划的时间间隔对法务、合规、内控、风险一体化管理体系进行评审．以确保其持续的适宜性、充分性和有效性，并与组织的战略方向保持一致。

9.3.2 管理评审输入

管理评审应包括对下列事项的考虑：

a) 以往管理评审所采取措施的状况以下方面的变化：

b) 与法务、合规、内控、风险一体化管理体系相关的内、外部问题；

c) 法务、合规、内控、风险一体化管理目标的实现程度；

d) 法务、合规、内控、风险一体化管理绩效方面的信息，包括以下方面的趋势：

1）不符合和纠正措施；

2）监视和测量的结果；

3）其一体化管理机制的履行情况；

4）审核结果。

e) 资源的充分性；

f) 来自相关方的有关信息交流，包括抱怨；

g) 持续改进的机会。

9.3.3 管理评审的输出应包括：

a) 对法务、合规、内控、风险一体化管理体系的持续适宜性、充分性和有效性的结论；

b) 与持续改进机会相关的决策；

c) 与法务、合规、内控、风险一体化管理体系变更的任何需求相关的决策，包括资源；

d) 如需要，法务、合规、内控、风险一体化管理目标未实现时采取的措施；

e) 如需要，改进法务、合规、内控、风险一体化管理体系与其他业务过程融合的机会；

f) 任何与组织战略方向相关的结论。

组织应保留文件化信息，作为管理评审结果的证据。

10 改进

10.1 总则

组织应确定改进的机会（见 9.1、9.2 和 9.3），并实施必要的措施，以实现法务、合规、内控、风险一体化管理的预期结果。

10.2 不符合和纠正措施

10.2.1 发生不符合时，组织应：

a) 对不符合做出响应，适用时：

1） 采取措施控制并纠正不符合；

2） 处理后果，包括减轻不利的环境影响。

b) 通过以下活动评价消除不符合原因的措施需求，以防止不符合再次发生或在其他地方发生；

1） 评审不符合；

2） 确定不符合的原因；

3） 确定是否存在或是否可能发生类似的不符合；

C） 实施任何所需的措施；

d) 评审所采取的任何纠正措施的有效性；

e) 必要时，对合规管理体系进行变更。

纠正措施应与所发生的不符合造成影响的重要程度相适应。

10.2.2 组织应保留文件化信息作为下列事项的证据：

a) 不符合的性质和所采取的任何后续措施；

b) 任何纠正措施的结果。

10.3 持续改进

组织应持续改进其法务、合规、内控、风险一体化管理的适宜性、充分性与有效性，以提升其法务、合规、内控、风险一体化管理绩效。

全国团体标准信息平台

参 考 文 献

[1] GB/T 19011-2021 管理体系审核指南

[2] GB/T 27914-2023 风险管理 法律风险管理指南

[3] GB/T 35770-2022 合规管理体系 要求及使用指南

[4] GB/T 24353-2022 风险管理 指南

[5] GB/T 26317-2010 公司治理风险管理指南

[6] GB/T 20032-2005 项目风险管理 应用指南

[7] GB/T 23694-2013 风险管理 术语

[8] GB/T 36000-2015 社会责任指南

全国团体标准信息平台